



GÖTEBORGS UNIVERSITET

Europeanizing Cybersecurity –
A Comparative Analysis of Governance
and Securitization in Estonia and Sweden

Author: Lowa Birge

Supervisor: Gustav Cederlöf

Gothenburg University, School of Global Studies

Bachelor's Thesis in Global Studies, 15 credits

Spring 2025

Word Count: 13 579

ABSTRACT

This study focuses on examining how Sweden and Estonia have adapted their national cybersecurity strategies after 2022 (following Russia's invasion of Ukraine), with particular attention to how frameworks from the European Union (EU) and NATO have influenced this adaptation process. The study is situated within the field of Global Studies and aims to contribute to the understanding of how global institutions shape national security policy in the digital age and a rapidly shifting geopolitical order. The research consists of a comparative qualitative case study of Sweden and Estonia, two EU and NATO member states with contrasting governance models and security traditions. The analysis is based on national cybersecurity strategies, legislative proposals, official government publications, and relevant documents from the EU and NATO published between 2022 and 2025. The material is analysed using a theory-driven thematic approach, applying concepts from institutional theory, securitization theory, and cybersecurity governance. These are combined in an analytical framework I refer to as "Cybersecurity Institutionalism," used to identify similarities and differences in how external frameworks are interpreted and implemented nationally. The study finds that Estonia has rapidly and proactively aligned its cybersecurity strategy with both EU and NATO standards, supported by centralized governance and a securitized framing of cyber threats. Sweden, by contrast, has adopted a slower and more decentralized implementation path, reflecting its administrative structure and recent entry into NATO. The study concludes that while both countries legally comply with EU and NATO strategies, the countries' individual institutional designs, threat perceptions, and political framings strongly shape how cybersecurity policy is developed and implemented at the national level.

Key Words: Cybersecurity Policy, European Union, NATO, Sweden, Estonia, Institutionalism, Securitization, Governance

ACKNOWLEDGMENTS

I would like to use this space to give my thanks to my supervisor for guiding me through this process and coming up with incredible ideas that made this thesis a hundred times better. His encouragement, academic insight and critical questions helped me sharpen my arguments and stay on track.

I also want to thank the faculty and staff at Gothenburg University for providing a supportive and stimulating learning environment during my studies.

Special thanks to my peers, whose thoughtful comments and discussions were of great help.

I am especially grateful to my friends here in Sweden as well as abroad, for their constant support, patience, and understanding during the different stages of this project. Thank you for always being up for fika-study sessions or digital sessions just to keep each other company.

Your encouragement kept me going.

Finally, to all those who contributed, no matter directly or indirectly, knowingly or unknowingly to the completion of this thesis: thank you.

TABLE OF CONTENT

ABSTRACT..... 2
ACKNOWLEDGMENTS 3
ACRONYMS 6
1. Introduction..... 7
1.1 Research Problem, Purpose and Questions..... 8
1.2 Academic Relevance to Global Studies 9
2. Background and Case Context..... 9
2.1 The Increasing Importance of Cybersecurity..... 9
2.2 Cyber threats post-2022 11
2.3 Estonia and Sweden as relevant case studies 12
3. Scope and Delimitations 12
4. Conceptual and theoretical framework..... 13
4.1 Previous research and academic relevance 13
4.2 Theoretical framework – Cybersecurity Institutionalism 15
5. Method..... 18
5.1 Research Design..... 19
5.2 Case Selections 19
5.3 Data Collection 20
5.4 Analytical Strategy..... 23
5.5 Ethical- and Research Method Considerations 23
5.6 Researcher Positionality..... 24
5.7 Delimitations..... 25
6. Analysis 26
6.1 Introduction to the Analysis Chapter 26
6.2 Institutional Influence and Policy Adaptation..... 26
6.3 Influence of NATO’s Cybersecurity 29
6.4 Securitization of Cyber Threats 32
6.5 Cybersecurity Governance and Resilience 35
6.6 Summary of Analytical Findings 38
7. Result and Conclusion 40
7.1 Institutional Adaptation and Governance Models..... 40
7.2 Securitization and Framing of Cyber Threats 41

7.3 Methodological and Theoretical Reflections	43
7.4 Limitations	44
7.5 Future Research	44
7.6 Chapter Summarisation and Final Conclusion	45
References	47

ACRONYMS

CCDOE - NATO Cooperative Cyber Defence Centre of Excellence

ENISA - The European Union Agency for Cybersecurity

EU – The European Union

FOI – The Swedish Defence Research Agency

FRA – The Swedish National Defence Radio Establishment

MKM – Estonia’s Ministry of Economic Affairs and Communications

MSB - Swedish Civil Contingencies Agency

NATO – North Atlantic Treaty Organization

NIS-2 - Directive on Security of Network and Information Systems (Made by the EU)

RIA – Information System Authority of Estonia

1. Introduction

In late April 2007, Estonia, one of the world's most digitally advanced nations, experienced an unprecedented series of cyberattacks that disrupted the functioning of its government, financial institutions, media outlets, and essential services. These attacks, which lasted for approximately three weeks, were primarily issued denial-of-service assaults that overwhelmed servers and rendered numerous websites inaccessible (Ottis, 2008, p. 3). These attacks targeted government websites, financial institutions, media outlets, and other critical services, successfully paralyzing one of the world's most digitally advanced societies (Davis, 2007, p. 2).

The 2007 cyberattacks on Estonia are widely regarded as the first instance of a coordinated cyber campaign against a sovereign nation, marking a significant moment in the history of cybersecurity and international relations (Ottis, 2008, p. 3). The attacks targeted various sectors, including government ministries, political parties, newspapers, banks, and communication infrastructures, highlighting the vulnerabilities of a highly digitised society (Ottis, 2008, p. 3). The scale and impact of these attacks prompted Estonia to invest heavily in strengthening its cyber defences, leading to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2008 (Pamment et al., 2019, p. 7). The 2007 attacks on Estonia serve as a foundational case study for understanding the intersection of cybersecurity, national security, and international relations. They underscore the necessity for robust cybersecurity policies and the importance of international cooperation in addressing cyber threats. These questions are today of vital importance across countries in the European Union (EU) and the North Atlantic Treaty Organization (NATO).

This thesis seeks to analyse how Estonia and Sweden have adapted their cybersecurity policies in response to evolving cyber threats and the influence of supranational entities such as the EU and NATO. By examining the institutional frameworks, securitization processes, and governance models employed by both countries, the study aims to understand the mechanisms through which national cybersecurity strategies are developed and implemented. The concept of "Cybersecurity Institutionalism" will serve as the analytical lens, integrating insights from institutional theory, securitization theory, and cybersecurity governance literature.

1.1 Research Problem, Purpose and Questions

This study is motivated by the need to understand how national cybersecurity strategies evolve under supranational influence (power or authority that transcends national governments), particularly in response to acute geopolitical threats. While EU regulations such as the *NIS2 Directive* and the *Cyber Resilience Act* aim to standardize cybersecurity across member states (European Commission, 2022), the degree of alignment in practice remains uncertain. National governments are tasked with implementing the directives from organizations and alliances while addressing their own security needs, leading to potential variations in approach although the countries might be members in the same supranational organizations (Christou, 2016, p. 188). By comparing Sweden and Estonia, the research examines both convergence and divergence in cybersecurity governance, helping to assess what EU and NATO integration looks like in the two countries.

The aim of this thesis is to compare how Sweden and Estonia have adapted their national cybersecurity strategies after 2022, with a particular focus on the role of EU and NATO influence, institutional governance, and the framing of cyber threats in official policy documents. The study applies a qualitative, thematic text analysis to examine how national differences in governance structures and strategic cultures shape the interpretation and implementation of supranational cybersecurity frameworks.

By mixing important terms from the theories of securitization, institutionalism/Europeanization, and cybersecurity governance, I created a new theory called “Cybersecurity Institutionalism” and it will be used to analyse the results. The thesis aims to contribute to a deeper understanding of the institutional and political dynamics that underpin national cybersecurity policy and supranational integration. Through a qualitative comparative analysis of official strategy documents and related publications, the study identifies both convergence and divergence in how Sweden and Estonia frame, implement, and coordinate their cybersecurity efforts.

This study is guided by the following three research questions:

1. How have Sweden and Estonia adapted their cybersecurity strategies after 2022, and how do they differ from each other?
2. How has Estonia and Sweden’s alignment with the EU and NATO influenced their cybersecurity policies based on official government documents?

3. In what ways have Estonia and Sweden framed cybersecurity as a national security issue, and how do their securitization processes differ?

1.2 Academic Relevance to Global Studies

The relevance of this research to Global Studies lies in its focus on how local responses to transnational problems unfold within a multilevel governance system. Cybersecurity exemplifies a global issue that transcends borders, demanding cooperation and shared norms while still being shaped by national contexts. Moreover, it raises deeper questions about justice and sustainability, how can digital systems remain secure and inclusive, and how are citizens' rights protected in an increasingly monitored world? By analysing national adaptations within the EU cybersecurity framework, this thesis contributes to understanding the intersection of global governance, security policy, and digital justice.

As McCormick (2018) argues in his book *Introduction to Global Studies*, global issues increasingly transcend national borders and require new forms of international cooperation. Cybersecurity, as both a transnational threat and a governance challenge, exemplifies this shift and highlights the need to study how states navigate shared institutional frameworks like those of the EU and NATO.

This thesis is also relevant to the International Relations field, closely aligning with the constructivist international relations theory. According to the constructivist theory (Dunne, Kurki, & Smith, 2016, p. 164), cybersecurity is not only shaped by material threats, but also by how states interpret and frame these threats. This is particularly evident in the securitisation differences observed between Sweden and Estonia.

2. Background and Case Context

2.1 The Increasing Importance of Cybersecurity

"As geopolitical and economic tensions grow, cyber warfare escalates with espionage, sabotage, and disinformation campaigns becoming key tools for nations to manipulate events and secure a strategic advantage" (The European Union Agency for Cybersecurity-ENISA, 2024, p. 14).

The growing digitisation of public infrastructure, commerce, and communication systems has created new vulnerabilities, making cyber threats a key challenge for governments and

supranational bodies alike (ENISA, 2024). Cyberattacks on critical sectors such as energy, health, and finance can have cross-border implications, making international cooperation essential.

In response to these threats, both the European Union and the North Atlantic Treaty Organization have intensified their efforts to develop coherent cybersecurity frameworks. The EU has positioned itself as a regulatory actor, aiming to strengthen cybersecurity resilience through legal harmonization, most notably via the EU's *Directive on Security of Network and Information Systems (NIS2)* and the proposed *Cyber Resilience Act* (European Commission, 2022). These instruments place significant requirements on member states to modernize national legislation, establish supervisory authorities, and implement risk-based security practices.

