TARTU UNIVERSITY

Faculty of Social Sciences

Johan Skytte Institute of Political Studies

Anna Kuus

The Emergence of Cyber Security as a National Security Policy Concern in NATO Member States

MA thesis

Supervisors: Thomas Michael Linsenmaier, Logan Emily Carmichael

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: 25468 words

Anna Kuus, 20/05/2024

Non-exclusive license to reproduce thesis and make thesis public

I, Anna Kuus, herewith grant the University of Tartu a free permit (non-exclusive license) to the work created by me, "The Emergence of Cyber Security as a National Security Policy Concern in NATO Member States", supervised by Thomas Michael Linsenmaier and Logan Emily Carmichael,

- 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 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 license does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Table of contents:

Table of contents 3

Abstract 5

Introduction 6

1. Theoretical framework: the emergence of cybersecurity as a policy concern 10

1.1 Emergence of policy concerns 12

1.2 Cybersecurity as a policy concern 15

1.2.1 Policy and norm diffusion as a mechanism 17

1.2.2 Economic factors 19

1.2.3 External events and crises 20

1.2.4 Innovations in science, technology and engineering 22

1.3 Summary 23

2. Methodology 25

3. Case selection 27

3.1 Operationalization of variables 33

4. Empirical data and sources 35

5. Analysis. Explaining the emergence of cybersecurity as a policy concern across NATO member states: the cases of Canada, Croatia, and Lithuania 38

5.1 Case 1: Croatia – the emergence of cybersecurity concern 38

5.2 Case 2: Lithuania – the emergence of cybersecurity concern 40

5.3 Case 3: Canada – the emergence of cybersecurity concern 44

6. Analysis: findings from the interviews and NCSSs 46

6.1 Drivers for the emergence of cybersecurity as a policy concern in Croatia 46

6.2 Drivers for the emergence of cybersecurity as a policy concern in Lithuania 50

6.3 Drivers for the emergence of cybersecurity as a policy concern in Canada 56

7. Discussion on the results 63

8. Conclusion 67

References 70

Annex 1 82

Annex 2 83

Glossary 84

Abstract

As everyday technologies progress at a fast pace, new risks and threats evolve for the users and operators of technology. Today, cybersecurity is a common concern for basically all states – however, this has not always been the case. The concern with cybersecurity has emerged gradually over time, with ever more states becoming concerned. Against this background, this study sets out to study the proliferation of cybersecurity as a policy concern among a more narrowly confined group of states, namely NATO member states. Drawing on the literature on cybersecurity, the study identifies at least four factors that might explain the emergence of cybersecurity as a national policy concern. Whereas some explanations, such as norm diffusion and economic considerations have been already studied, explanations such as policy diffusion and innovations in the field of science and technology have not been widely studied. Therefore, the empirical part of the study analyses which of these factors explains the proliferation of cybersecurity as a policy concern. This research traces different factors for policy concern emergence, by applying document analysis on national cybersecurity strategies and conducting interviews with 14 experts and policymakers involved in cybersecurity policy formulation and implementation, including policymakers involved in developing the first national cybersecurity strategies. By assessing the theories of policy change, norm and policy diffusion, this study lists a set of possible causes for policy concern emergence in the field of cybersecurity. The results of this study indicate that the emergence of cybersecurity across three selected states was mostly driven by policy diffusion among states and innovations in the field of science and technology, firstly – if a state has adopted a policy as a result of emerging policy concern in a region or an international organization, then a policy concern emerges in other states; secondly, if a state sees an increase in developments in the field of science and technology, then cybersecurity as a policy concern emerges. This research demonstrates how different aspects and factors for policy formulation are considered and why some considerations are deemed more critical for national security than others.

Introduction

The following research focuses on the proliferation of cybersecurity as a national policy concern across three North Atlantic Treaty Organization (NATO) member states. The field of cybersecurity is not broadly studied in International Relations (IR) and the existing literature mostly concerns the impact of different crises and norm diffusion in the field of cybersecurity (see: Finnemore, Hollis, 2016; Klimburg, 2012; Guitton, 2013; Robinson, Hardy, 2021; Adamson, Homburger, 2019; Homburger 2019; Crandall, Allan, 2015). Against this backdrop, the following research examines three NATO member states and their approaches to cybersecurity, exploring the causes of the emergence of cybersecurity as a policy concern.

The emergence of cybersecurity as a policy concern is reflected by the rise of national cybersecurity strategy implementation - from 2008 until 2018, the number of NATO member states' national cybersecurity strategies (NCSS) has drastically risen, and the agenda of cybersecurity has been formalised across national security strategies. More and more states have adopted a cybersecurity strategy – in 2003 the number of states that had adopted NCSSs was three: the United States, Norway, and Russia (e-Governance Academy, 2023). According to the National Cyber Security Index (e-Governance Academy, 2023), NATO member states have steadily adopted NCSSs since 2008, and as of 2018, the amount of separately adopted and implemented NCSSs in NATO member states rose from three (Estonia, United States, Norway) to 29 (all NATO member states).

The emergence of a policy concern is directly linked to the national cybersecurity strategy formulation, which indicates the emergence of cybersecurity as a policy concern. The proliferation of NCSSs and cybersecurity policies serve as research puzzles because this phenomenon, while indicating shifting concerns by states, has not yet been adequately explained. The observed proliferation of cybersecurity as a policy concern seems to be unrelated to experiencing attacks, as no specific correlation has been illustrated in the former literature. Furthermore, the reach and impact of cyber norms have not been systematically linked to the emergence of cybersecurity as a national policy concern. For example, Finnemore and Hollis (2016: 444) illustrate how cybersecurity norms proscribe or prescribe specific behaviour in the cyber-realm, yet the authors

do not examine their relevance to national policies. In addition, the causes for the emergence of cybersecurity as a policy concern may vary, taking into consideration how states differ regarding dependence on digital services, the extent to which they have experienced cyber-attacks, and resources allocated to the enhancement of cybersecurity, which indicates that states prioritize and perceive cybersecurity differently.

Cyberthreats vary in their extent – some states view it as a threat to their ICT or the public in general and in some cases, the policy implementation may hypothetically be linked to economic reasons, yet many states have not adopted any policies at all. Other authors (see: Klimburg, 2012; Guitton, 2013; Robinson, Hardy, 2021) have made a connection to Estonia's reaction to 2007 cyberattacks during the Bronze Night crisis, which evolved from political violence associated with the removal of the Bronze Soldier monument, implying that this served as a key impetus for the emergence of cybersecurity as a national policy concern. Hypothetically, this factor, among other large-scale cyber incidents, could have impacted the emergence of cybersecurity as a policy concern. However, there is a gap in cybersecurity research, that explains the proliferation of cybersecurity policies among NATO member states from 2008 to 2018, as an indicator of an emerging policy concern. Estonian advocacy could have been decisive in the emergence of cybersecurity as a national security concern among NATO member states, yet the relative importance of these factors in relation to other potentially relevant factors, such as policy and norm diffusion, the emergence of new technologies and economic considerations have not yet been systematically demonstrated.

The probable reasons for the emergence of a policy concern in the field of cybersecurity could be related to several other factors: the growing dependency on information and communication technologies (ICT) and digital services, the emergence of new technologies and innovations in the fields of science and technology, economic considerations and international norms – factors, which will be assessed later in the theoretical part of this research. The economic considerations could be potentially linked to the protection of the national economy, specific economic assets and the enhancement of digital services of a state. In a similar vein, the development of new technologies and platforms could potentially introduce new risks, which need to be mitigated on a national scale both for the users and operators of critical infrastructure. Against this, Crandall and Allan (2015: 347, 353) argue that Estonia, as a small state and a member of NATO, uses norm promotion in

cybersecurity to influence other states to follow suit - this is reflected by the fact that Estonia was the second state in the world after Russia to establish NCSS. Yet, the authors ignore the fact that the US and Norway had established their first NCSSs even earlier – in 2003 (The White House, 2003; Solberg, 2019: i). Other researchers (Tatar, et al. 2014: 215; Azmi, et al., 2016: 7), have listed specific reasons, such as the protection of economy and state services, and protection of critical infrastructure, based on the assessment of why states develop NCSSs, yet they do not explain systematically the factors that have led to the development of the strategies.

Against this backdrop, this study examines the different hypothetical reasons and impetuses for policy concern emergence in the field of cybersecurity, by studying the causes behind national cybersecurity strategy formulation. The objective of this thesis is to examine what factors were at play in the emergence of cybersecurity concerns and to offer explanations on why these policy concerns first emerged. The focus of the following research is to study *what explains the emergence of cybersecurity as a policy concern?* This research therefore assesses the explanations and reasonings behind the emergence of cybersecurity as a security concern, through the approach of policy concern emergence. To answer the research question, this study will base the analysis on the information gathered from the expert interviews and document analysis of the NCSSs. The interviews will be conducted with experts and policymakers, who were involved in the formulation and/or implementation of NCSSs or have extensive knowledge of cybersecurity or national ICT protection in a specific state. To reach the objective of the study, this research further relies on document analysis of the three selected states' NCSSs, which helps to outline the primary objectives and aims of cybersecurity measures and frameworks in each state. The document analysis and interviews help to trace and connect different causes of policy emergence in three states from different regions, that have adopted NCSSs at various times and differ in the degree of cybersecurity capabilities.

To answer the research question, this thesis relies on policy emergence literature and includes concepts such as norm and policy diffusion, to trace possible factors for policy concern emergence in cybersecurity. These strands of literature offer a framework to explore why cybersecurity emerged as a policy concern in the policy agenda of three different states and what factors led to the proliferation of cybersecurity as a policy concern. By outlining the different causes and relying on expert interviews and document analysis, this study, therefore, connects factors that have

contributed to the policy concern emergence and policy implementation in the field of cybersecurity.

This research is based on a comparative study (MDSD) of three different NATO member states. The cases were selected based on their region, cybersecurity capacities and cybersecurity dependency, and the reach of experiences with malicious cyber acts and cyber-attacks. The selected states offer a selection of states that are part of a security alliance but vary in the degree of cybersecurity capacities and threat landscape. A subset of NATO states is selected for this study, as these states are technologically and economically advanced, rely on digital services and allocate resources to cybersecurity capacity-building, indicating the proliferation of cybersecurity as a policy concern. This selection of NATO member states allows to study the causes of the emergence of cybersecurity as a policy concern, while each state differs in the extent to which they have experienced cyber-attacks, how reliant they are on digital services and how geographically distant they are from foreign threats, and the extent to which they have invested in cybersecurity capacity building on a national level. Therefore, these case studies offer insights into the considerations and factors that caused the emergence of cybersecurity as a policy concern.

This study is structured as follows: after the introduction of the study, the first section gives an overview of the theoretical framework of the research, by outlining findings from previous literature and framing the potential causes for policy emergence; the second chapter outlines the research design and methodology of the study and considers the strengths and weaknesses of the chosen research design; the third chapter describes the characteristics for case selection, justifies the selection of the cases of this study, and examines the variables that are applied to this research; the fourth chapter will describe the data of the research and outlines the main sources of the study; the fifth chapter provides an analysis of the policy concern emergence in the field of cybersecurity in three different states; the sixth chapter provides an assessment of the interview responses and NCSSs of each states, examining the hypothetical causes for the emergence of cybersecurity in each state; the seventh chapter concludes the findings of the analysis and compares the findings; the final section sums the findings of the study. Each section includes sub-chapters that will discuss different explanations and topics in more detail.

1. Theoretical framework: the emergence of cybersecurity as a policy concern

This section gives an overview of the theoretical framework of the study. The primary focus of this section is to outline the main causes of policy concern emergence, give an overview of the literature on policy emergence, and outline the main factors that are highlighted as the causes for the emergence of cybersecurity as a policy concern. This section is divided into several sub-chapters, with each covering one cause or factor of policy concern emergence, which will conceptualized and examined in detail. The final sub-section concludes the findings. The theoretical part of this study begins with examining the different concepts of the cybersecurity literature.

As this study focuses on cybersecurity, it is necessary to define the central concepts, that include a variety of terms related to cyberspace and critical infrastructure. In the literature on cybersecurity, there exists a variety of terms that encompass "cyber", "ICT", and "cyberspace", yet these terms often capture rather different meanings. The term "ICT" refers to *information and communication technologies*. Often interconnectedly used is the term critical infrastructure, which is used to refer to a state's physical and non-physical objects and subjects of critical importance (Aradau, 2010: 491) – this involves both physical objects and information and communication systems of the state. The profound variety of concepts of ICT, cyberspace, and digital infrastructure reveals how differently cyber domains are perceived in the cybersecurity literature. Kello's definition of cyberspace includes three main domains of operation:

> (1) the internet, encompassing all interconnected computers, including (2) the world wide web, consisting only of nodes accessible via a URL interface; and (3) a cyber "archipelago" comprising all other computer systems that exist in theoretical seclusion (i.e., not connected to the internet or the web). (Kello, 2013: 17)

This definition entails three main terrains of cyberspace, which are often overlapping and cross-sectoral. In this research, the terms cyberspace and ICT will be used to refer either to a state's communication and information systems (ICT), and to encompass a wider meaning, the term cyberspace is used to refer to the three domains of the internet, and computer systems, including cross-border information systems and the World Wide Web.

The term cybersecurity is used in various contexts to refer either to the protection of a state's, organization's, a specific sector's, or a company's ICT. In this research, the term cybersecurity refers to policies, regulations, directives, and agendas aimed at "the protection of information and communication technologies from unauthorized access or attempted access." (Finnemore, Hollis, 2016: 431). In sum, cybersecurity is defined as the protective measures for cyberspace, as well as for "the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace." (von Solms, van Niekerk, 2013: 101) It is important to distinguish here the terms "information security" and "cybersecurity", which are often used interchangeably – the term information security refers to the protection of information systems, where specifically information resources are stored (von Solms, van Niekerk, 2013: 98). Therefore information security concerns the protection of the data being stored and the technologies and systems where the information is stored. Von Solms and van Niekerk (2013: 97) argue that "cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources but also that of other assets, including the person him/herself." Cybersecurity involves therefore the protection of non-information, as well as information-based assets, the society and its values from potential risks (von Solms, van Niekerk, 2013: 100-101). In conclusion, this study opts for a definition of cybersecurity, which entails the standards, processes, and policies aiming at the protection of three domains of cyberspace and critical infrastructure.

Other key definitions regarding cybersecurity include *cybercrime, cyberattacks, and malicious acts in cyberspace*, which are connected to the changing security landscape and security considerations regarding the emergence of cybersecurity as a policy concern. Scholars often use these terms interchangeably, although the intent and the reach of these acts and events differ. *Cybercrime*, although there exists no distinct and agreed definition on that, includes: "illicit conduct by individuals/groups against computers, computer-related and other devices, information technology networks; or traditional crimes, as well as actions targeting individuals, supported by the use of the Internet and/ or technology." (Donalds, Osei-Bryson, 2019: 403) Similarly, the research by Phillips and others (2022: 391) illustrates how the classifications of illicit cyber acts by different states and institutions differ broadly, and categorisations do not always include the same cyber incidents and acts. A widespread example of this is phishing and spear-phishing –

phishing, which relies heavily on human error, is an attack conducted primarily through communication channels, based on persuasion and "socially engineered messages," with the aim of persuading the victim to carry out a specific task or action, (Khonji, et al., 2013: 2092).

Another concept in cybersecurity literature is *malicious acts and incidents* in cyberspace, which in broad terms refers to illicit actions conducted in or towards ICT systems. In cybersecurity literature, cybercrime is more used in terms of wide-scale attacks towards state institutions or a specific sector, the term malicious act is used to refer to a broad range of small-scale incidents, malicious behaviour, and actors in cyberspace. Malicious acts in cyberspace, as an umbrella term, describes ill-intended actions and intrusions, as defined by Lin (2016: 131), malicious acts are also regarded as intrusions, whereas cyberattacks are intended to halt or damage the technological information and communication systems – "Attacks are intended to destroy, degrade, damage, disrupt, manipulate, usurp, or reduce the availability of information and/or the computer and communications systems handling such information." (Lin, 2016: 131) In conclusion, this study uses the term malicious cyber act to refer to a broad range of actions aimed at damaging or disrupting ICT. Cybercrime is used to refer to a range of specific acts towards or in cyberspace or ICT with an illicit intent; and where the perpetrator, the objective, and the target can be defined (Donalds, Osei-Bryson, 2019: 408-409).

The next sections are based on policy emergence literature, and examine the hypothetical factors for the proliferation of cybersecurity as a policy concern. The existing explanations of the emergence of policy concerns that relate directly to cybersecurity are policy and norm diffusion among international organisations (IO) and states, economic considerations, technological and scientific developments, and external events that have drawn focus to cybersecurity capacity building and policy formulation in this area.

1.1 Emergence of policy concerns

To answer the research question, the study relies on policy emergence literature to explain the emergence of a policy concern. This literature is suitable for testing out several explanations for policy emergence and lays out different causes of why policies emerge internationally and on a national level. The emergence of policies is central to this research, as the formulation of NCSSs

varies across states and there are no specific worldwide regulations when it comes to national cybersecurity strategies. This framework therefore allows for to study of mechanisms, that have contributed to the emergence of policies. Scholars have previously widely relied on policy emergence literature to explain changes in policies or the absence of policies. Different models explain policy emergence, mostly applied are the multi-stream model by Kingdon (1984), the punctuated equilibrium framework (Baumgartner, Jones, 1993), and the advocacy coalition model (Sabatier, 1986).

The multi-stream model captures policy change as a dynamic between three dimensions - Kingdon's (1984) theoretical framework of policy emergence focuses on why some issues appear on governments' policy agenda and others do not. Kingdon (2001: 331-332) distinguishes different streams of organizations and institutions: the stream of separate problems, where it is decided on whether to focus on an issue or not; secondly, a stream of policies, which are going to be defined to answer a specific problem; and lastly, there exists a stream of politics – political actions and events. Therefore, the first stream concerns problems or issues, the second stream includes probable solutions and the third stream concerns political activities, which impact the way solutions are institutionally set forward. Kingdon (2001: 332) implies that when the conditions are right, the three streams join together and the government or a state institution sets a policy forward. Regarding policy concerns, this explanation outlines that when a policy area, security issue, such as cyber threats, or a problem becomes sensitized, a probable solution – such as a security measure or an action plan is provided and when the political conditions and actions, such as elections prioritize such policy concern, then a policy is set forward.

The multiple streams model itself is most often applied to US politics and not commonly applied in comparative contexts (Béland, Howlett, 2016: 224). Another critique of the MS model is that it is often difficult to empirically observe (Rawat, Morris, 2016: 608). The window of opportunity, when three different streams join together, is in certain circumstances difficult to measure (Cairney, Zahariadis, 2016: 100-101); this framework is rather used to study to predict policy implementation failure, often using other theories in conjunction with the MS framework (Rawat, Morris, 2016: 616, 624). In conclusion, this model is useful for studying policy implementation failure, yet it does not offer specific indicators for policy change and does not focus on the impact of external actors, events, and crises.

The punctuated equilibrium model was put forward by Baumgartner and Jones (1993), who studied how and why policies emerge. The policy outputs are affected by institutional settings, and cognitive capabilities and are divided into four stages of policy change: "social processes, government in-puts, policy processes, and outputs" (Baumgartner, et al, 2009: 604). How PET theory differs from other policy emergence theories is that it does not focus on extraordinary external events – "Even strong external forces, on their own, frequently fail to trigger immediate reactions" (Lundgren, et al., 2018: 551). The wider focus is on agenda setting and issue/topic definition, policies shift according to how agendas emerge in public discourse (True, et al. 2007: 156). In conclusion, this model does not explicitly clarify why these agendas emerge in the first place and discards the possibility of policy change as a result of external events and crises.

