UNIVERSITY OF TARTU
Johan Skytte Institute of Political Studies
Politics and Governance in the Digital Age

Catalina Mendoza Schmitz

Convergence or adaptation of cybersecurity policies: insights from Chile and Estonia

Master's Thesis (30 ECTs)

Supervisor(s): Dr. Kristina Muhhina and Professor Dr. Vincentius Martinus Franciscus Homburg

Tartu 2024

Authorship Declaration

I have prepared this thesis independently. All the views of other authors, as well as data from literary sources and elsewhere, have been cited.

Word count of the thesis: 22626.

Catalina Judith Mendoza Schmitz, May 20, 2024

Non-exclusive licence to reproduce thesis and make thesis public

I, Catalina Judith Mendoza Schmitz (personal code: 49001210438), herewith grant the University of Tartu a free permit (non-exclusive licence) to the work created by me [Convergence or adaptation of cybersecurity policies: insights from Chile and Estonia], supervisors Kristina Muhhina and Vincentius Martinus Franciscus Homburg,

- reproduce for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright;
- to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until the expiry of the term of copyright;
- I am aware of the fact that the author retains the rights specified in p. 1;
- I certify that granting the non-exclusive licence does not infringe other persons'intellectual property rights or rights arising from the personal data protection legislation.

Abstract [Ülevaade]:

The topic of this thesis is cybersecurity policies, particularly whether, how and why there may be differences and similarities between Estonia and Chile in the parliamentary debate. This study concludes that there are similarities, like the use of the EU directive policy or other cases, and differences, such as how the institutional system worked in each case. An explanation for this is that both respect international organisations and the policy they produce and that similar cases may produce emulation. However, internal elements may still have a significant role to play. This conclusion was formulated using policy convergence theory (PCT) and punctuated equilibrium theory (PET) as a theoretical foundation in a small-n, qualitative country comparison using parliamentary debates, policy documents and additional interview transcripts as data sources. This thesis ends with an overall reflection, lessons learned and recommendations for future research in this area. like the weight of PET in the elements discussed in the parliament, other factors that can contribute to the policy change in the domain of cybersecurity and further questions.

Keywords [Märksõnad]:

Cybersecurity Policy, Policy Convergence Theory, Punctuated Equilibrium Theory, Chile, Estonia

Table of Contents

Acknowledgements

I would like to express my deepest gratitude to my family, especially my mother, my father and Mari, for their unwavering support and for instilling in me a lifelong love of learning. Their encouragement has been instrumental in my academic journey. We know that the path of my formal education has not been easy.

I am also grateful to my siblings and extended family, both those who are with me today and those who have passed away. Their presence in my life has shaped who I am.

To my chosen family and my friends, few in number but irreplaceable, thank you for your constant support and friendship, even across vast distances. Even those friends whom I encountered on this journey in Estonia were there to support me when I was not sure if I would be able to do my thesis or just to have fun. I also want to thank the help to the PhD student Logan Emily Carmichael, who helped me with my first ideas for the thesis and in the research of cybersecurity.

Finally, I extend my sincere appreciation to my supervisors, professor dr. Vincent Homburg and dr. Kristina Muhhina, for their invaluable guidance and patience throughout this thesis process. Their expertise and understanding were especially helpful as I navigated the challenges of writing a theis being a non-native and with a precarious English background. Thank you.

To all of you, thank you very much.

Catalina

List of Abbreviations

CCDCOE: Cyber Defence Centre of Excellence

Cyber security: CS

National Cybersecurity policy/policies = NCsP

NATO: The North Atlantic Treaty Organization

OECD: Organisation for Economic Co-operation and Development

PCT: Policy Convergence Theory

PET: Punctuated Equilibrium Theory

UN: United Nations

List of Tables

Chapter 1: Introduction

1.1 Background of the study

In today's world, known as a digital one, can policy truly keep pace with the ever-evolving threats in cyberspace? Do we need a major incident in cybersecurity to create or change the laws in these areas, or does it come naturally with the progression of society? Does the policy change depend on whether it is a parliamentary regime or one with a National Congress?

When people think about cyberattacks or hear about them in the news, they usually do not think about whether the country was prepared or whether there was an emergency response team that handled the crisis. It is about the cyberattack itself. In practice, cyberattacks may trigger countries to develop or change cybersecurity policies. Below, three international cybersecurity cases are described, and it will be shown what changes in cybersecurity policies were triggered by these events.

Firstly, the Estonian cyberattack of 2007, attributed to Russia (Ottis, 2008), targeted Estonian government websites, banks, and media outlets. It crippled critical infrastructure and caused even economic damage. After that, Estonia had a change in their policies and the government established a national cybersecurity strategy (Pernik, 2021; MKM, 2019). Estonia increased investments in cybersecurity infrastructure, personnel training, and international cooperation. This crisis even helped NATO to recognise cyberattacks as potential threats to collective defence. Paving the way for developing cyber defence capabilities within the alliance, “the first politically motivated cyber-attacks against Estonia in 2007 acted as a wake-up call to other nations and the Alliance, alarming everyone of the growing relevance of potential threats in the cyber domain” (ccdcoe, n.d.). The attacks “triggered the cyber security strategy drafting in Estonia” (Czosseck et al., 2011, p. 61). As a consequence of the attack, “several laws and regulations were introduced, while others were amended, and there were several changes in the organisational landscape” (Günter, 2012, p. 108; Czosseck et al., 2011).

Another example is the “WannaCry Ransomware attack” in 2017. This global ransomware attack exploited a vulnerability in the Microsoft Windows operating system to encrypt files on infected computers. It disrupted healthcare, transportation, and government services in several countries. The policy changes that came from this were in

several countries or institutions representing different countries. The European Parliament mentioned that this ransomware campaign affected users in more than 150 countries and infected over 230'000 systems (European Parliament, 2017). It was a test for the National Cyber Security Centre (NCSC) of the United Kingdom, that had been created less than a year before the attacks. Later, this government agency provided guidance and support to organizations on the best cybersecurity practices (NCA, 2017). Just the Health System of the UK lost "£92m through services lost during the attack and IT costs in the aftermath" (NHE, 2018). It changed the National Cybersecurity Strategy[1]. In the case of the EU, passed [Network and Information System] the NIS Directive mandates that each Member State must incorporate its provisions into national legislation by May 9, 2018. This directive necessitates that Member States guarantee specific operators in critical economic sectors, as well as key digital service providers like cloud computing service providers, implement suitable technical and organizational measures to safeguard the security of their networks and information systems. (European Parliament, 2017).

The last example that will be mention is the "Colonial Pipeline Ransomware attack" (2021). This was a very interesting attack, it targeted just a major US fuel pipeline, leading to temporary fuel shortages and -some- panic buying across the East Coast (cisa, 2023; Falconer, 2021). It was announced even as an "emergency declaration issued in 17 states and D.C. over fuel pipeline cyberattack" (Falconer, 2021). It was one of the 'most significant, successful attack on energy infrastructure we know of in the United States we are lucky if there are no consequences, but it is a definite alarm bell'" (Gonzalez et al., 2021). This attack raised concerns about cyber threats to critical infrastructure and provoked calls for increased cybersecurity measures (Gonzalez et al., 2021). One of the policy changes that came after the attack was done through the 'Executive Order on Improving the Cybersecurity of Critical Infrastructure' (Gonzalez et al., 2021). It was issued by the US President, this order mandated risk assessments, collaboration between government and industry, and incident reporting for critical infrastructure entities (White House, 2021). And one important element was the increased US government funding for

[1] More information about the malware attack in England and their National Security, in: https://committees.parliament.uk/publications/42493/documents/211438/default/

cybersecurity: More resources were allocated to improve defences and resilience of critical infrastructure (cisa, 2023)[2].

These are just a few examples of cybersecurity breaches or cyberattacks, of thousands that have appeared in the last years, with significant impacts. The specific policy changes and their international coverage can depend on the individual attack, the specific circumstances, and the affected countries. This study focuses on the policy responses to the abovementioned incidents and, more particularly, whether these responses (security policies and changes in those policies as a response to incidents) are the same worldwide or reflect national idiosyncratic interests, peculiarities or other issues.

This triggers the question what policy change is. Pearson (2000) mention that is known that "public policies and formal institutions are usually design to [be] difficult to change (…)" (Dogaru, 2018, p. 171). So, what is it? Vries (2010) mention that what defines policy change is "the change of ideas, assumptions, priorities and goals, together with the shift in the dominant use of policy instruments and the changing roles of societal actors and policy-makers in the policy process" (Dogaru, 2018, p. 170). Normally this changes or policy process, do occur withing the 'institutional systems of a country', and it can be said that that "the institutional context can be an important barrier to the transformation of policy learning into concrete policy changes" (Moyson et al., 2017, p. 24).

1.2 Focus and scope of the study

The focus and scope of this study is whether there is policy change happening because of cybersecurity incidents, and if so, what the mechanisms of change or lack thereof, are. Following existing bodies of literature, the study focuses on possible instances of policy learning and transfer of knowledge between countries (suggesting convergence of policies) and policy learning that emerges within and is possibly unique to specific national contexts. To do so, this study uses a comparative design and compares policy making (and policy change) in two specific countries: Estonia and Chile. The choice for the countries will be explained in chapter four.

The digital age has transformed our world, looking up interconnectedness while simultaneously exposing us to a growing spectrum of cybersecurity threats. Governments

[2] More information can be found online in the America's Cyber Defense Agency (USA). In: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

entrusted with safeguarding their citizens and critical infrastructure, formulate cybersecurity policies to navigate this complex terrain. However, crafting these policies presents a fundamental challenge: reconciling inherent value conflicts, inside the country and outside of it.

On one side, prioritizing security often necessitates measures restricting individual freedoms in areas like privacy and free expression. On the other side, upholding these freedoms forms are the base of democratic societies. This inherent tension creates a delicate balancing act, played out through the choice of policy instruments, measurement approaches, and specific behaviours targeted. Determining the degree of restriction imposed on these behaviours and the conscious decision-making behind national approaches are crucial aspects of understanding this (new) dynamic.

While existing research highlights the presence of value conflicts in cybersecurity policies (Kaska et al., 2010; Ottis, 2008), it remains inconclusive on whether and how national contexts influence this balancing act. Some scholars postulate divergent approaches based on cultural and political differences, while others advocate for a universalized set of principles. This gap in knowledge motivates this study, which aims to delve deeper into the intricate relationship between cybersecurity policies and their national settings.

Some countries might prioritize technological solutions, relying on surveillance tools and data encryption to enhance security. Others, concerned about privacy, might favour regulatory frameworks that impose restrictions on specific online activities (Lewis et al., 2011). Yet another approach could focus on behavioural interventions, promoting digital literacy and responsible online conduct (GCSG, 2019). The measurement of these policies' effectiveness also varies. Similarly, data encryption mandates might vary in their scope and stringency (J. A. Lewis et al., 2017).

Howlett & Ramesh (2003) wrote about the concept of public policy that “at its most simple choice made by government to undertake some choices of action” (Dogaru, 2018; p.169). However, it must be acknowledged that the *intent of a policy* “is implemented via policy instruments such as regulatory, economic, expenditure and institutional instruments” (Tyler et al., n.d., p. 1). Therefore, for this thesis, cyber-policy is going to be defined as “a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and

user's assets (Yusif & Hafeez-Baig, 2021, p. 1). In other words, "is the measures taken to protect network systems and their data against [cyber] attacks or intrusions" (ibid.).

The strategic goals of the 2020 EU-US Cybersecurity Policy will be observed to illustrate the typical policy instruments used in cybersecurity cooperation. The EU conducts cybersecurity key policies in four areas: security of the digital single market, cybercrime, common foreign and security policy and common security and defence policy" (Schuetze, 2020; p. 20). In the USA, the "key policy area [are] national security, defence policy, cybercrime, foreign policy and economy policy" (ibid., p.30). On one hand, the instruments used the EU are: Directing: IT security and internal capacity building; Framing and imposing costs: Harmonising principles and long-term goals in foreign, security and defence policy; Gathering and sharing: Common situational picture about threats and vulnerabilities; Providing and innovating: Coordination and cooperation to get better at resilience and IT security; Funding: Research, vulnerability research, innovation and capacity. In the other hand, US used: Directing: Regulation of its federal agencies; Framing: Standards, taxonomy and best practices; Funding: Research and innovation; Gathering and sharing: Common situational picture of threats and vulnerabilities; Imposing costs: Public attribution, indictments, extradition, sanctions, ban of products, and other instruments of national power; Providing: Coordination, cooperation and services to get better at resilience and cybersecurity; Shaping and promoting: International norms for responsible behaviour, application of international law (Schuetze, 2020, p. 30).

By comparing and contrasting national approaches to policy changes; that can be seen through policy instruments, measurement methods, and targeted behaviours, this research seeks to identify similarities and differentiations in and between Chile and Estonia. Analyzing the conscious justifications behind these choices within individual countries will provide a more *nuanced understanding of the influence of national context*. Ultimately, this research seeks to contribute to the development of next policies more context-sensitive, especially in those cybersecurity policies, ensuring a safer and more just digital space for all.

In other words, beyond the inherent value conflicts in cybersecurity policies, another layer of complexity arises in the choice of policy instruments[3] and their implementation. How these instruments are designed, measured, and applied to specific behaviours significantly impacts the degree to which they restrict individual liberties. Understanding these shades across different national contexts is crucial. This variation, if their exists, raise crucial question that we need to think: Are these differences in policy choices and implementation conscious approaches driven by specific national contexts? Do cultural norms, political systems, or technological infrastructure play a role in shaping these decisions? How do these diverse approaches impact the delicate balance between security and liberties in each country?

By examining these questions in detail, this research aims to uncover the similarities and distinctions in how different nations navigate the cybersecurity policy landscape. This comparative analysis can provide valuable insights for policymakers, fostering a deeper understanding of how national contexts shape the complex dance between security and individual freedoms. Ultimately, this knowledge can guide the development of more effective and context-sensitive cybersecurity policies that ensure both a secure and a free digital space or not.

National cybersecurity policies are aimed at safeguarding critical infrastructure, protecting sensitive data, ensuring the integrity of online systems and societal well-being, and others. It has become increasingly crucial in an interconnected and digitally driven world, what has Estonia created in this matter and what has Chile created? Balancing national security and human rights and freedoms in the digital area within these policies poses a significant challenge for both countries.

1.3 Research question and research objectives

These two countries, Chile and Estonia, present intriguing case studies to examine their respective approaches to cybersecurity policy. The overarching research question is: What are the similarities and differences in cybersecurity policies in Chile and Estonia? How can these similarities and differences be explained?

[3] We can define, in a very general form, policy instruments as "tools used by governments to pursue a desired outcome" (Cairney, 2012, p. 1; Schuetze, 2020, p. 8).

This research question aims to explore and understand the factors influencing the development and implementation of cybersecurity policies through a comparative analysis of Estonia and Chile. This study seeks to achieve two key objectives:

1. Contribution to Academic literature. This research seeks to advance the ongoing academic discourse on policy learning and diffusion mechanisms by examining the contrasting cases of Estonia and Chile in the context of cybersecurity policy. By analyzing these divergent approaches, the study aims to contribute new insights and perspectives to the existing literature on policy transfer and adaptation.
2. Practical Implications. Beyond theoretical contributions, this research aims to provide pragmatic insights into the factors shaping cybersecurity policy development. By identifying the key drivers of similarities and differences between the Estonian and Chilean cases, the study hopes to generate valuable recommendations for other countries seeking to build and strengthen their own cybersecurity frameworks.

This paper aims to contribute to the existing literature by examining the interplay between cybersecurity and everything that entails, from two countries – Chile and Estonia – than beside democracy aren't equal in many elements. Even with different temporalities in constructing legal cybersecurity, can we create a better understanding of their policy change through a created framework from an overlap of Policy Convergence Theory and Punctuated Equilibrium theory?

1.4 Academic and Societal Relevance

These are two well-known theories that offer a valuable framework to understand, and potentially, close a little the gap between cybersecurity and policy change; to attract the attention to cybersecurity policies in the discipline of policy studies. Looking for material, a brief search was conducted in Scopus about "policy change" and "cybersecurity", finding 246 documents. Then, the finding was limited to "policy changes", founding just 12 documents. Upon reviewing the abstracts, only one document was identified that met the established criteria. Were one to examine the situation a little further back and expand the limit to "policy changes", "regulatory model", "public works" and "policy", it was found 19 documents in total. From those, reading just the abstracts, there are just three documents that could be interesting in this search.

However, there are some authors who have tried to close the gap between policy changes and cybersecurity. Myriam-Dunn-Cavelty (2009; 2019) writes about governance, policy in cybersecurity, cybersecurity policies, political fragmentation. Another author is Jason Healey, he has been helping in the last 25 years working at the White House about Cyber Policies and other places. He wrote that "meeting the needs of policymakers must be the end goal of attribution, not a by-product" (Atlantic council., 2012; p.1), understanding that the creation of law in cybersecurity aspects can have the same problem that other policymaking. About cybersecurity, law and policies, we can find Catherine Lotrionte, with the perspective of (cyber) security studies and policy analysis, especially in cyberthreats and cybersecurity in today's world (2011). Herbert S. Lin has written about public policy and governance and cybersecurity policy. Lastly, he wrote about challenges in effective cybersecurity, international relation and security studies. Being one of the editors of the book: "At the nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues" (2014), where they mention the importance of Cybersecurity, and that represents a continuous effort that must adapt to emerging threats. The intersection of Cybersecurity and Public Policy emphasizes the imperative of prioritizing cybersecurity as a matter of public safety, urging proactive measures to address this critical issue. These authors have contributed in trying to close the gap between cybersecurity policies. However, most of them have been written from the USA perspective, the western, a 'north' perspective. It is time to address this gap through interdisciplinary approach or, more than that, begin with a 'north-south' approach.