At the same time, NATO has increasingly emphasized the cyber domain as a critical element of collective defence. The *NATO Strategic Concept 2022* reflects a growing securitization of the cyber domain within the alliance's strategic vision. Member states are expected to enhance cyber defence capabilities, participate in joint exercises, and contribute to a secure digital ecosystem across the alliance (NATO, 2022).

Within this evolving landscape, Sweden and Estonia offer two highly relevant and contrasting case studies. Both are EU member states, and as of 2023, both are NATO members as well. However, their cybersecurity governance structures, strategic cultures, and historical experiences differ markedly. Estonia is often seen as a pioneer in cybersecurity policy and digital governance, especially following the 2007 cyberattacks, which targeted government and financial systems during a political crisis. After the attacks Estonia became a key advocate for cyber defence within NATO and the EU (Högenauer et al., 2024, pp. 166-167). Its governance model is characterized centralized and closely integrated with the defence sector, but the country itself states a decentralized approach (Estonian Ministry of Economic Affairs and Communications, 2024, p. 8)

Sweden, on the other hand, has historically maintained a more decentralized and civilian-oriented approach to national security, including cybersecurity. Its governance model emphasizes cooperation across levels of government, civil society, and the private sector. Sweden has only recently begun to deepen its integration with NATO cybersecurity frameworks, following its formal membership in 2023, and is in the process of adapting its

legal and institutional structures to meet both EU and NATO expectations (Swedish Ministry of Justice, 2025, p. 2).

2.2 Cyber threats post-2022

Multiple EU agencies, including The European Union Agency for Cybersecurity (ENISA) (2024), have documented a spike in cyber threats targeting public infrastructure, electoral systems, and media in member states. In response, the EU has accelerated its cybersecurity agenda, advancing regulatory frameworks such as the *NIS2 Directive* and the *Cyber Resilience Act* (European Commission, 2022). These frameworks aim not only to strengthen national cybersecurity capacities but to foster a harmonised and collective approach to digital defence.

Fujs et al. (2024) and Kianpour and Frantz (2024) note that post-2022 developments have made it increasingly urgent for member states to build robust cyber crisis management systems and improve cooperation. The securitisation of cyber threats has shifted cyber policy from a technical concern into an issue of existential national and regional security (Buzan et al., 1998, pp. 21-47). The year 2022 marks the starting point for this research due to the invasion of Ukraine, which has affected the whole of Europe.

The outbreak of Russia's full-scale invasion of Ukraine in 2022 marked a turning point for European cybersecurity policy. Alongside conventional military aggression, the conflict has been accompanied by an intensification of state-sponsored cyberattacks, disinformation campaigns, and digital sabotage (Google Threat Analysis Group, 2023). Russia's actions have demonstrated the strategic use of cyber operations as tools of geopolitical influence and coercion. For both Sweden and Estonia, the post-2022 period marks a turning point in cybersecurity strategy development. However, their different historical trajectories and governance models raise questions about how supranational frameworks are interpreted and implemented at the national level.

It is with this context the thesis will explore how Sweden and Estonia have adapted their cybersecurity strategies after 2022, and how EU and NATO frameworks influence national governance and threat framing. By comparing these two countries, the study contributes to a better understanding of the opportunities and challenges of cybersecurity coordination in a fragmented but interconnected European security landscape.

2.3 Estonia and Sweden as relevant case studies

Sweden and Estonia offer interesting examples of how EU and NATO member states approach cybersecurity. Both operate within the same supranational framework, yet their historical experiences, institutional capacities, and security cultures differ significantly.

2.3.1 Estonia

Estonia's reputation as a leader of digitalisation and cybersecurity was forged, in part, by the 2007 cyberattacks attributed to Russian-linked actors, which targeted Estonia's banking system, media, and government infrastructure (CSS, 2020). These events catalysed a major shift in Estonia's cyber strategy, leading to early investments in digital defence, the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, and active engagement in EU-level policy development (Högenauer et al., 2024, p. 167). Estonia's cybersecurity governance model is more centralized and proactive compared to Sweden's, and as Enescu (2020) highlights, Estonia consistently aligns closely with EU cybersecurity objectives, often serving as a model for other member states in policy implementation and strategic innovation (p. 281).

2.3.2 Sweden

Sweden's accession to NATO in 2024 marked a major shift in its traditional security policy. While historically neutral, the growing threat from Russia, both militarily and in cyberspace, has pushed Sweden to integrate more closely into Western defence and cybersecurity structures (Swedish Ministry for Foreign Affairs, 2024, p. 2). Sweden's national cybersecurity strategy reflects this shift by emphasising resilience, coordination with EU institutions, and alignment with NATO's cyber defence priorities (Swedish Ministry of Justice, 2025, p. 7). However, Sweden's cyber governance remains relatively decentralized, with multiple agencies sharing responsibility, which can complicate coordination (FOI, 2024). Sweden has also been more prone to disinformation attacks than other forms of coordinated cyberattacks (Pamment et al., 2019, p. 138), making the country an interesting comparison to Estonia due to this big difference in previous attacks.

3. Scope and Delimitations

This study focuses on the national-level cybersecurity strategies of Sweden and Estonia and their adaptation after 2022. The analysis is limited to official government documents, such as

national cybersecurity strategies, security policy frameworks, and implementation reports published by relevant agencies or ministries. EU-level documents (e.g., the *NIS2 Directive*) and NATO strategy papers are included only insofar as they influence national-level discourse and adaptation.

The study does not include interviews, technical assessments, or cyber threat intelligence reports. While such sources could offer valuable insights into operational practices or institutional challenges, this thesis prioritizes the discursive and institutional framing of cybersecurity policy. The goal is to understand how cyber threats are governed and interpreted, rather than how they are technically managed or mitigated. The study focuses exclusively on the post-2022 period, which means that longer historical happenings are discussed only as background (e.g., Estonia's 2007 cyberattacks) and not examined in depth. The thesis also excludes private sector cybersecurity strategies, municipal-level initiatives, and specific incident response mechanisms unless referenced in national documents.

Finally, the findings are not intended to be generalized to all EU or NATO member states. Instead, Sweden and Estonia have been selected as contrasting cases to illustrate how different governance traditions, threat perceptions, and institutional legacies shape the national adaptation of supranational cybersecurity strategies.

4. Conceptual and theoretical framework

4.1 Previous research and academic relevance

The foundation for this research is built on existing studies that have explored how nations, particularly within the EU, develop their cybersecurity strategies. RAND Europe's *Cybersecurity Threat Characterisation: A Rapid Comparative Analysis* (2012) provides an early insight into Sweden's approach, showing how the country integrated cybersecurity threats into its national defence strategy (pp. 50-51). While outdated, this study offers a reference point for understanding how Swedish policymakers have historically viewed cybersecurity in relation to national security. Building on this, Enescu (2020) provides a comparative analysis of EU cybersecurity strategies, highlighting how different member states interpret and implement common guidelines. This work is particularly relevant to this thesis, as it underscores the tension between national priorities and supranational directives, one of the core themes in the Sweden-Estonia comparison.

Estonia's role as a cybersecurity frontrunner has been well documented. In Högenauer et al. (2024) focus is on how smaller European nations contribute to EU policymaking. The Estonia chapter is very interesting for this thesis, illustrating how a small but digitally advanced nation can punch above its weight in shaping supranational security frameworks. An example of the author showcasing this is by bringing us back to when Estonia had the president position within the EU: "*Another Estonia's key strengths has been its ability to build coalitions with other EU member states, particularly through its role as the rotating presidency of the European Union. During its presidency, Estonia invested significant resources in cybersecurity policy and acted as a honest broker in setting the EU's cybersecurity agenda*" (Högenauer et al., 2024, p. 170). The European Liberal Forum's *European Cybersecurity in Context* (2022) details Estonia's leadership in EU cyber cooperation, particularly in shaping cyber assistance networks. Meanwhile, the Centre for Security Studies (2020) provides a historical account of Estonia's cybersecurity evolution, offering insights into how past experiences, such as the 2007 cyberattacks, continue to shape its approach today.

One last important contribution to this thesis and the study of national adaptation to supranational frameworks is *National and European Foreign Policies* by Wong and Hill (2011). It explores how EU member states adjust their foreign and security policies in response to European integration, offering conceptual clarity on the varied forms of Europeanization. Rather than assuming uniform alignment, the authors emphasise the diversity of national responses depending on institutional fit, strategic culture, and domestic political context. Their work is particularly relevant to this thesis, even though being over ten years old, as it supports the view that EU cybersecurity policies are not simply adopted wholesale, but are filtered, reinterpreted, and embedded within existing national structures. In the context of Sweden and Estonia, Wong and Hill's framework helps explain why two small EU member states may diverge in how they internalise shared security norms, even under similar supranational pressures.

Together, all these studies create a rich foundation for this thesis. They offer comparative frameworks, empirical case studies, and theoretical insights that help situate this research within the broader academic discourse on cybersecurity governance. By drawing from these works, this study not only builds on existing knowledge but also identifies key areas where further analysis is needed, particularly in understanding how two distinct EU member states navigate the dual pressures of national security and supranational coordination in the face of evolving cyber threats.

4.2 Theoretical framework – Cybersecurity Institutionalism

The purpose of this thesis is to examine how Sweden and Estonia have adapted their national cybersecurity strategies after 2022, and how EU and NATO frameworks have influenced these adaptations. By analysing how cyber threats are framed and governed in national policy documents, the study aims to identify key similarities and differences in how each country approaches cybersecurity within a shared European and transatlantic context.

This study is set to explore how national cybersecurity strategies in Sweden and Estonia have developed in response to the changing European security environment, and how supranational frameworks, particularly those of the European Union and NATO, have shaped these national responses. The study further aims to understand how differences in governance models and securitization dynamics affect the implementation and interpretation of cybersecurity policy.

To interpret these processes, I developed a combined analytical lens called Cybersecurity Institutionalism, which integrates concepts from institutionalism, securitization theory, and cybersecurity governance and resilience. Rather than treating these perspectives one-by-one in isolation, the framework weaves them into a single comparative model for understanding how cybersecurity is framed, operationalised, and implemented in each country.

4.2.1 Illustration of Cybersecurity Institutionalism Theory

The following figure illustrates the key components and processes of cybersecurity institutionalism as used in this thesis. It highlights what theory the key term chosen can be found in originally and what the purpose of the term in the analysis will be.

Table 1

Model of Cybersecurity Institutionalism

Theoretical Framework	Key Term	Purpose in Analysis
Institutionalism	Europeanization	Analyse how the EU influences national cybersecurity policies in Sweden and Estonia.
	Coercive Isomorphism	Examine how EU regulations (e.g., <i>NIS2 Directive</i>) shape national cybersecurity policies in Sweden and Estonia.