The advocacy coalition framework (ACF) captures policy change and was first put forward by Paul A. Sabatier (1986), the model was conceptualized into a framework that includes a system for policy emergence. Sabatier (1998: 102) distinguishes different subsystem actors and settings – "basic constitutional structure, socio-cultural values, and natural resources of a political system", which shape actions to a greater degree. Inside the coalition and political subsystem, actors coordinate their activities to shape policies (Weible, Sabatier, 2007: 125), yet the change occurs on two main levels: major or minor changes in the policy subsystem. Minor change occurs as a change in an aspect or component of policymaking, major change includes a systematical change in policymaking (Weible, Sabatier, 2007: 130). These changes occur due to "1) external shocks, 2) a hurting stalemate, and 3) the general accumulation of scientific/technological evidence" (Sabatier, Jenkins-Smith, 1999; in: Weible, Sabatier, 2007: 130). The external shocks, which take place outside the policy system, may change the advocacy coalition frameworks, and the availability of resources, and further change the dynamics within the political systems (Sabatier, Jenkins-Smith, 1999: 148; in: Weible, Sabatier, 2007: 130). The second impetus of change occurs through policy learning or knowledge accumulation. Policy-oriented learning happens over a long time, whereas external shocks lead to quick changes in policymaking. (Weible, Sabatier, 2007: 130). Thirdly, the hurting stalemate impetus involves disputes between different parties, where the continuation of a *status quo* is no longer deemed attainable and no more options, solutions and alternatives are available. (Zartman, 1991; in: Weible, Sabatier, 2007: 130).

In all models and theories of policy emergence, the focus is on what factors lead to policy change and when policy change is more likely to occur. Each model has its strengths and weaknesses. The ACF model emphasizes the role of different actors, including the role of non-state actors and stakeholders (Weible, Sabatier, 2007: 125-126). The success of policy change, according to the ACF model, is dependent on how policy core beliefs are shaped into real policies in the agenda, and how similar actors coordinate their actions (Sabatier, Jenkins-Smith 1999; in: Weible, Sabatier, 2007: 128). As both the multiple streams and PET model do not widely focus on the role of external influences, the ACF model is applied to this research, while it captures the role of different actors and settings of policy change. Furthermore, the ACF model emphasizes the role of knowledge accumulation and the role of scientific and technological evidence (Sabatier, Jenkins-Smith, 1999; in: Weible, Sabatier, 2007: 130). This model is useful in assessing the impact of both external actors and events and knowledge accumulation, which may have driven the proliferation of cybersecurity as a policy concern. Here, the coalition framework includes a variety of policy actors and stakeholders, who share a common mission to build a policy and who share common beliefs (Cairney, 2012: 1).

The following chapters discuss different factors that may have impacted the emergence of cybersecurity as a policy concern, relying on the literature on policy diffusion, norm diffusion, economic considerations, scientific and technological developments, and the impact of external events and crises.

1.2 Cybersecurity as a policy concern

This section draws on the findings of cybersecurity literature, which focuses on the framework of cybersecurity as a policy concern. This section outlines how cybersecurity has been framed regarding its appearance on the policy agenda and policy development surrounding cybersecurity. The next sections outline the main explanations for the emergence of cybersecurity as a policy concern.

The rise of the Internet and the increasing dependency on ICT systems has brought a wide array of risks both for the users and ICT systems managers, which is mirrored by national policies and legislative measures to protect these subjects from possible risks and exploitations. The subject,

cyberspace, and the users of cyberspace, entail a wide variety of stakeholders, systems, and areas of protection. Mishra and others (2022: 8) have compiled a list of the most common areas and attributes of cybersecurity policies, which include: "Telecommunication, network, Cloud computing, E-commerce, online banking, smart grid, consumer rights, cybercrime, national encryption, privacy, identity theft, digital signature, data security, and spam." This list illustrates how states emphasize different key areas, depending on the political situation, the overall awareness of ICT users, and the state's economy (Mishra, et al., 2022: 17). In conclusion, national security measures highlight the need for protection of the state at large, including the various domains of economic activity and public.

The various types and domains of cyberspace and types of attacks moreover blur the boundaries between a crime and an attack against national assets. As a result, the extension from distinct cybercrime incidents to national security has increased the importance of cybersecurity on a wider scale (van Eeten, Bauer, 2009: 222). Other aspects and implications of cybersecurity, besides national security, include the aspects of human rights, international norms and law, public-private sector relationship and cooperation, and civil liberties (Carr, 2016: 43). Framing cybersecurity as a national security concern involves cooperation between all parties and subjects, this includes an outline of public-private sector dynamics on the issue, including CI, as well as the interests of individuals (Carr, 2016: 45, 50). The development of cybersecurity and information security policies thus starts from consciousness and building awareness regarding possible risks and vulnerabilities (Maynard et al, 2011; in: Paananen, et al., 2020: 4). The NCSSs address a myriad of information and cybersecurity measures and standards, including a policy on CI protection and building awareness on cybersecurity-related issues. Although several models capture policy lifecycles, at the earliest stage of development, security policy requires input, which at the base level involves risk assessment and evaluation of possible requirements (Paananen, et al., 2020: 6, 10).

The overall emergence of cybersecurity as a security threat and a policy concern is often linked to external threat perception. Calderaro and Craig (2020: 918: 934) imply that the usual approach to cybersecurity emergence and cyber-capacity building, invoked by the cybersecurity threat landscape, diffusion of norms, and domestic policies is not backed up by evidence. The common assumption is that by investing in cyber capacity building, states "signal to rival political actors

that aggression will either be met with punishment or will not be worth their efforts" (Calderaro, Craig, 2020: 918). However, Calderaro and Craig (2020) argue that capacity building in cybersecurity is driven mainly by technological and scientific innovations and developments. Various initiatives and transnational cybersecurity programs call for a unified approach to cybersecurity, to promote common norms and security approaches in cyberspace (Calderaro, Craig, 2020: 921, 934), yet the impact and reach of those norms and policies remain understudied.

The next sections focus on how different models and explanations are linked to cybersecurity policy development and examine the different causes for the emergence of cybersecurity as a policy concern.

1.2.1 Policy and norm diffusion as a mechanism

One explanation for the emergence of policy concerns is related to policy and norm diffusion across international organizations and states. The diffusion of cybersecurity as a policy concern could be explained by policy-diffusion mechanisms - when a policy implementation leads to positive outcomes, it is further imitated by other states or units and vice versa (Shipan, Volden, 2008: 840). From the external perspective, states learn from other states, which is furthermore influenced by economic competition, as states consider the possible advantages of policy implementation for the economy. If the economic spillover proves to be positive, a state or a unit adopts the policy, and it is further diffused among other actors. (Shipan, Volden, 2008: 840-842) In broad terms, policy diffusion refers to the movement of policies or initiatives from one political entity to another. Dolowitz and Marsh (2000: 5) define policy diffusion as a transfer where "knowledge about policies, administrative arrangements, institutions and ideas in one political system (past or present) is used in the development of policies, administrative arrangements, institutions and ideas in another political system." The most common emphasis is to study the transfusion of policies from one government to another: "Specifically, diffusion occurs when one government's decision about whether to adopt a policy innovation is influenced by the choices made by other governments." (Graham et al. 2013: 673, 675). Here, advocacy coalition frameworks shape how and why certain policies are diffused or learned from other entities.

The literature on policy diffusion is widespread and often overlaps with the diffusion mechanism described by norm diffusion literature. The question of the referent object – what is being

transfused, could be answered from various perspectives. Graham and others (2013: 690) outline the four processes of diffusion, which capture the primary mechanisms and objectives of transfusion: "learning, competition, coercion, and socialization." In all models for policy diffusion, the outcomes are further shaped by when and where the initial policy implementation takes place and who is involved in this process. A common finding is that more similar entities are more likely to adopt changes of ideas and similar policies or mimic them (Dobbin, et al., 2007: 453-454).

Policy, in broad terms, refers to a direction of governance in a specific way and formulating a basis for action (Colebatch, 2009: 4, 19), whereas norms entail certain goals and standards that ought to be met. Norms, as well as policies, cover a wide range of areas, and entail "group-level evaluations of behavior" – both the content of the evaluation of behavior and its implementation at large (Horne, Mollborn, 2020: 468). More broadly – the content and nature of norms vary (proscriptive or prescriptive), as well as the degree of oughtness and sanctions for those who do not acquire the standards (Horne, Mollborn, 2020: 468). Finnemore and Hollis (2016: 427, 444) illustrate how cybersecurity norms, created in social contexts, proscribe or prescribe specific behavior, or generate new structures, actors, and institutions. Craig (2018) shows based on a study of cyber capability build-up between 2000 and 2017, how cybersecurity proliferation is correlated to cyber threats and incidents; in sum cyber incidents invoke an action on a national level, to decrease risks for individuals, ICT operators, states and on a regional scale. Obstacles regarding the fight against cybercrime and international regulations on cyber weaponry are difficult to overcome due to an increase in vulnerabilities, economic competition between states, and lack of attribution of cyber incidents on a wider scale (Goel, 2020: 74).

Diffusion of norms and policies is possible both within international organizations and among governments. Cybersecurity norms, even though no holistic approach exists in this regard, theoretically shape how operators of CI and ICT manage their systems and propose a unitary approach to cybersecurity. One of the examples of a wide-reach cyber-norm is the Tallinn Manual (published in 2013, the second version in 2017), which sets suggested standards and regulators for the NATO member states and is not legally binding (NATO CCDCOE). Although not obligatory, this Manual sets guidelines to enhance cybersecurity-related capacities among NATO member states. More known cybersecurity regulations are the EU's NIS directives, which set out mandatory standards and requirements for the EU member states in the field of cybersecurity. (first NIS

directive - European Parliament and the Council of the EU, 2016; second NIS directive – European Parliament and the Council of the EU, 2022) The first NIS directive, with the transposition deadline of 2018, specifically clarified cybersecurity and information security-related standards and requirements for all the EU member states. One of the requirements was also to establish a NCSS, with the deadline of May 2018. (European Parliament and Council of the EU, 2016: 5, 25)

To answer the research question, the study draws on several factors that might explain the emergence of cybersecurity as a policy concern. The impetus for developing a NCSS is from one perspective related to the perception of cyber threats and the protection of society. Hansel (2013) argues, based on the theory of public goods, that cyberspace becomes a national public good if a state has invested in its regulation and protection, as weakly guarded IT systems pose a risk for other systems across the state and elsewhere. The central takeaway from diffusion literature, considering the objective of this study, is to examine to what extent policies and norms in international organizations and neighbouring states diffuse among one another. This leads to a hypothesis, that concerns different actors, settings, and models of policy diffusion. Given the policy shifts in cybersecurity and security in general, this study seeks to *test if a state has adopted a policy as a result of an emerging policy concern in a region or an international organization or seeks to follow a transnational norm or a policy, then a policy concern diffuses to other states.* The diffusion, specifically of cybersecurity policies and norms, then hypothetically leads to the adoption of a NCSS.

1.2.2 Economic factors

This section discusses how different economic aspects are tied to the protection of ICT and critical infrastructure. Cybersecurity-related capabilities and readiness are most directly related to the extent to which a state exports its ICT, dependency on ICT, and the specific threat landscape, but not specifically the resources allocated to the technological developments of a state (Makridis, Smeets, 2019: 73). On a domestic level, securing the critical infrastructure (CI) and information systems requires balancing national interests, advancements and innovations in digital transformation and legislation (Tiirmaa-Klaar, 2016: 95, 96). Brangetto and Aubyn (2015: 5) conclude this by highlighting that cybersecurity: “As a global policy involving many stakeholders, the economic aspects are key to understanding the motivation of state actors”, yet it is often

difficult to assess based on the analysis of NCSSs whether the government's approach to economic protection is proactive or reactive (Brangetto, Aubyn, 2015: 15-16).

On the other hand, scholars have widely focused on the economic impact of cyber incidents, underlying that the impact is widespread (e.g. Vasiu, Vasiu, 2018). The field of cybersecurity economics assesses two sets of roles – firstly, in the prescriptive role – cybersecurity economics involves prescribing policies and rules, to improve the state of cybersecurity. In its descriptive role, cybersecurity economics predicts and analyses how different economic aspects and areas influence cybersecurity frameworks. (Kianpour, et al., 2021: 21) The economic risks of attacks against ICT have been widely studied throughout cybersecurity literature, and many economic estimates and predictions offer insight into how the risk assessment is conducted on a national level. Luiijf and others (2013) examined 19 different NCSSs, implying that most of the strategies involve economic prosperity issues of cybersecurity, concluding that: "Cyber security is considered to be a minimal requirement to enhance the prosperity of the population and to foster economic welfare." (Luiijf, et al, 2013: 11) Therefore, not only do the CS policies address the economic vulnerabilities but focus on the enhancement of (digital) economy.

Not only do malicious cyber acts and cyber crime involve direct financial losses, but the abruption of services and remediation, as well as reputational damage (Vasiu, Vasiu, 2018: 176). These breaches do not only affect the target but could have implications for stakeholders as well as the whole society (Bauer, Dutton, 2015: 18). Burt and others (2014) illustrate how the rise in connectivity to cyberspace increases the degree of cyberattacks, yet "As adoption rates further increase, this trend is reversed and security performance increases again" (Burt et al. 2014; in: Bauer, Dutton, 2015: 20). In conclusion, considering the effect of economic considerations in cybersecurity planning and risk assessments, this study explores *if a state is concerned with the national economy and seeks to strengthen digital economy capacities, then a policy concern emerges.* Thus, this hypothetical factor then leads to the adoption of a NCSS.

1.2.3 External events and crises

This section discusses how external events, more precisely cyber incidents, have been framed in former literature and how these events may have impacted the emergence of cybersecurity as a national policy concern. The change in cybersecurity-related approaches and policies came,

according to several scholars (e.g. Klimburg, 2012: 50; Guitton, 2013: 24; Robinson, Hardy 2021: 213; Tiirmaa-Klaar, 2016: 103), after the 2007 cyberattacks in Estonia, as digitally advanced states started to put more focus on national cyber resilience and capabilities. Some scholars (e.g. Harknett, Stever, 2011: 456) refer to the 9/11 terror attacks, stating that cybersecurity received more attention after the attacks. The rise in cyberattacks and cyberspace incidents is, in previous literature, stated to be one of the key explanations for the emergence of cybersecurity as a policy concern. Yet, the first NCSSs were adopted even before the rise of state-sponsored cyberspace incidents – before 2007, the US, Russia, and Norway had adopted national cyberspace protection strategies (e-Governance Academy, 2023).

Scholars outline that the change in cybersecurity approaches became more visible after 2007 and 2008, Herzog (2017: 69-70) argues that the attacks against Estonia served as "a training ground for future Russian cyberattacks in Kyrgyzstan and information warfare—alongside conventional military operations—in Georgia and Ukraine." During and after the Bronze Night cyber-attacks of 2007, Estonia strengthened its cybersecurity-related cooperation in NATO, and alongside other experts and states, established multiple frameworks and strategies to enhance and promote cybersecurity resilience in both the EU and NATO (Herzog, 2017: 73). Seger (2012: 4) concludes this, by implying that the 2007 attacks served as a "trigger-point" for the establishment of NCSSs in Europe and abroad, the attacks demonstrated the vulnerabilities of ICT systems in Estonia. Overall, the line of argument in the literature is that the more cyberattacks and malicious acts occur in cyberspace and against ICT systems, the more states invest in cybersecurity.

The common finding throughout the literature is that external crises serve as an impetus for strengthening cybersecurity measures, yet this explanation has not been systematically analyzed. On the one hand, external crises create shifts in existing beliefs, and changes in the availability of resources, which could accumulate into a policy change (Sabatier, Jenkins-Smith, 1999: 148; in: Weible, Sabatier, 2007: 130). Based on the findings in the literature, this study aims to find *if a state experiences an attack on its national assets, then a policy concern in other states emerges*. Thus, as a result of this hypothetical cause, a NCSS is adopted. This hypothetical question does not test out specific events, that have occurred, yet the overall findings from the literature mainly refer to the events in Estonia in 2007 and Georgia in 2008. This explanation focuses specifically

on external crises, not on reactionary international policies and norms which diffuse among states, neither mimicry nor diffusion of policies or policy concerns.

1.2.4 Innovations in science, technology and engineering

Throughout cybersecurity literature, a common impetus for the proliferation of cybersecurity is linked to innovations in the fields of science, technology, and engineering (ST&E). This is intertwined with ICT dependency and the primary connection is that the more the technology advances, the more states invest in cybersecurity. On the one hand, emerging technologies cause shifts in the target population due to changes in existing policies and regulations of technology (Lewallen, 2021: 1037). Secondly, equipment of new technologies creates cross-sectoral shifts, which further creates spillovers in different industries, and lastly: "through the adoption or mimicking of existing technologies across economic and social sectors and across geographic boundaries, so that different governing arrangements and jurisdictions designed to address different issues find themselves faced with similar challenges." (Lewallen, 2021: 1037). Therefore, the uncertainties of new technological advancements involve new vulnerabilities, as well as new possibilities for building cyber capabilities and strengthening resilience.

The developments in technology are closely connected to scientific developments, which aim to advance the technologies and systems being used. Developments in technology introduce and expose new risks, users and interests, which could potentially change the existing security dynamics (Lewallen, 2021: 1038). An increase in digital inclusion and technological innovations brings out new vulnerabilities and thus creates the need for regulations and policies to control cyberspace and ICT systems. NCSSs are often renewed in the light of new cybersecurity innovations and trends, specifically to respond to new crime-related, technological and cultural trends. (Dupont, 2012: 3) The inclusion of new technical measures and technologies into NCSSs is concluded by Dupont, who implies that the NCSSs:

> address the diversity of risks associated with the embededdness of this recent technology into every aspect of our lives, from the daily operations of key infrastructures to the flow of transactions that irrigate our financial system and the personal communication tools that sustain our social interactions. (Dupont, 2012: 2)

The technological innovations are a combination of research efforts, economics, infrastructure, and government policies, failure to adapt to the innovations could lead to "increasing technological obsolescence, and, eventually, diminished national power." (Kadtke, Wells II, 2014: 3) Another consideration is linked to the globalization of ST&E capabilities, as states compete for resources to develop new technologies (Kadtke, Wells II, 2014: 16). In conclusion, the national cybersecurity policies take into account the technological developments, as well as trends in ICT and ST&E innovations to suit the technological environment and realities. This shift is linked to scientific and technological evidence accumulation, as new information and evidence could lead to a change in policies (Sabatier, Jenkins-Smith, 1999; in: Weible, Sabatier, 2007: 130). The overall findings in ST&E and cybersecurity literature indicate interconnection between the two fields, the developments and innovations in ST&E and the competition for resources in ST&E introduce new vulnerabilities and risks for ICT users, which lead to ethical, legislative, economic, and legislative considerations to diminish possible risks. Therefore this study aims to answer *if a state sees an increase in ST&E developments, then a policy concern emerges.* Hypothetically, as the technologies evolve as a result of innovations, cybersecurity as a national policy concern emerges, leading to the adoption of a NCSS.

1.3 Summary

This section concludes the findings on policy emergence literature and draws on different hypotheses based on the explanations discussed above. Former research (e.g. Craig, 2018; Calderaro and Craig 2020: 918) on the emergence of cybersecurity and the proliferation of cyber capacities highlight the growing need for a systematic overview and research in this area.