Coming back to the theories that were discussed before, it can be said that the theory of Policy Convergence Theory (PCT) suggests that similar policies lean towards convergence policies across different jurisdiction or organizations. It can be from different reasons; best practices, imitation and pressure from international norms. In the sphere of cybersecurity, can be applied to different countries, adopting similar cybersecurity policies responses. It can be that they are facing similar challenges and threats.

On the other hand, there is the Punctuated Equilibrium Theory. This theory is part of the field of public policy. Baumgartner and Jones (Baumgartner et al., 2011) mention that policy change often occurs through - the so called - periods of stability. They are punctuated (disrupted) by a sudden 'burst' of significant change. If this is used in the

context of cybersecurity, this theory could be useful to understand how certain events or crisis can bring rapid shifts in the (cyber) policy. Analyzing those moments can help to identify where the intervention is most wanted.

Therefore, both theories offer valuable lenses through which to analyze and address the gap between cybersecurity and policy change with policy convergence emphasizing similarities and with punctuated equilibrium theory explaining differences. It can help to have a better understanding in the dynamics of each of the elements.

1.5 Research design, data, and methods

This document will use as a methodological approach through qualitative analysis. As a data collection method, the parliament debate will be used as a primary source, and as a second source, there will be interviews with different experts in Chile and Estonia. This last source will facilitate answers that it may not be in the parliament debate. As a method of analysis, we will use qualitative coding as a technique.

It is important to mention that because there are not many theories available on policy change, specifically on policy development, in relation to cybersecurity policies, it is necessary a more inductive approach. I will use my empirical data to shape policy science propositions that fit specific contexts and challenges of information security policy. However, since there are some concepts that overlap with the theories, there is a theoretical foundation that will be used in the empirical analysis, making use of deductive analysis, too. Finally, because there are just two cases, a small-n is better suitable for this thesis.

About the case selection, there are several reasons why Chile and Estonia are good as country selection. Chile and Estonia offer contrasting starting points for the analysis; both cases are in the top 5 in each continent in different cybersecurity indexes, making them relevant case studies. Another point is there are some advantages as data availability. There are some elements in the connection to the theoretical framework that its being use in this document that are interesting to study. Each of these elements will be discussed in chapter 4.

To comprehensively analyze and understand the dynamics of national cybersecurity policies, it is essential to employ theoretical frameworks that can capture the complexities, distinctions, and gradations of policymaking processes. Two plausible

theoretical orientations that offer valuable perspectives in this context, as stated before, are Policy Convergence Theory (PCT) and Punctuated Equilibrium Theory (PET). They offer promising perspectives for examining the evolution and divergence of cybersecurity approaches across different countries and provide valuable insights into the factors that can influence policy development, the processes of policy change, and the dynamics of international cooperation in cybersecurity.

The analysis will be done through qualitative coding as a technique. To conduct one, "we identify a body of material to analyze [parliament debate] and then create a system for recording specific aspects of its content" (Lawrence, 2014; 49). The operationalization of it is through "constructs with a coding system" (ibid., 378). A coding system is "a set of instructions or rules used in content analysis to explain how a researcher systematically converted the symbolic content from text into quantitative data." (ibid., p. 379)

About the collection of the data, in a social phenomenon, Bukve (2019) mention that it "is essential to collect data that are relevant to the phenomenon we are focusing on". (Bukve, 2019; 208). Because is qualitative research "we are not able to secure that the cases are statically representative of the population (…) [therefore] we must base our collection on strategic selections of cases" (ibid., 209). However, in the making of this document aims to achieve "credibility and confidence analyzing the data and presenting the findings" (Saldaña, 2014; 42).

1.5 Theoretical orientation

As a conceptual basis for accomplishing the purpose of this document, it will be draw upon Policy Convergence Theory (PCT) and Punctuated Equilibrium Theory (PET). It will explain briefly the two theories that will being used. These theories are going to help as theoretical lenses, that will allow to have a better understating the possible mechanism behind the similarities and differences that can be encounter. In chapter two and three it's going to be explained in more details on patterns leading more in the context of cybersecurity policy specifically; using these 'lenses' to analyse the issue of policy change and policy learning.

1.6 Outline of the thesis: The organization from here until the conclusion

This document it is organize, making each chapter dedicated to a specific aspect of the research. Chapter Two presents a review of the relevant literature, providing a foundation for the analysis. Chapter Three outlines the conceptual framework that will guide the

research. In Chapter Four, the methodology and research design are described, detailing how the data will be collected and analyzed. Chapter Five delves into the analysis of the empirical findings, presenting the results of the research. Next, Chapter Six provides a comparison and discussion of these findings, highlighting any significant patterns or relationships. Finally, the conclusion summarizes the key takeaways and overall significance of the research.

Chapter 2: Public Policy Theories

2.1 Introduction to this chapter

This chapter outlines the theoretical framework, or "lenses," utilized as the conceptual foundation for the comparative analysis of Chilean and Estonian cybersecurity policies that follow later in chapter 4. It explores the significance of this theoretical foundation for the study of cybersecurity policies in general. The chapter is structured as follows: Section 2.2 provides a conceptualization of cybersecurity and cybersecurity policies. Section 2.3 then delves into the first theoretical lens, "convergence theory", then it will elaborate on "punctuated equilibrium theory" as the second theoretical lens employed in this study. Lastly, in Section 2.4 the chapter concludes with a reflection on both lenses, including a discussion of any gaps identified within the existing literature.

2.2 Conceptualization of Cybersecurity in General.

Since the 1990's there has been a change in the way in which cyberspace is present in the everyday life of the people. There is an expansion of the function through Communication technology (ICT), Internet of things (IoT) solutions, Artificial Intelligence (AI). The cybersecurity aspect is equally important to a nation, to the private sector, or the citizens. In other words, the prevalence of cyberattacks poses a substantial threat to businesses, national economies, and individual internet users. These attacks can have devastating consequences; including service disruptions, diminished productivity, reputational damage, intellectual property theft, and operational dysfunction within critical infrastructure (Flowers et al., 2013).

There are different notions of the definition of Cybersecurity, generally, mention that Cybersecurity goes beyond the digital realm, encompassing a comprehensive set of practices and methods that protect data, information, and the integrity of all cyberspace components, including the underlying physical infrastructure. Adding, the International Telecommunication Union (ITU) "describes cybersecurity as set of tools, guidelines, and other approaches made to protect integrity and confidential nature of cyberspace for private organisations, government, and civil society" (GCSG, 2019, p. 32). Another conception about cybersecurity is "the collection of tools, policies security concepts, security safeguards. Guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment

and organization and user's assets" (Yusif & Hafeez-Baig, 2021, p. 1). Each of them gives us an overview of the different elements of cybersecurity and the aspects to take care of.

Another notion of cyber security is "a complex and multi-disciplinary challenge, combining the need to draw from information technology, strategic management and cyber conflict research" (Günter, 2012, p. 143). Ellis & Mohan (2019) mention that "security is (…) a key axis upon which decisions about communications technologies and network sit. Looking closely at these efforts as forms of governance" (Ellis & Mohan, 2019; xix). In other words, cybersecurity is part of the risk derived from using cyberspace; therefore, is there a is a way to have less risk? Probably not, but the creation of (cyber) policies is one of the first steps that are necessary to engage in the cyberspace – cybersecurity problems. However, there is an existing gap in the literature about this.

Protecting information assets requires robust cybersecurity policies. Developing security policies and procedures is equally crucial as implementing technical cybersecurity solutions. In this context, "security policies encompass a range of tools, regulations, rules, procedures, best practices, and management techniques. Additionally, technical solutions like encryption, error-checking, preventive systems, and detection tools can address various security threats" (Mishra et al., 2022, p. 2). It means that for this study "cybersecurity is the protection of cyberspace, electronic information, information and computer technologies that support cyberspace, as well as a person as a user of cyberspace" (Vakulyk et al., 2020, p. 776).

2.3 Public Policies

The creation of a public policy contains different parts as it is constructed (agenda setting, policy formulation, decision-making, policy implementation and policy evaluation) (Howlett & Cashore, 2014). Therefore, it is important to mention that cybersecurity policies interact with the decisions from different stakeholders at different times: government, public opinion, private business, and other actors that can be important. Cyber threats evolve, national cybersecurity policy/policies (NCSP) must continually adapt to safeguard digital environments effectively. This requires ongoing collaboration among governments, businesses, and citizens. NCSPs play a crucial role in proactively preparing and preventing cyberattacks, minimizing damage and facilitating quick recovery. They promote collaboration and public-private partnerships to share

information and resources, fostering public trust and demonstrating commitment to protecting citizens and businesses in the digital age. This document defines national cybersecurity policy as a strategic framework that outlines a country's approach to safeguarding its digital infrastructure, data, and systems from cyber threats. "A cybersecurity policy defines and documents an organization's intent, principles, and approaches to manage cybersecurity risks effectively in pursuit of its strategic objectives" (gartner, n.d) (see: meity, 2013). In this research the policy that will be studied is the legislative debate of the law of cybersecurity in two countries.

This document will focus on the "public" policies that are made by governments or national legislature that every member of a state or nation must follow (Howlett & Cashore, 2014). In specific, the cybersecurity law of each country.
There are different elements that go into making a public policy, Peter Halls (1989, 1993) identified three fundamental elements or components of public policies: overarching policy goals, the specific policy instruments utilized for their implementation, and the detailed operational settings or adjustments employed when applying these instruments. While Hall initially proposed only these three components mentioned before, his differentiation within the varying levels of goal specificity and means - ranging from 'abstract' to 'concrete' and 'specific' - implies the potential identification of up to six elements contributing to the formulation of public policy (Howlett & Cashore, 2014, pp. 21). This study will utilize the definition of policy focus from the modified taxonomy of policy components developed by Howlett & Cashmore (2014). The definition draws upon "policy ends or aims" and policy content at the "higher level of abstraction" which is "Goals: What general types of ideas govern policy development" (ibid., p.22). It is about seeing the differences and the similarities of the cybersecurity policies in two countries, the converging or diverging elements will be clear after the analysis of the parliamentary debate.

The National Cybersecurity policies are typically enforced through a combination of instruments that address different aspects of cybersecurity, such as laws and regulations, which are legally binding rules that mandate specific cybersecurity behaviours. A National Cybersecurity Policy/policies is a comprehensive strategy that serves as a roadmap for various stakeholders, including government agencies, businesses, and citizens, to enhance the nation's cybersecurity posture. Key aspects of NCSP include

protecting critical infrastructure and information systems from cyber threats, securing government systems, promoting economic growth, and safeguarding citizens' privacy (Whitehouse, 2023). Protecting critical infrastructure involves safeguarding essential services, such as power grids and financial systems, from disruptions caused by cyberattacks (RIA, n.d.). Securing government systems ensures the confidentiality, integrity, and availability of government data and operations in cyberspace. Promoting economic growth entails creating a secure digital environment that fosters innovation and economic development. Lastly, protecting citizens' privacy (private sector network) involves safeguarding personal information from unauthorized access or misuse.

There are other instruments that are used as standards and guidelines; these best practices provide a technical roadmap for robust cybersecurity measures. It should also take into consideration international cooperation, there are different types of reasons to do that, such as sharing threat Intelligence, coordinating cyber defence efforts to collaborate on responses to large-scale cyberattacks (NATO, 2023), or the one generated by the UN "Develop International Norms for Cyberspace: establishing international rules and expectations for responsible behaviours in cyberspace" (White House, 2011). The EU has similar documents.

In conclusion, relevant issues in cybersecurity policies are about critical infrastructure protection ensuring the resilience of essential services (water, energy, etc.), data privacy (safeguarding personal and sensitive information., cybercrime (addressing hacking, fraud, and other illicit activities), emerging technologies (managing risks associated with AI, IoT, quantum computing, etc.), digital economy (balancing security with economic growth), overall National security and international cooperation. A robust national cybersecurity policy combines legal, technical, and collaborative measures to create a secure digital environment for citizens, businesses, and government entities (Whitehouse, 2023).

2.4 Theoretical Lenses: Policy Convergence Theory and Punctuated Equilibrium Theory

In this section it will be discussed two framework theories that will guide the objective that this thesis has, and helping to explain similarities or not in cybersecurity policies. They already have been mentioned, but it will be explained more in detail.

2.4.1 Policy Convergence Theory

A focus is placed on the Policy Convergence Theory (PCT) within this analysis, it suggests that nations may be driven to adopt similar policies due to three key factors, which will be discussed in detail later. However, part of the explanation of why to use PCT is because this document compares national cybersecurity policies, it could help to explain the similarities in Chilean and Estonian policies and if they adopted or not similar approaches for the factors that it will be written in some paragraph a head. The changes that push a political system, towards a similar social structure or a new government (cyber) policy could be explain through this theory

The concept of policy convergence, particularly among developed nations, has been explored by various scholars: J.C. Thomas (1980) developed a theory of policy convergence, which was later expanded by Bennett (1991) to include processes such as emulation, elite networking, harmonization through international regimes, and penetration by external actors (the core instruments). Holzinger (2008) further integrated this type of study to policy convergence. In the theory of DiMaggio and Powell's (1991) they talked about the concept of institutional isomorphism, that can be result "from coercion, mimetic processes, and normative pressures" (Holzinger & Knill, 2005, p. 779). By other authors, policy convergence is described as "the approximation of policies" (Popp, 2021, p. 2). Decades later, Santos (2003) contributed to the discussion by analyzing the convergence properties of policy iteration in decision problems. These studies are just some examples that collectively highlight the complex and multifaceted nature of policy convergence and the various factors that contribute to it.

Policy Convergence Theory was introduced more deeply than before by Colin Bennett in 1991 when he was studying public policies to have a more nuanced understanding of why the convergence of national policies might occur, especially in the context of the emerging European Union at the time of the development of theory. He wrote "What Is Policy Convergence and What Causes It?" (1991) in the British Journal of Political Science: "convergence can be defined as 'the tendency of societies to grow more alike, to develop similarities in structures, processes and performances'" (Bennett, 1991, p. 215). He mentions that a general convergence argument would suggest that as societies become more industrialized, the argument goes, certain predictable changes start happening. Over time, these changes push societies towards similar social structures,

political systems, and government policies and can become more alike through various types of pressures that are not always shown as violent (for example, if the OECD mention some policies as the correct one for evaluating policies, the countries are going to go in that direction or when a country asked for "help" to the World Bank, they will impose their view to that country). However, policy convergence shouldn't denote the absence of state autonomy; it is just that through time, in industrial societies, government policies can become similar for various reasons.

Following Bennett's idea of Convergence Theory (2001), other authors *mention four mechanisms* by means of which national policies could converge: emulation, elite networking and party communities, harmonization and penetration (Holzinger & Knill, 2005, p. 779; Bennet 1991). The first instrument is "Emulation", which is very similar to the third one but copies directly successful policies from other countries. They have to adhere to shared rules and principles set by international organizations. Convergence is not just a "copy-paste", Bennett mentions that to conclude that "convergence is attributable to emulation often requires some leaps in judgement (…) confirmation of the emulation hypothesis requires the satisfaction of a number of conditions" (Bennett, 1991, p. 223). The author mentions that the challenge lies in assessing the relative importance of emulation compared to other influences (both domestic and transnational) that can impact the assumptions and perceptions of the numerous actors involved in shaping public policy.

The second instrument is "elite-expert networking" (sharing knowledge and the best practices of organizations or countries across borders). In today's society an epistemic community refers to a network of policy experts who share fundamental beliefs regarding goals, causal beliefs about methods, and shared standards for acquiring and evaluating new knowledge. These individuals play a significant role in domains where state leaders face uncertainty regarding the outcomes of various policy choices and where interconnectedness necessitates coordination. In such scenarios, those transnational epistemic communities can shape state preferences regarding regulatory options, facilitating smoother negotiations and increasing the likelihood of policy management (Drezner, 2001; p. 62). Following that, it is important to what the model of elite consensus emphasizes with the "role of international institutions in forging and promulgating an epistemic community" (ibid., 63) that are then used as a stakeholder in the agenda-setting and discussion of a policy.

Peter Haas argues that "the expansion and professionalization of bureaucracies and the growing technical nature of problems have fostered an increase in the deference paid to technical expertise and, in particular, to that of scientists" (Drezner, 2001, p. 63). In this sense, convergence is understood as “not the result of constraints imposed by the problem, or of collective insecurity, but of an identifiable elite bound by knowledge and expertise of a common policy problem and a shared concern for its resolution” (Bennett, 1991, p. 224). Another author mention that those actors play a role in those areas “where state leaders are uncertain about the consequences of different policy options and where interdependence demands coordination” (Drezner, 2001, p. 63). It’s about an interaction and a consensus on how to engage with a problem. Then, participants go to their respective society and tried to influence their national government agenda; “When attention focuses less on national governments and more on international organizations, the third and related convergence process of' harmonization' is evident” (Bennett, 1991, p. 225).

As is stated in the last paragraph, the third one, is harmonization. The principal author mentions that “they also require authoritative action by a responsible intergovernmental organization (…) under this process, convergence is driven by recognition of interdependence” (Bennett, 1991, p. 235). An abstract concept indicating a dependence on others to carry out particular tasks effectively and ensure seamless implementation or prevent troublesome discrepancies (ibid., 225). Holzinger & Knill (2005) mention that this mechanism involves international cooperation among participating countries, necessitating their compliance with legal obligations outlined in international or supranational law. Harmonization emerges as a specific outcome of this collaboration, requiring national governments to enact comparable policies and programs as part of their duties as members of international institutions. This approach entails governments addressing certain issues through cooperation within international institutions, in doing so they concede some autonomy for “the good of the community” (p. 782). To mitigate the unintended external consequences of domestic policies, the solution is provided through cross-national institutes or organizations, facilitating the development of a unified response to shared challenges (Holzinger & Knill, 2005). At the end, it can be said that “Where harmonization has occurred, it has been a conscious choice of states made under the aegis of an international organization” (Drezner, 2001, p. 75). In that sense, Bennett wrote that the efforts that are part of harmonization “may be more the

result of other processes that operate below the formal, and sometimes symbolic, level of the intergovernmental organization than primary causes of policy convergence" (Bennett, 1991, p. 227). However, some attempts at harmonization may exert a coercive influence on states that have been hesitant in their response to a particular issue (ibid.).