Theoretical Framework	Key Term	Purpose in Analysis
Securitization Theory	Securitizing Move	Investigate how Sweden and Estonia frame cybersecurity as an existential threat and the language used to justify this.
	Referent Object	Identify what Sweden and Estonia consider as critical assets (e.g., infrastructure, data) to protect in their cybersecurity strategies.
	Audience Acceptance	Assess how political actors and the public in Sweden and Estonia accept or challenge the framing of cybersecurity as a national security issue.
Cybersecurity Policy	Cybersecurity Governance	Understand how Sweden and Estonia structure and implement their cybersecurity governance frameworks.
	Cyber Resilience	Evaluate how Sweden and Estonia ensure their systems' recovery and adaptability in response to cyber incidents.
	Cybersecurity Directives	Analyse the influence of EU cybersecurity directives (e.g., <i>NIS2</i>) on national cybersecurity policy implementation in Sweden and Estonia.

4.2.2 Integrating Cybersecurity Institutionalism in Context

At the core of this framework is the concept of institutionalism, or more specifically Europeanization, defined as the process by which EU-level rules, norms, and policy expectations are integrated into national policy frameworks (Wong & Hill, 2011; Radaelli, 2003, p. 30). Within the tradition of institutionalism, DiMaggio and Powell (1983, p. 150) identify three mechanisms that explain how this adaptation unfolds:

- Coercive isomorphism, where states adapt due to binding legal obligations
- Normative isomorphism, shaped by professional standards and shared values.
- Mimetic isomorphism, where states emulate others seen as successful, particularly under uncertainty

These dynamics are central to understanding how Sweden and Estonia have responded to directives like *NIS2* and the proposed *Cyber Resilience Act*, which function not only as legal instruments but also as symbols of European cooperation (Greenwood et al., 2017, pp. 117-118; Kianpour & Frantz, 2024, p. 13).

Institutional pressure alone is not enough to determine and create cybersecurity policy. To understand how threats are interpreted and prioritised, this framework also draws on securitization theory, as formulated by Buzan, Wæver, and de Wilde (1998, p. 25).

Securitization theory provides a framework for understanding how issues are transformed into matters of security through discursive processes. Rather than viewing threats as inherently objective, securitization theory focuses on the construction of threats through what the authors refer to as “speech acts.” In this context, a securitizing actor (typically a government official, institution, or political leader) declares an issue to be an existential threat to a valued referent object, such as the state, societal stability, or national identity. If the audience (the public, legislature, or elite institutions) accepts this framing, exceptional measures, such as emergency funding, specialised agencies, or other legal powers, become politically legitimate and easier to pursue (Garhwal & Pareek, 2024, pp. 748-749).

The securitizing lens is particularly relevant to Estonia’s case, where the 2007 cyberattacks catalysed a deep securitization of digital infrastructure. Estonia’s institutional discourse has since framed cyber threats as existential, with state institutions (e.g., RIA and the Estonian Ministry of Defence) adapting (by theoretical standards) central roles (Pamment et al., 2019, pp. 3-4). In contrast, Sweden adopts a softer framing, emphasising societal resilience, continuity of public services, and encourages the whole of society to participate. The Swedish approach is grounded in civilian governance, a great example of a decentralized governance structure which the last framework of this theory explains further.

States must rely on cybersecurity governance structures to operationalise the framings they create. This concept refers to the institutional configuration, centralized or decentralized, through which cybersecurity is coordinated. A centralized model places responsibility in a few national agencies, streamlining decision-making and compliance. A decentralized or polycentric model, by contrast, spreads authority across several levels of government and private actors, which may increase inclusivity but slow down response and coherence (Rocket Me Up Cybersecurity, 2024).

In the EU context, governance is inherently polycentric, with overlapping mandates between supranational bodies and national governments (Kianpour & Frantz, 2024, p. 4). As a result, how each country manages its internal cybersecurity responsibilities significantly affects the speed and consistency with which supranational directives are implemented.

Cyber resilience is another core concept within this framework. Defined as a system's capacity to anticipate, withstand, and recover from cyberattacks (ENISA, 2024, p. 21), resilience is not only a technical or legal matter, but it also reflects strategic priorities, institutional design, and discursive framing.

Finally, the framework treats EU cybersecurity directives not only as legal obligations, but also as instruments of normative influence. Directives like *NIS2* require states to establish minimum standards for risk assessment, critical infrastructure protection, and incident reporting. However, they also leave room for national interpretation, allowing for different levels of implementation and institutional fits (Kianpour & Frantz, 2024, pp. 4–5).

By integrating these concepts, Cybersecurity Institutionalism provides a broad lens for comparing the national cybersecurity strategies of Sweden and Estonia after 2022. It allows the analysis to move beyond binary questions of compliance and instead investigate how international frameworks are interpreted, negotiated, and embedded within national institutional settings. The framework highlights how threat framing, governance architecture, and institutional traditions interact to shape cybersecurity policy in a rapidly evolving European security landscape.

5. Method

This chapter outlines the methodological approach used in this study with the help of Alan Bryman's book *Social Research Methods* (2018). The methods have been chosen to help investigate how Sweden and Estonia have adapted their cybersecurity strategies after 2022 in response to EU and NATO frameworks, and to compare how different institutional structures and strategic cultures influence national framing and responses to shared supranational cybersecurity policies.

To address the thesis' aim, the study adopts a qualitative, comparative case study design with a focus on thematic text analysis. The empirical material consists of official government strategy documents, implementation reports, and policy communications published between

2022 and 2025, with some exceptions like juridical documents or past cybersecurity policies that are needed to answer the research questions of this thesis (see **Table 2**). These texts were selected because they represent authoritative articulations of national cybersecurity priorities, institutional arrangements, and threat framings.

The following sections describe the research design, case selection, material, and analytical procedure in more detail, as well as reflect on the study's methodological strengths and limitations.

5.1 Research Design

This thesis adopts a qualitative comparative case study design, as outlined by Bryman (2018, p. 460), to explore how Sweden and Estonia have adapted their national cybersecurity strategies after 2022, and how these have been influenced by EU and NATO frameworks. A case study approach is appropriate when the research aims to generate deep, context-sensitive insights into complex, multifactorial processes (Bryman, 2018, pp. 102, 104, 106-108). By selecting two different EU/NATO member states, the study facilitates a systems comparison, allowing for exploration of variation in cybersecurity governance under similar external pressures.

The comparison is intended to interpret and explain policy variation through thematic and theoretical analysis. This reflects Bryman's emphasis on the interpretive perspective of theories in qualitative research, where the goal is to understand social phenomena in context rather than produce universal generalizations (Bryman, 2018, pp. 462-463).

5.2 Case Selections

Sweden and Estonia were selected as purposeful cases (Bryman, 2018, pp. 498-499) because they share key similarities, EU and NATO memberships, and exposure to post-2022 cyber threats, but differ significantly in digital infrastructure maturity, threat perception, and governance traditions. Estonia is a small country bordering Russia, with a history of cyberattacks as well as digital leadership, making it an interesting case to study. Sweden, being the newest member of NATO, an alliance where Estonia has contributed a lot with policymaking, also becomes an interesting case as Sweden's past cybersecurity policies has been created without any pressure or influence from an alliance. As a long-time EU member state balancing civilian resilience with a new growing alignment to transatlantic defence

structures, Sweden illustrates how national institutions can take on supranational cybersecurity pressures while maintaining domestic policy traditions.

5.3 Data Collection

5.3.1 Chosen Documents

The table below presents the key policy documents analysed in this study, organized by country, document title and type, year of publication and purpose for the thesis.

Table 2

Policy Documents Used in the Analysis

Country / Org.	Document Title	Year	Type	Purpose / Relevance
Estonia	Cybersecurity Strategy 2019–2022	2019	National Strategy	Baseline for Estonia’s pre-2022 policy approach; resilience and EU/NATO alignment.
	Cybersecurity Strategy 2024–2030	2024	National Strategy	Post-2022 adaptation; securitised language, stronger EU/NATO integration.
	National Security Concept of Estonia	2023	National Security Doctrine	Highlights Estonia’s view of cyber threats and defence within overall security strategy.
	Cybersecurity in Estonia – Annual Report (RIA)	2024	Technical/Policy Report	Offers insight into real implementation and changing focus in response to cyber threats.
	CCDCOE: The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis	2013	Strategic Analysis	Illustrates Estonia’s leadership within NATO and long-term cyber posture.
	Lex Mundi: Cybersecurity Overview – Estonia	2025	Legal Commentary	Summarises Estonia’s regulatory landscape, obligations under <i>NIS2</i> , and

Country / Org.	Document Title	Year	Type	Purpose / Relevance
				key implementation challenges from a legal perspective.
Sweden	National Cybersecurity Strategy	2017	National Strategy	Baseline policy document; decentralised approach and general risk framing.
	Strategy for Foreign & Security Policy on Cyber & Digital Issues	2024	Foreign Policy Strategy	Frames Sweden's international digital alignment post-Ukraine invasion.
	Cybersecurity 2025	2025	Forward-Looking Policy Summary	Sweden's updated national strategy with NATO and EU harmonisation.
	MSB: Annual Cybersecurity Report	2024	Technical/Policy Report	Implementation updates; Sweden's practical response to emerging cyber risks.
	FOI Research on Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval	2024	Research/Policy Analysis	Adds depth to institutional and governance structure of Swedish cybersecurity.
	Lex Mundi: Cybersecurity Overview – Sweden	2025	Legal Commentary	Provides expert commentary on Sweden's data protection and cybersecurity regulatory environment, especially considering the <i>NIS2</i> adaptation.
EU & NATO	EU Cybersecurity Strategy	2024	Supranational Strategy	EU-wide policy direction; baseline for member state alignment and obligations.
	NIS2 Directive	2022	EU Directive	Legal framework requiring national adaptation; central to both case studies.

Country / Org.	Document Title	Year	Type	Purpose / Relevance
	Cyber Resilience Act	2022	Proposed Regulation	Regulation affecting national implementation of cyber rules in digital product sectors.
	NATO Strategic Concept	2022	Alliance Strategy	Places cyber threats within NATO's core defence strategy; key post-2022 influence.
	NATO Cyber Defence Pledge	2016	Political Commitment	Background on cyber defence responsibilities. used differently by Sweden and Estonia.

The primary method of data collection is qualitative content analysis of publicly available policy documents, strategic frameworks, national cybersecurity strategies, legal texts, and agency reports from Sweden, Estonia, the EU, and NATO. This aligns with Bryman's (2018) guidance on qualitative document analysis as a valid method for exploring meaning, discourse, and policy development over time (pp. 677-680).

Documents were selected based on three criteria:

1. Relevance - They explicitly address cybersecurity strategy or governance.
2. Recency - Documents post-2022 are used (unless historical context or a comparison is required).
3. Authoritativeness - Preference is given to official publications from ministries, EU institutions and NATO.