The existing explanations for the emergence of cybersecurity are mostly concerned with shifts in policymaking and draw on factors such as policy and norm diffusion, economic considerations, external events and shocks, and innovations in ST&E. A wide variety of factors and considerations could explain the emergence of cybersecurity as a policy concern. On the one hand, the ACF model illustrates how policy change is linked to advocacy coalitions, which share common beliefs and shape the way policies rise on the agenda (Cairney, 2012: 1). The same framework connects policy change to factors such as accumulation of scientific knowledge and developments and the impact

of external crises and shocks. In addition, policies and norms diffuse among similar political entities, therefore creating a basis for policy concern emergence or policy continuity.

The analysis of this study explores the relative explanatory power of the explanations introduced above. It does so, by testing the following hypotheses: 1) if a state has adopted a policy as a result of emerging policy concern in a region or an international organization or seeks to follow a transnational norm, then a policy concern diffuses to other states 2) if a state is concerned with the national economy and seeks to strengthen the (digital) economic capacities, then a policy concern emerges; 3) if a state experiences a cyber-attack towards its national assets, then a policy concern in other states emerges; 4) if a state sees an increase in ST&E developments, then a policy concern emerges. The emergence of cybersecurity as a policy concern is indicated by the adoption of NCSS, and as for each hypothetical explanation, the expected outcome is the adoption of a NCSS. To find out which of these factors explains the emergence of cybersecurity as a policy concern across NATO countries best, the study conducts an analysis of the NCSS documents and examines the responses and insights from the interviews with policymakers and CS experts from the states of interest. The next section will outline how the analysis of this research is conducted and explains what methods are applied for conducting this research.

2. Methodology

This thesis uses qualitative research methods to answer the research question. The framework for conducting case studies is the Most Different Systems Design (MDSD) case study approach (Hupe, Sætren, 2015: 99) which seeks to find factors that have shaped the emergence of national cybersecurity strategies across selected NATO member states. The advantages of the case study approach are the opportunity to measure the variables by case while taking into consideration contextual factors and the ability to refine an adequate level of "construct validity" (Bennett, 2004: 34). Furthermore, "case studies can use process tracing to examine in detail the observable implications of hypothesized causal mechanisms in individual cases" (Bennett, 2004: 25). The MDSD case study approach is useful for studying cases, that share a similar outcome but vary in different areas. The outcome – namely the adoption of NCSSs, applies to all cases, yet the cases differ in various relevant aspects, specifically cybersecurity capacities. In sum, the MDSD approach is applied to this research while it is useful for determining causal mechanisms in cases that differ in the field of cybersecurity but share a similar outcome. By using process tracing, which is useful for analyzing competing explanations, and in studying causal mechanisms, the author analyses the observed outcome and traces the possible explanations (Bennett, 2010: 208-209). This method is useful for finding connections to the factors, that have served as catalysts for the establishment of cybersecurity strategies.

To answer the research question, this study relies on expert interviews and document analysis of NCSSs. The document analysis of the first NCSSs and cybersecurity policies from selected NATO member states is conducted to measure the emergence of cybersecurity as a security concern. Document analysis is useful in determining the factors, that led to the emergence of cybersecurity as a policy concern. These documents are publicly available cybersecurity strategies, action plans for policy implementation and in some cases specific laws and programmes which are interconnected to the strategies. As concluded by Karppinen and Moe (2012: 14): "The 'documents as sources' approach treats ideas as resources that political actors possess, thereby facilitating a mapping and comparison of policy developments." Policy documents therefore give an insight into policy developments, priorities, objectives, aims, goals and deliverables that are expected from policy implementation. To study the emergence of cybersecurity as a policy concern in a set of countries, the adopted policy documents will be empirically studied, namely the NCSSs and

policies for NCSS implementation in each state. However, document analysis as a method of qualitative research has certain weaknesses, specifically related to the limits and biases in publicly available documents and the contextual factors that influenced the development of certain documents (Morgan, 2022: 66-67). To mitigate these risks and to assess the contextual factors, the author conducts interviews with people involved in the NCSS formulation process and/or implementation.

To measure the factors that led to the implementation of NCSS, the author conducts expert interviews with the respective policymakers and policy advisors from each state. The expert, in this research, is defined as a person possessing expert knowledge, derived from either an institutional or organizational setting, in a specific field, that is not available or attainable to other people. This further includes knowledge on providing inputs and legitimate outputs regarding problem-solving. (Johnson, et al., 1987: 163) In conclusion, the expert possesses a plurality of (and in some cases, transnational) capabilities, tools, and knowledge, that are convenient for problem-solving in a specific field. An expert in the field of cybersecurity thus possesses knowledge that is distinct from common-sense and everyday knowledge of cybersecurity – an exclusive realm of knowledge and experience in the field (Meuser, Nagel, 2009: 18), accompanied by accreditation, that influences the actions of institutions and other individuals and is actively involved in the field. Interviewing cybersecurity experts further allows the author to attain information on policy development, which is otherwise not accessible, specifically motives, objectives, and the process behind the policy concern emergence in each specific case.

3. Case selection

To identify the factors for the proliferation of cybersecurity as a policy concern, this study investigates the establishment of NCSSs from most different NATO member states in the area of cybersecurity. The selection of NATO member states allows the author to find links across states, that differ, but share a similar outcome – the implementation of the NCSSs. All the selected states are NATO members, which allows to study of a group of states that are relatively homogeneous in many respects that might influence the emergence of cyber as a concern, yet NATO membership as such does not explain the implementation of NCSSs. NATO has not specifically required each member state to adopt NCSSs, although cybersecurity has become one of the core areas in NATO's overall security framework, however, the specific policy implementation is up to each state independently. This aspect is more specifically tied to military defence capacities, not domestic policies or regulations of NATO member states. In sum, the national cybersecurity policy formulation is up to each independent state, yet the emergence of cybersecurity as a policy concern could be explained by policy diffusion among similar entities – states, that are part of a security alliance. NATO member states are a particularly good subset for this study, while these states are relatively technologically and economically advanced, and rely on digital services. Therefore it is expected that cybersecurity has emerged as a policy concern in these states and these states have been able to allocate resources to deal with cybersecurity on a national level and to enhance the protection of ICT domestically. NATO membership is thus not itself an explanatory factor for the emergence of cybersecurity as a policy concern.

The selection of cases is further dependent on the following characteristics: 1) the degree of digitalization and digital dependency of the state (DDL); 2) the type and origin of cyber threats the states mostly face and previous experiences with cyberattacks 3) geographical location and region of the state; 4) the degree of cybersecurity capabilities (NCSI). The first characteristic – the degree of digitalization and digital development level (DDL) – outlines how dependent a state is on digital infrastructure and digital services, combining elements of the e-Governance Development Index (EGDI) and the Networked Readiness Index (NRI) assessments (e-Governance Academy, 2023). The NRI is furthermore based on 53 sub-indicators, combining areas of (1) ICT use and environment, (2) "networked readiness in terms of ICT infrastructure, affordability, and skills;" (3) use of technology by individuals and different sectors, and (4) the impact and reach of new

digital technologies (Baller, et al., 2016: 3). The DDL characteristic is based on a scale of 0-100, with 100 being the highest in terms of digital development, and: "is calculated according to the E-Government Development Index (EGDI) and Networked Readiness Index (NRI)" (e-Governance Academy, 2023). The EGDI element includes an assessment of surveys on online presence by evaluating e-government policies and their implementation and is calculated based on the categories of e-governance: "(1) scope and quality of online services (Online Service Index, OSI), (2) development status of telecommunication infrastructure (Telecommunication Infrastructure Index, TII), and (3) inherent human capital (Human Capital Index, HCI)" (UN E-Government Knowledgebase).

The second characteristic, the type and origin of cyber threats includes a combination of threat assessment and an overview of experiences with previous cyber incidents. This attribute is combined based on the information from ENISA Threat Landscape (ETL) reports, NCSS mid-term evaluations, and reports from responsible institutions. The third characteristic, the region of the state and location inside the NATO alliance, allows to selection of cases from a variety of geographic regions. The fourth characteristic – NCSI (E-Governance Academy, 2023), lists states based on assessing their cybersecurity capabilities, based on a score from 0 to 100, with 100 being the best in national cybersecurity capacities and ICT protection.

Although these states have similarities in security and military frameworks and are members of a security alliance, the characteristics listed above illustrate the differences in terms of cybersecurity capacities and threat landscape. Additionally, the directive on the requirement of NCSSs in the EU came into effect in 2016, with the transposition deadline of May 2018 (NIS 1 directive: European Parliament and Council of the EU, 2016: 5, 25), yet most of the EU member states had by that time already implemented NCSSs (e-Governance academy, 2023). Therefore, hypothetically, the NIS directive does not largely impact the case selection. In conclusion, this selection of cases allows to study the effects of different possible causes, especially the impact of external and internal events inside a security alliance, that might drive policy concern emergence. The characteristics listed above allow to trace and weigh different causes, that might be interconnected to different explanations for policy concern emergence. The ICT and level of digitalization, threat landscape in the field of cybersecurity, and the degree to which these states have experienced, for example, attacks on ICT, vary, allowing to study factors that served as an impetus for policy

implementation. The initially proposed cases are selected depending on the characteristics listed above and the availability of the data – namely the NCSS documents and interview subjects. However, the variety of cases and attributes allows the author to select more cases if needed. Each of the selected states has adopted a NCSS and an action plan and objectives, which vary in different areas. Table 1 lists cases, that fit into the requirements, and differ in all aspects. The diverse set of cases helps to trace possible causes and factors that have evoked the proliferation of cybersecurity as a policy concern emergence in different states. These states differ in their cyber capacities and regions, therefore diversifying the array and reach of possible causes.

Table 1. Case selection

State:	**Geographical location and overall location in NATO:**	**Type and origin of cyber threats, previous experience with cyberattacks:**	**Digital Development Level (the latest data, 2016-2023):[1]**	**National Cyber Security Index (the latest data, 2016-2023):[2]**	**Implementation of NCSS:**	**Potential explanations for the policy implementation:**
Croatia	Europe, Balkan region; primarily surrounded by other NATO Allies	Economically motivated cybercrime[3]; cross-border incidents, phishing and computer fraud[4]	64.63	83,12	2015[5]	?

[1] Based on: E-Governance Academy (2023). NCSI database.
[2] *Ibid.*
[3] Trkanjec (2021).; INA Group (2020).
[4] Council of the European Union. (2017). Pp. 17, 65, 110.
[5] Government of the Republic of Croatia. (2015).

Lithuania	Baltic region, Europe; border-state of the alliance	Phishing campaigns[6]; state-sponsored attacks originating from Russia[7]	67.34	93,51	Cybersecurity programme established in 2011[8], NCSS approved in 2018[9]	?
Canada	North America; distanced from other Allies	Foreign state-sponsored and non-state attacks[10], ransomware directed against CI[11]	75.96	70.13	2010[12]	?

All of the selected cases – Canada, Lithuania and Croatia – differ in multiple respects, but share the emergence of cybersecurity as a policy concern in the timeframe of interest. The three selected countries represent an ideal setup to study the emergence of cybersecurity as a policy concern, while each case displays a set of characteristics and capacities that differ, allowing to examine the different hypothetical factors that have led to the proliferation of cybersecurity as a policy concern.

Croatian cybersecurity capacities and proliferation have not been widely studied. Based on the assessment of each characteristic, Croatia represents a case with limited cybersecurity threats against national assets and institutions, yet instances of financially motivated cybercrime (Table 1). Croatia is primarily surrounded by other NATO Allies, which hypothetically limits the instances of state-sponsored attacks. Croatia is not heavily dependent on digital services, yet compared to Lithuania, the digital services are on a similar level. Croatia has largely invested in building

[6] CyberPeace Institute (2023) in: ENISA. (2023). P. 73.
[7] ENISA (2023). P. 97; Vilpišauskas (2024). Pp 1, 6, 14.
[8] Government of the Republic of Lithuania. (2011).
[9] Ministry of National Defence of the Republic of Lithuania. (2018).
[10] Public Safety Canada. (2017). Pp ii, 17.
[11] Public Safety Canada. (2022).
[12] Government of Canada (2010).

cybersecurity capacities, yet the first national cybersecurity strategy was adopted in 2015, one year before the EU-wide NIS directive was adopted. This indicates that the emergence of cybersecurity as a national policy concern was primarily motivated by national considerations. In sum, the case of Croatia represents a state with no extensive cybersecurity threat landscape and large-scale cyber incidents, and a state which is not heavily reliant on digital services but has widely invested in cybersecurity on a national level.

The earliest developments in the area of cybersecurity in Croatia took place following the ratification of the Budapest Convention, adopted by the Council of Europe in 2001. This document clarified the definition of different types of cybercrime and established the pillars of collaboration in the fight against cybercrime. (Protrka et al., 2017: 88-90) The National Program for Information Security of Croatia, adopted in 2005, aimed to clarify the existing legislative framework on cybersecurity and further distinguish institutions responsible for combatting cybercrime (Cvitić, et al., 2017: 13, 14). The next milestone in Croatian regulations on cybersecurity was the implementation of the Information Security Act in 2007, which clarified the measures, and mechanisms of data protection and information security in Croatia (The Croatian Parliament, 2007: 1). A more encompassing policy was adopted in 2015 when the Croatian parliament adopted the first NCSS (Government of the Republic of Croatia, 2015). This was preceded by an EU-wide cybersecurity strategy in 2013 by the European Commission, which sought to establish a unitary cybersecurity framework across the EU, and stated that the member states should (yet were not obliged to) adopt NCSSs (European Commission, 2013: 17). The institutions responsible for ICT protection in Croatia are the Office for the National Security Council and the Operational-Technical Coordination for Cyber Security (Vuksanović, 2019: 155-156). Regarding policy formulation, the Coordination consists of eight members from institutions such as the Ministry of the Interior, all of which are involved both in the policy implementation process and control mechanisms in Croatia (Vuksanović, 2019: 155-156).

The developments of cybersecurity policies and legislation in Lithuania have been studied widely. Lithuania has been at the forefront of cybersecurity capabilities, as the state invests widely in cybersecurity measures. The cybersecurity threat landscape in Lithuania is largely impacted by state-sponsored attacks, originating primarily from Russia (Table 1). The wide array of cyber-attacks against national assets and institutions has contributed to cybersecurity capacity building,

as Lithuania stands out in the area of cybersecurity on a global scale. Lithuania is not heavily reliant on digital services and the first programme on cybersecurity in Lithuania (although not a strategy), was established in 2011 and the NCSS was adopted in 2018. The programme on cybersecurity, compared to the strategy, lists out objectives and aims to improve cybersecurity, yet it does not set out specific responsibilities and deliverables for its implementation. Therefore, the adoption of NCSS illustrates a more substantive emergence of cybersecurity as a policy concern, as the NCSS sets out clear indicators, implementation plans and tasks to achieve, as well as focusing on building public awareness and engaging the private sector to achieve the goals.

The policy concern emergence aspect of cybersecurity in Lithuania has been studied by Vilpišauskas (2024), who researched the evolution of policy concern emergence in relation to the cybersecurity threat landscape of Lithuania. The earliest developments in Lithuania's cybersecurity proliferation started in 2001 when the Lithuanian government adopted the resolution "On the Approval of State Strategy for Information Technology Security and Its Implementation Plan" (Government of the Republic of Lithuania, 2001; in: Štitilis, Klišauskas, 2015: 47), which primarily assessed the information security protection of public institutions. This was followed by a similar resolution in 2006 (Government of the Republic of Lithuania, 2006; in Štitilis, Klišauskas, 2015: 47) which clarified the strategic objectives for public cyber-infrastructure. Lithuania's cybersecurity measures are closely intertwined with the geopolitical context and the security situation in Eastern Europe. This is illustrated by a relative growth of external DDoS (distributed denial-of-service) attacks in Lithuania, directed against Lithuanian state institutions: "cyber espionage against the state institutions of Lithuania, objects of the critical infrastructure of the country and the private sector remains one of the main threats to the country's national security" (CERT-LT, 2016; in: Štitilis et al., 2017: 362).

Canada represents an interesting case where the state is geographically distanced from possible threats, yet experiences a variety of cyber attacks against its national assets, institutions, as well as the private sector (Table 1). Canada is, compared to other states in interest, more reliant on digital services, yet scores a lot lower on the assessment of cybersecurity capacities. This represents a research puzzle, as the state experiences an array of cyber attacks, is reliant on digital services, but scores low on the cybersecurity capacities. However, compared to other states in this research, and on a global scale, Canada was on the other hand one of the earliest adopters of NCSS.

Responsibilities and control systems regarding cybersecurity in Canada are distributed between various institutions. These roles were first clarified in the NCSS in 2010, the overall focus of the first Canadian NCSS is threat repulsion, supplemented by cooperation between non-governmental actors and sector-specific coordination (Government of Canada 2010: 1, 7; in: Arnold, 2018: 5-6). These regulations are supplemented by sector-specific laws and various initiatives by non-state organizations (Arnold, 2018: 7). The first NCSS was supplemented in 2013 by the Action Plan, outlining specific initiatives and activities of the government of Canada in the field of cybersecurity (Government of Canada, 2013: 1-2). To supplement the domestic initiatives, the government of Canada has widely focused on cooperation with the US to improve cybersecurity measures against shared cyber and physical infrastructure, as the two states have interconnections within CI (Gendron, 2013: 185). Although the government of Canada has made various efforts to ensure the protection of critical infrastructure and ICT systems, cyberattacks and incidents related to foreign malware are common towards the public sector of Canada (Gendron, 2013: 187).

3.1 Operationalization of variables

To answer the research question, this study draws on several explanatory factors that are related to the emergence of cybersecurity as a policy concern. The dependent variable for this study is policy concern emergence. This represents a dichotomous variable – this is either present or absent. This variable indicates a change in the policy agenda and the emergence of a policy concern. A concern can be „emerging“ or „not emerging“, as reflected by a „first-time adoption of a strategy“ (“emerging“), or „absence of such strategy (“not emerging“). Therefore, the NCSSs with their specific tasks, objectives, measures and action plans for policy implementation are clear indicators for policy concern emergence of cybersecurity, while the policy is formulated to answer to a specific national objective or a measure for the protection of CI, ICT or cyberspace at large, involving the private sector and putting an emphasis on raising public awareness on cybersecurity. Therefore, a selected state either has adopted a NCSS, which indicates the proliferation of cybersecurity as a policy concern, or not, which indicates that cybersecurity has not emerged as a policy concern. The strategies are clear indicators for the emergence of cybersecurity as a policy concern while it clearly indicates, that a state allocates resources for the protection of ICT, addresses the concern publicly, aims to raise awareness on cybersecurity, and sets out specific

responsibilities, tasks and expected deliverables for national ministries and institutions, to enhance national ICT and CI protection.

The four independent variables of this study represent factors, that are hypothetically connected to the emergence of cybersecurity as a policy concern. Both the document analysis and interviews will measure the presence or absence of each independent variable, namely: policy and norm diffusion, economic factors, external events and crises, and developments in ST&E. Drawing on the findings of cybersecurity literature, the above-listed independent variables present possible causes for policy concern emergence of cybersecurity. A variable is present if the specific factor is mentioned and connected both in the interviews and NCSSs and absent if it is not mentioned in the documents and interview responses. All explanatory factors are similarly measured dichotomously, these factors are either "present" or "absent". Although the measurement of these factors is defined and specific, empirically, it is likely that in some settings, these factors will probably be "almost present" or "almost absent". Therefore, the analysis assesses whether these factors were decisive in the proliferation of cybersecurity as a policy concern.