Lastly, "Penetration/ Diffusion by external actors", is the influence that can come from global companies, NGOs, powerful states, etc. (Bennett, 1991; Plümper & Schneider, 2009). This process stands in contrast to the apparent cooperative dynamics of harmonization, which involves states being obliged to conform to actions taken elsewhere by external actors (Bennett, 1991, p. 227). In this context, penetration or diffusion by external actors, refers to the impact of outsider actors and interests on the formulation of a nation's domestic policies. Bennett (1991) suggests that this influence can originate from various external sources, including international organizations (such as the United Nations, European Union, OECD, etc.), foreign governments, multinational corporations, and non-governmental organizations (NGOs). These actors typically pursue specific objectives through policy convergence, such as promoting trade agreements, enhancing international cooperation on issues like cybersecurity, or aligning regulatory frameworks across borders (Bennett, 1991, p. 228; Drezner, 2001, p. 75).

There are different mechanisms through which penetration occurs. These include conditional aid, where foreign assistance is contingent upon the adoption of certain policies; the dissemination of 'best practices' from other countries; international agreements that outline policy obligations; and normative pressure exerted by international organizations or advocacy groups, among others.

This process typically results in two types of impact: policy homogenization, where external pressures lead to a degree of uniformity in policies across countries, particularly in areas with strong international influence or economic interdependence, and, less commonly, resistance and adaptation, where countries may not simply adopt external policies but instead modify them to suit their national contexts and priorities.

While penetration and other elements of this theory emphasize external influences, it's crucial to recognize the role of domestic factors. A country's political system, economic structure, and societal values all influence its response to external pressures and its ability to adapt international models to its own circumstances. In this case, the creation of a cybersecurity law.

Considering that Chile's political system (presidentialism) differs from Estonia's (parliamentarism), could this divergence impact the perception and acceptance of a particular decision regarding cybersecurity policy within a state? In table 1 is a summary of each element of this theory.

Nevertheless, it is important to mention that there are limitations to this model; for example, they might not fully explain differences arising from unique national contexts. This theory does not go deeper in that sense.

Despite recognising the concept of convergence and its supporting mechanisms, they have faced scrutiny within academic discourse. Critics like Pollitt (2002; 2007) argue that the process of policy adaptation from one context to another can lead to divergence, not convergence. Additionally, he mentioned that even when convergence occurs, it may manifest differently across various levels, ranging from mere discourse to actual decisions and implemented actions (see Pollitt, "Convergence: A Useful Myth" Public Administration).

Table 1: Summary of the four mechanisms of Policy Convergence Theory (based on Bennett, 1991).

Emulation	It is when there is a direct copy of a successful policy from another country.
Elite-expert networking	It is important to the epistemic community because it refers to connections, to a network of experts. It is about sharing new knowledge, too.
Harmonization	This concept is related to the dependence on others to carry something specific in an effective way, ensuring an implementation or preventing some discrepancies.
Penetration/ Diffusion by external actors	In this context, as it was already written, penetration or diffusion by external actors, refers to the impact of outsider actors and interests on formulating a nation's domestic policies. It is about power too.

2.4.2 Punctuated Equilibrium Theory

On the other hand, the Punctuated Equilibrium Theory (PET) originated in the field of evolutionary biology, and it was proposed by palaeontologists Niles Eldredge and Stephen Jay Gould in the decades of the ‘70s and had a connection with the so-called “gradualism”. Other authors mentioned it as an incrementalism model (Jolicoeur, 2018, p. 1). It can be said that the theory uses the analogy of a punctuated line to represent the fossil record, with long, stable periods punctuated by short bursts of change. Moreover, PET in policy change maintains the prevailing view of the first PET, stating that species changed slowly and continuously over time. There are some elements in this theory of policy change sustain, like: “stasis”, where the population maintain little change and adapts to their environment and “punctuations”, there are brief periods of rapid change (Monroe & Bokma 2010; Jolicoeur, 2018).

The almost “new” PET was developed by Frank Baumgartner and Bryan Jones in 1991; they maintain that it was inspired by the observation that policymaking often displays periods of stability punctuated by rapid change. Those observations, as the PET in the fossils, suggested a pattern of long periods of "policy equilibrium" punctuated by bursts of significant policy change. “The model implies that punctuations ought to occur at all levels of policymaking and at all levels of the budget, not to be driven simply by external (exogenous) factors in a top-down manner” (Baumgartner et al., 2006a, p. 19).
Paul Cairney (2012) mentioned that in the early studies, the researchers initially studied US policy changes over decades. They focused on the rise, duration, and collapse of "policy monopolies" - groups with solid control over policy issues. This approach explained why policy could be stable for long periods but also experience sudden shifts. Today, the modern PET focuses on how institutions handle information differently. They may focus more on smaller issues, leading to minor policy changes.
Conversely, they may overlook bigger issues, resulting in fewer but more significant policy shifts. Today’s version had a global application initially developed for US policy; it expanded the meaning of this theory through the "Comparative Policy Agendas". This project found similar patterns of frequent small and infrequent significant policymaking changes across various political systems (Baumgartner et al., 2006b, p. 30; Cairney, 2012, p. 175).

It is known that decision-makers can't consider all problems at all times; they ignore most issues and promote few decisions, usually those that climb to the top of their agenda. The limited attention and power dynamics on policy change explain two points: policy stability and policy punctuations. The first is that most policies remain unchanged due to the lack of attention from decision-makers; the latter explains intense periods of focus on specific issues can lead to new ways of framing and tackling old policy problems. Additionally, the power dynamic between participants plays a role in maintaining the status quo, which means that influential players may try to minimize attention to specific issues and preserve the existing approach (frame of reference). The other role is driving change: other actors might attempt to expand attention beyond the usual circle, engaging new audiences to generate conflict and debate, ultimately aiming for significant policy changes (Baumgartner et al., 2006b; Cairney, 2012; Capano & Howlett, 2009).

Policy diffusion occurs when policy makers who aim to be perceived as 'responsible' problem solvers search for proper solutions and import policies, which have been evaluated by experts and identified as 'best practices' (Blatter et al., 2022, p. 216). When this idea is examined through the framework of Punctuated Equilibrium Theory in policy change, there are different elements to consider. The first one is about the definition of "Frame" or the framing of a public policy; since public policies address complex issues, they are usually compatible with several images (Cairney, 2012, p. 185) or it can be understood as when discussing public issues, it can be approached from various perspectives. The "frame" can be understood as how it "defines a policy's image (how an issue is portrayed and categorized)" (Cairney, 2012, p. 175). Policymakers, who aim to be perceived as 'responsive' to the people's will, try to find 'quick fixes' and are open to importing promising solutions from other policies or policy fields (Blatter et al., 2022, p. 815). However, when the discussion is constrained, there is often a tendency to oversimplify matters, resulting in adopting a singular viewpoint. This singular perspective subsequently influences policy decisions (Jolicoeur, 2018, p. 3). It exists in a place where there are 'policy communities' -another element defined as "close relationships between interest groups and public officials, based on the exchange of information for influence (…) The links endure if participants establish a policy monopoly or a dominant image of the policy problem" (Cairney, 2012, p. 176). Policy images play a critical role in expanding issues beyond the control of the specialists and special interests that occupy what they termed "policy monopolies" (Baumgartner et al., 2006a, p. 2).

In that sense, we can add the element of "agenda setting", which is about the "public, media and government attention to policy issues" (ibid.). The focus of this is on the high level of attraction of some issues; it can be through a "triggering event", "rise in attention following a crisis", or "it can be caused by interest groups trying to draw attention to 'their' issues (…) connects shift to attention to venue shift"(Cairney, 2012, p. 176).

The concept of venue shift is where the 'authoritative decisions are made'; it can be through departments of the government, people of the congress/ parliament, courts, and others. It can have multiple jurisdictions (Baumgartner and Jones, 2006). Usually, groups excluded from "policy monopolies" might use various tactics to gain influence (one way or another). Cairney (2012) mentioned that they could shift the debate from within by, for example, appealing to public officials and questioning the existing approach (called venues). If unsuccessful, they have an incentive to venue shop or seek influential audiences elsewhere. It may involve an appeal to a different level or governing institution (such as a legislative committee or court) capable of deciding on the same policy issue (over internal efforts or shifting strategies). That is called venue shopping, where they "seek favourable audiences in other venues" (Cairney, 2012, p. 176). They could 'broaden the audience' where groups may seek to expand the size of the interested audience by making direct appeals to the public.

In other words, the punctuated equilibrium theory in policy change mentions the policy equilibrium; usually, the policy remains relatively stable due to factors like institutional inertia, vested interests, and lack of pressure for change. However, there can be "Punctuations" these are periods of rapid and significant policy change often triggered by the mobilisation of new/different actors and their leadership, new ideas or events (crises, scandals, type of window of opportunity to change the equilibrium that existed). Lastly, it is important to acknowledge the so-called "policy feedback" mentioned in Chapter 6 of Sabatier (2007). After an outburst or punctuation, the existing policies could create new conditions that "either reinforce the change – positive feedback loop – or generate pressure for further change – negative feedback – (True et al., 2007, p. 160). *This theory emphasises the importance of punctuation in understanding how significant policy shifts happen*.

Therefore, the Punctuated Equilibrium Theory (PET) can explain differences in the cybersecurity policies if Chile and Estonia have experienced different "trigger" events, framing cybersecurity differently or having important actors with different agendas. The relevance of this theory is that it suggests that change happens in "spurts" (punctuation), resulting in three actions: I) "Disproportionate attention to local crises", meaning that the events that are raised by security concerns can trigger policy shifts. II) "Framing and policy monopolies" denoted how an issue is framed and who controls the debate can shape the policy direction. The last one, III) "The venue shopping", is about the different actors pushing for change who might pursue political arenas favourable to their goals (Baumgartner et al., 2006b; Shively, 2022).

There are similarities/convergence in some elements. For example, Chile emulated Estonia's data breach notification policy due to international best practices. Nevertheless, there are cases of divergence/difference; for example, Estonia focused on critical infrastructure protection (RIA, n.d.), differing from Chile's emphasis on combating cybercrime and educating the population (Achavar Barrios, 2018).
About the limitations of this theory, it might not fully explain the similarities that arise from international cooperation, shared global threats and others.

2.5 Cybersecurity Policy and the "lenses" (PCT and PET)

The assumption is that Cybersecurity policies are often created in response to specific incidents or threats unique to a particular jurisdiction or incident; for example, Estonia developed policies in response to a Russian threat (Herzog, 2011; Ottis, 2008). Then, it can be assumed that cybersecurity policies reflect each nation's unique policy preferences and interests, resulting in differences in national cybersecurity policies across various jurisdictions. These differences likely stem from past policy learning opportunities. In the context of the last example, it can be assumed that those countries that face cybersecurity threats more frequently are more likely to have stronger measures compared to a country that experiences fewer or no such risks (like Chile[4]) (see Ellis & Mohan, 2019). It can be attributed to policies and regulations reflecting unique origins and development pathways, and global issues such as cybersecurity threats are often addressed through different and varied policy responses. This "suggests that cybersecurity incidents are

[4] It does not mean there are no risks, but Chile has no immediate security risk or threats to their neighbours. At least known to the public.

deeply entangled with the regional political and security situation (…) a range of factors shape cybersecurity governance, it is initially catalysed by events that both stem from and are interpreted according to their regional context"(Ellis & Mohan, 2019, p. 22). In other words, this line of reasoning suggests that policies and types of government reflect unique origins and development paths. Moreover, global issues such as cybersecurity threats often result in diverse and varied policy responses (Pollitt et al., 2007).

Nevertheless, a rival line of reasoning mentions that cybersecurity threats are global in nature and, therefore, cybersecurity policies should be designed and developed to withstand temporal changes or geographic differences. Understanding this idea, one might infer that both mimetic and normative pressures can influence National cybersecurity policies; mimetic pressures refer to the tendency of countries to copy policies from one another, while normative pressures refer to the desire to conform to international standards and expectations (through recommendations from international communities of experts and cybersecurity associations, such as the UN Group of Governmental Experts on Cyber Issues, the Global Forum on Cyber Expertise, and others). As a result, these policies can often resemble one another, as similar external factors shape them.

The question of national cybersecurity policies is a complex issue that revolves around understanding the differences and similarities (or resembling each other) between (cyber) policies across different nations. This also involves examining how values related to security, civil liberties, and human rights are balanced within specific national contexts. This issue is part of a more extensive debate on policy diffusion and policy transfer that remains as an unresolved debate to this date (Blatter et al., 2022; Marsh & Sharman, 2009) and the mechanisms behind the convergence and divergence of policy and policy development. Scholars have identified four specific mechanisms of policy diffusion (learning, competition, emulation, and coercion) (Blatter et al., 2022, p. 806). Nonetheless, there is a deficiency of a consistent theory, and there are large areas of overlap and inconsistencies between these mechanisms. This gap in the literature highlights the need for further research to understand the mechanisms behind policy convergence (or divergence) or even theories like the punctuated equilibrium theory.

Relating this theory to cybersecurity, differences and similarities in national cybersecurity policies can be observed differently. PCT may explain why many countries adopt similar

cybersecurity strategies and measures. Being 'cyber threats' global, nations have a strong incentive to align their policies to address common vulnerabilities and risks (for example, the EU and the EU countries). Additionally, international organisations, like the United Nations or regional bodies, often promote cybersecurity cooperation and the adoption of best practices. PCT mentions that a country emulates another policy, there is a discussion in elite networking and policy communities about the problem (cybersecurity or the cyber threats), which could be taken through harmonisation of different intergovernmental organisations and, lastly, through penetration where it is almost a country or institution impose the creation or the change of a public policy.

In the context of cybersecurity policies, in the view of PCT, relevant national actors and (international) expert forums can shape, influence and develop cybersecurity policies. Those actors (states, powerful companies, international forums, international agreements, NGOs, or others) are likely to influence on convergence of cybersecurity policies. Usually, the manifestation of it is through harmonisation and standardisation. This means the alignment of CS policies and approaches from different countries; it involves adopting a similar framework, sharing protocols, and others. With it, we can talk about standardising and developing technical standards for cybersecurity measures or good practices. This can be seen in international agreements on cybercrime, best practices, and other formal documents.

The Punctuated Equilibrium Theory can also shed light on differences in national cybersecurity policies. While there may be a general trend towards convergence driven by global pressures, individual countries may experience sudden shifts in policy due to unique circumstances or critical events. They can change agenda setting, venue shifts, policy monopoly changes, etc. For example, a cyberattack targeting a country's critical infrastructure could prompt swift changes in cybersecurity regulations or investments (like the case of Estonia). Similarly, changes in government leadership or shifts in public opinion can lead to abrupt policy shifts.

In the context of cybersecurity policy, venue shopping means the strategic selection of places and forums for policy discussion. In this sense, a country chooses to participate in forums aligned with its policy. The venue shopping can be involved by the national government or international organisations that act as venues for policy discussion (for example, the UN). Those forums could limit the exposure to others' perspectives. It could even hinder convergence through harmonisation when there is already a strategy between

countries and there is not enough cooperation between all the participants. However, it is known that there are strategic alliances between countries, so they tend to choose those places to foster cooperation in cybersecurity issues. About the other concepts of PET, the case of local crises can be seen in the case of a significant cyber event that could impact a specific nation. As mentioned, these local crises can trigger those bursts, leading to significant changes in cybersecurity policies. In that sense, framing is seen in how the information about that crisis is presented to the public and the policy responses. Lastly, this can change the policy monopolies or influence the cybersecurity policy development, making them prioritise their agenda and limiting to other voices in the cybersecurity policy. This study links up to this ongoing debate on policy diffusion and policy transfer (and/or on the relevance of 'context' for policy-making) by studying possible similarities and differences in two national cybersecurity policies (of Estonia and Chile).

2.6 Chapter Summary

As a summary of this chapter, it can be said that, on the one hand, Policy Convergence Theory mentions that countries tend to adopt similar policies over time due to different factors, like globalisation (imitations) of other state policies, international norms, external pressure or the spread of best practices by NGOs or international agents. This theory suggests that nations may converge on specific policy approaches as they respond to common challenges or pressures from international actors. PCT tries to explain the pressure on national policies to be more similar due to external factors. On the other hand, Punctuated Equilibrium Theory suggests that policy change occurs in sudden bursts rather than through gradual evolution. PET try to explain how the internal factors and major events (burst) lead to a policy change (and possible divergences) or not. It proposes that policies tend to remain stable for long periods until external shocks or critical events prompt rapid changes. Therefore, to answer the research question about similarities and differences in cybersecurity policies in Chile and Estonia, it must consider each of the elements that PCT and PET have because, through them, it is possible to see if there is some pattern.

Chapter 3: Conceptual Framework

3.1 Introduction of this chapter

Chapter 2 explored the concepts of Policy Convergence Theory and Punctuated Equilibrium Theory and identified core concepts and mechanisms that explain both similarities and differences in national cybersecurity policies. These mechanisms include elite networking and party communities, emulation, harmonization and penetration, and framing and coalition formation within institutional venues where crucial decisions are made regarding specific security issues or threats. Building upon these foundations, chapter 3 proposes a framework that synthesizes the discussed concepts and mechanisms. This framework will help this document observe and explain similarities and differences between Estonian and Chilean cybersecurity policies.