For Estonia, the material includes the *National Cybersecurity Strategy 2023–2027*, legal acts related to the Estonian Information System Authority (RIA), as well as publications from the Estonian Ministry of Economic Affairs and Communications and the Ministry of Defence. Sweden, documents include the *2023* and *2025 National Cybersecurity Strategies*, policy frameworks from agencies such as MSB (Swedish Civil Contingencies Agency), FRA (Swedish Signals Intelligence Agency), and statements from the Ministry of Defence.

To provide a comparative baseline, the analysis also draws selectively on EU-level documents such as the *NIS2 Directive*, the *Cyber Resilience Act*, and ENISA reports, as well as NATO's *Strategic Concept 2022*, its Cyber Defence Pledge, and other relevant communiqués.

5.4 Analytical Strategy

The analysis follows a thematic, theory-driven content analysis, in line with Bryman's discussion of interpretation in qualitative research (2018, pp. 702-708). The theoretical framework of Cybersecurity Institutionalism (see **Table 1**) provides predefined categories, including:

- Institutional adaptation and isomorphism
- Securitizing moves and referent objects
- Governance structure and resilience framing

Each document was analysed for language, structure, and framing strategies relevant to these dimensions.

5.5 Ethical- and Research Method Considerations

This study relies exclusively on public, non-sensitive documents and does not involve human subjects. As such, no formal ethical review was required. However, following Bryman's (2018) recommendations, the research sticks to principles of transparency, honesty, credibility, transferability, dependability, confirmability and source attribution (pp. 467-470). All sources are properly cited, and no confidential data has been used.

Like previously mentioned, this study adopts a qualitative comparative case study design based on document analysis. The choice of method is guided by the study's aim: to understand how Sweden and Estonia have adapted their national cybersecurity strategies post-2022, how these are shaped by EU and NATO frameworks and the framing of cyber threats in official policy documents. The research questions focus on meaning, framing, and institutional response, factors best explored through qualitative, interpretive methods (Bryman, 2018, p. 487).

A document-based approach is particularly appropriate for this topic, as national cybersecurity strategies, government reports, and policy documents represent the authoritative positions of each state. These sources also reflect how states communicate security priorities to both domestic and international audiences. Since the thesis aims to examine both formal alignment

and discursive framing, analysing policy documents offers direct access to institutional language, legal structures, and national threat narratives.

Alternative methods such as interviews, quantitative content analysis, or surveys were considered but ultimately rejected for the following reasons:

- Interviews with policymakers or cyber professionals could offer in-depth insights but were not feasible within the time and ethical constraints of this study. Moreover, interviews tend to reflect personal or organizational perspectives rather than the state's official strategic posture.
- Quantitative content analysis could measure the frequency of certain terms or themes but would not capture the discursive and contextual nuances or themes needed to understand securitization or institutional alignment. Such an approach would risk oversimplifying the data.
- Surveys of public or expert opinion were deemed unsuitable, as the thesis is focused on state-level strategy and institutional behaviour, not individual perceptions or attitudes.

Ultimately, the selected method allows for a focused and theory-driven analysis of national adaptation within a supranational framework. It is well-suited to identifying patterns of convergence and divergence in official strategies, governance models, and threat framings. While qualitative document analysis has its limitations, such as a reliance on public texts and an inability to assess internal decision-making (Bryman, 2018, pp. 674-675), it remains the most appropriate approach for answering the study's research questions.

5.6 Researcher Positionality

As Bryman (2018) emphasizes, internal credibility and external transferability are crucial in qualitative research (p. 467). As a researcher based in Sweden with a background in global studies and interest in international security, I bring both regional familiarity and academic interest to the topic. My close ties to one of the cases (Sweden) raises the risk of implicit bias. It is also important to note that the Swedish cybersecurity strategy of 2025 was not available in English while writing this thesis. To try and translate as exact as possible I compared my personal translation of sentences to a translator software to see which version was the most spot-on. To reduce this possible bias even more, I have used clear analytical criteria, consistently applied to both cases, and maintained reliance on official sources rather than

subjective interpretation. Furthermore, the inclusion of a highly contrasting case (Estonia) serves as a balancing mechanism to enhance analytical neutrality.

5.7 Delimitations

Qualitative document analysis cannot capture informal practices or insider perspectives available through interviews or fieldwork (Bryman, 2018, p. 484). Moreover, the reliance on official documents may reflect policy aspirations more than actual implementation. However, as Bryman (2018, pp. 674-675) notes, such documents are valuable for exploring institutional discourse, official framing, and governance priorities, which are the key interests of this thesis. As a qualitative study based on document analysis, this thesis does not aim for generalizability in the statistical sense. Instead, it prioritizes trustworthiness, understood as the credibility, transparency, and consistency of the research process (Bryman, 2018, p. 467). To ensure this, the thesis applies a clearly defined theoretical framework, Cybersecurity Institutionalism, and systematically analyses and compares official documents from both Sweden and Estonia. This creates a structured and replicable basis for the analysis.

The use of public and official documents also strengthens the reliability of the findings. These documents represent formal policy commitments and provide a clear window into how states present their cybersecurity strategies to both domestic and international audiences. However, they may also reflect idealized or political versions of reality, which is a known limitation of document-based research (Bryman, 2018, pp. 674-675).

The study does not include interviews, internal communications, or classified materials, which means it cannot fully assess informal practices or behind-the-scenes negotiations. Moreover, the focus on state-level strategy excludes local initiatives and private-sector implementation, even though these actors are important in cybersecurity governance.

Finally, since the thesis is interpretive and theory-driven, there is a degree of subjectivity in how concepts such as securitization or institutional alignment are identified in the texts (Bryman, 2018, p. 483). To address this, the analysis remains transparent about how theoretical terms are operationalized and consistently applied across both cases.

6. Analysis

6.1 Introduction to the Analysis Chapter

This chapter uses the theoretical framework Cybersecurity Institutionalism (see **Table 1**) to analyse the chosen documents (see **Table 2**) and answer the three research questions: how have Sweden and Estonia adapted their cybersecurity strategies after 2022, and do they differ from each other? How has Estonia and Sweden's alignment with the EU and NATO influenced their cybersecurity policies, based on official government documents? In what ways have Estonia and Sweden framed cybersecurity as a national security issue, and how do their securitization processes differ?

With the backdrop of Cybersecurity Institutionalism, the analysis will look for divergences between Estonia and Sweden's governances and national influences on their cybersecurity policies versus EU and NATO's influence and alignment.

6.2 Institutional Influence and Policy Adaptation

This section examines how Estonia and Sweden have responded to the European Union's NIS2 Directive and other key EU cybersecurity frameworks, assessing how these supranational strategies have shaped national cybersecurity policy through mechanisms of Europeanization and coercive isomorphism. These concepts help us understand the pressures for convergence in policy among EU member states, either through normative alignment (Europeanization) or through external expectations and obligations (coercive isomorphism).

6.2.1 EU Influence - Estonia

Estonia has taken significant steps to transpose the NIS2 Directive into national legislation. A draft law amending the existing *Cybersecurity Act* was published in December 2024, aiming for full implementation by July 2025 (Lex Mundi, 2025a). This reflects Estonia's ongoing alignment with EU standards, a trend visible already in the *Cybersecurity Strategy 2024–2030*, which builds on EU frameworks such as NIS2 and the *EU Cybersecurity Strategy* (Estonian Ministry of Economic Affairs and Communications, 2024, p. 3).

The Estonian government's explanatory memorandum highlights that many NIS2 provisions are already reflected in Estonia's cybersecurity regime, including the national *Information Security Standard* (Estonian Ministry of Economic Affairs and Communications, 2024, p. 16). Estonia's early development of sector-specific security obligations shows a strong

convergence with EU expectations (RIA, 2023, pp. 4-5). The 2024 strategy further emphasizes Estonia's role as a committed EU and NATO member in cyber policy, with specific references to alignment with EU regulations and mentioning collaborating with other "like-minded countries" (Estonian Ministry of Economic Affairs and Communications, 2024, p. 5-6).

Estonia exhibits high institutional alignment. The 2023 strategy integrates EU obligations into national priorities while expanding the scope of regulation to include approximately 2,000 more entities (Lex Mundi, 2025a). Estonia's approach can be seen as an example of coercive isomorphism, where EU directives strongly influence national law, yet Estonia also demonstrates proactive agency in adapting these norms.

6.2.2 EU Influence - Sweden

Sweden is implementing NIS2 through the proposed *Swedish Cybersecurity Act*, outlined in *SOU 2024:18*, a government inquiry published in March 2024 (Swedish Ministry of Defence, 2024, p. 72). The Act, expected to enter into force in mid-2025, includes extensive adjustments to ensure compliance with both the NIS2 and CER Directives (Lex Mundi, 2025b). The updated direction is also reflected in *National Strategy for Cybersecurity 2025-2029*, a forward-looking strategy document emphasizing stronger EU and NATO alignment (Swedish Ministry of Justice, 2025, p. 2).

The new legal framework introduces increased supervisory powers and sanctioning mechanisms (Swedish Ministry of Justice, 2025, pp. 2). While it mirrors *NIS2*, Sweden uses slightly different terminology (e.g., "operators" vs. "entities"), which might reflect national legal preferences but doesn't signal divergence in policy intent (Lex Mundi, 2025b). Sweden's foreign and security policy strategy on cyber issues (2024) also points to EU alignment in digital governance and regulation (Swedish Ministry of Foreign Affairs, 2024, p. 9).

Sweden is aligning with the *NIS2 Directive* but at a more measured pace than Estonia. Although the structure of the new policy closely follows the EU directive, Sweden's traditionally decentralized governance has shaped the way responsibilities are distributed across agencies (FOI, 2023, pp. 8–10). This could be seen as a softer form of Europeanization, still following EU norms but with more emphasis on domestic interpretation.

6.2.3 Comparison

When comparing Estonia and Sweden's adaptation of EU cybersecurity directives through the lens of cybersecurity institutionalism, distinct differences and similarities emerge in how EU influence shapes national policy and institutional structures.

Estonia demonstrates a strong case of coercive isomorphism, where the influence of EU directives is directly reflected in national legislation and institutional design. Estonia has been proactive in aligning its cybersecurity policies with EU frameworks, as evidenced by the draft law amending the *Cybersecurity Act* published in December 2024, which aims for full implementation by July 2025 (Lex Mundi, 2025a). *The Estonian Cybersecurity Strategy 2024–2030* explicitly builds on NIS2 and the EU Cybersecurity Strategy (Estonian Ministry of Economic Affairs and Communications, 2024, pp. 5-6). Many requirements were already embedded in Estonia's national cybersecurity regime through instruments such as the national *Information Security Standard* (Estonian Ministry of Economic Affairs and Communications, 2024, p. 16), indicating a high level of institutional alignment even before the formal adoption. The inclusion of approximately 2,000 new entities under the regulation's scope (Lex Mundi, 2025a) further underscores Estonia's strong convergence with EU norms. Estonia's strategic framing of itself as a committed EU and NATO member in cyber affairs (Estonian Ministry of Economic Affairs and Communications 2024, pp. 5-6) also illustrates normative isomorphism, while its anticipatory reforms and sector-specific obligations suggest mimetic isomorphism, where EU best practices are not only adopted but also adapted to national ambitions (Estonian Ministry of Economic Affairs and Communications, 2024, pp. 40, 49, 52).