The diffusion mechanism is present if the interviews and documents draw on external policies or norms, be it specific guidelines, norms or cybersecurity policies of other states. The economic considerations factor is present when the interviews and document analysis indicate a concern for the protection of the national economy at large, the enhancement of economic capabilities or the protection of specific economic assets. This aspect is also interconnected to the possible financial damages or economic damages related to cybercrime or state-sponsored cyber-attacks, which indicates a concern for the protection of economic assets. The external events variable is present when the interviews and document analysis draw on external events or processes, that have raised a national policy concern and evoked reactionary measures for policy adoption. This variable is more related to developments and events related to cybersecurity, but could also involve events such as large-scale crises, natural disasters, political events etc. The ST&E development factor is present when both the document analysis and interviews indicate the impact of new technologies and advancements, which have raised a policy concern as they pose new risks to the users and operators of ICT. This is marked by a concern related to the development of new technologies and platforms and the regulation for their use and operation.

4. Empirical data and sources

This research relies on the data gathered from the expert interviews and NCSS document analysis. The interviews, as well as the document analysis, will measure the presence or absence of each factor, namely: *policy and norm diffusion, economic considerations, the impact of external events and crises, and developments in ST&E* – that could have impacted the emergence of cybersecurity policy in the respective states. The document analysis was conducted based on the NCSS of each state and accompanying action plans, as well as other policy documents which outlined specific measures for enhancing cybersecurity that were related to the NCSSs. The primary documents were publicly available NCSSs in English, which include various objectives, aims and goals for cybersecurity and list specific actions and implementation plans in each state. The selection was dependent on whether these documents were publicly available and published in English by a national institution or a ministry of the state of interest. The selection of interviewees was based on whether they were involved in the implementation or drafting of the NCSSs, which is in most cases directly related to the responsibilities of Ministries of Defence (MoD), and the contacts were gathered based on that information. These policymakers and experts are either active or former members of Ministries of Defense or have provided legal or academic input for policy formulation. In sum, the participants have been or are in the position to formulate, change, review or affect in other ways the formulation of a national policy.

For the interviews, the author used purposive sampling and snowballing to gather the contacts of the participants of the interviews. Purposive sampling is suitable considering the objectives of this research, while this sampling method matches the logic of the study and is useful for opting for participants based on the specific characteristics, knowledge and expertise or qualities they possess (Etikan et al., 2016: 2-3). This research uses expert interviews with specific people who were involved in the NCSS formulation process or implementation to gain insights into the motives for policy formulation. In sum, 47 interview requests were sent to different policymakers, cybersecurity experts, and policy and legal advisors of three states of interest. The primary method for contact gathering was through snowballing, as most of the interview respondents consulted the author on additional contacts and gave recommendations for contact gathering. The interviews were semi-structured, as this allowed the author to get an insight into the motivations and

perspectives of the participants and provide explanations that are not specifically framed in the research beforehand.

As this study employs online in-depth expert interviews, there exist biases and limitations to this method. Firstly, the list of interviewees was gathered based on the available information on government institutions and policy documents. The range of policymakers and advisors has mostly changed since the adoption of the first NCSSs, as well as the information on specific persons involved is not mostly public. Therefore, the sampling was supported by the insights and information from the current CS policymakers and experts, as well as the recommendations from the interviewees. Another limitation is related to the confidentiality of the government institutions involved. As implied by the respondents, the information regarding CI protection and national cybersecurity is a confidential subject, therefore, the participants were anonymized. The interviews were conducted online, which creates other limitations – specifically obstacles regarding the contact gathering and the interview process itself. As the interviews are conducted online, the participants are more likely to have confirmation bias in the responses, both parties could have technical issues, as well as complications regarding the audio recordings, privacy, complications regarding the interview environment and lack of trust. To eliminate the possible drawbacks, the author ensured the participants' awareness of possible risks beforehand, by informing them about the interview process, data collection measures and procedures regarding the collected data.

The interviews were conducted online, using Webex, Zoom and MS Teams applications, ensuring that each participant has access to the applications in use. The interviews were audio-recorded and transcribed after the completion of the interview. The transcriptions were analysed based on the responses on specific variables and the responses were thematically categorized based on the variables. The interview respondents were informed beforehand about the procedure of the interview and signed a consent form, which outlined how the interview data was going to be used in the research. The audio recordings were deleted after the transcriptions were complete and the transcriptions will be deleted after the completion of the analysis to ensure the confidentiality of the interview respondents. The participants of the interviews were numbered based on the order the interviews were conducted, therefore the first participant – P1, last interviewee – P14.

For the interviews, the author compiled an interview guide, which includes two sets of questions. The questions were prepared taking into consideration of cybersecurity policies of each state and

the background of each participant, a list of primary and thematic interview questions is available in Annex 2. The interview guide includes a list of core questions related to the emergence of cybersecurity as a policy concern in each state and a list of thematic specifications related to specific cybersecurity policies. During the interviews, the author included questions and specifications based on the answers and cybersecurity frameworks of each state. The list of the interviewees, with information regarding their former and current positions, is available in Annex 1. The author conducted interviews with four subjects from Canada, four subjects from Croatia, five subjects from Lithuania and one additional interview with a representative of the Council of Europe. The opinions and responses of the interviewees do not reflect the positions of the government institutions they are or have been related to, but their personal perceptions of cybersecurity policies.

The document analysis was conducted based on the NCSS of each state and accompanying action plans. The primary documents were publicly available NCSSs in English, which include various objectives, aims and goals for cybersecurity and list specific actions and implementation plans. In sum, this involved the analysis of seven primary documents – the NCSSs, action plans for policy implementation and in some cases – resolutions and laws in cybersecurity that were connected to the content of the NCSSs. The criteria for selecting NCSS documents was whether a selected state has adopted a NCSS, including specific tasks, objectives, deliverables and aims for cybersecurity for the state's public and private sectors. The author assessed whether and how specific factors were presented in the documents, and what were the central impetuses for establishing each NCSS as described by the document itself.

The author measured the presence of each variable, based on the assessment of the objectives, aims and content of each NCSS. NCSSs list specific measures and describe how the goals in areas such as science, economy and CI protection are reached. The key aspects that set NCSSs and other cybersecurity-related documents aside and which indicate the proliferation of cybersecurity as a policy concern is that the strategies involve not only the public sector and the protection of national CI, but also the private sector and focus largely on raising public awareness. As a result, the document analysis gives insight into how cybersecurity policy is framed to the public and the priorities in each case. The content of each NCSS was categorized based on the variables – policy and norm diffusion, economic considerations, external events, and innovations in technology. For

example, not every NCSS describes the aspect of public awareness on cybersecurity and the extent to which each NCSS involves the private sector varies by case. Thus, throughout the analysis, the author assessed how each factor is described, what is the context for each factor and what are the primary objectives for each factor, if mentioned in the NCSS. The document analysis therefore offers a comparative insight into the themes, priorities, topics and objectives described by the NCSSs and how each hypothetical factor is described by the document.

5. Analysis. Explaining the emergence of cybersecurity as a policy concern across NATO member states: the cases of Canada, Croatia, and Lithuania

This section assesses what drivers were behind the emergence of cybersecurity as a policy concern in each selected NATO member state. The analysis of this research begins by outlining the context and characteristics of the emergence of cybersecurity in selected states. The following sections are further divided into individual sections, with each focusing on variables and possible explanations for cybersecurity policies. The proliferation of cybersecurity in each state is measured by the implementation of strategies – either the absence or presence of a NCSS. Each analysis section presents the empirical evidence of the factors behind the emergence of cybersecurity as a policy concern, devoted to interviews with respective policymakers, who were involved in the process of NCSS formulation or implementation, and analysis of each NCSS of the states of interest. This data provides evidence on the causes and factors, which influenced the proliferation of cybersecurity as a policy concern in three states of interest, to find out why states have adopted NCSSs and why cybersecurity has emerged as a policy concern.

5.1 Case 1: Croatia – the emergence of cybersecurity concern

Before the establishment of the NCSS in Croatia, various information security acts and specific laws clarified specific regulatory aspects of information security and data protection, but a more encompassing cybersecurity policy was established in 2015. The primary goals of NCSS of Croatia are to improve the key areas of cybersecurity and to “recognise organisational problems in its

implementation and broaden the understanding of the importance of this issue in the society" (Government of the Republic of Croatia, 2015: 4).

Although the strategy states that it needs to be reviewed every three years (Government of the Republic of Croatia, 2015: 28), the renewed NCSS has not been formulated since the first strategy. This has been confirmed by an interviewee from Croatia (P4 Interview), who stated that: "/…/ our NCSS has not been updated for how long… 7 or 8 years. We have not been focusing on that but hopefully there are going to be changes" – this tendency is explained by them as a result of the post-Communist political culture, where public policies do not receive wide public attention and no specific actors take the lead in formulating policies. In sum, it could be observed that the adoption of Croatian NCSS in 2015 is a clear indicator of the emergence of cybersecurity as a policy concern, while the strategy sets out specific objectives, aims, goals, deliverables and an action plan for cybersecurity in Croatia.

Regarding the formulation of the NCSS, the strategy states that the central impetus was related to the responsibility of the society to acknowledge the importance of cybersecurity: "Recognising the importance of security within cyberspace as a common responsibility of all the society's segments prompted the making of this Strategy." (Government of the Republic of Croatia, 2015: 4). In conclusion, the primary objectives for formulating the NCSS according to the strategy itself were related to building public awareness and recognizing the risks of ICT, as well as to acknowledge the economic potentials and risks related to cyberspace, to enhance Croatia's capabilities in this field (Government of the Republic of Croatia, 2015: 4). Aside from defining cybercrime and cyberspace protection areas, the strategy further aims to achieve a common understanding of cybersecurity principles and objectives among various sectors and stakeholders. The strategy elaborates on the key areas and provides mechanisms for the implementation of the NCSS, including authorities and institutions responsible for the policy implementation. (Government of the Republic of Croatia, 2015: 4, 27).

The strategy aims to enhance coordination within state institutions, authorities and society, as well as listing the tasks, competencies and responsibilities of different actors and authorities. (Government of the Republic of Croatia, 2015: 4). The strategy has listed, among the objectives and principles of cybersecurity, the general goals of the NCSS, which include raising public awareness on cybersecurity, as well as through education programs; enhancing transnational

cooperation, e-services, research efforts, legal framework and regulations, and information sharing measures in the field of cybersecurity (Government of the Republic of Croatia, 2015: 7). With regards to the threat landscape of Croatia's cybersecurity, the strategy separates the cyber defense measures and objectives and cybercrime-related measures, stating that cyber defense: "/…/ is the subject of separate elaboration and action, which will be pursued using all the necessary elements arising from this Strategy" (Government of the Republic of Croatia, 2015: 9). Similarly to other NCSSs, this strategy seeks to enhance cyber crisis management, as well as addressing the need to establish a cyber crisis management framework and establishing "contact points" in case of cyber incidents (Government of the Republic of Croatia, 2015: 16, 17).

The overall NCSS formulation is according to one of the NCSS developers (P4 Interview) not related to "strong business and social motivators." The participant concluded this by stating that the NCSS of Croatia is simply "a list of to-do things", a set of priorities, and goals that need to be followed (P4 Interview). The policy paper formulation aspect of Croatia is concluded by them as an action where the policy is drafted by an external consulting agency or an enterprise, and the paper is later assessed by the respective authorities and policymakers and adopted: "Usually the policy papers are made by some other enterprise, for example, Ernst & Young. And then we look at it and think OK, we like this." (P4 Interview). The policy concern emergence of cybersecurity was concluded by P4, as a process, where no strong motivators or drivers were at play: "There are no motivators, but some political, when the Parliament says to do it – we do it". This indicates that there are certain policymakers, that drive the policy formulation and political will to formulate policies in the field of cybersecurity in Croatia. In conclusion, the proliferation of cybersecurity as a policy concern in Croatia can be traced to the adoption of NCSS in 2015. These findings suggest that the emergence of policy concern was present. The hypothetical explanations for the emergence of cybersecurity as a policy concern are assessed together with the interview responses in Section 6.1.

5.2 Case 2: Lithuania – the emergence of cybersecurity concern

The first national cybersecurity program in Lithuania was adopted in 2011, which outlined the regulation of state institutions' ICT and of the private sector (Government of the Republic of

Lithuania, 2011). The first national law on cybersecurity measures in Lithuania was adopted in 2014 – after several cyber incidents in 2012-2013 (Štitilis, Klišauskas, 2015: 48, 49) The initial framework of NCSS was laid down already in 2011, which was established in the form of a program, coordinated by the Ministry of Interior (Government of the Republic of Lithuania, 2011: 5). It should be noted that the measures of ICT and CI protection in Lithuania, as well as the policies of cybersecurity, as well as the responsible authorities, and control mechanisms, have been systematically amended throughout the years. The first time information security was included in the national security policy was in 2002, when the national security strategy briefly outlined an objective on the protection of informational technologies (version of 2005 - Government of the Republic of Lithuania, 2005: 1).

Vilpišauskas (2024: 1) concludes the developments of cybersecurity policies in Lithuania by implying that: "despite the growing number of cyberattacks, political and institutional change has initially been slow and it has taken a decade to establish an adequate legal and institutional framework." The drivers for policy concern emergence in Lithuania have been, according to Vilpišauskas (2024: 1, 17), despite the lack of coordination and attention on cybersecurity issues, specifically related to the start of Russian aggression towards Ukraine in 2014. The rise of cybersecurity on the policy agenda since has been further impacted by expert networking with external authorities, as well as cyber-attacks against Lithuania's institutions and companies (based on Vilpišauskas' interviews with the Lithuanian officials - Vilpišauskas, 2024: 5-6). Therefore, the emergence of cybersecurity as a policy concern is in many ways connected to the changing threat landscape and geopolitical developments in neighbouring states.

The first more encompassing cybersecurity regulation in Lithuania was established as a program, which foresaw a measure of the protection of CI, although not specifically stated as a NCSS, this document formally established the initial national cybersecurity priorities. This framework clarified the purposes of electronic information security and objectives for the security of ICT systems and entities, primarily to safeguard electronic information security (Government of the Republic of Lithuania, 2011: 1). Therefore, this short policy document clarified the primary objectives of national ICT protection but did not set out a specific strategy and an action plan to reach these aims. An overarching NCSS was later adopted in 2018, which was developed by the Lithuanian Ministry of National Defense (Ministry of National Defence of the Republic of

Lithuania, 2018). In sum, it could be assessed that the adoption of the Lithuanian NCSS in 2018 is a clear indicator of the emergence of cybersecurity as a policy concern, while the strategy sets out clear aims, objectives, goals, deliverables and actions for policy implementation.

The "Programme for the Development of Electronic Information Security (CyberSecurity)", adopted in 2011 and implemented by the Ministry of Interior, outlines the general objectives, aims and tasks for national cybersecurity. The Programme prioritizes the security of state-owned systems, as well as compliance with "the requirements of international standards" and aims to extend the cybersecurity protection measures to other areas as well (Government of the Republic of Lithuania, 2011: 2). The Programme highlights the need to establish a better basis for coordination between institutions to better detect vulnerabilities, concluding that:

> The dependence of different state and public activity areas on the use of information resources and services varies, therefore, in order to use funds efficiently, it is necessary to consolidate efforts and information resources in the areas where this dependence is stronger; the rate of criminal acts in cyberspace is rapidly increasing and large scale incidents in cyberspace can lead to a national crisis. (Government of the Republic of Lithuania, 2011: 2)

Besides the need to enhance coordination, this Programme outlines the need for ensuring a legal basis for incident response, backup solutions for security breaches, and incident management framework highlighting that cyber threats spread across states. Hence, the document goes further to propose that the principle of collective security should apply to the international level as well. (Government of the Republic of Lithuania, 2011: 3, 4) Besides the programme, a national law on the regulation and principles of cybersecurity (established in 2014) came into effect in 2015 (Government of the Republic of Lithuania, 2014). This law restructured the responsibilities objectives and tasks for enhancing cybersecurity, and most importantly - declared this area of security responsibility of the Ministry of Defense (Government of the Republic of Lithuania, 2014). As reflected by an interviewee from Lithuania, this shift reflects the change of priorities in the area of security:

> /…/ at that time people assessed that for a small country as we are and knowing the geopolitics, where we are surrounded, it should be somehow attached to security and defense. That's why the policy was in the Minister of Defense and the National Cyber Security Center was established at the Ministry of Defense. (P2 Interview).

The law on cybersecurity outlines that the principles and strategic goals were to be set by the Government of Lithuania and the implementation is set out by the Ministry of Defense and coordinated by the National Cyber Security Center, which was shortly established after (Government of the Republic of Lithuania, 2014). Aside from the law, the government of Lithuania approved the "Information Society Development Programme for 2014–2020 'Digital Agenda for the Republic of Lithuania'" (approved by the Government of Lithuania in 2014; Government of the Republic of Lithuania, 2017), which includes some aspects of cybersecurity and public awareness. This Programme does not set out specific targets but outlines the need to address cybersecurity-related vulnerabilities and enhance the use of digital technologies, further stating that: "Cyber security is the basis of Lithuanian economic growth and the information society" (Government of the Republic of Lithuania, 2017: 1, 12). On the risk assessment aspect, this Programme implies that the cybersecurity situation in Lithuania is "unsatisfactory", concluding that the number of threats has been growing faster than the capacities and the technologies related to national cybersecurity enhancement (Government of the Republic of Lithuania, 2017: 12).

A research project (Štitilis et al., 2017) was conducted that established a model for the Lithuanian cybersecurity strategy, which served as a guideline and a framework for NCSS formulation and implementation (P9 Interview). The groundwork for a national CS strategy had been laid down by the Programme (2011-2019) and Law on Cybersecurity (2014) in Lithuania. The Programme set out specific objectives, tasks, and responsibilities for enhancing cybersecurity, however, the NCSS goes further to set out specific criteria for policy implementation, as well as targets, by including responsibilities and rights for the private sector, aspects of public awareness and education on cybersecurity (Ministry of National Defence of the Republic of Lithuania, 2018: 7, 13).

The NCSS of Lithuania was adopted in 2018, and it outlines five core targets and objectives, the main aim being "/…/ to provide the Lithuanian people with the opportunity to explore the potential of information and communications technology (ICT) by identifying cyber incidents timely and effectively, by preventing cyber incidents and their recurrence, and by managing the impact of cybersecurity breaches." (Ministry of National Defence of the Republic of Lithuania, 2018: 4) In contrast to former policies, the strategy as a public policy focuses largely on public awareness and educational aspects of cybersecurity. In the case of Lithuania, the strategy, as well as the programmes and the law on cybersecurity in Lithuania focus on four main areas: firstly, the

documents point out the cybersecurity threat landscape in Lithuania, although the documents do not mention the specific actors. This aspect is tied to state-sponsored attacks, organized cybercrime and the need to decrease vulnerabilities related to the public sector and CI, which is further tied to military capacities in cyberspace. In conclusion, the main factors for the emergence of cybersecurity as a policy concern in Lithuania could be traced to the adoption of the NCSS in 2018. The strategy focuses largely on cyber threats and public awareness, as being one the key drivers for policy formulation in the area of cybersecurity. In conclusion, these findings suggest that the emergence of policy concern was present. The hypothetical factors for the proliferation of the emergence of cybersecurity as a policy concern will be examined together with the interview responses in Section 6.2.