Therefore, this chapter is structured as follows. Section 3.2 will delve into the overlaps between theoretical perspectives and specific contributions. This section will also translate abstract theoretical concepts and mechanisms into the specific context of cybersecurity policies. Subsequently, Section 3.3 will present the framework and the concepts within it. Finally, Section 3.4 will discuss the framework's application.

3.2 Theoretical concepts and mechanism in the context of cybersecurity policies

This section explores the synergies and unique contributions that the Policy Convergence Theory and Punctuated Equilibrium Theory can bring under the realm of cybersecurity policies. While presenting distinct perspectives, both theories share some common ground. They acknowledge the influence of external forces like globalization and technological advancement in shaping policy decisions across nations. Additionally, both theories recognize the importance of domestic factors like political institutions and policy coalitions in influencing policy outcomes. Both theories are already defined in the upper pages, but in this section, they are defined and connected to cybersecurity policy.

Each theory offers specific strengths applicable to the analysis of cybersecurity policies. Convergence theory emphasizes the homogenizing tendencies driven by global pressures, potentially explaining similarities in the broad frameworks of Chilean and Estonian cybersecurity strategies. Conversely, punctuated equilibrium theory sheds light on the localized dynamics that can lead to policy divergence. It highlights the role of policy entrepreneurs and political coalitions in framing specific cybersecurity threats and

advocating for changes within relevant policy venues, potentially explaining unique features or deviations in implementing these strategies between the two countries.

Nevertheless, to effectively apply these theories to the realm policies of cybersecurity, it is crucial to translate their abstract concepts and mechanisms into this specific context of cybersecurity. For example, elite networking can be translated into the collaboration between national security agencies across different countries to exchange best practices and develop joint cyber defence strategies. Similarly, emulation can manifest in adopting a successful cybersecurity framework from one nation to another, adapting it to their specific needs. By translating these concepts, a more nuanced understanding of how these theories can explain both convergence and divergence in the cybersecurity policies of Estonia and Chile is strived..

3.2.1 Unpacking the Policy Convergence Theory and its mechanism

To understand how a policy convergence happens, it is important to acknowledge what the 'original' author thought about the concepts itself "should also see as a process of 'becoming' rather than a condition of 'being more alike': Convergence means moving from a different position towards some common point" (Bennett, 1991, p. 219). Four processes cause policy convergence, as it was mentioned before. Each of them, the author mentioned, "are related to different empirical conditions" (Bennett, 1991, p. 229).

1. Convergence through Emulation: Policymakers sometimes copy successful policies from other countries or regions. This intentional copying, called emulation, is one way in which policies can become more similar over time, a phenomenon known as stated before, policy convergence. The copy of the policy can backfire because it could be challenging to adapt a policy from one place to another; there could be a lack of resources, political pressure/resistance and even cultural problems.
2. Convergence through elite networking and policy communities: Convergence through elite networking and policy communities arises from a desire to exchange expertise, often observed in academic discussions focused on introducing new ideas or disseminating information.
3. Convergence through Harmonization is about the convergence within international regimes that emerges from interdependence and the perceived necessity for cooperation. This can manifest through diverse factors like environmental preservation, security considerations, or economic integration.

Lastly, 4. Convergence through **Penetration**: is about the diffusion of knowledge, problems and possible solutions. In this case, we have an unequal power relation between the actors; there could be elements of coercion (directly, like military threats or indirectly, for example, economic pressure) or even 'legitimacy' concerns. In essence, it is not a negative concept, but as a struggle for power, it could have negative impacts.

For a better understanding, the author mentions, "(…) while regulatory outcomes are highly similar across countries, the political processes by which these outcomes are reached display persistent differences" (Bennett, 1991, p. 230), meaning that sometimes is what we see and some time is more than that. In other words, policy convergence theory (PCT) emphasizes the tendency of policies across different jurisdictions to move towards similar goals and approaches over time; they tend to converge on similar policy solutions. This can occur due to various factors, including international norms, economic pressures, or shared technological advancements. Dolowitz and Marsh (1996) define this as policy transfer, and it can be through different elements. However, they identified three mechanisms: cross-national policy learning, diffusion of ideas, or emulation of successful policies in other countries

In the context of cybersecurity, policy convergence can be observed as nations adapt their strategies to address common threats, such as cybercrime, cyberwarfare, data breaches, and others. In other words, Policy Convergence Theory suggests that, over time, countries facing similar challenges and external pressures are likely to adopt comparable policy solutions, leading to the convergence of policies across borders. When confronted with similar issues, this theory assumes that states will independently arrive at analogous policy responses influenced by shared international norms, best practices, and the global diffusion of ideas. This shared vulnerability has spurred international cooperation and collaboration in cybersecurity, leading to some degree of convergence in national cybersecurity policies. Threats often transcend national borders, and PCT provides a lens through which to explore commonalities in policy approaches between Chile and Estonia, shedding light on whether these nations converge in their responses to shared cybersecurity challenges and what that entails.

3.2.2 Unpacking the Punctuated Equilibrium Theory and its concepts

Punctuated Equilibrium Theory (PET), on the other hand, emphasises the dynamic nature of policy change. The authors highlighted the dynamic nature of policy change, and the stability and inertia of policy systems. It suggests that policy processes often exhibit long periods of stability or stasis, punctuated by brief periods of rapid change and realignment. These critical junctures, or "punctuations," can be triggered by external events, crises, or shifts in political power. In the context of cybersecurity, punctuations could arise from major cyberattacks, technological breakthroughs, or shifts in geopolitical alliances.

PET was used to review "new empirical studies in the USA and elsewhere, discuss new theoretical developments (…) broadened PET to incorporate a general theory of information processing in the policy process" (Baumgartner et al., 2006b, p. 2). Is about disruptive events and policy change. The elements of PET were defined in the above pages, yet it is about policies displaying prolonged periods of relative stability due to limited attention from policymakers and politicians. However, this theory acknowledges instances of rapid and significant change ("abrupt punctuations") triggered by specific events within localized contexts. These events involve the framing of an issue by political or societal actors (policy image) and a shift in policy venue, both of which can lead to substantial policy alterations. Also, other elements could disturb like *mobilization*, *agenda-setting*, positive[5] and negative feedback[6]. Into this, we can add that bounded rationality is also essential, "decision makers are subject to cognitive limitations in making choices" (True et al., 2007, p. 2). PET offers a different perspective on policy adoption, *by emphasizing the notion that policy change occurs in punctuated bursts rather than through a continuous and gradual process*. By "burst", the authors explained them as "of change and policy punctuations as arising from interactions of image and institutions" (ibid., p. 14). According to PET, long periods of policy stability or stasis (those periods of incremental policy adjustments) are punctuated (interrupted) by short, intense bursts of change triggered by external shocks or critical events.

[5] Positive feedback "occurs when a change, sometimes a fairly modest one, causes future changes to be amplified" (True, et al., 2006; 9). This is also known as 'feeding frenzy' or 'bandwagon effect'.
[6] "A successful policy monopoly systematically dampens pressures for change, we say that it contains a negative feedback process. Yet policy monopolies are not invulnerable forever" (True, et al., 2006; 8).

Therefore, the rudimentary elements in this theory are: first, framing policy image; second, “policy communities”; third, it is the change of policy venue; fourth, it is about agenda-setting. Lastly, it is about the venue shop/ shopping. In the context of cybersecurity, this theory could explain different instances where sudden and significant shifts in policy are driven by emerging threats (for example, cyber-attacks), technological breakthroughs, or different shifts like a geopolitical event making a catalyst for “punctuated equilibrium”; leading to significant changes in national cybersecurity strategies. By applying PET, one can explore whether the cybersecurity policies of Chile and Estonia exhibit (or not) periods of stability punctuated by rapid and transformative changes.

3.3 Framework and concepts

In this study, the combination of elements from Policy Convergence Theory and Punctuated Equilibrium Theory is noteworthy, especially for the understanding of differences in decisions in cybersecurity policies. It could offer a robust analytical framework to search through the complexities of national cybersecurity policies in Chile and Estonia and to understand differences in decisions in cybersecurity policies. While PCT highlights the potential for convergence over time, PET focuses on policy change's abrupt and discontinuous nature. These theories are not mutually exclusive but rather complementary. It could offer a robust analytical framework to search through the complexities of national cybersecurity policies in Chile and Estonia. It is important to note that while there are areas of overlap, these theories have distinct emphases and conceptual frameworks. PCT focuses more on the gradual position of policies across countries due to various factors, while PET emphasizes the ‘burst’ and often abrupt nature of policy change, particularly in response to critical events. The dimensions mentioned above represent points of intersection but are situated within the broader context of each theory's unique propositions and assumptions. Together, these theories provide a different framework for examining the creation of national cybersecurity policies.

Consequently, following the definition and discussion of key concepts and mechanisms within each relevant theory, this document created six new concepts to encompass the analysis for the parliamentary debate focused on the cyber-policy of Chile and Estonia through the overlapping concepts of PCT and PET. These concepts are called 1) the Dynamic Nature of Policy, 2) External Shocks and critical events, 3) international

influences, 4) learning and adaptation, 5) Policy transfer and diffusion (plus international influences and 6) the Window of opportunity. For each concept, it will be briefly explained how it overlaps with the mechanisms of each specific theory.

First, the "dynamic nature of policy": in this case, both theories recognize that policies are dynamic and subject to change. Policy Convergence Theory focuses on the gradual alignment of policies over time, while Punctuated Equilibrium Theory emphasizes the punctuated nature of policy change. In second place, the "external shocks and critical events"; in this case, both theories recognize the importance of external events or shocks (moments) in influencing policy change. PCT acknowledges that global events or crises can create pressure for a specific type of response (beginning with emulation), while PET suggests that critical events can trigger abrupt policy shifts (from framing differently, putting it on the agenda or changing the venue). The third section, "international influences", comes from the consideration that both theories contemplate the impact of international factors on domestic policy; PCT emphasizes the role of international norms and organizations, while PET may involve external pressures or influences during punctuation events. For example, the concept of elite network/policy communities or harmonization and policy community, respectively. Next, the fourth concept, "learning and adaptation", is about an idea that is in both theories: the concept of learning. In Policy convergence theory, countries learn from each other's experiences and adopt similar policies (either through emulation, elite networking, harmonization or penetration). Punctuated equilibrium theory is about learning from past events or policy feedback and how it can be a catalyst for policy change during punctuation moments. In fifth position, the concept of 'policy transfer and diffusion' appears; both theories recognize the role of it. In the case of PCT, it explicitly involves the transfer of policies across countries (beginning with emulation), and PET acknowledges that external factors and new ideas can be introduced into the policy process, potentially leading to significant changes (if there is a discontinuity in the policy stability in that country). In the sixth position appears "window of opportunity"; both theories recognize the existence of windows of opportunity or something similar for policy change. In PCT, they may align with moments when countries are open to adopting similar policies (from emulation until penetration of the ideas), while in PET, these windows coincide with critical events.

3.4. Framework application analyzing parliamentary debates

This section demonstrates the application of the previously defined six overlapping areas (as outlined in Section 3.3) to analyse the parliamentary debates concerning cyber-policy in Chile and Estonia. Each concept within the framework will be individually utilised to examine the respective debates. For example, the concept of "windows of opportunity" will be explored within each country's parliamentary debate, divided into ‘Policy entrepreneurs’ or ‘policy window’. This analysis will explore whether the adoption of specific cyber-security policies, such as the creation of a dedicated law, resulted from an internal critical event (this will involve examining if the policy change comes from domestic events causing significant disruption) or from external pressure (examining if the policy change was influenced or imposed by other countries or international agencies). In other words, if the policy change comes from emulation of the reality of another country or it was in a specific moment and was influenced enough (punctuation) to create change and to frame the agenda setting.

Furthermore, the analysis will consider how the concept of legislative feasibility applies to each case. This will examine how the idea of ratifying specific cyber-security measures was perceived as attainable within the context of the respective parliamentary debate.

The subsequent paragraph will delve into this phenomenon through the lens of the core elements of Policy Convergence Theory (PCT) and Punctuated Equilibrium Theory (PET).

The core elements of Policy Convergence Theory (elite-expert networking, emulation, and harmonisation) align with convergence pressures. Nations often emulate successful strategies from other countries, resulting in the harmonisation of policies across different nations. Both PCT and PET also acknowledge the disproportionate attention paid to local crises. For instance, a major cyberattack on a specific nation can serve as a wake-up call for other countries, prompting them to adopt similar policies to prevent similar attacks (PCT). This shared focus on a common threat drives convergence.

A deeper exploration into domestic factors and divergence reveals that while PCT emphasises penetration or diffusion by external actors, PET does not directly address it. External actors, such as international organisations, can advocate for policy convergence (PCT), yet their influence may be limited in countries with strong nationalistic tendencies (PET's domestic factors). These countries may resist external pressure to adopt policies compromising their sovereignty.

Conversely, elements emphasised in PET but not in PCT, such as policy monopoly and venue shopping, offer alternative explanations. Policy monopoly refers to dominant actors shaping cybersecurity policy within a country. In the case of a strong policy monopoly, a nation might prioritise its cybersecurity vision, even if it deviates from international best practices. Venue shopping involves selecting specific venues for policy discussions, allowing countries to participate in forums aligned with their existing policies, thus limiting the influence of alternative approaches on policy development. These elements relate to domestic factors (PET) influencing how a country approaches convergence pressure.

Therefore, the observed similarities and differences can be attributed to some influences; convergence promotes similarities when there is a strong elite network and emulation of successful strategies. Additionally, major cyber crises create a shared sense of urgency for all nations, often within the same international organisations. Domestic factors from PET can contribute to differences in other ways: weak external pressure for convergence, resistance due to nationalistic tendencies, policy monopolies dictating cybersecurity priorities, and venue shopping, leading countries to forums aligned with their existing policies.

In summary, the interplay of these elements creates a dynamic tension. Convergence pressures advocate similar policies across nations, while domestic factors can lead to divergence. The specific national cybersecurity policy that emerges is contingent upon the strength of each force in a particular context.

Chapter 4: Methodology

4.1 Introduction to this chapter

This chapter outlines the methodological approach employed in this document. It builds upon the conceptual framework established in Chapter Three and details how the investigation will be planned. The chapter is structured as follows. Section 4.2 Research Design: details the research design, encompassing the selection of cases, the data to be utilized, and the timeframe for analysis. Section 4.3 Methodological Approach: Focuses on the methodological approach chosen for this study: qualitative method and coding as technique. Section 4.4 Parliamentary Debates and Information Extraction: delves into the analysis of parliamentary debates. It will outline the process of extracting relevant information from these debates. Section 4.5 is the operationalization of the overlapping concepts (referring to how the concept is translated into terms for qualitative analysis).

4.2 Research Design

There are several reasons for choosing a small-n research design to study cybersecurity policies. To focus "on a few cases allows for intensive study and deep knowledge of these cases and thus the operationalization of variables" (Blatter & Haverland, 2012, p. 65). Access to the information was another element to take into consideration when doing a small study. The parliament debate was online and, in the Estonian case, was translated using DeepL. Finally, this type of studies "are ideal for investigating new, complex, or abstract phenomena" (ibid; 19). In the following pages, it is mentioned why those two countries were selected. However, first, a short background on each country will be provided to give a general context for each country. Considering their different backgrounds, it is interesting to know how the elements of cybersecurity were created. How did the debate in the parliament start? Was it an outsider element? Was it a burst on the normality of that country (an external shock or critical event)?

4.2.1 Chile

It is a "full freedom"[7] country with a Presidential system[8], and the legislative debate it is in the Congreso Nacional de Chile (National Congress)[9]. Unlike the Estonian case, Chile had no defining moment, like Estonia's Information Security Strategy in 2007 or others. The only related thing is the Law of Intellectual Property in 1994, which indirectly addressed aspects of digital security related to intellectual property protection. In 2002, the Law on Crimes Related to Computer Systems was established, specifically addressing cybercrimes like hacking and unauthorized access, but was directed more to private companies. It was not about the nation and cybercrime or cyberattacks. Chile signed the Budapest Convention on Cybercrime in 2001, but it was signed by the Chilean Congress many years later. In 2004, The Cybersecurity Plan was launched, outlining a national strategy for addressing cyber threats, for the first time. In 2008, the Cybersecurity Department was created within the Ministry of Interior, a dedicated government body focused on cybersecurity; but it was more the creation of it, more for the image. In 2022 the Cybersecurity strategy was updated, reflecting evolving cyber threats and adapting national response strategies. Finally, in 2024, the first law about cybersecurity was created in Chile, called "Ley Marco General de Ciberseguridad" (Cybersecurity Framework Law). Published on the on the eighth of April, in the Official Gazette of Chile, "which aims to establish the institutional framework, principles and general regulations to structure, regulate and coordinate the cybersecurity actions of state agencies and private individuals who provide essential services for the functioning of the country" (Diario Oficial, 2024).

The Chilean law[10] began the process on 15th March of 2022 when the President of the Republic initiated the project to the National Congress, specifically to the senate chamber. It was discussed for two years, being accepted by the Congress in December of 2023, and

[7] Freedom House's index established it as a "full freedom" of 95/100 points. More information in: https://freedomhouse.org/country/chile/freedom-world/2024

[8] There are clear reasons for the differentiation between the political systems of each country, which means that the influences of power have different distributions, such as the relationship between executive power (government) and the legislative system, how laws are made, etc. The construction of the national political framework varies. However, for this thesis, congressmen and parliamentarians shall be understood as synonymous.