Sweden, by contrast, reflects a more moderate form of institutional convergence. Sweden is implementing NIS2 through a proposed *Cybersecurity Act* presented in *SOU 2024:18*, which is expected to enter into force in mid-2025 (Swedish Ministry of Defence, 2024, pp. 5–6). While this legislation largely mirrors NIS2, Sweden's decentralized administrative tradition influences how responsibilities are distributed across agencies (Swedish Ministry of Justice, 2025, p. 15). This reflects a form of soft Europeanization, where EU directives are mediated through existing national structures. For example, the Swedish proposal uses slightly different terminology which may indicate legal-cultural preferences without signalling something entirely different (Lex Mundi, 2025b). Sweden's *Cybersecurity 2025-2029* strategy also confirms EU and NATO alignment, though in a more progressive manner (Swedish Ministry of Justice 2025, p. 2). Additionally, the foreign and security policy strategy on cyber issues

from 2024 emphasizes EU digital governance values while allowing room for national interpretation (Swedish Ministry of Foreign Affairs, 2024, p. 9). Sweden thus exhibits coercive isomorphism in response to EU legal obligations, but filtered through domestic path dependencies, leading to a more measured form of institutional alignment.

With the help of cybersecurity institutionalism, we can see that Estonia has high institutional alignment driven by both external pressures and proactive internal adaptation, whereas Sweden shows more moderate, building towards, high alignment with a more nationally contextualised response. Both cases illustrate how EU institutionalism shapes national cybersecurity policy, with Estonia embracing stronger coercive and normative pressures, and Sweden navigating these influences through a more interpretative governance lens. So, while both countries are legally aligned with the EU's cybersecurity framework, particularly through NIS2, their domestic implementation approaches reflect deeper governance logics. These differences raise important questions about the EU's ability to achieve a unified harmonization across diverse national models.

6.3 Influence of NATO's Cybersecurity

This section investigates the extent to which NATO has shaped cybersecurity strategies in Estonia and Sweden, particularly following the post-2022 threat spike outlined in Chapter 2. NATO's strategic shift toward cyber as a core domain of collective defence is emphasised in the *NATO Strategic Concept (2022)* and *Cyber Defence Pledge*.

6.3.1 Estonia's Integration

Estonia, as a NATO member since 2004, views the alliance as the cornerstone of its national security. This is explicitly stated in the *National Security Concept of Estonia (2023, p. 4)*, which frames cyber threats as part of a broader hybrid threat environment, often attributed to state actors like Russia (Estonian Ministry of Defence, 2023, pp. 4–5). NATO's strategic shift has further validated Estonia's emphasis on collective cyber defence.

The *Cybersecurity Strategy 2024–2030* integrates NATO doctrines throughout. The document emphasizes coordination with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), located in Tallinn, and the use of NATO frameworks to assess national vulnerability and readiness (Ministry of Economic Affairs and Communications, 2024, pp. 12–14). The CCDCOE analysis (2023) further reinforces Estonia's position as a cyber defence

leader within NATO, noting its contribution to policy development and cyber exercises (CCDCOE, 2023, pp. 6–7). The older *Estonian Cybersecurity Strategy 2019-2022* also mentions NATO throughout but focuses a lot on Estonia’s role and hopes to be a role model within international cooperations, an example being “*The objective of the activity for Estonia to have a visible footprint on European Union and NATO cyber cooperation and a continuing participation in UN cyber processes. The precondition for achieving the objective is substantive messaging and expertise in setting foreign policy goals. The prerequisite of successful international cooperation is for Estonian diplomats and other officials representing Estonia to be capable of forwarding uniform messages coordinated domestically regarding policies in the Estonian cybersecurity field. Estonia’s active participation in the EU, NATO, UN and other international 59 organizations’ processes allows the country to advocate better for its interests and priorities.*” (pp. 58-59). Estonia’s alignment with NATO goes beyond rhetorical commitment. It participates in NATO’s exercises and has embedded NATO’s strategic objectives into domestic legislation and institutional frameworks (Estonian Ministry of Economic Affairs and Communications, 2024, p. 8).

6.3.2 Sweden’s Emerging Alignment

Sweden’s historical non-alignment limited its formal integration with NATO cybersecurity structures prior to its accession process. However, the 2022 invasion of Ukraine triggered a rapid shift. *The Strategy for Foreign and Security Policy on Cyber and Digital Issues (2024)* outlines Sweden’s growing alignment with NATO cyber doctrine, acknowledging collective defence as a future cornerstone (Swedish Ministry of Foreign Affairs, 2024, pp. 3–5).

Although Sweden had very newly joined NATO at the time of the *National Strategy for Cybersecurity 2025-2029* publication, the strategy signalled full preparedness to meet NATO interoperability standards (Swedish Ministry of Justice, 2025, pp. 2–4). Sweden is aligning doctrinally with NATO, but full institutional integration remains in progress. While Estonia has embedded NATO cyber doctrine into its operational structures, Sweden is transitioning from observer to participant. Sweden clearly states that full cooperation with NATO is a goal, for example writing “*To continuously map, identify and assess cyber threats on the full scale often requires extensive cooperation between national authorities and with authorities in other states, not least through established collaborations within EU and NATO.*” (Swedish Ministry of Justice, 2025, p. 24).

This said, the current difference illustrates varying degrees of strategic adaptation, Estonia as an institutionalised NATO cyber actor, Sweden as a rapidly adapting entrant.

6.3.3 Comparison

Both Estonia and Sweden have made significant strides in adapting their cybersecurity strategies in areas like critical infrastructure protection, national defence, and public sector cybersecurity. According to *Estonia's Cybersecurity Strategy 2024–2030* and *National Security Concept* (2023), the country focuses heavily on defending its digital infrastructure, given its high reliance on digitalization for governance (Estonian Ministry of Economic Affairs and Communications, 2024, p. 16). Sweden's *MSB Annual Cybersecurity Report* (2024) similarly emphasizes the protection of critical infrastructure, though in the context of encouraging the private sector to engage in cybersecurity checks, also proving decentralized governance (MSB, 2024, p. 135). Both countries also underline the importance of international cooperation with frameworks like NATO and the European Union, signalling a shared commitment to regional and international cybersecurity standards (RIA, 2024; Swedish Ministry of Justice, 2025).

In terms of union adaptations, both countries align their cybersecurity strategies with EU directives, such as the NIS2 Directive, which aims to strengthen the EU's cybersecurity resilience (European Commission, 2022). For example, both countries emphasize enhancing resilience in digital infrastructures and strengthening the protection of critical sectors against cyber threats. Additionally, both Estonia and Sweden participate actively in the EU's Digital Single Market initiatives, which aim to create more standardized cybersecurity measures across the union (European Commission, 2024).

The Strategy for Foreign and Security Policy on Cyber and Digital Issues (Swedish Ministry of Foreign Affairs, 2024) discusses the need for both national and international cooperation to counter threats ranging from state-sponsored attacks to criminal activities in cyberspace.

While both countries recognize the threat from state actors, Sweden's broader approach reflects its (previous) neutral stance and role in international diplomacy, focusing more on universal digital security frameworks. Both Estonia and Sweden share a focus on resilience and security, but their language differs. Estonia emphasizes digital sovereignty as part of its cybersecurity narrative, given its role in digital governance and focus on safe information security standards (RIA, 2024, p. 47). In contrast, Sweden uses terms like societal importance

and sustainability, highlighting its broader societal focus that integrates both public and private sector efforts in cybersecurity (MSB, 2024, p. 19).

The asymmetry in NATO integration reflects not only Estonia's longer membership but also the degree to which cyber defence is securitized in national strategy. Sweden's evolving relationship with NATO and gradual integration into its cyber structures point toward a different path, one that highlights flexibility but also raises questions about cohesion within the alliance.

6.4 Securitization of Cyber Threats

This section analyses how cyber threats are framed and politicized in Estonia and Sweden by applying core concepts from securitization theory: the securitising move, the referent object, and audience acceptance (Buzan et al., 1998, p. 25). This process is central to understanding national adaptation post-2022, as well as the influence of EU and NATO strategies.

6.4.1 Estonia - Strong Framing

Since 2007, Estonia has adopted a highly securitized view of cyber threats due to the cyberattacks that disrupted key national institutions (Davis, 2007, p. 2). These events positioned cybersecurity as an existential issue and catalysed the institutionalisation of Estonia's cyber defence capacities (CCDCOE, 2013, p. 5). *The Cybersecurity Strategy 2024–2030* explicitly frames cybersecurity as integral to defending national sovereignty, democratic processes, and societal continuity, even framing specific countries as threats; (...) *most directly influenced by Russia's actions, in the longer term, greater attention must also be paid to other authoritarian states active in cyberspace, such as Iran, North Korea and especially China.*“ (Estonian Ministry of Economic Affairs and Communications, 2024, p. 5).

Estonian governmental actors and their statements and strategic texts about cybersecurity reflect a securitising move that links resilience against cyber threats to national survival. The *National Security Concept of Estonia* (2023) identifies cyber threats as part of broader hybrid warfare and includes them among threats requiring military preparedness, stating that a hybrid attack can activate NATO's Article 5 (p. 7). The referent objects in Estonian policy are clear: critical infrastructure, elections, national sovereignty, and governmental continuity. These are framed as under potential existential threat from hostile state actors, especially Russia.

Estonia's leadership in NATO's cyber agenda, particularly through its role in the CCDCOE

shows audience acceptance due to the national focus of the subject and lack of complaints from the general public. In fact, the *Cybersecurity in Estonia 2024* mentions the Estonian government's free course in cybersecurity "Cybertest" and states that during 2023 "(...) more than 200 private and public sector organisations joined the initiative and more than 15,000 people underwent training and testing." (RIA, p. 5)

6.4.2 Sweden - Gradual Securitization

Sweden's approach to cyber threats is more cautious. While cyber threats are acknowledged in strategic documents, they are typically framed within broader contexts of societal resilience, digital sovereignty, and public trust. *The Strategy for Foreign & Security Policy on Cyber & Digital Issues* (Swedish Ministry of Foreign Affairs, 2024) and the forward-looking *Cybersecurity 2025* (Swedish Ministry of Justice, 2025) prioritize coordination, preparedness, and democratic values over militarized threat responses, perhaps not wanting to scare the public with its phrasing.