5.3 Case 3: Canada – the emergence of cybersecurity concern

This section outlines the main developments of cybersecurity policy implementation in Canada. Canada first established its NCSS in 2010, which was put forward by the Canadian Department for Public Safety. This document outlines the principles of cyberspace protection, as well as defining key areas, terms, and objectives of cybersecurity. (Government of Canada, 2010) The NCSS of Canada established a system consisting of three pillars: “1. Securing Government systems”; “2. Partnering to secure vital cyber systems outside the federal Government”; “3. Helping Canadians to be secure online” (Government of Canada, 2010: 7), which reflect the priorities and considerations in the field of cybersecurity. Compared to other states in this study and globally, Canada was one of the earliest adopters of NCSS. The strategy, as well as the tasks of responsible authorities and institutions, have been systematically amended since. Primarily, cybersecurity policies in Canada have been the responsibility of the Department of Public Safety and Emergency Preparedness Canada (PSEPC) (Shackelford, Bohm, 2016: 66). Besides the Cyber Security Centre, established in 2018, cybersecurity policy implementation, education, and assessment are further divided between institutions and entities such as the National Cybercrime Coordination Unit, the Canadian Security Intelligence Service, the Communications Security Establishment, and the Royal Canadian Mounted Police. (Ministry of Public Safety and Emergency Preparedness of Canada, 2019: 6-7).

The first NCSS of Canada was adopted in 2010 by the Government of Canada. The strategy firstly highlights the need for securing cyberspace, as the number of users of ICT is growing and the economy is reliant on Internet services. Not only had businesses become more reliant on ICT, but the government of Canada had become dependent on online services, which had introduced new vulnerabilities to the users. (Government of Canada, 2010: 2—3) The strategy lists possible threats both to the users of ICT and the operators of CI. As concluded in the introduction of the strategy:

> The threat is becoming more serious. We cannot allow our cyber security efforts to remain fixed on the threat as we understood it in the past. To ensure that our advanced use of cyberspace remains a strategic asset, Canada must anticipate and confront emerging cyber threats. (Government of Canada, 2010: 3)

The first NCSS of Canada continues by listing the most common threats, their origin, and methods for cyber attacks, which are categorized into three sections: 1) "State Sponsored Cyber Espionage and Military Activities"; 2) "Terrorist Use of the Internet"; and 3) "Cybercrime". (Government of Canada, 2010: 5) The document further highlights what other states have done to increase cybersecurity capacities and address the threats, by outlining that cybersecurity has become an integral part of security and military elsewhere, especially in NATO.

In addition to the first NCSS of Canada, the action plan for NCSS implementation in Canada, published in 2013, lists responsible institutions for policy implementation, specific actions together with timelines and deliverables, and comments on the status of the NCSS implementation process (Government of Canada, 2013). The strategy was revised in 2018 and the revised document firstly outlines that malicious actors use new technologies and low cybersecurity awareness increases risks (Public Safety Canada, 2018: 2), yet the aims, tasks, and objectives for enhancing cybersecurity have not drastically changed compared to the first strategy. The renewed NCSS focuses on new three core areas: 1) "Security and Resilience" 2) "Cyber Innovation" and 3) "Leadership and Collaboration" (Public Safety Canada, 2018: 3). Similarly to the first strategy, the renewed strategy focuses on the protection of CI, civilians, and private sector, and emphasizes the emergence of new threats and technologies with the aim to: "Proactively adapt to changes in the cyber security landscape and the emergence of new technology" (Public Safety Canada, 2018: 4). In conclusion, it could be inferred that the adoption of the Canadian NCSS in 2010 is an indicator for the emergence of cybersecurity as a policy concern, while it put forward national measures, objectives, aims and deliverables for policy implementation in the area of cybersecurity.

In sum, both strategies focus largely on cyber threats, as well as economic considerations and innovations in ST&E. These findings suggest that the emergence of policy concern was present and the hypothetical factors for the proliferation of cybersecurity as a policy concern, together with the insights from the interview respondents, will be examined in Section 6.3.

6. Analysis: findings from the interviews and NCSSs

The following sections will focus on the findings from NCSSs and interviews. To measure each variable, the author measured the presence of each factor, namely – policy and norm diffusion, economic factors, the impact of external events and crises and innovations in ST&E. The analysis focuses on whether or not each variable is present in the interviews and NCSS documents. Each sector sums up the findings from the interview data and document analysis.

6.1 Drivers for the emergence of cybersecurity as a policy concern in Croatia

This section examines the potential drivers for the emergence of cybersecurity as a policy concern in Croatia. By examining the different factors based on the interview data and NCSS, this section traces the causes of the emergence of cybersecurity as a policy concern in Croatia and concludes the findings.

In the case of Croatia, the main impact and impetus for policy development came from the EU, as outlined by the interview respondents of Croatia (P3, P4, P13, P14 Interviews). The Croatian NCSS highlights the need for acquiring international standards and regulations of data protection, specifically those related to the EU and NATO; which is specifically addressed by the risks and inadequacies related to data protection (Government of the Republic of Croatia, 2015: 19, 20, 23). The central drivers for cybersecurity policy are, according to the Croatian interviewees (P3, P13, P14 and P4 Interview), related to the EU regulations and directives on the one hand and evolving cyber threats (P3 Interview). A key impulse for the emergence of cybersecurity as a policy concern came, according to current advisors on cybersecurity (P13 and P14 Interviews) in Croatia, in 2013, when Croatia became a member of the EU.

The regulations of the EU, as well as the directives on cybersecurity, have served as milestones and guidelines in cybersecurity policy development in Croatia, the examples of cybersecurity policies and strategies of other states are also closely monitored in Croatia. As implied by one of the advisors on cybersecurity – "I'm not aware of any particular national or international event which triggered this. As I said, there is a set of people who work on this. I think the NIS directive certainly helps us to materialize these ideas in which way we should go." (P13 Interview). Both the NCSS (Government of the Republic of Croatia, 2015: 10, 24) and all of the Croatian interviewees (P3, P4, P13, P14) highlighted the need for adherence to the regulations and standards of the EU and the practices of other states. In conclusion, the interview participants concluded that the main driver for policy formulation in this area has been the standards and directives of the EU on cybersecurity, which set standards for cybersecurity regulation and ICT protection. The policies of other EU member states have also impacted how cybersecurity policies are set forward. For example, one of the interviewees (P14) outlined: "we are always looking at Belgium. Netherlands, Italy, and sometimes Austria. I think that's it. We are monitoring every publicly published document. /…/ We will see the various ways of implementation for example." Therefore, the policies of other states, but more specifically the regulations and directives on the EU level, have impacted how cybersecurity has emerged as a policy concern in Croatia and have served as guidelines for policy formulation. The EU has not only set specific regulations and standards, but as seen from the case of Croatia, the policies of other EU member states have also had an impact on domestic policies and policy concern emergence. In conclusion, based on the findings from Croatia's NCSS and interview responses, the factor of policy diffusion was present and is connected to the emergence of cybersecurity as a policy concern in Croatia.

On the economic considerations, the Croatian Strategy calls for the enhancement of the development of new services and products, and to further promote these developments on a global scale (Government of the Republic of Croatia, 2015: 26). One of the interviewees (P3) stated that one of the drivers for cybersecurity policies is related to the considerations, potentials, and prospects of the digital economy and enhancing the digital services and products of Croatia, to gain attraction on the global market. Against this, one of the policymakers, P4, argued that there have been no strong business or economic considerations related to the emergence of cybersecurity as a policy concern, while small enterprises of Croatia rent their services to bigger companies of other states and cybersecurity culture and services do not receive wide attention.

Compared to the strategies of other states and the responses from interview participants, the economic considerations had the lowest impact on the emergence of cybersecurity as a policy concern in Croatia. This could be explained by the lack of involvement with the private sector on cybersecurity matters and as implied by one of the interview respondents of Croatia, there is a lack of business motivators for policy development in the field of cybersecurity (P4 Interview). The small enterprises of Croatia rent their services to foreign companies (P4 Interview), which implies that in these cases, the regulation of cybersecurity falls under the responsibility of other states or companies. In conclusion, the economic considerations factor is almost present but had a rather limited impact on the emergence of cybersecurity as a policy concern in Croatia.

Regarding the impact of external events and crises, a current advisor on cybersecurity in Croatia highlighted that the drivers for cybersecurity policy development have been events, that have a large-scale impact on a domestic level, specifically the COVID-19 pandemic and the earthquake in Croatia, where the necessity to ensure the smooth functioning of public services gained more attention (P4 Interview). Yet, the emergence of cybersecurity as a policy concern in Croatia has not been interconnected to the cybersecurity threat landscape or specific cyber incidents: “The practice of the European Union, the connections with other CERTs and with other member states have been the drivers. But we don’t have many large incidents or something like that to drive the policies.” (P14 Interview). In sum, the NCSS of Croatia and the interviewees did not mention external events or crises, that could have had an impact on the emergence of cybersecurity as a policy concern in Croatia. One of the interviewees (P4) highlighted the impact of events, that have had internal impacts, specifically the COVID-19 pandemic and the earthquakes in Croatia, yet these internal developments have raised a concern regarding the protection of CI and certain critical services, evoking reactionary measures. In conclusion, this indicates that the factor of external events and crises was not present in the case of Croatia, as indicated by the NCSS and interview respondents.

On the impact of new technologies, the NCSS of Croatia highlights the impact of new technologies, implying that the use of new technologies brings about risks, while the users are not aware of the security characteristics of the new digital products (Government of the Republic of Croatia, 2015: 3, 27). This is further highlighted in relation to the rise of cybercrime, as the new technologies create new measures and tools for committing cybercrime (Government of the

Republic of Croatia, 2015: 16, 17). The abnormal functioning and abruption of ICT could also end with serious consequences: "for the functioning of the State; it can cause loss of life, damage to health, great material damage, pollution of the environment and the disturbance of other functionalities essential for the proper functioning of the society as a whole" and could lead to serious impacts on global security (Government of the Republic of Croatia, 2015: 3). An expert on cybersecurity in Croatia, P3 highlighted the need to address the risks related to the changing landscape of technologies, as well as the considerations related to the digital economy and competitiveness in the global market. The P3, P14 and the NCSS of Croatia (Government of the Republic of Croatia, 2015: 3) implied that the innovation of technologies brings about new risks, which need to be regulated on a national level. Thus as technology advances, so do the tools and measures for committing cybercrime, and risks for the users and operators of ICT increase. In sum, the factor of innovations in ST&E was present in the case of Croatia, as the emergence of cybersecurity as a policy concern and policy formulation was connected to the emergence of new technologies and innovations in this field.

In sum, the analysis examined the impact of each factor on the emergence of cybersecurity in Croatia. In conclusion, the emergence of cybersecurity as a policy concern in Croatia is interconnected to two main factors. The NCSS itself implies the need to enhance public awareness, as well as to realise the economic potential of cybersecurity and the need to address the risks related to new technologies. The interviewees did not largely focus on the economic considerations but on the need to adhere to the EU regulations and directives in the area of cybersecurity. The need to formulate or reform policies by certain policymakers and cybersecurity expert groups in Croatia is illustrated by one of the current information security advisors who implied that it is important to have certain groups who advocate for policy formulation and without this support, the policies are difficult to implement (P13 Interview). This illustrates how a certain group, with a specific mission, can raise a policy concern and advocate for a policy change on a national level.

In the case of Croatia, the EU regulations as well as the policies of other member states had the largest influence on the emergence of cybersecurity as a policy concern. This refers directly to policy diffusion, as the EU member states share their practices and are informed about the developments in the area of cybersecurity elsewhere. Norms and external events had practically no impact on policy concern emergence, as no developments, events and norms were mentioned

by the NCSS and the interview respondents and the causal link to international norms on cybersecurity was denied. The technological innovations and economic considerations had a limited impact, as these causes were not highly mentioned. As explained by one of the NCSS developers of Croatia (P4), this is explained by several factors. On the one hand, the post-Communist political culture in Croatia does not prioritize public policies and involvement with stakeholders and the private sector. Additionally, there are no economic or business motivators, as Croatian enterprises rent their services to bigger companies outside of Croatia (P4 Interview). Therefore, the economic considerations are not strongly connected to the emergence of cybersecurity as a policy concern. The cybersecurity threat landscape is not illustrated by large-scale incidents or state-sponsored attacks, but rather by economically motivated cross-border cybercrime, which requires responses on a regional scale and cooperation with CERTs from other states. In sum, the factor of policy diffusion was present and the most decisive cause for the proliferation of cybersecurity as a policy concern. The factor of innovations in the fields of science and technology was also present, as being one of the drivers for the emergence of cybersecurity as a policy concern. The factors of norm diffusion, external events and crises were absent in the case of Croatia and the factor of economic considerations was almost present.

6.2 Drivers for the emergence of cybersecurity as a policy concern in Lithuania

This section examines the potential drivers for the emergence of cybersecurity as a policy concern in Lithuania, based on the findings from the interviews with policymakers and cybersecurity policy documents. Based on the empirical evidence, this section traces the factors that are connected to the emergence of cybersecurity as a policy concern in Lithuania.

Similarly to the case of Croatia, the regulations and directives of the EU have also had a large impact on the emergence of cybersecurity as a policy concern. A policymaker (P9 Interview) from Lithuania, who was involved in the NCSS formulation, recalled that the impetus for the NCSS development stemmed from both national needs and the evolving threats, and the EU regulations and directives in the area of cybersecurity. Speaking of the practices of other states, the participant concluded that they were influenced by the Netherlands' approaches to cybersecurity, especially the vulnerability-disclosure aspect, which was included in the Lithuanian NCSS (P9 Interview).

Regarding the contents of the strategies, the same interviewee highlighted that these were both related to the political climate and the policies of other states:

> When we talk about strategy, the politicians and policy issues overcome the threat landscape. /…/ Also, ENISA has a framework for cyber security strategies, but they didn't make a great influence. Because we already had the researchers' document for Lithuania and the best example from the Netherlands. (P9 Interview).

All of the interview respondents highlighted the role of the EU regulations and guidelines in the area of cybersecurity, specifically the NIS directives. As outlined by policymakers from Lithuania (P2, P7, P9, P10 Interviews), the main guidelines currently come from the EU level. Speaking on practices and policies of other states, P10 highlighted that the US is the main partner in this regard, yet the practices of neighbouring states and the Baltic region are also important for policy insights. According to one of the policymakers from Lithuania, the cybersecurity guidelines from NATO, although related to the area of defense, have also had an impact on how the regulations and policies are formulated in Lithuania, but this is specifically related to the area of defense (P2 Interview). Another policymaker from Lithuania concluded that the EU is not only a source for cybersecurity standards, obligations and guidelines, but is important for sharing experiences and approaches across the member states:

> At the end of the day, I believe we should be all on the same page and we can learn from each other, from their societies, the strategies, to share our knowledge, to see what and why it works. Sometimes it's great to see the different approaches, but achieving maybe the same or even higher result results in cyber at the same time. (P7 Interview)

The aspect of collaboration in policymaking was also mentioned in the NCSS of Lithuania, specifically with the focus on international cooperation being one of the targets of the strategy (Ministry of National Defence of the Republic of Lithuania, 2018: 18). In this regard, the NCSS specifically highlights the example of the US: “Lithuania shall also strengthen bilateral political and technical cooperation with other countries which adhere to the principles of democracy, especially, with the United States of America.” (Ministry of National Defence of the Republic of Lithuania, 2018: 18). In sum, policy diffusion had an impact on the emergence of cybersecurity as a policy concern in Lithuania. The EU has set standards, regulations and laws on cybersecurity, which are mandatory for each member state. Not only have the EU regulations and directives impact on national policies, but the policies of other member states inspire and diffuse among the

EU member states, as seen in the cases of Lithuania and Croatia. In conclusion, the standards of the EU, as well as the policies of the EU member states and the US have had an impact on the emergence of cybersecurity as a policy concern in Lithuania.

In the case of Lithuania, one of the main considerations for NCSS formulation was according to one of the authors of the Lithuanian NCSS (P9 Interview), the need to enhance cybersecurity capabilities and the need to address the cybersecurity aspects of public-private partnership (PPP), specifically regarding CI operators. The latter was proposed by the private sector representatives themselves, who implied that the PPP objectives of cybersecurity should be addressed in the NCSS (P9 Interview). On the considerations of the (digital) economy, the Lithuanian NCSS briefly implies that the nature of cybercrime tools is evolving, which has negative consequences on the global market (Ministry of National Defence of the Republic of Lithuania 2018: 8, 10, 11). In sum, the NCSS of Lithuania does not widely focus on the economic considerations, but rather on the partnership between the public and private sectors to prevent cybercrimes and promote cybersecurity culture (Ministry of National Defence of the Republic of Lithuania 2018: 11, 12). Besides state-sponsored cybersecurity threats, another threat that drives policy concern is related to organized crime and the financial losses related to it:

> Cybercrime is like a platform, as a service software. /…/ It's like buying arms and in the darknet, everyone can do a lot of damage. You can even destroy businesses using cyber. It is not necessary to have knowledge of how to program, how to deal with the Internet, or how to deal with cybersecurity – just order an attack and you will achieve your goals (P7 Interview).

The economic side of cybersecurity is, according to the interview respondents from Lithuania, one of the key drivers for policies and regulation in this field as the economic considerations are closely interconnected to the cybersecurity threat landscape (P2, P7, P10). On the one hand, national cybersecurity efforts are the key to tackling cybercrime and decreasing financial losses related to cybercrime. Additionally, as some of the interview respondents (P7, P10) from Lithuania stated, cybersecurity policies and measures are instruments to enhance economic prospects and attract foreign investments. This is closely intertwined with the threat landscape and threat management, as the increase in cyber incidents decreases economic opportunities. As concluded by one of the interview respondents from Lithuania (P7 Interview), cybersecurity policies serve also as a tool to enhance compliance in the private sector. One of the core areas of the Lithuanian strategy is related

to the enhancement of public-private partnership (PPP), which is said to be vital for the private sector to better combat cybersecurity incidents and to reduce vulnerabilities (Ministry of National Defence of the Republic of Lithuania 2018: 16, 17). Aside from the closer engagement with the private sector, one of the policymakers from Lithuania (P7 Interview) implied, that cybersecurity is intertwined with freedom, as well as sustainable economic growth of the state. In sum, compared to Croatia, economic considerations had more impact on the emergence of cybersecurity as a policy concern. This is primarily indicated by the involvement and cooperation with the private sector, to mitigate possible cybersecurity risks and ensure compliance with cybersecurity policies. In conclusion, the factor of economic considerations was present in the case of Lithuania, as economic considerations and specifically cooperation with the private sector was connected to the proliferation of cybersecurity as a policy concern.