[9] More information about the National Congress and the creation of a new law in Chile can be found on their Library web page: https://www.bcn.cl/formacioncivica/detalle_guia?h=10221.3/45763 [in Spanish]

[10] The case of Chile can be seen on the web page of the Senate (Senado), looking for bill 14847-06, in: https://www.senado.cl/appsenado/templates/tramitacion/index.php

the law was decreed by the president of the Republic of Chile the first of April 2024 (see appendix 1: Summary of the formation of the Cybersecurity law in Chile). Still, in the following table 2 is a small summary of what one can find on the draft of this law, and the documents used for this research. It is important to mention that although the law now exists, the regulations and other official documents still need to be prepared. Therefore, there are still public administrative processes that need to be done.

Table 2: Documents used in the research.

Date	Sub-phase	Phase
30/09/2022	Primer informe de comisión de Defensa Nacional. Pasa a Comisión de Seguridad Pública. [First report of the Committee on National Defence. Passes to the Committee on Public Security].	Primer Trámite consituticional / Senado. [First constitutionalconstitutional procedure / Senate.]
12/10/2022	Primer informe de Comisión de Seguridad Pública. [First reporto of the Public Safety Comittee].	Primer Trámite consituticional / Senado. [First constitutional procedure / Senate.]
14/11/2022	Boletín de indicaciones. Oficio N° 183-370 Informe Financiero. [Indications bulletin. Financial report]	Primer Trámite consituticional / Senado. [First constitutional procedure / Senate.]
20/04/2023	Segundo informe de comisión de Defensa Nacional y Comisión de Seguridad Pública, unidas. [Second report of the Committee on National Defence and the Committee on Public Security, together].	Primer Trámite consituticional / Senado [First consitutional procedure / Senate.]
25/04/2023	Segundo informe de comisión de Hacienda. [Second report of the Finance Committee].	Primer Trámite consituticional / Senado
27/11/2023	Primer Informe de Comisión de Seguridad Ciudadana. Pasa a Comisión de Hacienda.	Segundo Trámite consituticional / C. de Diputados.

	[First report of the Committee on Public Safety. Passes to the Finance Committee.].	[Second consitutional procedure / C. de Deputies]
05/12/2023	Primer informe de comisión de Hacienda	Segundo Trámite consituticional / C. de Diputados. [Second consitutional procedure / C. de Deputies]
12/12/2023	Discusión general. Aprobado en general y particular con modificaciones. [General discussion. Adopted in general and in particular with amendments]	Segundo Trámite consituticional / Senado. [Second consitutional procedure / Senate]

Source: The table was created based on the information on the web page of the Senate. Translated by me. 2024.

4.2.2 Estonia

It is a Democratic Parliament Republic, considered by Freedom House as a full freedom country, with 95/100 points. A parliamentary system rules Estonia; therefore, there are some differences with the Chilean system. It is not about which political system is better, they are different. Some literature talks about one system offering advantages over the other in terms of democratic stability, good governance, policy outcomes and others (Eaton, 2016; Gerring, 2009; Soete, 2011). Different factors influence complex systems, from historical perspectives to institutional mechanisms. Cameron Ross (2003) mentions that "presidential systems are thus often prone to chronic conflict, legislative stalemate and even complete [legislative] paralysis" (Ross, 2003, p. 122). However, this research will not focus on that. It is about the legislative debate of the cybersecurity law. The law in Estonia was created in 2018; however, before that year, they had already some elements about cybersecurity.

Everything related to the cyber-sphere has been a significant issue in the Estonian Parliament since the early 2000s. In 2007, the Estonian government created the Estonian Information Security Strategy, which was the first document of its kind in the world. The strategy was updated in 2010 and 2017. The Estonian Parliament has debated cybersecurity on numerous occasions. In 2008, the Parliament passed the Information

Security Act, which established the legal framework for the protection of information in Estonia. The law has been updated several times since then. In 2014, the Parliament created the Information Systems Authority, which oversees the implementation of the Information Security Act. The authority is also responsible for investigating cybersecurity incidents.

In recent years, the Estonian Parliament has passed several new laws related to cybersecurity. In 2017, the Parliament passed the Cyber Defense Act, establishing the legal framework for Estonia's defence against cyber-attacks. In 2018, the cybersecurity law was passed; in 2019, the Parliament passed the Artificial Intelligence Act, which establishes the legal framework for developing and using artificial intelligence in Estonia. The Estonian Parliament continues to debate cybersecurity regularly. In 2022, the Parliament created a working group to analyse cyber threats and develop recommendations for improving Estonia's cybersecurity. Czosseck et al. (2011) mention that the changes after the 2007 cyberattack "prompted major changes in the Estonian legislative landscape (…) legal amendments involved several areas of law related to cybersecurity" (p.59). This could be one of the reasons why cybersecurity law in 2018 did not take too much time in Parliament. The following table (3) summarises the laws related to cybersecurity in one way or another.

Table 3 "Law related to cyber security"

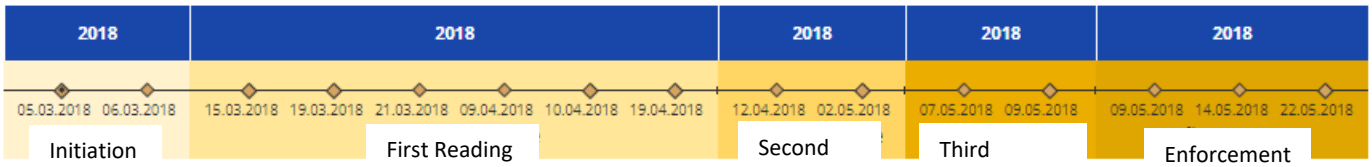
Constitutional law				
Fundamental rights and freedoms; Organisation of the state; Execution of public authority				
Private law	Public administrative law	Criminal law	Crisis management law	War-time law / national defence law
Information society services	General administrative procedure law supporting the accessibility of information society	Substantive criminal law	Critical infrastructure protection (CIP)	National defence organisation
eComms infrastructure provision	Availability of public information and public e-services	Criminal procedure law	Critical information infrastructure protection (CIIP)	National defence in peacetime
Provision of eComms services to end users	Data processing and data protection	International cooperation		National defence in conflict/wartime
General private law supporting the functioning of information society (eCommerce, digital signatures)				

Source: Czosseck et al. (2011; 59)

In the Estonian case, the creation of the cybersecurity law was fast[11]: it was initiated on the 5th of March 2018 and was enforced and published in May of the same year, as the image below shows. However, it is important to acknowledge that Estonia already had some legislation about cybersecurity scattered among different policies and strategies (confirmed in the parliamentary debate and even by one of the interviewees).

It was interesting to add that in 2018, the question of whether it should be implemented in some existing legal act or if it was time for a specific law about cybersecurity[12] was raised. The result was the creation of the cybersecurity law, but it does not include cybersecurity aspects in other institutions. However, there is the question of whether this type of law should have been legislated sooner or not after the breach in cybersecurity in 2007. Was there any change? After the 2007 cyberattacks, Estonia implemented a broad national defence concept; therefore, the cyber element is a vital part of the National defence strategy[13]. Hence, the creation of the law in 2018 was very important, especially for the coordination of national security and defence[14] and to accept the directive of the EU, which will be discussed in the following pages.

Fig.1 Estonian Legislation of their Cybersecurity Law



Source: Cybersecurity Act 597 SE[15]

[11] More information about the cybersecurity law of Estonia, can be seen on the web page of the Parliament (Riigikogu) of Estonia: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/kuberturvalisuse-seadus

[12] More information about that can be read in different documents. For example, two that have free access, good development and are in English: "Cyber deterrence: A case study on Estonia's policies and practice" by Piret Pernik (2021) and the Annual Cyber Security Report (2015) of Estonia.

[13] More information on various policies, programmes and strategies, provided by the expert Greta Toompere: https://riigikantselei.ee/en/supporting-government-and-prime-minister/organisation-and-planning-work-government/national

[14] More information is available at: https://www.riigikogu.ee/en/press-releases/riigikogu-approved-national-security-concept/

[15] In the Parliament web page, the Cybersecurity law can be found in: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/kuberturvalisuse-seadus

With the overview of each country, three reasons can be mentioned as to why they were selected. First, Chile and Estonia offer contrasting starting points for the analysis; both are part of the best of each continent in cybersecurity (see National Cybersecurity Index, and others)[16]. Estonia is a small, technologically advanced European nation with a strong digital identity, which has been around for almost two decades. This starkly contrasts with Chile, a larger, geographically diverse country with a recently evolving digital infrastructure[17], located in Sud America. This difference allows exploring how PCT and PET play out in distinct contexts. There are no extensive studies about cybersecurity that use those theories. To comprehensively analyse and understand the dynamics of national cybersecurity policies, it is essential to employ theoretical frameworks that can capture the complexities, distinctions, and gradations of policymaking processes. As stated before, two plausible theoretical orientations that offer valuable perspectives in this context are Policy Convergence Theory (PCT) and Punctuated Equilibrium Theory (PET). They offer promising perspectives for examining the evolution and divergence of cybersecurity approaches across different countries and provide valuable insights into the factors that can influence policy development, the processes of policy change, and the dynamics of international cooperation in cybersecurity.

Secondly, cybersecurity usually focuses on a national and international context; each of these countries is part of an international community in each geographical space. As mentioned before, both cases are in the top 10 of each continent in cybersecurity, making them relevant case studies. It is globally recognised the Estonian cybersecurity and digital development, while Chile is actively investing in strengthening its capabilities. Therefore, comparing their approaches reveals valuable insights into policy development and implementation.

Thirdly, the cases were selected because they made their cybersecurity policies easily available, and even had national strategies that provided advantages, giving more information about each country. Both states have clear policies in cybersecurity (Estonia

[16] In the Digital Develop Index (2023), Chile had 93,4% and Estonia had 96,4%. More information in: https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-2/

[17] In the OECD Digital Government Index (2023), which considers the digital infrastructure, Estonia is in sixth place and Chile is in 32nd. The last one was number one in Sud America. For more information, see: https://www.oecd-ilibrary.org/docserver/1a89ed5e-en.pdf?expires=1715354230&id=id&accname=guest&checksum=00652F28E49BEE01709E5EE2F9F41815

with an "old one"[18] and Chile with one approved by the National Congress in December of 2023). It cannot generalised from just two cases; nevertheless, it is hoped that the findings will provide broader insights into the interaction between policy convergence and punctuated equilibrium theory in shaping national cybersecurity approaches.

Concerning the connection with the theoretical framework: On one hand, the contrasting nature of these countries allows me to examine how far convergence in cybersecurity policy exists despite their differences. It can be can analyse factors driving convergence, such as international norms, best practices, and external pressures. Additionally, areas where PCT theories diverge can be explored, reflecting national priorities and contexts. Conversely, through PET, a comparison can be drawn between the specificities of each country's approach, with particular attention paid to the focus on stakeholders. Furthermore, an investigation can be conducted to determine whether the emphasis placed on the "burst" of this theory has any impact on policy changes.

This paper will focus on documents published between 2018 to 2024. This timeframe was chosen as the discussion took place between those years.

4.3 Parliamentary Debates and Information Extraction (Data sources)

The information was taken from the online pages of the National Congress[19] of Chile and the Parliament of Estonia[20]. The documents are part of the debate in each country's parliament. In addition, there will be interviews with some people from Chile and Estonia who have been part of the process of the law or who are experts in the theme of cybersecurity and the legislative process in each country. Therefore, the research method will be a qualitative analysis of the parliamentary debate on cybersecurity law in each place, and information will be gathered through interviews. They can give more in-depth answers to the research question.

---

[18] The institution in charge of cybersecurity in Estonia is RIA (the Estonian Information System Authority). It has evolved since 1993, when it was only the State Information Systems Department (RISO) under the Government Office. Then, in May 2003, the Estonian Informatics Centre (EIC) was formed, merging the Public Procurement Centre and the existing Estonian Informatics Centre. In 2022, the Estonian Informatics Centre was officially renamed the Estonian Information Systems Authority. (RIA, 2024).

[19] The web page from which the parliament discussion and more about this law can be found is on the Senate web page, under bill number 14847-06. More in: https://www.senado.cl/appsenado/templates/tramitacion/index.php

[20] The information about the Estonia Law is on the parliament web page. More in: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/kuberturvalisuse-seadus

4.4 Methodological approach

The parliamentary debate about the cybersecurity law of both countries was analysed through a qualitative coding system. The parliament discussion can be recognised as "a body of material to analyse and then create a system for recording specific aspects of its content" (Neuman, 2014, p. 49). The operationalisation was created through the overlap of the theories. The coding system will be explained in a subsequent paragraph. The purpose of coding in research is to facilitate a dynamic exploration process between data and theory. This iterative process allows for the identification and analysis of intriguing data points and theoretical insights, ultimately leading to the development of explanations for the similarities and differences in cybersecurity policies between Chile and Estonia. As Bukve (2019) mention, it "is essential to collect data that are relevant to the phenomenon we are focusing on" (Bukve, 2019, p. 208). One of the limitations of qualitative research is that it is "not able to secure that the cases are statically representative of the population (…) [therefore] we must base our collection on strategic selections of cases" (ibid., 209).

Consequently, the primary method used in this research is the parliamentary debate on the cybersecurity law of each country and interviews, which can add depth to the conversation that may not be present in the debate.

4.4.1 Qualitative coding as a technique

The rationale behind adopting this methodological approach is grounded in several factors. Through qualitative research and coding techniques, a systematic examination of parliamentary debates concerning cybersecurity law is examined, involving textual data extraction. By analysing these debates, a comprehensive understanding of the various arguments, perspectives, and distinctions presented by lawmakers in each country can be achieved. Secondly, this method allows for a systematic comparative analysis. Employing clear coding categories ensures consistency when applying the analysis to the data, thus providing a structured and objective means of examining debate transcripts. Moreover, by focusing on specific elements like arguments, positions, or others, it becomes possible to gain insight into the policymaking process within each country, including the positions and debates among different stakeholders and the internal dynamics at play. Lastly, systematically examining the documents facilitates clear comparisons between debates in the two countries.

A guided qualitative coding approach was employed, utilising MAXQDA software to analyse the parliamentary debates and answer the research question. This software facilitated the efficient management (retrieval, sorting, and analysis) of transcripts. The coding scheme itself was pre-defined and developed based on the two central theories (Policy Convergence Theory and Punctuated Equilibrium Theory). While the term "guided qualitative coding" may not have a single source, it aligns with established practices in qualitative research (like Auerbach & Silverstein, 2003; Gibbs, 2007; Saldaña, 2014, 2016; Witt, 2013). This approach ensured a systematic analysis through the application of pre-defined codes. These codes facilitated the organisation of information, the identification of categories and patterns within the debates, and maintained consistency throughout the coding process. As the pre-defined codes proved effective, the creation of new codes during the analysis (as suggested by Witt, 2013) was not necessary. This resulted in time saved and a maintained focus on the chosen theories. Ultimately, by employing MAXQDA software and guided coding, a structured framework was established for analysing the debates. This framework allowed for extracting key insights relevant to the research question from the analyzed data.

4.4.2 Interviews

The raison d'être of the interviews was to generate information that may not be found in the parliamentary discourse, therefore adding a little bit more information to answer the research question of this research. The interview method is highly beneficial for qualitative research activities, as it facilitates obtaining detailed insights into researched issues that might be challenging to gather through alternative research approaches. There are several benefits associated with employing interviewing as a method in qualitative research, beyond the element that using interviews helps with the bias that the researcher could have.

First, reach the data. Interviews make good and detailed data, allowing researchers to explore deeply into the people and their experiences, behaviours, expectations that they had, etc. (Mosley, 2013, p. 21). In second place, it could foster participant engagement and understanding, providing individuals with a platform to express themselves freely. Third, this type of interviews offer flexibility, allowing researchers to adjust some questions in response to participant responses, facilitating thorough exploration of related topics. Another element is that researchers can utilise interviews to clarify responses, ensuring a comprehensive understanding of the participants' viewpoints. Conducting

interviews involves delving into abstract and complex issues, focusing on the unique insights and experiences of experts and elite groups within specific fields (Blee & Taylor, 2002; Mosley, 2013).

Various challenges are associated with interviews, ranging from selecting suitable interviewees to determining whether open-ended or closed-ended questions are appropriate. Therefore, for this case, semi-structured question types were selected because they enable the interviewees to concentrate on answering the questions asked by the researchers. However, at the same time, they can freely express their views, thereby clarifying the essence of the research question (Blee & Taylor, 2002). This type of questions "provide greater breadth and depth of information, the opportunity to discover the respondent's experience and interpretation of reality" (Blee & Taylor, 2002, p. 92). Understanding the perspectives and motivations behind certain beliefs, particularly in political contexts, is a compelling aspect of conducting interviews.

Nonetheless, interviews come with drawbacks, such as technical issues (especially in video calls) (Mosley, 2013), time consumption, and potential reluctance or unclear communication from either the respondent or interviewer (for instance, when interviewing Estonian participants, the interviews will be conducted in English, which is not the participants or the researcher native language) (Blee & Taylor, 2002). Another reason to use semi-structured interviews is to address cultural differences that may appear. In order to ensure that those types of problems do not affect the interview, the semi-structured allows the interviewer more flexibility to digress and to probe based on interactions during the interview. Moreover, there may be inherent inaccuracies in the data due to the passage of time between the enactment of laws and the interviews, as well as the possibility of researcher influence and bias from participants. The researcher considered those elements. Despite these challenges, researchers must rely on participants' honesty and willingness to share accurate information to gather valuable insights from interviews.