Swedish securitizing actors are more dispersed. Agencies such as the Swedish Civil Contingencies Agency (MSB), the Swedish Ministry of Justice, The National Defence Radio Establishment (FRA) and the Swedish Defence Research Agency (FOI) are central players (MSB, 2024, FOI, 2024), but there is no single lead authority making repeated securitising moves. The language in policy documents is more moderate, with fewer references to specific threats and more focus on maintaining continuity and protecting services. External threats are mentioned way more carefully than in Estonian documents, for example, the *Strategy for Foreign & Security Policy on Cyber & Digital Issues* (2024) only mentions "A number of countries carry out cyber-attacks on Sweden. The capacity to manage cyber threats and cyber attacks is fundamental to Sweden's security." (p. 6). This aligns with Sweden's traditionally more careful and neutral global stance.

Referent objects in the Swedish case are also broader. Cybersecurity is framed as essential for ensuring "(...) a safer Sweden" (Swedish Ministry of Foreign Affairs, 2024, p. 2), but national survival is not specifically mentioned. As a result, the degree of audience acceptance appears more conditional and technical rather than emotionally charged, not linking cybersecurity with the nation's survival.

6.4.3 Comparison

Estonia and Sweden illustrate contrasting securitization dynamics. Estonia has adopted a high-intensity securitization model, built around a legacy of direct cyber aggression and a centralized defence posture. Its policy language is urgent, existential, and militarised, with clear threat perceptions. Sweden, by contrast, has another focus on its securitisation process, emphasising resilience and multilevel governance instead.

Both countries align with EU directives, such as the *NIS2 Directive* (EU, 2022) and the *Cyber Resilience Act* (EU, 2022) and acknowledge NATO's growing cyber defence role (NATO Strategic Concept, 2022). However, Estonia's strategies more closely echo NATO's deterrence framing and cyber defence pledges (NATO, 2016), while Sweden's documents lean toward the EU's language of digital sovereignty and capacity-building (European Commission, 2024).

These differences suggest that while both external actors shape national cybersecurity discourse, domestic factors, particularly history, threat perception, and administrative culture, play a decisive role in how cyber threats are securitized. The government documents showcase what Buzan et al. (1998) mentions. For example, in the case of Estonia, securitization theory helps explain how past cyber incidents have been used to justify a framing of cybersecurity as a matter of national survival. Here, the state itself functions as the referent object, and institutions like the Ministry of Defence and RIA act as securitizing actors. Estonia's audience, including the public and political elites, has largely accepted this framing, enabling a strong and centralised response.

In contrast, Sweden illustrates a more moderate securitization process. Cyber threats are framed as serious, but not existential, with a focus on societal resilience and service continuity. The referent object is broader, encompassing citizens, businesses, and infrastructure, and securitizing actors are more varied, including civilian agencies like MSB. The audience response is more cautious, which means that cybersecurity in Sweden stays as a general political problem, not reaching emergency-level politics like in Estonia. This, according to the theory, means Sweden will have a harder time justifying bigger changes to the country's cybersecurity policy, as it has not been explained as an emergency issue before. (Buzan et al., 1998). These contrasts demonstrate how institutional structure and historical experience mediate the securitization of cybersecurity across national contexts.

6.5 Cybersecurity Governance

This section explores how cybersecurity governance is structured in Estonia and Sweden, focusing on institutional arrangements, coordination models, and operational capacities. Using concepts from cybersecurity governance theory, including centralized versus decentralized models and cyber resilience, it analyses how national systems enable or constrain the adaptation of EU and NATO policies. The analysis reveals key differences in how Estonia and Sweden govern cybersecurity, which in turn affects their implementation capacity, institutional agility, and long-term resilience.

6.5.1 Estonia's Governance Model

Estonia's cybersecurity governance is marked by a (in theory) centralized and strategically integrated model, with strong ties between civilian and defence sectors, most likely a direct legacy of the 2007 cyberattacks, which acted as an important event for deciding on cyber governance within a national security framework and creating The Cyber Defence Unit of the Estonian Defence League which was one of the first of its kind (CCDCOE, 2013, p. 5). Interestingly, *the Estonian Cybersecurity Strategy 2024-2030* describes the governance model to be decentralized quoting “*Due to the decentralised management model, central policymaking is more challenging, and funding is more focused on individual institutions rather than on the national level.*” (Estonian Ministry of Economic Affairs and Communications, 2024, p. 8). This could be questioned due to the strategy's explicitly positioning cybersecurity as a domain of national defence, with the Ministry of Defence, the Estonian Information System Authority (RIA) at the centre of coordination (Estonian Ministry of Economic Affairs and Communications, 2024, pp 7-8).

The Estonian model demonstrates several features of centralized governance, clearly defined lines of authority, a limited number of key actors, and direct vertical integration between strategy and implementation. The RIA plays both regulatory and operational roles, ensuring alignment between strategic vision and technical execution and is continuously growing, going from 30 to over a hundred in just a couple of years (RIA, 2024, pp. 6). Estonia's *National Security Concept (2023)* further reinforces the integration of cyber into national defence, supporting joint civil-military planning and rapid crisis response. Perhaps this is what makes Estonia's governance decentralized, the ultimate goal being to cooperate more

collaboration between different actors, an example being in *the Estonian Cybersecurity Strategy 2024-2030* (2024) on page 3; “As a horizontal strategy, its objective is to make agreements between the actors involved in ensuring Estonia’s cybersecurity – the public sector (both civilian and military defence), providers of services that are vital and essential for the functioning of society, companies operating in the sector, universities and other research institutions – and to create the conditions for implementing a comprehensive, systemic and inclusive cyber policy.”

The theoretical Estonian centralization would allow for rapid decision-making and coherent messaging, especially in times of heightened threat. It also supports Estonia’s ability to respond quickly to EU directives, such as the *NIS2 Directive* (EU, 2022), and align with NATO’s collective defence principles (NATO, 2022). However, this model can potentially limit broader societal engagement and may rely heavily on the efficiency and expertise of a small group of institutions. The decentralized governance method can slow down the response time but also include more actors in the important work of cybersecurity.

6.5.2 Sweden’s Governance Model

In contrast, Sweden adopts a more decentralized, civilian-led model of cybersecurity governance. Responsibility is distributed across multiple ministries, agencies, and local governments, reflecting Sweden’s traditional model of administrative autonomy and municipal preparedness. The newer cybersecurity 2025-2029 strategy articulates this decentralized governance as a strength, emphasizing collaboration, subsidiarity, and democratic legitimacy (Swedish Ministry of Justice, 2025, pp. 5-6). Key actors include the Swedish Civil Contingencies Agency (MSB), the Swedish Ministry of Justice, the Swedish Armed Forces (in limited roles), and sectoral agencies. According to the FOI’s 2024 study, Sweden’s cyber governance is shaped by legal mandates and inter-agency coordination rather than a single command structure, resulting in slower, but potentially more robust, policy development (FOI, 2024, pp. 724-725). The *MSB Annual Cybersecurity Report (2024)* highlights ongoing challenges in coordination, especially in translating EU requirements into cohesive national implementation plans. In the report, the section of NIS-actors had to be ignored due to the lack of answers as well as hardships in getting in contact (MSB, 2024, p. 15).

This decentralized governance structure supports inclusivity and resilience at the societal level. Municipalities, civil society, and the private sector are actively engaged in cyber preparedness, especially through exercises and public-private partnerships (MSB, 2024, p. 135). However, the fragmentation of responsibility can delay decision-making and lead to inconsistent interpretations of EU regulations like *NIS2* and the *proposed Cyber Resilience Act* (EU, 2022).

Sweden's civilian emphasis is also evident in its response to the Ukraine war's digital implications. The *Strategy for Foreign and Security Policy on Cyber and Digital Issues* (2024) focuses more on international collaboration and digital autonomy than direct deterrence with the Minister for Foreign Affairs, Maria Malmer Stengard, stating, "*Sweden will pursue a policy based on solidarity within the scope of the European Union (EU) and the North Atlantic Treaty Organization (NATO). Based on our interests and values, Sweden will be a key actor in international contexts, including in relation to strategic partners. Cooperation with the private sector on international and cross-border threats and attacks is also an important part. To strengthen its role and influence internationally, it is crucial that Sweden pursues a coherent and integrated foreign and security policy on cyber and digital issues.*" (Swedish Ministry for Foreign Affairs, 2024, p. 3). Thus reflecting Sweden's longstanding preference for multilateralism and rule-based cyber governance.

6.5.3 Comparison - Governance Models

The contrasting governance models of Estonia and Sweden illustrate two paths toward cybersecurity resilience, each with distinct strengths and limitations. Estonia's (in theory) centralized, defence-integrated approach allows for fast responses and a high degree of coherence in adapting EU and NATO strategies. Its alignment with NATO frameworks is facilitated by institutional clarity and operational readiness, particularly through the CCDCOE and cyber defence units (CCDCOE, 2013, NATO, 2022).

In Sweden, the decentralized model offers resilience through societal participation and layered institutional robustness. However, it also results in a slower and more fragmented adaptation to supranational strategies. The FOI (2024) report indicates that some agencies wait for political signals before acting on EU directives (p. 726), reflecting weaker vertical command chains compared to Estonia.

Ultimately, the effectiveness of cybersecurity governance depends on the national context. Estonia's small size, security history, and NATO orientation favour a (in theory) centralized approach. Sweden's large administrative structure and civilian protection ethos favour decentralization. Both models have managed to adapt EU and NATO strategies post-2022, but in different ways and at different speeds, illustrating the importance of governance architecture in cybersecurity resilience. The governance structure directly affects implementation speed, policy coherence, and institutional resilience. As Chapter 7 will discuss, these structural differences have broader implications for European cybersecurity governance and the operationalization of resilience in a rapidly evolving threat environment.

6.6 Summary of Analytical Findings

Chapter 6 has examined how Estonia and Sweden have adapted their cybersecurity strategies after 2022, and how EU and NATO frameworks have shaped those adaptations. This section clearly shows how the analysis has answered each of the research questions (RQs).

6.6.1 National Adaptation and Divergences (RQ1)

The first research question asked how Sweden and Estonia have adapted their cybersecurity strategies after 2022, and how they differ from each other. The results show a clear divergence in both pace and structure. Estonia has rapidly and comprehensively updated its national cybersecurity framework through (in theory) centralized institutions and direct integration with defence planning (Estonian Ministry of Economic Affairs and Communications, 2023). In contrast, Sweden has followed a more fragmented, calculated process, shaped by its decentralized administrative tradition and more civilian-oriented security culture (Swedish Ministry of Justice, 2023).