Regarding the impact of external events and crises, the Lithuanian NCSS firstly outlines that Lithuania has become an increasingly attractive target for cyber attacks not only for organized groups but for other states, which put strategic entities and critical information infrastructure at risk (Ministry of National Defence of the Republic of Lithuania 2018: 7). Similarly, the document outlines, based on the assessments from NATO and the EU, that cyberspace is increasingly being used as an instrument of hybrid warfare, which is specifically illustrated by the examples of the attacks on Ukrainian nuclear facilities and the use of Stuxnet virus against Iran (Ministry of National Defence of the Republic of Lithuania 2018: 8). Compared to cybersecurity policies of other states in interest, both the Lithuanian NCSS and interview respondents focused widely on the domestic and international cybersecurity threat landscape. Some respondents highlighted the state-sponsored attacks from Russia and China, and the start of Russian aggression towards Ukraine in 2014 as being triggers for cybersecurity policy formulation (P2, P10 Interviews). One of the policymakers from Lithuania (P2 Interview) concluded that the key drivers for cybersecurity policies are threats:

> The main driving force is threats. When we talk about threats, first of all, of course, we look to those that are state-sponsored. So knowing our geopolitical situation and seeing what's happening in Ukraine, we are developing our policies in line with the current developments. You have to be prepared for the threats and understand them and then develop the measures, and policy of course, how to be more resilient. (P2 Interview)

Aside from the aforementioned policy concern drivers, the respondents from Lithuania also highlighted the impact of internal events, such as data leaks or political events, such as high-level political summits (P2, P6, P9, P10 Interviews). These events and incidents have, according to the interview respondents, served as triggers for enhancing cybersecurity capabilities, as well as policies and regulations in this area. Therefore, the events in Lithuania's neighbourhood and the resulting changing threat landscape have impacted the emergence of cybersecurity as a policy concern, especially the latest events and crises in Lithuania's neighbouring states. Compared to other states in this research, the strongest impact of the events is rather geopolitical, as seen in the case of Lithuania. The external events and crises had the largest impact in Lithuania's case, where geopolitical developments have played into the changing cybersecurity threat landscape. As seen from the interview responses and the NCSS of Lithuania, the threat landscape aspect is a critical aspect of cybersecurity policies and risk assessment. Thus, Lithuania's cybersecurity policies are developed in line with the geopolitical developments in Lithuania's neighbourhood, as implied by the interview respondents from Lithuania (P2, P10 Interviews).

Regarding the innovations in ST&E, the various innovations in technology and the risks related to them were highlighted by Lithuanian policymakers and experts. As it was concluded by one of the legal experts from Lithuania, in cybersecurity, innovations in technology evolve at a rapid speed, therefore it is critical to keep up with the regulations and policies in this area (P6 Interview). The changing cybersecurity threat landscape is further related to the emerging technologies and developments in ST&E. As outlined by the interviewees (P6, P7, P10) and NCSS of Lithuania (Ministry of National Defence of the Republic of Lithuania 2018: 8, 13), emerging technologies introduce new risks and vulnerabilities, as well as opportunities to enhance cybersecurity capacities. Some interview respondents (P7, P10) from Lithuania outlined that the new technologies also create new instruments and tools for committing cybercrime and malicious cyber acts. In conclusion, the lack of standards and regulations creates a space for criminal activities, as well as state-sponsored attacks. In conclusion, the factor of new technologies and innovations in ST&E was present in the case of Lithuania, as the emergence of cybersecurity as a policy concern has been connected to the changes in the cybersecurity threat landscape as a result of the development of new technologies. A policy advisor from Lithuania outlined that this aspect is also related to the lack of regulation in this area, as some states do not regulate the use of new technologies and ICT:

> Unfortunately, authoritarian states are not regulating cyberspace. They're not setting AI strategies, cyber strategies, certification systems, or security requirements. /…/ But they move forward very fast. They invest a lot in technologies, and in criminals, they allow criminal activities. /…/ We all have good technologies, but our mentality is different and I believe this is the main threat here. (P10 Interview)

In sum, the cyber threat aspect is highlighted by the cybersecurity policy documents and the interview respondents of Lithuania (P2, P9, P10 Interviews), who imply that cybersecurity policies are driven by state-sponsored threats, as well as threats related to cybercrime. The second dimension of the emergence of cybersecurity as a policy concern in Lithuania is related to the digital economy and economic considerations – in this regard, the documents and interview respondents outline the economic risks (as well as risks regarding economic prosperity) and direct financial losses specifically related to cybercrime. The growing dependency on IT introduces new risks therefore outlining specific tasks for reducing vulnerabilities related to the use of new technologies. This is closely intertwined with public awareness, which is a focal point for the NCSS of Lithuania.

In conclusion, the emergence of cybersecurity as a policy concern in Lithuania is connected to several factors and developments. As one of the NCSS developers (P9 Interview) outlined, the policy development has been influenced by the examples of other states, namely the Netherlands, which is observable as policy diffusion in the area of cybersecurity. Another key driver has been the technological developments, as well as the new platforms and technological tools, which introduce new risks to the users. Compared to other states in this research, Lithuanian policies on cybersecurity, as well as the interview respondents largely focus on the geopolitical threat landscape and risk management. In addition to addressing threats, a key component of cybersecurity policy development has been acquirements and directives on the EU level, which set out standards and regulations in the area of cybersecurity for the EU member states. This consideration has been mentioned by all of the Lithuanian interviewees and NCSS. Finally, an aspect which was covered by the interviewees and NCSS is related to economic considerations. Although the considerations have not been largely focused on, the interview respondents and the policy documents addressed the need to enhance economic potential, as well as compliance within the private sector, to address the threats posed by other states and organized cybercrime.

The threat landscape aspect was closely connected to the geopolitical developments and events in Lithuania's neighbourhood, as state-sponsored cyber-attacks are viewed as the largest threat to Lithuania's CI and ICT. In sum, technological innovations have created a need to impose regulations in this area, to raise awareness of cybersecurity, as well as to decrease vulnerabilities related to cybercrime and state-sponsored cyber-attacks. Compared to other states in this research, the geopolitical dimension and the aspect of external events were strongest in the case of Lithuania. Additionally, no norms were mentioned in the documents and the interview respondents or related by the interview respondents to the proliferation of cybersecurity as a policy concern, therefore this factor was not present. In sum, the key factors for the emergence of cybersecurity as a policy concern in Lithuania were policy diffusion, economic considerations, the impact of external events and crises, and innovations in ST&E.

6.3 Drivers for the emergence of cybersecurity as a policy concern in Canada

This section examines the drivers for the emergence of cybersecurity as a policy concern in Canada. By examining the different drivers for the proliferation of cybersecurity as a policy concern, this section traces the factors that are connected to the emergence of cybersecurity as a policy concern in Canada.

In the case of Canada, the external impulse for the emergence of cybersecurity as a policy concern is closely linked to the developments and events in the US. The CI of Canada and the US are closely interconnected, which requires unitary standards and regulations for the operators of ICT and CI on both sides, as indicated by the interview respondents of Canada (P1, P5, P8, P12). As illustrated by one of the interviewees, the harmonization of regulation and policies in both countries is necessary for the protection of CI with the US and with the Canadian companies in Europe:

> Whatever we're doing generally has got to be reasonably consistent with what certainly our closest ally, even geographically, the United States, but also consistent with what's going on in Europe. Because a lot of Canadian companies do business with Europe and are impacted there. /…/ we talked to other countries as well and coming out of that, we said, OK. These three topics that we built our strategy around seemed to be fairly consistent with what other countries are also taking a look at. (P1 Interview)

According to all of the interviewees of Canada (P1, P5, P8, P12), Canada is closely building its cybersecurity capacities together with the US, some respondents implied that Canada is always observing what other NATO allies are doing in the cyber realm, but more specifically focusing on Five Eyes alliance partners (P1, P12 Interviews). On cybersecurity incidents and collaboration, a former policy advisor implied that Canada is always cooperating with other states to attribute malicious acts in cyberspace, but never doing attribution alone:

> Canada has never done an attribution by itself, ever. We always do it with our allies. /…/ We've had some pretty serious incidents of our foreign affairs ministry being hacked at least twice in the past two years and we've never attributed that. I mean - everyone knows it's Russia. But they won't formally attribute it. (P12 Interview)

On the impact of norms, no specific cybersecurity laws or international norms were mentioned in the NCSS documents. Only one of the interview respondents mentioned international norms, specifically the Tallinn Manual, yet the impact it has specifically in the case of Canada is arguable as implied by the participant (P12 Interview). The former policy advisor stated that the proliferation of cybersecurity as a policy concern is not traceable to external events and crises on the one hand, and is not connected to international norms either (P12 Interview). The first NCSS of Canada highlights that the NCSS "Builds upon our close working relationships with our allies." (Government of Canada, 2010: 8). This is further illustrated by the cooperation with Australia, the US and the UK, outlining that the priorities and principles on cybersecurity of those states resemble with those of Canada, which demonstrates the similar experiences of Canada's allies (*ibid*). In addition, the second NCSS of Canada mentions the aspect of international coordination (Public Safety Canada, 2018: 17). On collaboration, the second NCSS outlines that the national efforts will be supplemented by international cooperation to mitigate cybersecurity risks and promote the interests of Canadian citizens (Public Safety Canada, 2018: 27, 32). In conclusion, the CI of Canada is closely connected to the US, which requires common standards, policies and regulations in the field of cybersecurity. This indicates, that specifically in the area of critical information infrastructure, the policies of Canada and the US diffuse and are formulated in collaboration. The policies and standards of cybersecurity are closely connected to the US, as both states share parts of CI and ICT. Thus, the emergence of cybersecurity as a policy concern in Canada has been driven by the policies and developments of the US, indicating a diffusion of policies.

Compared to other states in this research, Canada focuses widely on the economic considerations in the field of cybersecurity. Aside from the protection of CI, Canada's first NCSS highlights the economic considerations for cybersecurity capacity building, especially the economic prosperity and growth of Canada, and the reputation of Canada on an international scale. This is closely related to the actions of Canada's allies, who also put increasing effort into cybersecurity frameworks and policies. (Government of Canada, 2010: 7, 8, 10) Domestically, the security of cyberspace is framed in the strategy as "a matter of national security and sovereignty, protecting the lives of our foreign service, military and law enforcement personnel, the integrity of our economy, and safeguarding the personal information of Canadians." (Government of Canada, 2010: 9) This aspect highlights the economic and security interconnections to cybersecurity, which is further outlined by its relevance to the economy and reputation:

> The economic success of Canada's private sector depends in large measure on its ability to secure cutting edge research and intellectual property, business transactions and financial data. Failing to secure these assets inevitably leads to lost market share, fewer customers and corporate breakdown. (Government of Canada, 2010: 11)

The private-sector involvement, as well as the economic prosperity aspects, were also highlighted by the interviewees of Canada (P1, P5, P8, P12). In comparison to other NCSSs studied in this research, Canada puts a great effort into private-sector involvement in building cybersecurity capacities, as well as collaboration with Canadian companies. As stated by one of the former policy and legal advisors (P8 Interview) – the private sector is like a glue that holds together the efforts made by different levels of government, municipalities, and communities of Canada. Participant 1, who was involved in the formulation of the first NCSS of Canada, emphasized that one of the key considerations and drivers for strategy formulation was related to enhancing cybersecurity capacity building in collaboration with the private sector and building awareness of the business risks related to cybersecurity vulnerabilities. Participant 5 concluded this by outlining that:

> Canadian governments have been slow in developing their own capacities. I think they have tried to be careful not to put too much pressure on economic growth in other areas by imposing regulations on the Canadian private sector with respect to cyber security. Canada has chosen to sort of side with the private sector, in trying to develop cyber security capacities more so than in Europe. (P5 Interview).

Similarly, the revised NCSS of Canada focuses on a variety of cybercrimes, more specifically malicious cyber acts that are conducted for financial gain, hacktivism, and cyber tools that are

developed by other nation-states with military or hostile intents that could pose risks to Canada's CI. Despite the growing number and sophistication of attacks on the public sector, the Government highlights the potential of digital innovation. (Public Safety Canada, 2018: 9, 13, 14) As outlined by the first strategy, the revised strategy, and one of the interview respondents, a focal point for establishing coordination and an overarching cybersecurity-related policy was to either establish or enhance the existing capacities of one point of the government that answers to cybersecurity emergencies (P1 Interview; Government of Canada 2010: 10; Public Safety Canada, 2018: 11). The private-public partnership is highlighted by the standards, information-sharing, and guidelines that are expected from the government to enhance cybersecurity culture and foster cooperation (Public Safety Canada, 2018: 11). The risks on both public and private sector are described as following:

> As malicious cyber tools become increasingly accessible and as rates of cybercrime continue to rise, there is a real threat to Canada's economic well-being. Furthermore, as more of Canada's critical infrastructure can be controlled remotely and essential services are managed online, cyber incidents have the potential to compromise national security and public safety. (Public Safety Canada, 2018: 14)

On the economic considerations, the revised NCSS of Canada highlights the potential of digital innovation, specifically related to economic opportunities, prospects as well as breakthroughs in cybersecurity research. A critical aspect is to raise awareness of cybersecurity, as well as to overcome the cybersecurity skills gap and one of the aims of the strategy is for Canada to become a leader and a good example of cybersecurity on a global scale. (Public Safety Canada, 2018: 19, 20, 14, 26, 29, 31) As some of the interviewees of Canada highlighted (P1, P12 Interviews), the overall aim is to guide not only Canadian citizens but other states in developing cybersecurity policies and becoming an example of well-sophisticated cybersecurity management. In sum, the economic considerations had a large impact on the proliferation of cybersecurity as a policy concern in Canada. Compared to other states in this research, the economic considerations had the strongest impact in the case of Canada, where a great emphasis is both on the economic prosperity, digital innovations, and cooperation with the private sector, as well as the economic risks related to state-sponsored cyberattacks and cybercrime.

On the impact of external events and crises, a former advisor to the government of Canada (P12 Interview) outlined that cyber attacks were becoming more frequent around the world, which did

raise a policy concern on a global scale. Another impulse for cybersecurity capacity building in Canada came around 2017, after the US elections and due to foreign threats, mainly posed by China and threats against other NATO allies (P12 Interview). However, both the the first NCSS and the revised NCSS of Canada do not mention external events or crises, that could have raised the concern related to cybersecurity. The state-sponsored attacks and the sophistication of instruments for committing cybercrime have been highlighted both by the Canadian NCSSs and the interviewees, as was concluded by one of the cybersecurity experts in Canada:

> I would view the ransomware situation in Canada as a crisis. We are seeing sophisticated attacks against the public and private sectors, attacks against organizations, hospitals and we're seeing attacks against financial institutions, municipalities, and all levels of government and I don't think Canadians understand how serious it is. I don't think Canadians understand that we are essentially on the front lines of a global cyber conflict that involves geopolitical considerations – Russia's expansionist agenda. (P5 Interview)

One of the cybersecurity experts of Canada (P5 Interview) traced the cybersecurity threat landscape awareness aspect to the technological counter-measures response to the Bronze Night cyberattacks against Estonia in 2007 – "The innovations that Estonia has developed in reaction to Russian cyberattacks have, I think, made the world critically aware of that domain" (P5 Interview). However, one of the former policymakers of Canada argued against that, implying that the threat considerations are, considering public attention, a distraction – "Part of that, I think is useful, it is a useful force, and it does kind of drive greater understanding. I think it's also an enormous distraction." (P8 Interview). In sum, the external events have had practically no impact on the emergence of cybersecurity as a policy concern. As such, external events have not led to specific reactionary measures or the proliferation of cybersecurity as a policy concern in the case of Canada.

On the innovations in ST&E, one of the main threat considerations in Canada's first NCSS is related to the emerging technologies – as the ICT evolves, it is further reflected in the evolution of cyber attack tools, which have recently accelerated and the trustworthiness of suppliers and technologies' reliability is in question (Government of Canada, 2010: 5, 6, 11). The ST&E development aspect is concluded in the NCSS concerning cybersecurity measures: "For each new technology or practice adopted to enhance our cyber security, another is developed to circumvent it." (Government of Canada, 2010: 10). Therefore, as the technology advances, so do the means

and tools for committing cybercrime and conducting cyber-attacks. The revised NCSS of Canada focuses throughout the document largely on the emergence of new technologies and the opportunities and risks they bring about. Regarding the threat landscape, the 2018 NCSS version assesses that the magnitude of cybersecurity threats is increasing and the overall number of state- and non-state-sponsored attacks against the Government has grown. (Public Safety Canada, 2018: 6, 9, 15) The interview respondents from Canada (P1, P5, P8, P12), highlighted the seriousness of the changing threat landscape in cybersecurity, concluding this as one of the drivers for the proliferation of cybersecurity as a policy concern. As Participant 5 outlined: "The pace of cyber-attacks and the sophistication of cyber-attacks across Canada and our public sector, private sector, and critical infrastructure has significantly increased now over the years." (P5 Interview)

The development of new technologies and innovations in ST&E have created a need for new regulations and raising public awareness of the risks associated with the use of new technologies. As one of the former policymakers from Canada concluded, the NCSS authors knew that the risks were going to evolve as the technologies advance, therefore it was and is necessary to keep up with the developments in ST&E and regulate this area (P1 Interview). On the policy concern emergence of cybersecurity, a policymaker who was involved in the first NCSS formulation highlighted that the government was becoming more aware of the cybersecurity risks since the mid-2000s:

> Cybersecurity, in the sort of mid-2000s, was starting to become more of an issue for both the public and government. /…/ Most of the cyber-attacks were coming in against the government. DDoS attacks were probably the biggest issue. Ransomware attacks basically did not at that time did not exist, so it was up to us how to enhance the security of government systems. We knew that was coming. Looking at security, the private sector was also going to be a concern. (P1 Interview).

On the one hand, the changing cybersecurity threat landscape created a hurting stalemate, where the *status quo* was no longer sustainable and regulatory measures were needed. On the other hand, the mission of policymakers at that time was to raise public awareness of cybersecurity, as well as the evolvement of the awareness in the private sector. According to one of the NCSS developers (P1 Interview), at the time when cybersecurity emerged as a policy concern in Canada, there were attacks on CI, but the reach and volume of the attacks were not as extensive as it is today, yet the policymakers were aware that the situation was going to get worse if a national CS policy was not

put forward. In sum, as seen from the both NCSSs of Canada and the responses from the interviewees, the proliferation of cybersecurity as a policy concern is connected to the innovations in the field of ST&E, while the new technologies bring about new risks and uncertainties, which need to be regulated domestically.

In conclusion, both the NCSSs and interview respondents of Canada mainly focused on three topics on cybersecurity: economic considerations, risks posed by new technologies and the threat landscape. Compared to other states in this research, Canada largely focuses on cooperation with the private sector, to realize the economic potentials of cybersecurity. The threat aspects and the risks posed by new technologies and platforms, interconnected to other factors, were outlined by all of the interview respondents, as well as the NCSSs. As concluded by one of the developers of Canada's first NCSS (P1), the impulse for policy concern emergence stemmed from the changing threat landscape, proliferation of new technologies, as well as economic considerations on cybersecurity. In addition, the changing technologies and new platforms create new risks, as implied by the interview respondents and NCSSs of Canada. Therefore, the innovations in ST&E and the accumulation of knowledge have affected why cybersecurity has emerged as a policy concern. Another aspect, which was highlighted by some of the respondents and NCSSs, is related to the security interconnections with the US – as the CI of Canada is closely connected to the CI of the US, cybersecurity measures and standards need to be harmonized to ensure the functioning of cross-border CI. This refers to policy diffusion, as the specific standards and policies for CI protection are developed in accordance with the responsible partners and CI operators of the US. Norms and external events had practically no impact on the emergence of cybersecurity as a policy concern in Canada. This could be related to the geographical distance from the potential threats as well as the low reach of international cybersecurity norms. In sum, the key factors for the emergence of cybersecurity as a policy concern in Canada were policy diffusion, innovations in ST&E and economic considerations. The factors of norm diffusion and external events and crises were absent in the case of Canada.

7. Discussion on the results

This section discusses the results of the analysis and provides a systematic overview of the results of the research. The discussion on the results of the study identifies the factors and causes that have influenced the emergence of cybersecurity as a policy concern across the three selected cases. This includes a comparison of the case studies and concludes the results for each factor, by summarizing and interpreting the gathered data.