It is worth noting that the interviews were non-randomly sampled. This aspect won't poses an issue since this study does not aim to test a specific theory. Mosley (2013, p. 19) suggests that non-randomly sampled interviewees can still offer the researcher valuable inferential insights. Lastly, the same codes were not applied to the legislative debate

because the idea behind the interviews was to have a deeper understanding of the elements of the debate to respond to the research question.

Some questions were asked to every participant: “Why the cybersecurity law was created now”? The Estonian case would have been more ‘obvious’ that they had a cybersecurity law after the attacks of 2007. Therefore, why now? “What did you (not) like about the new cybersecurity law?” “Was anything discussed in the parliament debate that was left behind in the final bill?” From then on, there were more open questions on how the discussion was organised, how the parliaments reacted, elements of the cybersecurity law and the mechanisms. More information in Appendix 3.

Five interviewees collaborate with this research (appendix 2: letter of consent), two from Chile and three from Estonia. The interviews were between the 18th of April and the 10th of May of the present year. For anonymity reasons, no names will be mentioned: each of the participants was assigned a number. The lines below indicate some information – for reference –of the interviewee (participants) (more information in Appendix 4).
The contact information from Participant 1 (P1) of Chile was given by a Professor who is part of the “Law and Technology Observatory” of the Universidad (University) Del Desarrollo in Chile. She (P1) is a lawyer and an expert in these types of themes (data protection, cyber security, etc.). She is currently working on approving the bill on personal data protection and creating a new agency. Chilean Senator gave the contact information of the next participant (P2). P2 is an engineer who currently works in the National Congress in Chile. He was one of the organisers of meetings held by senators' advisors to speed up the discussion of the cybersecurity bill. The information of one of the Estonian interviewees was given by an expert adviser who worked on the elaboration of a paper with Participant 3 (P3); she is a cybersecurity adviser. Then, Participant 4 (P4) information was asked directly to him, because he worked in the Estonian Information System Authority (RIA) since 2019, when he was appointed as the Deputy Director General. He is a lawyer. Lastly, Participant 5 (P5) was the ‘Protokollija’ (the recording secretary) of the Estonian Parliament when the law was discussed. She currently works in the Minister of Defence.

4.5 Operationalization of concepts

The concepts mentioned in Chapter 3 are going to be used as instruments to reveal those elements that are being looked at in the parliament discussion. Table 4, next page shows the concept, its definition, and examples taken from the theories or the parliamentary debate from Chile or Estonia.

Table 4: Concept and codes

Concept (category)	**Code (sub-category)**	**Definition**	**Examples or what to expect according the theory:**
Dynamic Nature of Policy	Political Factors (PF)	Changes in government shifts in political ideology.	"The government is evaluating the possibility of the institutionalisation of a public service and not an agency [as had been agreed the Congress with the previous government]". (Report of the National Defence Committee, first constitutional procedure, N°201. Chile).
	Institutional Factors (IF)	Changes in institutional structure and policy capacity.	The National Cybersecurity Agency is an urgent necessity, as it will be the institutional coordinating body for the virtual security ecosystem. (Report Of The Committee On National Defence, N°508. Chile).
External Shocks and Critical Events	Crisis Events (CE)	Cybersecurity breaches, national security incidents.	Various cyber-attacks were recalled, such as the recent Russian attack on Ukraine, the one suffered by Estonia, and the one in Georgia in 2008, among others. (Report Of The Committee On National Defence, N°571. Chile).
	Technological Advances (TA)	Emergence of new technologies and vulnerabilities.	About the regulation and this new law "affects different information systems and e-solutions, increasing their security and reducing their vulnerability, which in turn makes life more difficult for criminals". (Initiation: explanation letter. N°317. Estonia).
Learning and Adaptation	Capacity Building (CB)	Investments in cybersecurity education and training.	Two deputies mentioned that "the Agency should propose and cooperate with the design and implementation of [cybersecurity] education plans and actions". (First report of the Committee on Citizen Security, N° 1268. Estonia).
	Policy Evaluation (PE)	Evaluation of existing policies and/or lessons learned.	The former Subsecretary of Telecommunications, Mr. Jorge Atton commented that the model suggested in the project is similar to the one envisaged in Israel. He called for an analysis of the cybersecurity system in Australia, a state with similar governance to Chile's. (Report of The Committee on National Defence, N°390. Chile).

Policy Transfer and Diffusion	Cross-border Exchange (CBE)	Transfer of policies between countries, best practices.	This is similar to the case of "learning and adaptation". However, in this case, it is about copying best practices, which are not just for learning; they will be part of the law of that country.
	Imitation and Adaptation (IAA)	Adoption of policies from other countries, adaptation.	It is the transfer of a successful policy and its adoption into the new institutional/political system into which it is integrated.
	International Influences	From Transnational Organizations (UN, NATO, etc.) or from Bilateral Agreements.	Some mention of the EU NIS 2 Directive is expected, for the Chilean and Estonian case. The latter is more likely to have more examples.
Window of Opportunity	Policy Entrepreneurs (PE)	Individuals or groups pushing for policy change.	This was expected more in the Chilean case than in Estonia. People who push the agenda of the Government (or Congress) to create a policy change.
	Policy Windows (PW)	Opportunities for policy change, political moments.	In this case, it was expected that that the change in policy was created through policy windows or political moments that created a shift in reality.

Source: the concepts on the table were created based on the overlap of PCT and PET. Examples are drawn from theories and what should be expected or direct examples from parliamentary debate. Abril, 2024.

Chapter 5: Analysis & Empirical Findings

5.1 Introduction

The last chapter was about the method and methodology used in this thesis. Now, it is about the analysis and the empirical findings through the elements mentioned in chapter four. Therefore, this chapter is structured in the following form: Section 5.2 is about the Cybersecurity policies as outcomes, describing those elements. Section 5.3 is the analysis of the process through the results from the parliamentary debate and the interviews. Section 5.4 is about Comparison, analysis and propositions.

5.2 Cybersecurity policies as outcomes

In Estonia, policies, programmes, and strategies are clear but are scattered between different institutions. Just as an example, the cybersecurity strategies already mentioned are key elements in cybersecurity policies and outcomes in this country. Another element of information about cybersecurity is provided by the chancellery, where they coordinate - according to their website[21]- "national security and defence management". Another element in Estonian case is the National Security and Defence and how they coordinate between military and civic (Cyber Defense League) (CDL) cooperation between parts in themes like cybersecurity: "CLD relies on civilian talent to help fill security gaps and to augment its traditional government defense apparatus" (Grzegorzewski et al., n.d., p. 51). In the case of Chile, there are national strategies in cybersecurity, too, and they were modified last year until 2028[22]. The Cybersecurity Incident Response Team (CSIRT) of the Minister of Interior write a newsletter that every Minister should take into consideration too. The regulation of the Cybersecurity Framework Law, which has to be ready less than six months after the law was proclaimed, is awaited.

[21] More information on various policies, programmes and strategies, can be read at che chancellery website. https://riigikantselei.ee/en/supporting-government-and-prime-minister/organisation-and-planning-work-government/national

[22] More information can be found in: https://ciberseguridad.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf

5.3 Analysis of the process

5.3.1 Intro

This section delineates the theoretical foundations that were mentioned before, using the overlap of the theories in the legislative debate and adding elements that the interviews have left. The analysis shows that there are some theoretical concepts that are more prevalent in the parliamentary debates, while others do not even appear. Firstly, attention is directed towards the 'Dynamic Nature of Policy', encompassing institutional and political factors. Subsequently, focus shifts to the encounter, or lack thereof, with 'External shocks and critical events' in both national contexts. Following this, analysis is placed on 'learning and adaptation mechanisms'. The discourse then delves into the intricate processes of 'policy transfer and diffusion', particularly in the realm of international influences. Finally, the concept of 'window of opportunities' is elucidated, concluding the theoretical framework under consideration.

5.3.2. Dynamic Nature of Policy: Institutional Factors in Estonia and Chile

This is an element that is different from the two countries. The institutional factors of the creation of cybersecurity law for the Estonian case was not hard, they had already an institution and an agency (RIA) for cybersecurity; the institutional structure was already there. In contrast, for the Chilean case, it was/is a very complex endeavour, it was created to generate the foundation of cybersecurity in Chile: creating the law, a new institution, the institutional framework and the regulation.

A member of the Chilean Congress noted similarities between the proposed model and the system envisioned in Israel (Report Of The Committee On National Defence. First constitutional procedure, N°396). They emphasized the importance of analyzing cybersecurity frameworks in countries with similar governance structures to Chile. Specifically, they highlighted Australia and Estonia: Australia was cited as a relevant example, while Estonia's experience following significant cyberattacks from Russia was presented. The congressman acknowledged Estonia's subsequent cybersecurity law as a leading international example, emphasizing its comprehensive approach with guidelines,

obligations, and inter-agency coordination. However, they stressed the need for any chosen system to be adaptable due to the evolving nature of cybersecurity threats[23].

The Chilean case was about the state's cybersecurity and the private sphere; it was about having the institutional infrastructure, law, regulation, etc., and in the end, it was about the modernization of the State.

Following the last idea, it is interesting to acknowledge the Chilean legal culture and mentality of creating laws; as said by an author, there is a "legal culture (normative)" (Baraona González, 2010) mind. However, that is not the Estonian case. Before the creation of the cybersecurity law, Chile did (almost) not have elements or formal normative regulation on cybersecurity[24], but Estonia already had elements of cybersecurity, but it depended on the public service and/or the Ministry. It is important to mention what the research participant who contributed to the drafting of the bill of cybersecurity in Estonia (P5) said about that. She indicated that the NIS directive was:

> "a very good opportunity to have an overall cybersecurity legislative framework. Before that, it wasn't so centralized. Different departments and various ministries had their own task. So that means every government institution had their own legislation. So, in a way, it's like we have the parliamentary legal acts and regulations. And under those, we have the stipulations that govern a certain sector. So, it was sector-based".

When it was asked why is was not done before, she said that "maybe it was difficult to reach a consensus of having one entity responsible for the overall cybersecurity, especially for critical infrastructures and from government perspective" (P5, 2024). However, that is exactly what was done with the passing of this new law.

About that, not having one legislation about cybersecurity, "A research participant who works for RIA mentioned that "we didn't change that much [after the creation of NATO – CCDCOE] because we had the cybercrime legislation in place already, which is coming

[23] More information can be found in the bill under the Report of the National Defense Committee [Comisión de Defensa Nacional], establishing a Framework Law on Cybersecurity and Critical Information Infrastructure in the first constitutional proceeding.

[24] There is one exception that was created by the Financial Market Commission. They are a collegiate regulatory body of a technical nature, autonomous and with its own assets. They have a long track record in technology and cybersecurity issues, as was said by their spokesman in the parliament debate. They created a regulation on cybersecurity for the Banks in Chile.

from the Budapest Convention (…) and we had the Cyber Emergency Situation [act]". He mentioned that the problem was those laws or institutions were more for the military, not for the "civilian infrastructure" (P4, 2024).

One of the interviewees mentioned that this law was not about that [institutional factors] that were given by others. In the legislature debate it can be seen what Urve Palo, a minister in that time, mentioned that [the laws] "they have been scattered in different legislation[s]" (Cybersecurity Bill, 15. 03. 2018, Parliament Debate), therefore there was no order in that sense. The RIA's lawyer (P4) mentioned that the Emergency Act (2009) provided already a legal base to act in case of a cyberattack. As it is mentioned in the normative, this act gives "legal bases for crisis management, including preparing for and resolving an emergency as well as ensuring the continuity of vital services" (Emergency Act, § 1[25]). That act and others, gave some infrastructure in cybersecurity to Estonia and institutional factors too. Lastly, interviewee 4 said, "what is interesting about the Estonian approach is not necessarily what is written down in the law, because that is just a transposition of the European framework*"*; she highlighted how the networking in Estonia work behind the institutions.

In the case of Chile, the institutional factors were created with the law that was passed this year (2024). As Senator Pugh mentioned, "as a country we are moving forward in agreements to have an institutional framework with a new ecosystem" (Second Report of the Finance Committee. First constitutional procedure. N°85). However, without legal regulation - they need to be created - the institutional factors will not exist. As the private lawyer (P1) mentioned "there are no consequences [for the State], unlike other laws. There is no accountability, nor is it known who will operate on the state side. The laws speak of standards that do not exist as there are no regulations".

5.3.3 Dynamic Nature of the policy: political factors in Estonia and Chile

Another element that is different is in the category 'Dynamic Nature of Policy', especially the sub-category of 'Political Factors', in both countries. The description of it (table 4) is about 'changes in government, shifts in political ideology'.

[25] More information about that act (2009) can be found in the Parliament web page: https://www.riigiteataja.ee/en/eli/525062014011/consolide. In 2017 it was modified, more information in: https://www.riigiteataja.ee/en/eli/511122019004/consolide

In both countries, in the legislative debate, there are no major discrepancies between what the executive wants from the law and what the parliament accept -normally-. In the Estonian case, it makes sense because it was a directive of the EU; therefore, it needed to be accepted. In the Chilean case, there were some opportunities where the executive and legislative branches did not converge on one idea, making the agreement for a cybersecurity law harder to achieve. For example, in one of the parliament debates in Chile, it was said that: "(...) The Government is evaluating the possibility that the institutional framework may take the form of a public service and not an Agency - as suggested in the text under discussion - [and which had been agreed]" (Report of the National Defence Committee. First constitutional procedure. N° 201). This created friction with executive power because it was previously agreed upon. In the end, the Congress won that impasse, the executive accepted the idea of an Agency. After that, there are no significant frictions between powers, as Senator Pugh said, "As this is a state policy that transcends the governments in office"[26].

It is interesting to highlight what the engineer (P2) mentioned, the bill finally came out because it was negotiated with the government. A political agreement was made. With what they had already delayed, it was preferable to have something "not so perfect, but that exists" (P2).

Therefore, that played a role in the creation and passage of the cybersecurity law in Chile, but there were almost none in the Estonian case.

5.3.4 External Shocks and Critical Events in Estonia and Chile

It was expected that there would be many examples of the parliamentary debate, but this was not the case in reality. On the contrary, in Chile it was mentioned one time in three different documents of the parliamentary debate. However, those comments were made by the spokesman of the executive power, not by congressmen/women.

In the Estonian case, the only time that it was mentioned was by the Estonian lawyer - participant N° 4, when he said: "We started thinking about the cybersecurity dilemmas

[26] It was translated by deepL. The original text is: "tratándose de una política de Estado que trasciende a los gobiernos de turno, como país se avanza en acuerdos para contar con una institucionalidad con un nuevo ecosistema" (Second report of the Committee on Finance, Report of the Finance Committee on the draft law, in first constitutional procedure, which establishes a Framework Law on Cybersecurity and Critical Information Infrastructure. N°85)

and challenges after this world-famous attacks on Estonian infrastructure in 2007. But then that did not really spark the discussion in the civilian infrastructure (…)" (P4, 2024).

This suggests that, in this case, external shocks or critical events were (almost) unrelated to *creating pressure* for creating a cybersecurity law, in each country.

5.3.5 Learning and Adaptation in Estonia and Chile

Another difference can be found in the parliament debate on the cybersecurity law in Estonia is that they didn't mention other cases outside the NIS directive. The debate did not mention any countries and what they could learn about them. However, the recording secretary (P5) mentioned something interesting, "the discussion [about CS] started earlier. So, the overall law-making procedure is quite long. So, all the interested stakeholders are included in the negotiations before the parliamentary level" (Protokollija, 2024). Had it not been for the interview, it would not have been known, because none of the documents analysed mentioned the earlier debate. In the Chilean case, on the other hand, it is written in some documents and in one of the interviews with a Chilean person, it was also mentioned.

It is a very different case for the Chilean position, where they mention, for example, the case of the congressmen that made a trip to Estonia where they learn from "a world reference in cybersecurity, has allowed them to acquire sufficient knowledge to contribute to the construction of this framework law" (Second Report Of The Committees On National Defence And Public Security, United, N°85, 2023)[27]. Other examples were when they mentioned, more than once, the cases of the Belgian law of cybersecurity, the Australian, Israeli and from England (First Report of the Committee on Public Safety, N°91) .

5.3.6 Policy Transfer and Diffusion in Estonia and Chile: International influences (EU)

Another similar element can be found in the category of 'Policy transfer and diffusion' (under the subcategory of "international influences"). Both countries took into

[27] It was translated using DeepL. The chilean text said: "referente mundial en ciberseguridad, les ha permitido adquirir los conocimientos suficientes para contribuir a la construcción de esta ley marco" (Second Report Of The Committees On National Defence And Public Security, United, on the draft law, in first constitutional procedure, which establishes a Framework Law on Cybersecurity and Critical Information Infrastructure. 2023).

consideration NIS 2 (2022/2555); this is a Directive of the European Council, and therefore, it counts as a legislative act. In other words, this law aims to improve all EU countries' cybersecurity management. It sets basic requirements for managing cybersecurity risks and reporting incidents across important sectors like energy, transportation, healthcare, and digital infrastructure[28] (NIS 2, n.d.).

Nevertheless, there are differences in why was introduced in their parliamentary debate. Estonia was bound by law to make NIS2 as part of their legislation[17]. The then Minister of Entrepreneurship and Information Technology, Urve Palo, mentioned in the first reading of the cybersecurity Bill in the parliament:

> "First of all, with this law, we will transfer the European Network and Information Security Directive to the Estonian legal space. To be honest, in Estonia, it is not necessary to do much for this in itself, *because the principles and requirements of the directive have largely been guaranteed in the past, although they have been scattered in different legislation. Such dispersion has sometimes caused confusion about how exactly to act in a cyber threat situation and resolve incidents*."
>
> (Cybersecurity Bill, 15. 03. 2018, Parliament Debate).