Estonia's adaptation reflects high institutional convergence, where cybersecurity is not only a policy priority but also an extension of its national security strategy (Estonian Ministry of Economic Affairs and Communications, 2023; NATO, 2022). Sweden's adaptation is more procedural, reflecting a risk-based and resilience-oriented model, where cybersecurity is treated as one of many critical infrastructure concerns rather than an existential issue (MSB, 2023).

6.6.2 Supranational Influence and National Alignment (RQ2)

The second research question focused on how Estonia and Sweden's alignment with EU and NATO frameworks has influenced their national cybersecurity policies, based on official

documents. The findings show that both countries formally align with EU directives, particularly the *NIS2 Directive* (European Commission, 2022) but differ significantly in how these frameworks are interpreted.

Estonia's swift integration of *NIS2* illustrates strong institutional convergence with EU policy, underpinned by both legal compliance and strategic alignment (Estonian Ministry of Economic Affairs and Communications, 2023). Rather than merely meeting requirements, Estonia has expanded regulatory reach and embedded EU priorities into national planning, an example of both normative and coercive adaptation (European Commission, 2022; NATO, 2022).

Sweden, while politically committed to EU and NATO alignment, adapts these frameworks more cautiously. The proposed *Cyber Resilience Act* (European Commission, 2022) and national legislation mirror *NIS2* structurally but reflect Sweden's legal traditions and decentralized administrative model (Swedish Ministry of Justice, 2023). NATO influence remains more symbolic or aspirational at this stage, following Sweden's recent accession (NATO, 2022), representing a softer form of Europeanization, where supranational norms are integrated gradually and selectively through national filters (Wong & Hill, 2011; Radaelli, 2003).

6.6.3 Framing and Securitization of Cyber Threats (RQ3)

The third research question examined how Estonia and Sweden frame cybersecurity as a national security issue, and how their securitization processes differ. The analysis reveals a stark contrast in the intensity, language, and structure of securitization.

Estonia applies a strong, existential securitization of cyber threats. Government documents describe cybersecurity as vital to state survival and democratic sovereignty, drawing on the collective memory of the 2007 cyberattacks (Estonian Ministry of Economic Affairs and Communications, 2023; NATO, 2016). Defence-related actors play key roles in making securitizing moves, and the referent object is clearly the Estonian state (Buzan et al., 1998).

Sweden, in contrast, frames cybersecurity primarily through the lens of societal resilience and crisis preparedness. Official documents emphasize risk management, cooperation, and the protection of critical infrastructure but largely avoid existential or militarized language (MSB, 2023; Swedish Ministry of Justice, 2023). The referent object is broader, often framed as the need to ensure societal continuity, and the securitization process is more dispersed, involving multiple civilian agencies (Buzan et al., 1998).

7. Result and Conclusion

This chapter discusses the results of the comparative analysis of Sweden and Estonia's post-2022 cybersecurity strategies, with the aim of understanding how national governance models and strategic cultures shape the implementation of EU and NATO cybersecurity frameworks as well as how the countries' securitization processes differ. Grounded in the framework of Cybersecurity Institutionalism, the chapter interprets the broader implications of these findings for both national governance and supranational efforts to harmonize cybersecurity policy within the EU and NATO.

The analysis showed that while both countries align in principle with shared external frameworks, most notably the EU's NIS2 Directive and NATO's Strategic Concept, they differ significantly in how they interpret and implement cybersecurity policy. These differences stem from structural and cultural factors that go beyond legal compliance, raising important questions about the capacity of supranational governance to harmonize cybersecurity responses across diverse national settings.

7.1 Institutional Adaptation and Governance Models

A central finding from the analysis is the clear divergence in how Estonia and Sweden adapt to shared cybersecurity frameworks, particularly those developed by the EU and NATO. While Estonia has taken a rapid, top-down approach to implementing instruments like the *NIS2 Directive*, Sweden's progress has been slower and filtered through a more decentralized governance model, as discussed for example in section 6.5. Although this contrast is visible at the structural level, it also reflects deeper institutional logics and strategic cultures.

Rather than repeating the descriptive distinctions, it is more important to ask: What does this divergence reveal about the institutional conditions for supranational governance, and what are the implications of partial or selective compliance? Estonia's alignment with EU and NATO frameworks is not just a matter of legal compliance, it illustrates what Wong and Hill (2011) refer to as transformational Europeanization, where external norms are internalised and actively shape domestic priorities. This is enabled by Estonia's institutional structure, which concentrates cybersecurity responsibilities in a small number of well-positioned state bodies, such as the Ministry of Economic Affairs and Communications and the RIA. As a result,

Estonia appears not only as a compliant actor, but as a norm creator within EU and NATO cyber domains.

Sweden, on the other hand, demonstrates what could be described as adaptive pluralism, a governance model that balances supranational expectations with domestic legal traditions and administrative decentralization (Wong & Hill, 2011). While this results in a slower implementation of directives like NIS2, it arguably strengthens democratic legitimacy and fosters broader stakeholder inclusion. However, it also introduces coordination challenges and risks of fragmentation, particularly when rapid crisis response is needed.

These differences raise critical questions about the institutional fit of supranational frameworks within diverse national systems. Estonia's experience suggests that when national and supranational goals align, adaptation can be swift and strategic. In Sweden, the less integrated institutional alignment requires negotiations, internal consensus-building, and legal reinterpretation, steps that delay but may deepen long-term institutionalisation.

In theory, this comparison highlights that Cybersecurity Institutionalism needs to focus not just on whether countries adjust their cybersecurity policies, but also on how they do it. The way institutions are built, how public administration works, and the level of political trust and legitimacy all shape the form that adaptation takes.

In practice, this means that efforts by the EU and NATO to harmonise cybersecurity policies must take national differences into account. This doesn't mean lowering standards, it means designing policies that are flexible enough to match each country's institutional setup. If a one-size-fits-all model is used, there's a risk of estranging countries that need more time, dialogue, or coordination to successfully adapt, pushing them away from the organization or alliance.

7.2 Securitization and Framing of Cyber Threats

Another major insight from this study lies in the distinct ways Sweden and Estonia frame cyber threats in their national strategies. As the analysis has shown, Estonia adopts a more existential and state-centric framing, while Sweden favours a broader, resilience-oriented approach. This section explores what these divergent securitization processes mean for policy effectiveness, public legitimacy, and strategic alignment.

Drawing on securitization theory (Buzan, Wæver, & de Wilde, 1998), security is not simply about objective threats, it is a process through which issues are presented as existential risks requiring extraordinary measures. In Estonia's case, securitizing actors such as the Ministry of

Defence and RIA have successfully framed cyber threats as dangers to national sovereignty, democratic integrity, and state continuity. This framing draws on Estonia's 2007 cyberattack experience, which remains a key national memory and helps justify a more serious, security-focused cyber policy. The referent object here is the Estonian state itself, and the audience, both public and political, appears receptive, reinforcing the legitimacy of securitizing moves.

In contrast, Sweden's securitization is more procedural, diffuse, and embedded in a tradition of civilian-led crisis management. Instead of describing cyber threats as direct dangers, Swedish strategy documents emphasise societal resilience, continuity of services, and decentralized preparedness. The referent object is broader, encompassing municipalities, infrastructure providers, and individuals and the audience is similarly fragmented. As a result, the framing of cyber threats does not trigger the same level of political urgency or institutional focus.

These divergent securitization logics have practical consequences. Estonia's framing allows for rapid centralization of authority and resource prioritisation, contributing to fast-paced adaptation of EU and NATO directives. Sweden's softer securitization, while democratically inclusive, may slow political consensus and complicate cross-agency coordination, particularly when urgent legislative or security action is needed.

Importantly, this divergence also affects how supranational policies are internalised. In Estonia, EU and NATO directives are framed as natural extensions of an already securitized domain. Their implementation is not only bureaucratic but ideologically and strategically aligned. In Sweden, the same directives might be seen more as technical management tools. This can create tension with existing national ways of working and may require them to be adjusted or reinterpreted to fit into a more complex and divided institutional system.

Theoretically, these findings demonstrate that securitization is not only about speech acts, but also profoundly shaped by institutional setting, strategic culture, and historical narrative. Estonia's strong security institutions provide a platform for successful securitizing moves, while Sweden's multi-actor, civilian-led system demands broader consensus and fosters more gradual framing. This highlights the need for securitization theory to be more attentive to the governance context in which speech acts occur, especially in areas like cybersecurity where technical, civilian, and military domains overlap.

Overall, the comparison between Estonia and Sweden reveals two equally valid but strategically different approaches to framing cybersecurity. One is driven by urgency,

centralization, and geopolitical proximity, the other by inclusiveness, and institutional pluralism. Recognising these differences is essential for understanding not only how cybersecurity is governed, but how it is legitimated and sustained in the public. It is also important to note that these variations are not a failure of supranational coordination but a reflection of the institutional diversity that supranational actors must strategically navigate.

7.3 Methodological and Theoretical Reflections

The analysis in this thesis was based on a qualitative, thematic text analysis of official cybersecurity strategies and policy documents from Sweden and Estonia between 2022 and 2025. This method made it possible to explore how cyber threats are framed, how institutional roles are articulated, and how supranational directives are integrated into national discourse. By focusing on documents such as national strategies, legal proposals, and implementation reports, the study could capture the formal articulation of cybersecurity governance and map changes over time.

The decision to focus on official texts brought several advantages. It allowed for a structured comparison of strategic intent, alignment with EU/NATO frameworks, and the presence of securitising language. It also provided insight into the institutional architecture of each country's cybersecurity system. However, the method also involved important limitations. First, document analysis cannot fully account for the implementation gap, that is, the difference between what is written in strategy documents and what is practiced in real-time. Second, the method provides limited insight into political motivations, institutional resistance, or informal power dynamics, which could have been better captured through interviews or ethnographic fieldwork.

Despite these limitations, the Cybersecurity Institutionalism framework proved useful in interpreting the data. Europeanization theory, particularly as elaborated by Wong and Hill (2011), helped clarify the ways in which EU policy instruments are filtered through national structures. It highlighted the importance of institutional fit and domestic mediation in shaping the degree of alignment. Similarly, securitization theory (Buzan et al., 1998) offered a valuable lens for comparing how different national actors frame cyber threats, and how those framings are tied to institutional authority, audience engagement, and political culture.

The use of cybersecurity governance and resilience theory also added explanatory power to the Cybersecurity Institutionalism framework, especially in understanding how the structure of institutions affects a country's ability to respond to supranational directives. Concepts such

as centralization versus decentralization, resilience, and coordinated capacity were essential in revealing how institutional design influences both policy speed and legitimacy. Mixing the theories together to create a new framework was proven insightful as the documents could be analysed by the most relevant terms from the different theories. However, the most relevant and interesting terms of each theory is individual, and it is important to note that Cybersecurity Institutionalism might have consisted of other terms and aspects of the theories if someone else wrote this thesis.