The potential impulses for the policy concern emergence of cybersecurity, assessed in the theoretical part of the research, were all mentioned by the documents and interview respondents of the research, except for the impact of international cybersecurity-related norms. Each case represents a sum of different factors and causes, that were related to the policy concern emergence of cybersecurity, as more than one factor was present in each case. In sum, the policy concern emergence of cybersecurity has been connected to economic considerations, policy diffusion, innovations in ST&E and the changing threat landscape related to the development of new technologies. The key factors, which were present in all cases, for the proliferation of cybersecurity as a policy concern were policy diffusion and innovations in ST&E. The impact of norms has not been confirmed, yet the reach of external policies has had an impact in all three cases. Specifically, the emergence of cybersecurity as a policy concern in Canada has been related to the policy concerns of the US, as the two states share interconnected CI. The EU NIS directives, which had been transposed in the member states, have had an impact on the domestic policies of the EU member state cases. The NIS directives have set guidelines, as well as standards, which are required for all the member states to enhance the cybersecurity capacities of each state. As can be observed from the cases of Lithuania and Croatia, collaboration among the EU member states, as well as sharing practices in cybersecurity, has also had an impact on the domestic policy formulation in cybersecurity. The policies of other EU member states therefore have impacted the emergence of cybersecurity as a policy concern in Lithuania and Croatia.

As the findings of the analysis suggest, the impact of external events on cybersecurity policy emergence has been limited, yet the Lithuanian case illustrates how the external developments, as well as events in other states, have had an impact on policy concern emergence. In conclusion, the impact of external events is directly related to geopolitical developments and state-sponsored cyber-attacks from Lithuania's neighbouring states. Lithuania has also formulated its cybersecurity

policies in accordance with the developments and events of its neighbouring states, mostly taking into consideration the changing cybersecurity threat landscape. Therefore, the external events and crises are, among economic considerations, policy diffusion and innovations in ST&E, a factor which has raised cybersecurity as a policy concern in Lithuania. On the impact of specific incidents or events, an additional interview with an expert on cybersecurity and head of the Cybercrime unit of the Council of Europe was conducted. In addition to specific cybercrime trends and threat landscape, the interviewee highlighted that in terms of specific triggers and drivers, the 2007 cyberattacks against Estonia served as a turning point in the EU's approach to cybersecurity:

> A major driver for cyber security policies and strategies was in 2007 when Estonia was attacked. This brought it home to many governments, that cybersecurity threats or cyber attacks against infrastructure could have a tremendous impact. (P11 Interview).

As further emphasized, this event had an impact on a larger scale:

> After the attacks against Estonia, Estonia then started to contribute to this and that triggered many things. I saw a difference in terms of the resources and their availability by the European Union, but also by the Member States, the Council, other governments, and the private sector in this field. I think 2007 indeed was not a coincidence. (P11 Interview)

In sum, it could be outlined that the 2007 attacks changed the cybersecurity landscape of the EU, but the specific implications that these events had on member states' national policies could be argued, as stated by the respondents from states of interest and as the policy documents illustrate. As the analysis of this research illustrates, norms on cybersecurity did not affect the emergence of cybersecurity as a policy concern. This could be explained by a lack of obligations and limited reach of cybersecurity norms, as well as limited knowledge of international cybersecurity norms. As one of the interview participants implied, international cybersecurity norms as such do not drive policy concern emergence and policy formulation, but rather decision-making in some areas (P12 Interview).

With regards to policy concern emergence and its continuation in the field of cybersecurity, participants from all three states of interest highlighted the impact of the Russian war against Ukraine and the threats, vulnerabilities as well as risks related to Russian cyber-attacks and ransomware. This aspect was prominently highlighted by the interviewees from Lithuania (P2, P6, P7, P9), who indicated that the geopolitical context has been one of the key drivers for cybersecurity policy concern emergence, specifically regarding the impact of Russian cyber-

attacks towards Lithuania. The same impact was noted by some Canadian policy-makers and experts, which indicates that the geographical distance from main threats does not decrease the risks and vulnerabilities related to state-sponsored cyber-attacks. As one of the respondents from Canada concluded:

> I don't think Canadians understand that we are essentially on the front lines of a global cyber conflict that involves geopolitical considerations - Russia's expansionist agenda. /…/ And I call out Russia directly. I don't think there's any question. We know that the attributions are quite clear. (P5 Interview).

As the evidence of this research suggests, the economic considerations had an impact on the proliferation of cybersecurity as a policy concern in the cases of Lithuania and Canada, but limited impact in the case of Croatia. The strategies highlighted the economic potentials, as well as the economic risks, that need to be assessed in collaboration with the private sector. This was the strongest driver for policy concern emergence for Canada, which largely focuses on cooperation with the private sector and the economic potential of cybersecurity. As recalled from the NCSS developers from Lithuania (P9 Interview) and Canada (P1 Interview), a key impetus for strategy development came from the private sector, and the stakeholders' requirements were involved in the formulation of NCSSs. All NCSS documents mentioned the potential of the digital economy and the importance of cybersecurity to secure digital services on a national scale. The presence of economic considerations indicates, that states prioritize securing their economic assets and cooperation with the private sector on the development of cybersecurity policies, as seen specifically in the cases of Canada and Lithuania. The economic considerations factor was almost present in the case of Croatia, this could be explained by the lack of involvement with the private sector, and as outlined by one of the interview participants (P4 Interview) from Croatia, a political culture where public policies do not receive wide attention. Furthermore, as the small enterprises of Croatia rent their services to bigger foreign companies, cybersecurity regulation falls under the responsibility of other enterprises (P4 Interview).

Similarly, as the findings of this study suggest, the aspect of new technologies and innovations in ST&E was outlined in all three cases of this research. In sum, as outlined by the NCSS documents and the interview respondents, the new technologies pose risks to the users and create new instruments and measures for committing cybercrime. This has created a situation, where the use and operation of new technologies and platforms need to be regulated, in order to mitigate the risks

and uncertainties involved with it. It could be inferred, that as the technologies and ICT platforms advance, the risks for the operators of ICT and users increase, while it creates new security vulnerabilities and uncertainties. In addition to the new risks, the innovations in technology create also new measures to commit cybercrime. Therefore, technological innovations have created a need to regulate this area, as well as the use of new technologies to ensure the awareness of ICT operators and users of the possible vulnerabilities.

In the cases of Lithuania and Canada, technological developments have had a stronger impact. In the case of Croatia, the factor of new technologies had lower prominence, but the factor was present, which could be explained by a lower level of cybersecurity threats in the state, as compared to other states in this research. Overall, the accumulation of scientific and technological knowledge and innovation has an impact on the emergence of cybersecurity as a policy concern, while it creates new vulnerabilities to the users and operators of ICT and new instruments for committing cybercrime. Additionally, the policy development in cybersecurity is further connected to raising public awareness, as well as setting standards for the use of ICT on a domestic level. In addition to the factor of innovations in ST&E, the second key driver for the proliferation of cybersecurity as a policy concern was policy diffusion. The evidence of this study indicates that the emergence of cybersecurity across three selected states was mostly driven by policy diffusion among states and innovations in the field of science and technology. Therefore, if a state has adopted a policy as a result of emerging policy concern in a region or an international organization, then a policy concern emerges in other states; secondly, if a state sees an increase in developments in the field of science and technology, then cybersecurity as a policy concern emerges. All of the factors, which were assessed in this research, are summarized in Table 2.

Table 2. Factors connected to the emergence of cybersecurity as a policy concern

Factors:	Canada	Lithuania	Croatia
Policy diffusion	+ Policy emergence connected to the policies of the US (shared CI)	+ EU member states' policies, NIS directives	+ EU member states' policies, NIS directives
Innovations in ST&E	+	+	+
Norm diffusion	-	-	-

Economic considerations	+	+	+/-
External events and crises	-	+ Regional events and developments, specifically Ukraine	-

8. Conclusion

This research examined the emergence of cybersecurity as a policy concern based on a study of three states. The focus of the following research was to study *what explains the emergence of cybersecurity as a policy concern*? To answer the research question, this study used interviews and document analysis to trace different causes for policy concern emergence of cybersecurity. As the results of this study indicate, the emergence of cybersecurity as a policy concern in each specific case is connected to several factors. The impact and reach of each specific factor differ in all three cases of this research, yet in sum, it could be indicated that the strongest drivers for the emergence of cybersecurity as a policy concern are related to policy diffusion and innovations in ST&E. The latter has implications for the cybersecurity threat landscape, as the new technologies create risks for the users, and operators of ICT, as well as create new measures for conducting malicious acts in cyberspace.

Based on the findings from the analysis of this study, the impact of external events and crises was low, as few of the interview respondents and one cybersecurity policy document mentioned specific events and their outcomes. One respondent and no policy documents mentioned specific international norms in the area of cybersecurity, and as the evidence of this study suggests, the impact of cybersecurity norms on domestic policies is arguable. The EU standards and directives for cybersecurity capacity enhancement are outlined by the interview respondents, as well as the policy documents of EU member states' cases. The EU not only sets specific requirements and standards, which need to be transposed into national obligations, but has created a collaborative environment for policymakers and CI operators to share their practices and challenges in cybersecurity. Interview respondents have outlined the examples and practices of other member states, which have had an impact on policy concern emergence and policy implementation.

As the evidence from the case of Canada suggests, the CI of Canada is closely interconnected to the US, and the two states collaborate on regulations and policies to enhance ICT protection measures. Therefore, the emergence of cybersecurity as a policy concern is furthermore connected to policy diffusion among states, as indicated by the interview respondents. In conclusion, the proliferation of cybersecurity as a policy concern, as demonstrated in the assessment of Lithuania's, Canada's and Croatia's cybersecurity policies and the responses from the cybersecurity experts and policy advisors, is connected to innovations in ST&E and policy diffusion. Therefore, if a state has adopted a policy as a result of emerging policy concern in a region or an international organization, then a policy concern emerges in other states and if a state sees an increase in developments in the field of science and technology, then a policy concern emerges.

The literature on the emergence of cybersecurity as a policy concern has outlined that the phenomenon is largely caused by norm diffusion and the impact of external events and crises. Against this, the findings of this study suggest that the emergence of cybersecurity as a policy concern is mostly driven by innovations in the field of science and technology and policy diffusion. Therefore, as the empirical evidence of this study illustrates, the wider focus in the literature on cybersecurity should focus on policies and policy diffusion across states and the impact of new technologies. New technologies, which are connected to innovations in ST&E, bring about new risks and uncertainties, therefore states see the necessity to regulate this field on a national scale. This research also illustrates how the emergence of cybersecurity as a policy concern is connected to external policies – states cooperate closely to regulate this area, share their practices and learn from others, or share parts of cross-border CI which are necessary to co-regulate.

The impact of external events and crises, specifically in cybersecurity, is more related to the regional connections and implications. As seen in the case of Lithuania, external events and crises do raise a policy concern, and the policy formulation follows the external developments. Yet, this does not indicate that cyber incidents and crises do not have an impact elsewhere. As the evidence of this study illustrates, cybersecurity policymakers and experts cooperate with colleagues from other states, to share their practices, mitigate possible risks and inform counterparts on trends, practices, incidents and risks in the field of cybersecurity. This study illustrates, based on the insights from the interviews with policymakers and experts on cybersecurity and NCSSs, that in

each specific case, the causes for the proliferation of cybersecurity as a policy concern is a sum of different factors, as the policy development is related to political developments and political culture, history, dependency on digital services, cooperation with the private sector etc.

This research was conducted by using expert interviews, accompanied by document analysis on cybersecurity policies. Although the interview method had its limitations, the responses of expert interviews offered valuable insights into the field of cybersecurity and policy formulation across three NATO member states. As cybersecurity is not widely studied in IR, this research thus contributes to this literature by assessing the policies of three different states, as the goal of this research has been achieved. Although the study assessed several factors and theoretical explanations, a wider examination of possible causes and theoretical assumptions could have been tested. For example, a comparison of non-NATO member states and their CS policies would be useful to assess the different approaches and causes for the emergence of cybersecurity as a policy concern. As the document analysis of this research indicates, approaches to CS regulation and policies, as well as CS capacities vary, referring that each state has specific causes for such developments. As the research method, as well as the theoretical background of this research, are general, the case selection for this study could be widened. More insight could be gathered from a study of other states and regions, which could widen the array of factors that have contributed to the emergence of cybersecurity as a policy concern. Another insightful comparison would be between states that not have adopted cybersecurity strategies and states that have NCSSs, assessing the causes why cybersecurity has not emerged as a policy concern in some states.

In sum, the goal of this study has been achieved and the author of the study traced factors for the proliferation of cybersecurity as a policy concern in three different states. The subset of NATO member states proved to be useful for this study, as the selected cases include different cybersecurity capacities, regions and are technologically and economically advanced, allocating resources to the enhancement of cybersecurity. Although this study examined different causes for policy concern emergence and continuity and no specific correlation related to NATO guidelines and policies was detected, this research illustrates how different considerations and factors contribute to the policy concern emergence. As the results of this study indicate, the emergence of cybersecurity as a policy concern is correlated to specific internal and external factors, yet NATO membership as such does not determine whether cybersecurity emerges as a domestic policy

concern in a state or not. More specifically, the NATO membership aspect is more related to defence capabilities and cyber warfare, and cyber incidents inside the Alliance do not largely contribute to the proliferation of policy concerns on a domestic level. It could be argued, that similar research in other regions or non-NATO member states would lead to similar results, as no specific correlation was found in this regard. The EU membership had a strong correlation to the emergence of cybersecurity as a policy concern, as the EU member states transpose specific directives and standards into national legislation for the protection of ICT and member states collaborate closely on cybersecurity issues and standards.

In addition to the study of the research question, the participants and policy documents also highlighted several issues in this area. States have different capacities and regulations in cybersecurity and unregulated ICT poses risks to other states. As concluded by one of the interview respondents (P1 Interview) – 80% of cyber attacks could be avoided if proper cyber hygiene was applied by the users of ICT. Additionally, many participants highlighted the need to raise awareness of cybersecurity and the need for cybersecurity expertise and specialists at large. In conclusion, this study demonstrates the need to build awareness of cybersecurity and the need to enhance international cooperation in this area, to build common cyber norms and regulations, which protect the users of technology on a daily basis.

References

Adamson, L, Homburger, Z. (2019). Let Them Roar: Small States as Cyber Norm Entrepreneurs. *European Foreign Affairs Review*, 24(2), pp. 217–234. Kluwer Law International BV, The Netherlands.

Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue*, 41(5), pp. 491-514. Available at: https://doi.org/10.1177/0967010610382687.

Arnold, B. J. (2018). Cyber Security in Canada: Structure and Challenges. Leuprecht, C., MacLellan. S. (Ed.). Governing Cyber Security in Canada, Australia and the United States. Centre for International Governance Innovation, 2018. Pp. 5-8. Available at: http://www.jstor.org/stable/resrep17311.6.

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind cyber security strategy development: a literature review of national cyber security strategy. Australasian Conference on Information Systems, Wollongong. University of Wollongong Australia.

Baller, S., Di Battista, A., Dutta, S., Lanvin, B. (2016). The Networked Readiness Index 2016. In: Baller, S., Dutta, S., Lanvin, B. (Ed.) (2016). The Global Information Technology Report 2016: Innovating in the Digital Economy. World Economic Forum, INSEAD, pp. 3-37.

Bauer, J. M., Dutton, W. H. (2015). The new cybersecurity agenda: Economic and social challenges to a secure internet. *SSRN Electronic Journal*, June. http://doi.org/10.2139/ssrn.2614545.

Baumgartner, F. R., Jones, B. D. (1993). Agendas and instability in American politics. Chicago: University of Chicago Press.

Baumgartner, F.R., Breunig, C., Green-Pedersen, C., Jones, B.D., Mortensen, P.B., Nuytemans, M. and Walgrave, S. (2009) Punctuated Equilibrium in Comparative Perspective. *American Journal of Political Science*, 53, pp, 603-620. https://doi.org/10.1111/j.1540-5907.2009.00389.x.

Béland, D., Howlett, M. (2016). The Role and Impact of the Multiple-Streams Approach in Comparative Policy Analysis. *Journal of Comparative Policy Analysis: Research and Practice*, 18(3), pp. 221-227. DOI: 10.1080/13876988.2016.1174410.

Bennett, A. (2004). Case study methods: Design, use, and comparative advantages. In: Models, numbers, and cases: Methods for studying international relations. Detlef F. Sprinz, D., F., Wolinsky-Nahmias, Y. (Eds). The University of Michigan Press, Ann Arbor. Pp. 19-55.

Bennett, A. (2010). Process Tracing and Causal Inference. In: Brady, H. E., Collier D. (Eds). Rethinking Social Inquiry. (2nd ed.). Rowman & Littlefield Publishers, pp. 207-219.

Brangetto, P., Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. Economic Aspects of National Cyber Security Strategies: project report. Tallinn, Estonia.

Burt, D., Nicholas, P., Sullivan, K., and Scoles, T. (2014), The Cybersecurity Paradox: Impact of Social, Economic, and Technological Factors on Rates of Malware. Microsoft Security Intelligence Report.

Cairney, P., Zahariadis. N. (2016). Multiple Streams Approach: A Flexible Metaphor Presents An Opportunity To Operationalize Agenda Setting Processes. In: Handbook Of Public Policy Agenda Setting. Zahariadis, N. (Ed.). Pp. 87-105. Edward Elgar Publishing Limited. doi:10.4337/9781784715922.00014

Cairney, P. (2012). Understanding Public Policy: Theories and Issues. Basingstoke: Palgrave, Macmillan.

Calderaro, A., Craig, A., J., S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), pp. 917-938, DOI: 10.1080/01436597.2020.1729729.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), January 2016, pp. 43–62. Available at: https://doi.org/10.1111/1468-2346.12504.

CERT-LT (2016). CERT-LT ACTIVITY REPORT FOR THE SECOND QUARTER OF 2016. National Electronic Communications Networks and Information Security Incident Response Team of the Communications Regulatory Authority of the Republic of Lithuania (CERT-LT). National Cyber Security Centre under the MoD.

Colebatch, H. K. (2009). Policy. Third Edition, McGraw-Hill Education, United Kingdom, Open University Press.

Council of the European Union. (2017). Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Croatia. Report, April 11, Brussels. Available at: https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf.

Craig, A. (2018). Understanding the Proliferation of Cyber Capabilities. Council on Foreign Relations. Available at: https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities.

Crandall, M., Allan, C. (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy*, 36(2), pp. 346-368. DOI: 10.1080/13523260.2015.1061765.

Cvitić, I., Peraković, D., Periša, M., Botica, M. (2017). An overview of the cyber security strategic management in Republic of Croatia. In: RCITD—Proceedings in research conference in technical

disciplines (pp. 13-18), conference paper. Zilina: EDIS—Publishing Institution of the University of Zilina.

CyberPeace Institute (2023). Attack Details. CyberPeace Institute. Available at: https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details. In: ENISA. (2023). ENISA THREAT LANDSCAPE 2023: July 2022 to June 2023. October 19, 2023, European Union Agency for Cybersecurity (ENISA). Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Dobbin, F., Simmons, B., Garrett, G. (2007). The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning? *Annual Review of Sociology,* August 2007, 33(1), pp. 449 – 472. DOI: 10.1146/annurev.soc.33.090106.142507.

Dolowitz, D. P., Marsh, D. (2000). Learning from abroad: the role of policy transfer in contemporary policy-making. *Governance*, 13, January, pp. 5-23.

Donalds, C., Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, 92, pp. 403-418. https://doi.org/10.1016/j.chb.2018.11.039.

Dupont, B. (2012) The Cyber Security Environment to 2022: Trends, Drivers and Implications. Prepared for the National Cyber Security Directorate. Public Safety. Canada. Her Majesty the Queen in Right of Canada, 2012. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208548.