There were opposite groups against some elements of this Bill, like the 'The Estonian Information Technology and Telecommunications Union' (ITL), where in the proposal they mentioned that "ITL believes that it is misleading to refer to this Bill as the Cyber Security Act (…) the draft primarily concerns the transposition and supervision measures of the NIS Directive" (Parliament Debate: Draft Cybersecurity Act to the explanatory memorandum[29]).

On the opposite side, in the case of Chile, it didn't have to use NIS 2, but they took it into consideration multiple times by different congressmen and congresswomen. For instance,

[28] More information can be found in the European Parliament at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[29] More information can be found in the Parliament debate, Bill of Cyber Security Act 597 SE, in: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/kuberturvalisuse-seadus%20%20(CS%20Estonia%20Parliament%20Debate,%20Pos.%202)

in the discussion in the Chilean Congress, NIS 2 is repeatedly mentioned by different politicians, making statements like:

- "The European directive NIS2 has been taken into account" (Daniel Álvarez, N° 874. Second report of the Committees on National Defense and Public Safety)[30].
- "(...) includes the requirements foreseen in comparative experience. Specifically, he stated, the standard of the European Union's NIS2 Directive and the Belgian one; the practices recently incorporated in Israel, and the reforms introduced in the Dominican legislation" (the Government, N° 2180, Committees on National Defense and Public Safety)[31].
- "suggested by the group of advisors formed to accelerate the processing of this law initiative will transform Chile into a proactive country in cybersecurity, since it includes the European directive NIS2" (Senator Pugh, N° 2197, Second report of the of the committees on national defense and public safety, 2023[32]).

5.3.7 'Policy transfer and diffusion': International influences

Another difference is in the same category of 'Policy transfer and diffusion' subcategory of 'international influences'. This time is about the law itself; both are called "cybersecurity law", but the core of it is different. The Estonian case was to put in their national law the statement of the NIS 2. However, some said that "*It is therefore misleading to call it a cybersecurity law. The title of the Act should reflect the content of the Act."* (Parliament Debate: Draft Cybersecurity Act to the explanatory memorandum[33]). In the documents that were analysed for this research, it does not appear other countries as examples. However, in the interview with the recording secretary of the cybersecurity law (P5) mentioned that in the analysis that was done in the pre-parliamentary discussion, when they were drafting, it appeared the comparison with

[30] The original text is in Spanish; it was translated using DeepL: "se ha tenido a la vista la directiva europea NIS2". Daniel Álvarez it's the National Cybersecurity Coordinator [Coordinador Nacional de Ciberseguridad].
[31] The original text is is in spanish, it was translated using DeepL: "(...) recoge las exigencias previstas en la experiencia comparada. Concretamente, enunció, el estándar de la Directiva NIS2, de la Unión Europea, y el belga; las prácticas incorporadas recientemente en Israel, y las reformas introducidas en la legislación dominicana".
[32] The original name is "segundo informe de las comisiones de defensa nacional y de seguridad pública unidas". The translation is based on Deepl.
[33] More information can be found in the Parliament debate, Bill of Cyber Security Act 597 SE, in: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/kuberturvalisuse-seadus%20%20(CS%20Estonia%20Parliament%20Debate,%20Pos.%202)

different countries. So, it is possible that there has been some influence from other countries, but it is not known what was taken from these countries and which countries were considered.

5.3.8 Window of Opportunity in Estonia and Chile

Another similar element in both countries is the category of 'Window of opportunity'. In the case of Estonia, with the cybersecurity attack of 2007 and with the relations between Russia and Estonia during all these years, it would have been expected that a Window of opportunity for creating or changing a cybersecurity law in Estonia would have appeared, but it did not. In the case of Chile could have had (new) opportunities in this category, taking into consideration that they recently have had some cyberattacks; especially worry were those in the Public Sector: in the National Consumer Service in August 2022, the Judicial Power in September 2022, the Minister of Defence in 2023, and others. They were mentioned lightly one time in the discussion in the Chilean Congress. However, in the interview of the parliamentary assistant to a senator in Chile (P2), mentioned that there were rumours that the Executive wanted to get out of this law quickly, not only because of the agreement it had with the opposition in the Senate for the approval of another law, but also because of the embarrassment that the Executive had suffered with the cyber-attack on the Minister of Defense[34].

It is interesting that the Chilean study mentions Russia, Ukraine, and Estonian cases just as an opportunity to learn or to take things into consideration, but they were not used as a 'window of opportunity'.

5.4 Comparison, analysis and propositions

This section discusses the differences and similarities in outcomes with the concepts of the Policy Convergence Theory and Punctuated Equilibrium Theory in Chile and Estonia. In addition, recognising likely or plausible patterns that one can identify between the concepts derived from the analysis and the outcomes.

In the first case of similarities, using the category of "Policy transfer and diffusion" (under the subcategory of "international influences"), taking the example of NIS2, it can be said the following. Policy Convergence theory can highlight the internal and external factors

[34] It is important to consider how the creation of laws works in the Chilean context, as well as how the political forces work and how a balance is created with the executive power.

that contribute to implementing policies across different regions or countries. For this category, the elements of Policy diffusion and policy transfer mechanisms are part of it; how policies spread across borders and transfer between countries make the PCT theory very alive. Just as a reminder the elements of this theory are: emulation, harmonization, epistemic community and penetration. Being part of NIS 2 for Estonia was mandatory, but for Chile it was not, but in the discussion, it was considered to implement a foreign directive into Chilean law. Behind that, there is not only an international organisation, but also the participation of an epistemological community that could be accessed. The harmonization and penetration/diffusion elements are not so clear; however, the diffusion of that policy is a reality. In this case, it can be seen that external actors, such as international organizations, advocate for policy convergence in Chile and Estonia.
The elements of the Punctuated Equilibrium theory for this case are not visible; there are no punctuations in either case. If we go by each element of PET, we can see in the Chilean case some of them: the frame is used by the government and the legislature, as well as the agenda setting. The cases of cybersecurity in the Chilean case could have made this theory very valid, but it did not appear in the legislature debate. In another aspect, there is no venue shift or any other element as expected with this theory.
Therefore, in this case, it can identify patterns of both theories; however, PET elements are clearly more diffuse.

In the case of differences, the category of 'learning and adapting' is seen through the example of the NIS 2 directive it can be found some reasonable elements of policy convergence theory. There is emulation, a copy of a policy (directive), beyond the fact that it was compulsory in one case, and in another, it was optional. To create this directive, the EU already had a network between the countries; therefore, an epistemic community can be found. The other two elements of the PCT, harmonization and penetration/diffusion, can be found in the Estonian case. Harmonization is about ensuring the implementation of a policy; this case is very clear in the Estonian case. In the diffusion by external actors, it is the same. The EU had an impact on the creation of a policy in Estonia. For Chile, these two elements are not present; there was no harmonization nor penetration/diffusion. It is identifiable that there is an impact of outsider(s) actor(s) and interests on the formulation of the Chilean national domestic policy, but there was no dependence on others to carry it.

The elements of Punctuated Equilibrium Theory were present in none of the cases; there was no ‘punctuation’, and there was not a specific moment in time that created a shift in the narrative that framed the topic or created a change in the agenda setting, policy monopoly or venue shift. This theory is about stability and incrementalism in time, but there are short periods that create changes in different policy areas. Those in both countries are not clearly seen. Thus, it can be said that PET elements are not presented in this case.

Another example of the differences, under the category of ‘policy transfer and diffusion’, explicitly in the subcategory of ‘international influences’, is the creation of the cybersecurity law itself. There are elements of both theories. PCT is visible in the Estonian case because they needed to have that law in their legislation, it was mandatory for them. Therefore, there were external pressures to adopt it, leading to a convergence of policies across borders in Europe. The other elements are networking, which is part of it, and harmonization, which can be seen in how put the directive into consideration in an effective way. Lastly, the case of penetration/diffusion by an external actor (EU) refers to the impact that this outsider had, which was very big (again, it was mandatory for every EU country).

In the case of Chile, there are elements of emulation, such as copying successful policies of other countries; those are mentioned by different representatives in the legislative debate. There was networking of experts, but coordinated by the advisors of the politicians. About the elements of harmonization or penetration/diffusion by external actors in this case were not seen.

In the case of Punctuated Equilibrium Theory, it should explain why some sudden shifts create policy change, but it was not present in the Estonian example. In the Chilean case, framing was unclear, but the ‘agenda-setting’ is blurred. The other elements of this theory were not present.

Then the next difference is in the ‘Dynamic Nature of Policy’ category, over the sub-category of 'Political Factors' in both countries. In the Estonian case, PCT is present. There is emulation; they needed to ‘copy’ the directive into their law. The networking is not as clear as the other elements. About Harmonization, it can be seen in the

implementation of it was guaranteed; they had a datum that they could not pass[35]. Considering that penetration/diffusion is about outsider actors and interest in formulating that law, it is very present in the Estonian case. In the case of Chile, emulation can be found, but as learning cases. Other elements of PCT are not found.

The case of PET in Estonia can be found through the element of agenda setting. It was imposed on the parliament to discuss this law because of the grip that the EU has. Anything else is not visible. The Chilean case has almost no element of this theory. Maybe the Agenda setting, because it was in the agenda of legislation in the Congress, but that is part of the legislation, therefore is not a clear aspect. Political factors are part of it, but it cannot be said that those factors are what pressured this bill.

[35] As is stated by the web page of NIS2, the deadline for the Member States to adopt and publish the measures necessary to comply with the NIS 2 Directive is by 17 October 2024. "They shall apply those measures from 18 October 2024". For more information, see: https://www.nis-2-directive.com/.

Chapter 6: Conclusion, limitation and future research

6.1 Introduction: A recap of the research journey

In this chapter, the research question: "What are the similarities and differences in cybersecurity policies between Chile and Estonia? How can these patterns be explained by Policy Convergence Theory and Punctuated Equilibrium Theory?" It will be answered in the following pages. This study aimed to achieve two primary goals. First, a contribution was pursued to the existing academic literature on policy learning and diffusion in two contrasting countries by applying the aforementioned theoretical frameworks (theories). Second, an effort was made to offer practical insights by examining the potential convergence (or divergence) of cybersecurity policies across nations through the lens of overlapping theories. First, based on the line of reasoning set out in the previous chapters, the research objectives will be addressed, and the research question will be answered. Furthermore, the contribution to the existing literature on cybersecurity policy and cybersecurity policy learning and transfer will occur by proposing two propositions based on the empirical analyses of cybersecurity policy-making in Chile and Estonia. The chapter will end with recommendations for further research and an epilogue.

The methodology and tools used to achieve these objectives, as a primary source of data, were the parliamentary debates from both Chile and Estonia. A qualitative coding approach was adopted to analyse the debates within the Policy Convergence Theory and Punctuated Equilibrium Theory framework. A detailed analysis of these debates was presented in Chapter Five. In order to address certain limitations of the methodology, interviews were also conducted to provide a different perspective to that provided by the parliamentary debate.

6.2 Limitations and future research

The contrasting nature of Chile and Estonia allows the researcher to examine how far convergence in cybersecurity policy exists despite their differences. It can analyse factors driving convergence, such as international norms, best practices, and external pressures. Additionally, areas where Policy Convergence Theory diverges can be explored, reflecting national priorities and contexts. Conversely, through Punctuated Equilibrium Theory, a comparison can be drawn between the specificities of each country's approach,

with particular attention paid to the focus on stakeholders. Furthermore, an investigation can be conducted to determine whether the emphasis placed on the "burst" of this theory has any impact on policy changes. However, in connection with the theoretical framework, there are some limitations.

While convergence theory and punctuated equilibrium theory offer valuable insights, it's essential to acknowledge their limitations when analysing cybersecurity policies. PCT could oversimplify complex policy processes by neglecting the complicated and multilayer nature of domestic political dynamics and historical contexts that can lead to variations in policy implementation. One limitation of the Punctuated Equilibrium theory is that it is difficult for a generalisation because PET emphasises localised dynamics and specific events across different national contexts and policy arenas.

In terms of boundaries within the qualitative approach, various elements can be found. First, assigning codes and categories to sections of texts remains, to a degree, subjective. The subjectivity in the coding, despite the efforts to establish a clear path for coding categories, is always a degree that can make discrepancies from one analysis to another. The researcher established the codes; therefore, there is subjectivity there too. Hence, there is a limit to the replicability of the study. Another element is that there is a limited contextual understanding of what happened that is not written; there are non-verbal cues (or irony) to body language surrounding the debate that were not present. Therefore, the aim was to be as open as possible about the data collection method and how the coding was formed. In order to address these limitations and the bias that could be present, there were interviews with different people that were part of the parliament discussion and/or are experts in the realms of cybersecurity laws. This helped not only in addressing these limitations, but also in providing useful information to answer the research question of this paper.

6.3 Conclusion

This study aimed to identify similarities and differences between cybersecurity policies in Estonia and Chile using punctuated equilibrium theory and convergence theory as theoretical foundations, more specifically as conceptual lenses. Based on the analyses that were presented in Chapter Five, the following similarities can be identified: international organizations were important in both cases. Policy transfer and diffusion appear in the

international influences. Also, PCT elements were present in Chile and Estonia. The category of Window of opportunities and external shocks were (almost) not visible.
Additionally, the following differences could be identified: 'learning and adaptation' were present in both countries, but the Estonian case was not identifiable through the parliamentary debate but through one interview. It was present, but very shortly, the sub category of 'Dynamic Nature of policy' in the case of Chile, but in Estonian parliamentary debate was not found. As an explanation, the following two propositions could be derived from the empirical analysis.

The first proposition is about *Convergence over punctuations*. Despite institutional and historical differences between Chile and Estonia, critical events can be identified, however those critical events in both countries did not trigger significant policy changes in the parliament debate. The policy change of both countries may converge in some elements when international institutions, such as the European Union consider them. The countries that are part of the EU are obligated to comply with specific directives, which is not the case for Chile, but as an international institution, the EU is very highly esteemed. However, the results of this research cannot indicate whether the punctuations shape national cybersecurity policies and how much they change.
The findings suggest a stronger influence of PCT compared to PET. Despite historical and institutional differences, both countries tended to converge on certain cybersecurity policy elements when influenced by international institutions like the European Union (EU). This highlights the persuasive power of external pressures from powerful actors in driving policy alignment.

Continuing with the above idea, it can be said that policy convergence directly affects countries that have international communities, like the EU. Yet, other countries follow those policies even when it is not mandatory for them. Making convergence in those countries that are obligated and those who are not. Therefore, when the adoption of cybersecurity policies are implemented, it can be through convergence, but it is not clear if PET play a role, too. This thesis emphasizes the intricate relationship between internal and external factors shaping legislative evolution in cybersecurity. Convergence theory highlights how external pressures, such as directives from powerful entities like the EU, can nudge domestic actors towards alignment. Conversely, punctuated equilibrium theory emphasizes how critical junctures, like cyberattacks, can create windows for rapid policy

shifts, however this was not the case. The impact of these forces hinges on their nature. External pressures from powerful actors can be highly influential, while internal consensus-building among state powers requires negotiation and compromise to achieve optimal outcomes.

The second proposition is that a nation's cybersecurity policy learning *is more likely to be influenced by supranational governance structures than by domestic responses to particular events*. The research suggests that supranational governance structures may exert greater influence on a nation's cybersecurity policy learning compared to domestic responses to specific events (partially contradicting PET). While critical events like cyberattacks can trigger policy discussions, they didn't necessarily lead to significant policy shifts in either country. It is important to acknowledge that there are gradation of Policy Convergence, convergence isn't absolute. The research doesn't definitively establish whether PET plays a role in convergence beyond external pressures. However, it does suggest that convergence can occur even in countries not formally bound by international directives like the EU.

The trajectory of legislative development within the cybersecurity domain is intricately moulded by a multifaceted interplay of internal and external dynamics, as highlighted by the intersection of Policy Convergence and Punctuated Equilibrium theories. The extent to which these factors exercise influence varies depending upon the nature of external pressures, such as directives from supranational bodies like the EU, and the internal dynamics of state governance, where achieving consensus among diverse branches of authority is pivotal for realising optimal outcomes in this critical sphere. To clarify, Policy Convergence suggests that external pressures, notably from international organisations, prompt countries within these frameworks to emulate, harmonize, and adopt external elements, thus exerting considerable influence over domestic actors. Consequently, these influential actors often steer parliamentary deliberations towards alignment, facilitating constructive discourse on the ultimate goals of state action. Conversely, while Punctuated Equilibrium theory posits that critical junctures, such as cyberattacks or political upheavals, can precipitate swift policy shifts, such instances are notably scarce in these contexts.

Lastly, the imperative of internal consensus-building among state powers remains consistent across both countries, necessitating adept negotiation and compromise to navigate cybersecurity policy complexities effectively. Thus, the question arises for future research: Does this conclusion change using MSSD or MDSD? Is there a differentiation between approval or rejection by political parties to the cybersecurity law? Can parliamentary debates assume precedence in such scenarios? Or the focus can change more into the notions of isomorphism, policy transfer and learning that may or may not be happening at various levels of abstraction: (1) at the level of policy formulation, (2) at the level of policy implementation, and (3) at the level of more specific technicalities of cybersecurity.

6.3 Epilogue

At the end of the thesis, there is reason not only to sum up the findings but also to reflect on the learning process. Below, some observations of my own journey are described in such a way future Master's students may benefit from these experiences. I will not take into consideration the typical – and important! – parts, such as having a research question, objectives, methodology, and method, and all those elements that are known to make a thesis. For most people, I don't think this is easy, but it is doable. All these elements are based on my experience. I hope it can help a little.