In future work, these theories could be further refined or expanded by including a longitudinal element, looking at how cybersecurity strategy evolves across political cycles or in response to real cyber incidents or

7.4 Limitations

While the study offers valuable insights, it is important to acknowledge its empirical and analytical limitations. First, the focus on two countries, Sweden and Estonia, means that findings cannot be easily generalized to the entire EU or NATO context. Although the cases were chosen for their strategic contrast, additional cases from other governance models (e.g., France, Germany, or Poland) could have further strengthened the comparative element.

Second, the time frame (2022–2025) captures a highly dynamic period in European security, including Sweden’s NATO accession and ongoing adjustments to EU directives like NIS2. This snapshot offers timely insights but may miss longer-term developments, such as delayed implementation or institutional reform that unfolds gradually.

Third, the study’s reliance on official documents means that the analysis reflects state-centric and formal narratives. It does not incorporate views from private sector actors, or local authorities, especially important in a decentralized model like Sweden’s. These perspectives could have revealed issues or innovation occurring below the national level.

Finally, the use of English-language and translated sources may also limit the full nuance of national debates, particularly in Estonia, where key discourse may unfold in Estonian.

7.5 Future Research

This study opens several opportunities for future research. First, a more in-depth, actor-focused study could investigate how different agencies and stakeholders interpret and implement cybersecurity policy. Interviews with officials, cybersecurity professionals, and municipal actors could provide valuable data on institutional dynamics and friction points.

Second, future research could explore the role of political leadership in shaping cyber policy adaptation. Do party ideologies or electoral cycles influence how cyber threats are framed or how supranational rules are adopted? This would build on securitization theory by emphasizing not just structure, but also agency and political choice.

Third, a more long-term study made over a longer period of time comparing policy evolution from pre-2022 to post-2025 would help assess whether early divergences eventually converge under continued EU/NATO pressure, or whether path dependency deepens national differences over time.

Finally, there is significant potential in studying regional cyber cooperation and norm entrepreneurship among small states. Estonia, for instance, has positioned itself as a leader within NATO through the CCDCOE, while Sweden has emphasized resilience and innovation. Comparative studies on how small states shape, rather than just receive, cybersecurity norms could add depth to both Europeanization theory and international relations research.

7.6 Chapter Summarisation and Final Conclusion

This chapter has discussed and reflected on the comparative findings of Estonia and Sweden's post-2022 cybersecurity strategies found in chapter 6, viewed through Cybersecurity Institutionalism. It has shown that while both countries operate under the same EU and NATO frameworks, their responses diverge in meaningful ways, shaped by institutional design, historical experience, and national security cultures.

Estonia exemplifies a model of centralized, security-driven adaptation, where supranational directives are rapidly internalized and legitimized through strong state institutions and a well-established narrative of cyber threat urgency. Sweden, by contrast, represents a decentralized, resilience-oriented approach, where adaptation occurs more slowly and is facilitated through various governance structures and a civilian framing of cybersecurity challenges.

These contrasting models highlight that legal alignment does not automatically produce strategic convergence. National adaptation is filtered through existing administrative traditions, the degree of centralization, and the framing power of state actors. For the EU and NATO, this presents a key governance challenge: how to foster harmonization while respecting domestic diversity.

The discussion of this chapter also underscores the utility of combining multiple theoretical lenses into a broader framework of Cybersecurity Institutionalism. This approach allowed for a more nuanced understanding of how institutions, discourses, and supranational pressures interact. It also showed that securitization is not just a matter of language, but of institutional capacity and historical legitimacy.

To officially conclude, this study reveals that cybersecurity governance in Europe is not only about capacity or compliance, but it is also fundamentally about how states interpret, frame, and institutionalize shared threats in ways that resonate with their own governance type and history. Harmonization efforts must move beyond formal alignment to consider the cultural, strategic, and administrative pathways through which policy is internalized. Understanding these differences is key to creating cyber policies that are more flexible, trusted, and better coordinated, especially in a digital world that is becoming more divided, competitive and threatened.

References

- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Börzel, T. A., & Risse, T. (2003). *Conceptualizing the domestic impact of Europe*. In K. Featherstone & C. M. Radaelli (Eds.), *The politics of Europeanization* (pp. 57–80). Oxford University Press.
- Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Springer.
- Christou, G. (2024). *Cyber diplomacy: From concept to practice* (Tallinn Paper No. 14). NATO CCDCOE. <https://ccdcoe.org/library/publications/cyber-diplomacy-from-concept-to-practice/>
- CSS (Centre for Security Studies). (2020). *Estonia's national cybersecurity and cyberdefence posture*. ETH Zürich.
- Davis, J. (2007). Hackers take down the most wired country in Europe. *Wired*, 15(9), 2–3. <https://www.wired.com/2007/08/ff-estonia/>
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160.
- Dunne, T., Kurki, M., & Smith, S. (2016). *International Relations Theories: Discipline and Diversity* (4th ed.). Oxford University Press.
- Enescu, S. (2020). A comparative study on European cybersecurity strategies. *Redefining Community in Intercultural Context*, 9(1), 277–282.
- ENISA. (2024). *2024 Report on the State of the Cybersecurity in the Union*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf>
- Estonian Ministry of Defence. (2023). *National Security Concept of Estonia*. Republic of Estonia. <https://vm.ee/en/national-security-concept>
- Estonian Ministry of Economic Affairs and Communications. (2019). *Cybersecurity Strategy 2019–2022*. Republic of Estonia.
- Estonian Ministry of Economic Affairs and Communications. (2024). *Cybersecurity Strategy 2024–2030. 'Cyber-Conscious Estonia'*. Republic of Estonia.

European Commission. (2022). *The NIS2 directive – Summary and objectives*. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

European Commission. (2022). *Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454>

European Commission. (2024). *EU cybersecurity strategy*. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

European Parliament. (2021). *Cybersecurity in the EU: An overview*. <https://www.europarl.europa.eu>

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*, L 333, 80–152. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>

FOI – Swedish Defence Research Agency. (2024). *Cybersecurity work at Swedish administrative authorities: Taking action or waiting for approval?* <https://www.foi.se>

Fujs, D., et al. (2024). Analyzing cybersecurity strategies of the European Union: Challenges and opportunities for public administration. *ELEKTROTEHNIŠKI VESTNIK 91(1-2): 8-20, 2024 OVERVIEW SCIENTIFIC PAPER*

Garhwal, A., & Pareek, S. (2024). Cybersecurity threat framing in national policies: A securitization perspective. *Journal of Cyber Policy Studies*, 12(3), 742–751.

Google Threat Analysis Group. (2023). *Fog of war: How the Ukraine conflict transformed the cyber threat landscape*. <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/>

Greenwood, R., Oliver, C., Lawrence, T. B., & Meyer, R. E. (Eds.). (2017). *The SAGE handbook of organisational institutionalism* (2nd ed.). SAGE Publications.

Högenauer, A.L., & Mišić, M. (2024). Small States in EU Policy-Making. In *Routledge eBooks*. Informa. <https://doi.org/10.4324/9781003380641>

Information System Authority (RIA). (2024). *Cybersecurity in Estonia – Annual Report*. <https://www.ria.ee/en/news/cybersecurity-estonia-2023.html>

Kianpour, M., Øverby, H., Kowalski, S. J., & Frantz, C. (2019). Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. *HCI for Cybersecurity, Privacy and Trust*, 149–163. https://doi.org/10.1007/978-3-030-22351-9_10

Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, 116, 102493.
<https://doi.org/10.1016/j.simpat.2022.102493>

Kianpour, M., & Frantz, C. (2024). Analysis of institutional design of European Union cyber incident and crisis management as a complex public good. *Regulation & Governance*.
<https://doi.org/10.1111/rego.12640>

Kolnberger, T., & Koff, H. (2023). *Agency, Security and Governance of Small States*. Routledge. <https://doi.org/10.4324/9781003356011>

Lex Mundi. (2025a). *Cybersecurity overview – Estonia*.
<https://www.lexmundi.com/guides/status-of-the-nis2-implementation-act-in-the-european-union/jurisdictions/europe/estonia>

Lex Mundi. (2025b). *Cybersecurity overview – Sweden*.
<https://www.lexmundi.com/guides/global-data-privacy-guide/jurisdictions/europe/sweden>

Mccormick, J. (2018). *Introduction to global studies*. Red Globe Press.

Mueller, M. (2017). *Will the internet fragment? Sovereignty, globalisation and cyberspace*. Polity Press.

NATO. (2016). *Cyber defence pledge*.
https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2022). *Strategic concept: Adopted by heads of state and government at the NATO summit in Madrid 29 June 2022*. <https://www.nato.int/strategic-concept/>

Ottis. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Cooperative Cyber Defence Centre of Excellence*.
https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Pamment, J., Sazonov, V., Granelli, F., Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., ... & Terra, J. (2019). *Hybrid threats: 2007 cyber attacks on Estonia*. NATO Strategic Communications Centre of Excellence. <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>

RAND Europe. (2012). *Cyber-security threat characterisation: A rapid comparative analysis*. Swedish Centre for Asymmetric Threat Studies.

Rocket Me Up Cybersecurity. (2024). *Cybersecurity Governance Models — Centralized vs. Decentralized Approaches*. Medium.com
<https://medium.com/@RocketMeUpCybersecurity/cybersecurity-governance-models-centralized-vs-decentralized-approaches-e952ec0c3ea7>

Saunders, N. (2024). *A sustainable future needs cybersecurity: 8 ways they work together*.
Schneider Electric. <https://blog.se.com/digital-transformation/cybersecurity/2024/06/20/a-sustainable-future-needs-cybersecurity-8-ways-they-work-together/>

Swedish Civil Contingencies Agency (MSB). (2024). *Annual Cybersecurity Report (2024)*.
<https://www.msb.se>

Swedish Ministry of Defence. (2024). *SOU 2024:18*. Government of Sweden.
<https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf>

Swedish Ministry for Foreign Affairs. (2024). *Strategy for Foreign & Security Policy on Cyber & Digital Issues*. <https://www.government.se/reports/2024/01/strategy-for-cyber-and-digital-foreign-policy/>

Swedish Ministry of Justice. (2017). *A national Cybersecurity Strategy*. Government of Sweden. <https://www.government.se/information-material/2017/06/national-cybersecurity-strategy/>

Swedish Ministry of Justice. (2025). *National strategy for cyber security 2025-2029 (Nationell strategi för cybersäkerhet 2025–2029)* Government of Sweden.
<https://www.government.se/reports/2025/02/cybersecurity-2025/>

Wong, R., & Hill, C. (Eds.). (2012). *National and European Foreign Policies*.
<https://doi.org/10.4324/9780203816035>