E-Governance Academy (2023). National Cyber Security Index. NCSI 2016-2023 database. E-Governance Academy Foundation. Available at: https://ncsi.ega.ee.

ENISA. (2023). ENISA THREAT LANDSCAPE 2023: July 2022 to June 2023. October 19, 2023, European Union Agency for Cybersecurity (ENISA). Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Etikan, I., Musa, S. A., Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1), pp. 1-4.

European Commission. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE

COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY. JOIN(2013) 1 final, Brussels, Belgium.

European Parliament and Council of the EU. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. NIS Directive, Official Journal of the European Union, L. 194, Official Journal of the European Union, EUR-Lex. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

European Parliament and Council of the EU. (2022). DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU). No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). L 333, Official Journal of the European Union, EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN.

Finnemore, M., Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, 110(3), pp. 425–479. doi:10.1017/S0002930000016894.

Gendron, A. (2013). Cyber threats and multiplier effects: Canada at risk. *Canadian Foreign Policy Journal*, 19(2), pp. 178-198. DOI: 10.1080/11926422.2013.808578.

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections*, 19(1), pp. 73–86. Available at: https://www.jstor.org/stable/26934537.

Government of Canada. (2010). Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada. Government of Canada. Her Majesty the Queen in Right of Canada, Canada.

Government of Canada. (2013). Action Plan 2010-2015 for Canada's Cyber Security Strategy. Her Majesty the Queen in Right of Canada.

Government of the Republic of Croatia. (2015). The national cyber security strategy and action plan for the implementation of the strategy. 7 October, Official Gazette No 108/2015, Zagreb. Government of the Republic of Croatia.

Government of the Republic of Lithuania. (2001). Resolution of the Government of the Republic of Lithuania of December 22, 2001 No. 1625 "Regarding Approval of State Strategy for Information Technology Security and Its Implementation Plan".

Government of the Republic of Lithuania (2005). REPUBLIC OF LITHUANIA SEIMAS RESOLUTION ON THE APPROVAL OF THE NATIONAL SECURITY STRATEGY. 28 May 2002 No IX-907, Vilnius (Version of 20 January 2005 No X-91).

Government of the Republic of Lithuania. (2006). Resolution of the Government of the Republic of Lithuania of June 19, 2006 No. 601 „Regarding Approval of Electronic Information Security Strategy in State Information Systems till 2008".

Government of the Republic of Lithuania. (2011). Programme for the Development of Electronic Information Security for 2011-2019. Resolution no. 796, June 29. Available at: https://nsarchive.gwu.edu/document/19000-national-security-archive-lithuanian-government.

Government of the Republic of Lithuania (2014). REPUBLIC OF LITHUANIA LAW ON CYBER SECURITY. 11 December 2014 No. XII-1428, Vilnius. Last amended on 27 June 2018 – No XIII-1299).

Government of the Republic of Lithuania. (2017) RESOLUTION ON THE APPROVAL OF INFORMATION SOCIETY DEVELOPMENT PROGRAMME FOR 2014–2020 'DIGITAL AGENDA FOR THE REPUBLIC OF LITHUANIA'. 12 March 2014 No. 244, Vilnius. Consolidated version as of 23/12/2017, No. 1085, 20/12/2017, published on TAR 2017-12-22, i. k. 2017-20759.

Graham, E. R., Shipan, C. R., Volden, C. (2013). The Diffusion of Policy Diffusion Research in Political Science. *British Journal of Political Science*, 43(3), pp. 673–701. doi:10.1017/S0007123412000415.

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, 22(1), pp. 21-35. DOI: 10.1080/09662839.2012.749864.

Hansel, M. (2013). Cyber Security Governance and the Theory of Public Goods. *E-International Relations*, 27. June. Available at: https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/.

Harknett, R. J., Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, 71(3), pp. 455-460.

Herzog, S. (2017). Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity. *Georgetown Journal of International Affairs*, 18(3), pp. 67-78. Available at SSRN: https://ssrn.com/abstract=3101677.

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society*, 33(2), pp. 224-242. DOI: 10.1080/13600826.2019.1569502.

Horne, C., Mollborn, S. (2020). Norms: An integrated framework. *Annual Review of Sociology,* 46, pp. 467-487.

Hupe, P., Sætren, H. (2015). Comparative Implementation Research: Directions and Dualities. *Journal of Comparative Policy Analysis: Research and Practice*, May 11, 17(2), pp. 93-102. DOI: 10.1080/13876988.2015.1015360.

INA Group (2020). Announcement Cyber-attack. February 21, INA - Industrija nafte. Available at: https://www.ina.hr/en/announcement-cyber-attack/.

Johnson, P., Zualkernan, I., Garber, S. (1987). Specification of expertise. *International Journal of Man-Machine Studies*, 26, pp. 161–181.

Kadtke, J., Wells II, L. (2014). Policy challenges of accelerating technological change: Security policy and strategy implications of parallel scientific revolutions. September 2014, Center for Technology and National Security Policy, National Defense University, Fort McNair DC.

Karppinen, K., Moe, H. (2012). What we talk about when we talk about document analysis. In: Trends in communication policy research: New theories, methods and subjects. Just, N., Puppis, M. (Eds.). Bristol and Chicago: Intellect. Pp. 177-193.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2), pp. 7–40. Available at: http://www.jstor.org/stable/24480929.

Khonji, M., Iraqi, Y., Jones, A. (2013). Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), pp. 2091-2121.

Kianpour, M., Kowalski, S. J., Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, 13(24), pp. 1-28. https://doi.org/10.3390/su132413677.

Kingdon, J. W. (1984) Agendas, alternatives, and public policies. Harper Collins, New York.

Kingdon, J. W. (2001). Model of agenda-setting, with applications. *Law Review of Michigan State University Detroit College of Law*, (2), pp. 331-338.

Klimburg, A. (Ed.) (2012). National Cyber Security Framework Manual. NATO CCD COE Publication, Tallinn.

Lewallen, J. (2021), Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, 15 (4), pp. 1035-1052. https://doi.org/10.1111/rego.12341.

Lin, H. (2016). Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Journal of International Affairs*, 70(1), pp. 75–137. Available at: https://www.jstor.org/stable/90012598.

Lindsay, J., R. (2013) Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), pp. 365-404. DOI: 10.1080/09636412.2013.816122.

Luiijf, E., Besseling, K., de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, 9(1-2), pp. 3-31.

Lundgren, M., Squatrito, T., Tallberg, J. (2018). Stability and change in international policy-making: A punctuated equilibrium approach. *Rev Int Organ,* 13, pp. 547–572. https://doi.org/10.1007/s11558-017-9288-x.

Makridis, C. A., Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy*, 4(1), pp. 72-89. DOI: 10.1080/23738871.2019.1604781

Maynard, S., B., Ruighaver, A., B., Ahmad, A. (2011). Stakeholders in security policy development. Proceedings of the 9th Australian Information Security Management Conference, pp. 182-188. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84864557861&partnerID=40&md5=747bf7665deac4a0e37b554c610286b.

Meuser, M., Nagel, U. (2009). The expert interview and changes in knowledge production. In: Interviewing experts (pp. 17-42). London: Palgrave Macmillan UK.

Ministry of National Defence of the Republic of Lithuania (2018). National Cyber Security Strategy. Ministry of National Defence, Republic of Lithuania (Managing ed. Pipirienė, A., ed. Zujevaitė-Rinė, J.). Approved by Resolution No. 818 of the Government of the Republic of Lithuania on 13 August 2018.

Ministry of Public Safety and Emergency Preparedness of Canada (2019). National cyber security action plan 2019–2024 of Canada. Budget 2018 Investments. Her Majesty the Queen in Right of Canada. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf.

Mishra, A., Alzoubi, Y., I., Anwar, M., J., Gill, A., Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, pp. 1-23. 102820, ISSN 0167-4048. https://doi.org/10.1016/j.cose.2022.102820.

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, 27(1), pp. 64-77. Available at: https://doi.org/10.46743/2160-3715/2022.5044.

NATO CCDCOE. The Tallinn Manual. CCDCOE's homepage, available at: https://ccdcoe.org/research/tallinn-manual/.

Paananen, H., Lapke, M., Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88, pp. 1-14. 101608, ISSN 0167-4048. https://doi.org/10.1016/j.cose.2019.101608.

Phillips, K., Davidson, J. C., Farr, R., R., Burkhardt, C., Caneppele, S., Aiken, M., P. (2022). Conceptualizing Cybercrime: Definitions. Typologies and Taxonomies. *Forensic Sciences*, 2(2), pp. 379-398. https://doi.org/10.3390/forensicsci2020028.

Protrka, N., Marić, K., Plečaš, M. (2017). CHALLENGES AND ASPECTS OF CYBER SECURITY OF THE REPUBLIC OF CROATIA. Preliminary report, *Acta Economica Et Turistica,* 3(1), pp. 87-95. Available at: https://doi.org/10.1515/aet-2017-0010.

Public Safety Canada. (2017). Horizontal Evaluation of Canada's Cyber Security Strategy: Final Report. September 29. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx#s3.

Public Safety Canada (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. Public Safety and Emergency Preparedness Canada, Her Majesty the Queen in Right of Canada, 2018.

Public Safety Canada. (2022). Mid-Term Evaluation of the National Cyber Security Strategy – Public Safety Canada's Initiatives - Evaluation Report. Executive Summary, March 28. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2022-vtn-ntnl-cbr-strtgy/index-en.aspx.

Rawat, P., Morris, J. C. (2016). Kingdon's "Streams" Model at Thirty: Still Relevant in the 21st Century?. *Politics & Policy*, 44(4), pp. 608-638. Wiley Periodicals, Policy Studies Organization.

Richardson, R., North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), pp. 10-21.

Robinson, N., Hardy, A. (2021). Estonia: From the "Bronze Night" to cybersecurity pioneers. In: Romaniuk, S. N., Manjikian, M. (ed.). Routledge Companion to Global Cyber-Security Strategy. 1st ed., Routledge, pp. 211-225.

Sabatier, P. A. (1986). Top-down and bottom-up approaches to implementation research: a critical analysis and suggested synthesis. *Journal of public policy*, 6(1), pp. 21-48.

Sabatier, P. A. (1998). The advocacy coalition framework: revisions and relevance for Europe, *Journal of European Public Policy*, 5(1), pp. 98-130. DOI: 10.1080/13501768880000051.

Sabatier, P. A., Jenkins-Smith, H. C. (1999). The advocacy coalition framework: an assessment. Sabatier, P. A. (Eds). Theories of the policy process. Westview Press, Boulder, pp. 117-166. In: Weible, C., M., Sabatier, P. A. (2007). A Guide to the Advocacy Coalition Framework. Fischer, F., & Miller, G. J., Sidney, M. S. (Eds.). (2007). Handbook of public policy analysis: theory, politics, and methods. (1st ed) Routledge. Pp. 123-136.

Seger, A. (2012). Cybercrime Strategies. Discussion paper, 30 March. The Council of Europe, Global Project on Cybercrime, Strasbourg, France.

Shackelford, S. J., Bohm, Z. (2016). Securing Critical North American Infrastructure: A Comparative Case Study in Cybersecurity Regulation. *Canada-United States Law Journal*, 40(1), pp. 61-70.

Shipan, C., R., Volden, C. (2008). The Mechanisms of Policy Diffusion. *American Journal of Political Science*, 52(4), October 2008, Midwest Political Science Association, pp. 840–857.

Solberg, E. (2019). Foreword. In: Norwegian Ministries (2019). National Cyber Security Strategy for Norway. Strategy, Ministry of Justice and Public Security, Ministry of Defence. P. i. Available at: https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/.

Štitilis, D., Klišauskas, V. (2015). Aspects of cybersecurity: the case of legal regulation in Lithuania. *Journal of Security and Sustainability Issues,* 5(1), pp. 45-57.

Štitilis, D., Pakutinskas, P., Laurinaitis, M., Malinauskaitė-van de Castel, I. (2017). A model for the national cyber security strategy. The Lithuanian case. *Journal of security and Sustainability Issues*, 6(3), pp. 357-372.

Zartman, W., I. (1991). Conflict and resolution: Contest, cost, and change. *The Annals of the American Academy of Political and Social Science*, 518, pp. 11-22.

Tatar, Ü., Çalik, O., Çelik, M., Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. International Conference on Cyber Warfare and Security, pp. 211-218. Tubitak Bilgem Cyber Security Institute, Ankara, Turkey. Academic Conferences International Limited.

The Croatian Parliament (2007). Information Security Act. Decision on Promulgating the Information Security Act. Official Gazette, 79/2007. Class: 011-01/07-01/98, Reg. No.: 71-05-03/1-07-2, Zagreb, 18 July 2007.

The White House (2003). The National Strategy to Secure Cyberspace. Washington, DC: White House, February. Available at: https://nsarchive.gwu.edu/document/21412-document-16.

Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. Journal of Cyber Policy, 1(1), pp. 94–106. https://doi.org/10.1080/23738871.2016.1165716.

Trkanjec, Z. (2021). Croatia targeted by dozens of state-sponsored cyber attacks. EURACTIV, September 27. Available at: https://www.euractiv.com/section/politics/short_news/croatia-targeted-by-dozens-of-state-sponsored-cyber-attacks/.

True, J. L., Jones, B. D., Baumgartner, F. R. (2007). Punctuated-equilibrium theory: explaining stability and change in public policymaking. In: Theories of the Policy Process. Sabatier, P. A. (ed.). Second Ed., pp. 155-187. Routledge, New York.

UN E-Government Knowledgebase. E-Government Development Index (EGDI). United Nations, 2024. Available at: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index.

van Eeten, M., Bauer, J., M. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management*, 17, pp. 221-232. https://doi.org/10.1111/j.1468-5973.2009.00592.x.

Vasiu, I., Vasiu, L. (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. *European Journal of Sustainable Development*, 7(4), pp. 171-178. https://doi.org/10.14207/ejsd.2018.v7n4p171.

Vilpišauskas, R. (2024). Gradually and then suddenly: the effects of Russia's attacks on the evolution of cybersecurity policy in Lithuania. *Policy Studies*, pp. 1-22. Routledge. DOI: 10.1080/01442872.2024.2311155.

von Solms, R., van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, pp. 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

Vuksanović, I., P. (2019). Analysis of Possibilities for the Establishment and Implementation of Cyber Security in the Republic of Croatia. 61st International Symposium ELMAR Zadar, Croatia. Pp. 155-158. doi: 10.1109/ELMAR.2019.8918670.

Weible, C., M., Sabatier, P. A. (2007). A Guide to the Advocacy Coalition Framework. In: Fischer, F., & Miller, G. J., Sidney, M. S. (Eds.). (2007). Handbook of public policy analysis: theory, politics, and methods. (1st ed) Routledge. Pp. 123-136.

Annex 1

List of respondents

Participant number:	Current and held positions:	Based in:
P1	Head of the NCSS formulation task force in Canada, cybersecurity policy advisor	Canada
P2	Ministry of Defense Lithuania, head of the Cyber Security and IT Policy Department	Lithuania
P3	Armed Forces of the Republic of Croatia, Ministry of Interior of Croatia, Security Council of the President of the Republic of Croatia, cybersecurity researcher	Croatia
P4	Director of Cyber Security Centre of Croatia, Office for the Development of Digital Society	Croatia
P5	Cybersecurity policy analyst and researcher in Canada, director of Toronto Metropolitan University's national center for cyber training and cyber education	Canada
P6	Legal advisor, researcher on data protection and cybersecurity regulation, Lithuania	Lithuania
P7	Policy advisor, policy group director on cybersecurity at MoD Lithuania; deputy director of the National Cyber Security Centre	Lithuania
P8	Policy and legal advisor on cybersecurity, Government of Canada; researcher and professor on cybersecurity policy and law	Canada
P9	Advisor to Cybersecurity and Information Technology Policy Group MoD Lithuania; chief specialist of the NCSS formulation task group	Lithuania
P10	Policy advisor to MoD Lithuania	Lithuania

P11	Executive Secretary of Cybercrime Convention Committee, Council of Europe; coordinator of Cybercrime Programme Office of the Council of Europe; United Nations Office on Drugs and Crime; Council of Europe: Head of Cybercrime Division;	France
P12	National security advisor and analyst, Government of Canada; Associate Professor on security and IR	Canada
P13	Information security coordinator and advisor, Croatian Academic and Research Network	Croatia
P14	Legal advisor and policy analyst on cybersecurity, Croatian Academic and Research Network	Croatia

Annex 2

Interview questions for interview subjects, who were involved in NCSS development:

1. Could you tell me a little about in what context you became involved in the process of working on the NCSS and what was your role in this process?
2. Can you walk me through how this strategy development started and where this initiative started from?
3. Can you recall what motivated the drafting of this strategy, or what led to it?
4. Can you walk me through the stages of the process by which this strategy came about and reflect on the considerations at the time concerning why to develop such a strategy
5. Who were the main initiators behind this process or was the initiative already underway somewhere else?
6. Was this the first time that cyber was nationally seen as a policy concern, or was it already around?
7. How did you come up with the contents of the strategy, and what areas were seen as most critical in your opinion? (thematic specifications listed below, if needed)
8. Before we finish up – is there anything you would like to specify or add on that is important for me to understand how the strategy came about, and perhaps also why it was felt at the time that such a strategy needed to be developed, or anything else?

Potential drivers and motivations for policy formulation:

1. Was there a specific example or a guideline that was followed throughout the process?
2. Were there any specific developments or events, that triggered the process? If not specific events, then could you elaborate on how the NCSS developments and implementation in other states were perceived in your country?
3. Were there any economic considerations, related to digitalization, the interests of CIIP operators, or telecommunication operators, that evoked the development process?
4. Given the rapid development in the technology sector and scientific developments in ICT, were there any considerations or concerns regarding these developments?
5. In your view, what role (if any) did stakeholders or NGOs play in this process or were there any groups outside the public sector involved in this process?

Glossary

ACF – advocacy coalition framework

Budapest Convention – Council of Europe convention on cybercrime (2001)

CERT - Computer Emergency Response Team

CI – critical infrastructure

CIIP – critical infrastructure protection

CS – cybersecurity

DDL - the degree of digitalization and digital dependency of the state

ENISA – European Union Agency for Cybersecurity

ETL report - ENISA Threat Landscape report

EGDI - e-Governance Development Index

DDoS attack – distributed denial of service attack

HCI – Human Capital Index

ICT – information and communication technologies

IO – international organisation

IT – information technologies

Malware – malicious software

MDSD - Most Different Systems Design Case Study Approach

MoD – Ministry of Defense

MoI – Ministry of Interior

MS model/framework - multiple streams model

NATO CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence

NCSI – National Cybersecurity Index

NCSS – National Cybersecurity Strategy

NIS directive – EU directive on network and information systems

NRI – Networked Readiness Index

OSI - Online Service Index

P – Participant

PET - the punctuated equilibrium theory (Baumgartner, Jones, 1993)

Phishing – an attack conducted primarily through communication channels, based on persuasion and "socially engineered messages," with the aim of persuading the victim to carry out a specific task or action, for the benefit of the perpetrator (Khonji, et al., 2013: 2092)

PPP - public-private partnership

PSEPC - Department of Public Safety and Emergency Preparedness Canada

ST&E – science, technology, and engineering

Stuxnet – Computer worm, used against Iran's nuclear program in 2010 (Lindsay, 2013: 365)

Ransomware – a type of malware, that is used to encrypt files of a victim's device, the files and data are not decrypted until reimbursement is paid (Richardson, North, 2017: 10)

TII – Telecommunication Infrastructure Index