First, organisation is everything. Organise your weeks from the starting point of writing your thesis until the day that you submit it. If you know if you are going to travel, celebrate birthdays, etc. Put that into the schedule, too. It will help you to organise your free time and your thesis time. Don't think that months in advance is a lot of time, it is not. I organised myself, after already having the research question, objectives and all that, nearly four months in advance. Almost the last month, I was very ill; for two weeks, I couldn't make any progress, and the following weeks, I didn't feel 100%. If it wasn't for the fact that I organised myself and that my supervisors demanded a lot from me in the first month, I wouldn't have made it.

Second, supervisor(s). When you know who is going to be your supervisor, be transparent about your struggles and what you are good or at least, you don't struggle too much. After that, organise with she/he/them when and how the feedback is going to be. Being transparent from day one with your supervisor will help you know each other's boundaries

and expectations. If you don’t understand a feedback or you still struggle with something, ask! I’m an introvert, so this was hard for me. Obviously, you need to find for yourself most of the time, but when you put in time and effort and still struggle, just ask.

Third, something my supervisor told me, and it was very nice advice for me, is that if you are stuck with one part of the thesis, it is ok! Go to another part, there is always something to write about: to create, to improve, to make it better, etc. Some days you are going to feel that you are not going to succeed, do not despair. Breath. Another advice, is you can organise with pomodoro technique or others, it is useful.

Lastly, have fun and hopefully do some sports. Do some excercising, it’s important for your health and your mind. You can gather with your friends to write the thesis or just to have fun. I had heard that there are people who feel lonely when they write their thesis. I did not feel isolated writing it, but I was lucky enough that my acquaintances and friends wanted to meet to write the thesis or just to have fun. Another good aspect about that is that you can ask them or your family to read your thesis, which is a good way to see if others understand what you are trying to write.
Good luck!

List of References

Achavar Barrios, V. (2018). *Política Nacional de Ciberseguridad: 2017-2022*.

Antantic council 2012.pdf. (n.d.).

Auerbach, C. F., & Silverstein, L. B. (2003). *Qualitative data: An introduction to coding and analysis*. New York University Press.

Baraona González, J. (2010). La cultura jurídica chilena: Apuntes históricos, tendencias y desafíos. *Revista de Derecho (Valparaíso)*, *35*, 427–448. https://doi.org/10.4067/S0718-68512010000200013

Baumgartner, F. R., Jones, B. D., & Mortensen, P. B. (2006a). Part III. Punctuated Equilibrium Theory: Explaining Stability and Change in Public Policymaking. In C. M. Weible & P. A. Sabatier (Eds.), *Theories of the Policy Process* (4th ed., pp. 55–101). Routledge. https://doi.org/10.4324/9780429494284-3

Baumgartner, F. R., Jones, B. D., & Mortensen, P. B. (2006b). Punctuated Equilibrium Theory: Explaining Stability and Change in Public Policymaking. In C. M. Weible & P. A. Sabatier (Eds.), *Theories of the Policy Process* (4th ed., pp. 55–101). Routledge. https://doi.org/10.4324/9780429494284-3

Baumgartner, F. R., Jones, B. D., & Wilkerson, J. (2011). Comparative Studies of Policy Dynamics. *Comparative Political Studies*, *44*(8), 947–972. https://doi.org/10.1177/0010414011405160

Bennett, C. J. (1991). What Is Policy Convergence and What Causes It? *British Journal of Political Science*, *21*(2), 215–233. https://doi.org/10.1017/S0007123400006116

Blatter, J., & Haverland, M. (2012). *Designing Case Studies*. Palgrave Macmillan UK. https://doi.org/10.1057/9781137016669

Blatter, J., Portmann, L., & Rausis, F. (2022). Theorizing policy diffusion: From a patchy set of mechanisms to a paradigmatic typology. *Journal of European Public Policy*, *29*(6), 805–825. https://doi.org/10.1080/13501763.2021.1892801

Blee, K. M., & Taylor, V. (2002). Social Movements, Protest, and Contention. In B. Klandermans & S. Staggenborg (Eds.), *Methods of Social Movement Research* (pp. 92-117.). University of Minnesota Press.

Bukve, O. (2019). *Designing Social Science Research*. Springer International Publishing. https://doi.org/10.1007/978-3-030-03979-0

Cairney, P. (Ed.). (2012). *Understanding Public Policy: Theories and Issues* (2nd ed.). Palgrave Macmillan. https://paulcairney.files.wordpress.com/2020/01/cairney-2nd-proof-combined.pdf

Capano, G., & Howlett, M. (2009). Introduction: The Determinants of Policy Change: Advancing the Debate. *Routledge*, *11*(1), 1–5. https://doi.org/10.1080/13876980802648227

CCDCOE. (n.d.). The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/about-us/

cisa. (2023, May 7). *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA*. Cybersecurity Infrastructure Security Agency. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Clark, D., Berson, T., & Lin, H. S. (Eds.). (2014). *AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY*. National Academies Press (US). https://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-20150303-SD006.pdf

Cybersecurity Trends & Statistics For 2023; What You Need To Know. (2023, March 5). Forbes. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *Cooperative Cyber Defence Centre of Excellence or NATO*, 8.

Dogaru, C. (2018). *CHANGE AND PUBLIC POLICY: A MUTUAL DEPENDENCY RELATIONSHIP*. *14*, 10.

Drezner, D. W. (2001). Globalization and Policy Convergence. *International Studies Review*, *3*(1), 53–78.

Ellis, R., & Mohan, V. K. (Eds.). (2019). *Rewired cybersecurity governance* (First edition). Wiley.

European Parliament. (2017, September). *Parliamentary question | Answer to Question No E-003340/17 | E-003340/2017(ASW) | European Parliament*. Parliamentary Question. https://www.europarl.europa.eu/doceo/document/E-8-2017-003340-ASW_EN.html

Falconer, R. (2021, May 10). *Emergency declaration issued in 17 states and D.C. over fuel pipeline cyberattack*. Axios. https://www.axios.com/2021/05/10/fuel-pipeline-cyberattack-us-state-of-emergency

Flowers, A., Zeadally, S., & Murray, A. (2013). Cybersecurity and US Legislative Efforts to address Cybercrime. *Journal of Homeland Security and Emergency Management*, *10*(1). https://doi.org/10.1515/jhsem-2012-0007

GCSG. (2019). *CyberSecurity_Governance_ENG_Jan2021_0.pdf* (Cybersecurity Guide to Good Governance in Cybersecurity; p. 100). Geneve Centre for Security Governance.

Gibbs, G. (2007). *Analyzing Qualitative Data*. SAGE Publications, Ltd. https://doi.org/10.4135/9781849208574

Gonzalez, G., Lafebvre, B., & Geller, E. (2021, August 5). *'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack—POLITICO*. Politico. https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984

Grzegorzewski, M., Smith, M., & Koven, B. (n.d.). *Civil Cyber Defense – A New Model for Cyber Civic Engagement*.

Günter, C. (2012). *An Evaluation of State—Level Strategies Against Botnets in the Context of Cyber Conflicts* [PhD]. Estonian Business School.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Holzinger, K., & Knill, C. (2005). Causes and conditions of cross-national policy convergence. *Journal of European Public Policy*, *12*(5), 775–796. https://doi.org/10.1080/13501760500161357

Howlett, M., & Cashore, B. (2014). Conceptualizing Public Policy. In *Comparative Policy Studies: Conceptual and Methodological Challenges*.

Jolicoeur, M. M. (2018). An Introduction to Punctuated Equilibrium: A Model for Understanding Stability and Dramatic Change in Public Policies. *Québec*. https://www.ncchpp.ca/docs/2018_ProcessPP_Intro_PunctuatedEquilibrium_EN.pdf

Kaska, K., Talihärm, A.-M., & Tikk, E. (2010). *Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007*.

Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). *The effect of encryption on lawful access to communications and data*. Center for Strategic & International Studies ; Rowman & Littlefield.

Lewis, T. G., Mackin, T. J., & Darken, R. (2011). Critical Infrastructure as Complex Emergent Systems: *International Journal of Cyber Warfare and Terrorism*, *1*(1), 1–12. https://doi.org/10.4018/ijcwt.2011010101

Ley de Ciberseguridad, Publicación En El Diario Oficial de Chile. https://ciberseguridad.gob.cl/noticias/ley-marco-de-ciberseguridad-es-publicada-en-el-diario-oficial/

Marsh, D., & Sharman, J. C. (2009). Policy diffusion and policy transfer. *Policy Studies*, *30*(3), 269–288. https://doi.org/10.1080/01442870902863851

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 35. https://doi.org/10.3390/s22020538

Mosley, L. (2013). Introduction. "Just Talk to People"? Interviews in Contemporary Political Science. In *Interview Research in Political Science* (pp. 1–28). https://doi.org/10.7591/9780801467974-003

Moyson, S., Scholten, P., & Weible, C. M. (2017). Policy learning and policy change: Theorizing their relations from different perspectives. *Policy and Society*, *36*(2), 161–177. https://doi.org/10.1080/14494035.2017.1331879

NATO. (2023, September 14). *Cyber defence*. NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches* (Vol. 30).

NHE. (2018, October). *WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled | UK Healthcare News*. National Health Executive. https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Inf. *Ccdcoe*.

Pernik—Cyber deterrence A case study on Estonia's polici.pdf. (n.d.). Retrieved 2 February 2024, from https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf

Plümper, T., & Schneider, C. J. (2009). The analysis of policy convergence, or: How to chase a black cat in a dark room. *Journal of European Public Policy*, *16*(7), 990–1011. https://doi.org/10.1080/13501760903226724

Pollitt, C., Van Thiel, S., & Homburg, V. (Eds.). (2007). *New Public Management in Europe*. Palgrave Macmillan UK. https://doi.org/10.1057/9780230625365

Popp, T. R. (2021). Explaining Policy Convergence and Divergence through Policy Paradigm Shifts: A Comparative Analysis of Agricultural Risk Governance in OECD Countries. *Journal of Comparative Policy Analysis: Research and Practice*, *23*(3), 310–327. https://doi.org/10.1080/13876988.2019.1674623

RIA. (n.d.). *Cyber defence of critical infrastructure.* https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure/cyber-defence-critical-infrastructure

Ross, C. (2003). 7 Federalism and political asymmetry: Executive versus legislative power. In *7 Federalism and political asymmetry: Executive versus legislative power* (pp. 122–136). Manchester University Press. https://doi.org/10.7765/9781526120762.00011

Saldaña, J. (2014). Coding and Analysis Strategies. In P. Leavy (Ed.), *The Oxford Handbook of Qualitative Research* (pp. 580–598). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199811755.013.001

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3E [Third edition]). SAGE.

Schuetze, J. (2020). *EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals.* https://eucyberdirect.eu/research/eu-us-cybersecurity-policy-coming-together-recommendations-for-instruments-to-accomplish-joint-strategic-goals

Shively, J. (2022). *Cybersecurity Policy, Punctuated Equilibrium Theory, and the Biden Administration* [Preprint]. Politics and International Relations. https://doi.org/10.33774/apsa-2022-rcn85

True, J., Jones, B., & Baumgartner, F. (2007). Chapter 6: Punctuated-equilibrium theory: Explaining stability and change in public policymaking. In P. Sabatier (Ed.), *Theories of the policy process* (pp. 155–187).

Tyler, S., Swanson, D. A., Venema, H., Barg, S., Tyler, S., Drexhage, Bhadwal, S., Tomar, S., Nair, S., & Kelkar, U. (n.d.). Adaptive Policies Meeting the Policymakers Challenge in Today's Complex, Dynamic and Uncertain World. *International Institute for Sustainable Developmen*. Retrieved 25 March 2024, from https://www.academia.edu/14881142/Adaptive_Policies_Meeting_the_Policyma

kers_Challenge_in_Todays_Complex_Dynamic_and_Uncertain_World?auto=download

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE. *Journal of Security and Sustainability Issues*, *9*(3), 775–784. https://doi.org/10.9770/jssi.2020.9.3(4)

White House. (2021, 05). *Executive Order on Improving the Nation's Cybersecurity | The White House*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Whitehouse. (2023, March). *National-Cybersecurity-Strategy-2023.pdf*. National Cybersecurity Strategy 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Witt, N. H. (2013). *Coding: An Overview and Guide to Qualitative Data Analysis for Integral Researchers*. *1*.

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995

List of Appendices:

Appendix 1: Summary of the formation of the Cybersecurity law in Chile.

Date	sub-phase	Phase	Comments
15/03/2022 to 26/04/2023	Start of the Bill.	First constitutional procedure in the Senate. (As is presented by the executive – the President –, can choose in which chamber can start).	Among the other committees that studied this proposal were: the Public Security and Defence Committee, the Finance Committee and others.
08/05/2023	Project account. Passes to the Committee on Public Safety, and to the Finance Committee as appropriate.	Second constitutional procedure in the Chamber of Deputies.	Second constitutional procedure
12/12/2023 to the 14/12/2023	General discussion. Adopted in general and in particular with amendments in the Deputies chamber.	Third constitutional procedure in the Chamber of Senate.	On these dates, it passes through one Office Document of the President of the Republic where it promotes indications to the project (of the deputies), it is part of a complementary financial report, again it is part of the Finance Commission, among others.
21/03/2024	Bill to the Executive (Presidential Office).	Proceedings finalised in the Chamber of Origin (Senate).	Finalization of procedure in the Chamber of Senate.
01/04/2024	Account in the Revising Chamber of the Constitutional Court, by means of which it sends an authorised copy of the judgement of control of constitutionality referring to the project.	Senate and Presidential approval procedure.	If it is accepted in the Constitutional Tribunal, it is sent to the President of the Republic to be signed and published in the Official Journal of the Republic of Chile.

Source: table created for this document, based on information provided on the Senate's website, 2024.

Appendix 2: Letter of consent

This document sent by email to each interviewee. They all sent it back signed after the interview.

CONSENT FORM

Dear____,

Please allow me to introduce myself. I'm Catalina Mendoza Schmitz, a student at the University of Tartu's Johan Skytte Institute of Political Studies in the Master of "Politics and Governance in the Digital Age" 2022-2024.

As part of my research, I would greatly appreciate the opportunity to interview you, given your position and political experience. I know your heavy workload. Nevertheless, I assure you that this interview will be as short as possible and will be of invaluable help to my research. The overarching research question of my thesis is: What are the similarities and differences in cybersecurity policies in Chile and Estonia? How can these similarities and differences be explained?

If you would like to know anything more about me and/or my research, please do not hesitate to ask, and I would be happy to provide more information.

With best regards,
Catalina

Informed And Voluntary Consent

I have been told about the purpose and topic of the interview and how my responses will be used.
I have been able to ask questions about the interview, and they have been answered.
I understand that any attributed quotes from the interview will only be used for the purposes of published academic work. If you want to have an interview anonymously, I understand that quotes will be attributed to a party source familiar with the situation.
I understand that I am not required to answer any of the questions, and I can withdraw from the interview at any time.
I agree to participate in this interview and to have it digitally recorded.

Name: (print name) _____

Signature: _____ Date:

Appendix 3: Interview guide and some questions

Introduction

- Introduction of who I'm, my university and my Research Question.

[Thank them for participating]

- Asked them if I can record this meeting.

[Thank them for -whatever decision they take-]

The questions:

- "Why the cybersecurity law was created now"? "Why now"?
- "What do you thing about the law"? "What did you (not) like about the new cybersecurity law?"
- "Was anything discussed in the parliament debate that was left behind in the final bill?"
- "Were some countries used as examples? Why them?"
- About the coordination with the civil organization, did they get involved somehow? Or how did RIA in this case organize with these rural areas? How was that process?

Questions that came up in the interviews:

- Why do you think that, what was different between those acts (regulation that was not created by the parliament) and the law created in 2018? [Discussing about the law and the acts, in the case of Estonia, and about the cybersecurity strategies in both countries].
- Did something change in a notorious way after the creation of the cybersecurity law?
- Why do you think it didn't make compulsory? What was the hard part of it?
- Estonia had a more informal approach for the framework in cybersecurity, why do you think it was this way? In case of Chile, the question that was similar was "why it was necessary to create a law, regulations, etc. instead to do something like Estonia"?
- In case of Ria and the organization with the civil society: how did RIA in this case organize with these rural areas? How was that process?

- Chile has now a cybersecurity law, but without the regulation on paper, is almost as it does not exist, “what do you think about that?”
- In the Chilean case, Do you think this law will help for the education of the society? [Having in mind the Tiger Leap Program]
- “Do you think that the cybersecurity law has an Estonian/Chilean style? Something that is characteristic of it?”
- What change did the political advisors do? What about the organization of this law?

Conclusion

- Is there anything else you want to say to me?

Thank them for their participation.

Appendix 4: Information of the interviewees

Name	**Country**	**Date of the interview**	**What did they do?**	**About them.**
(Participant 1) (P1)	Chile	18.04.24	Lawyer. Participated as a private individual in the parliamentary debate (she was already known in the Congress as someone that knows about Cybersecurity). She is part right now in the legislative debate in the National Congress about the bill of Protection Data.	For years she has worked in topics like cybersecurity, personal data, etc.
(P2)	Chile	22.04.24	Engineer. Parliamentary assistant of Senator Pugh.	He was one of the organizors of the legislative debate in cybersecurity law in Chile.
(P3)	Estonia	18.04.24	Worked in the area of cybersecurity, digital government, etc. in Estonia.	Her thesis was about elements of cybersecurity too, but she did not engage in aspect of the law itself.
(P4)	Estonia	29.04.24	He works in RIA.	He is part of RIA. He has been since before the cybersecurity law. Therefore, he knew that there was a debate. The NIS2 Directive maked

				some modification to that organization too. He what changed.
(P5).	Estonia	10.05.2024	Was the Protokollija (recording secretary) of the then bill of cybersecurity in the estonian parliament.	She now works in the Ministry of Defense in Estonia.