# THE DIGITAL EUROPEANIZATION: A PROCESS-TRACING ANALYSIS

Mikkel Toft

Aalborg University | European Studies 2020 | Master of Science

## Abstract

Cybersecurity has evolved into an essential element of national security for all Member States of EU. New threats over the internet have given rise to institutional changes and a legal framework at the national and EU levels covering cybersecurity. The development of computer technology and its increased consumption affect European integration because it presents new societal problems that cannot be solved independently. The collaboration between The European Union and the EU Member States on strong cyber resilience and transparent information sharing is being addressed and assessed in this project to identify whether the concept of Europeanization fits into this development of domestic cybersecurity strategies.


**Keywords:** Cybersecurity, The European Union, Europeanization, Strategies, Policymaking, NIS-Directive, Institutional changes.

# Table of Contents

## Chapter 1: Introduction

In the history of humanity, information and data have never been more convenient to receive, transfer, and even steal due to software technology development during the information age. Globalization incorporates digitalization, and it has a significant impact on the international community by revolutionizing how people are interacting in countless areas. Although computer technology contributes to improvements in the private and public sectors, the increased use of Internet-facing servers has a risk of consequences for everybody, from individual internet users to international cooperation. International laws have proved not to cover some aspects of cyberspace well enough, and comprehensive policymaking on the political issue is necessary. The lack of cybersecurity by limited regulations make private data and confidential information valuable and easily accessible for trespassers and culprits with the right technological capacity.

Since the cyberattack against Estonia in 2007, the European Union (EU) has intensified the work for a robust legal framework of Information technology law (Cyberlaw). It aims to protect EU citizens and organizations and Member States against cybercrime and information warfare by drafting cybersecurity strategies and making supranational legal framework. So far, it has led to the legislative process of the Network and Information Security Directive (NIS-directive), the General Data Protection Regulation (GDPR). Institutionally, new EU agencies and databases are established, consulting the EU institutions and domestic institutions' work and cooperation to ensure national security by updating research and supporting strategies. As a political issue, cybersecurity impacts various areas within the Justice and Home Affairs Council (JHA) and the EU's Common Security and Defense Policy (CSDP) that it plays a role in national policy structures and the EU's normative power. National security is the priority of any government, and it is therefore interesting to study the preconditions, regulatory and institutional changes they undertake to maintain national security.

This project assesses the EU Member States' approximation towards the EU's cybersecurity strategy and the cybersecurity legal framework by using a tracking-process to explore Europeanization effects as a possible factor for regulatory changes in institutions on domestic and EU level. This inductive research project adds new observations towards European integration's theoretical perspectives and thus challenges the classical integration theories by researching new political issues with an innovative research design.

## 1.1 Glossary

### 1.1.1 Cybersecurity strategy

A strategy is a plan drawn up to achieve its (political) goals. Ideally, the GDPR and the NIS Directive are results of the EU's cybersecurity strategy because the policy has been transformed into a legally binding agreement. This project considers existing cyber legislation as part of the cyber strategies (European Commision, 2020).

### 1.1.2 The legal framework of Cyber legislation

The legal framework of cybersecurity is everything that cyber legislation entails and affects. It is basically the drafting of the Budapest Convention on Cybercrime. However, all legal documents have generated legislation on concepts such as the internet, artificial intelligence, online child pornography, network security (Budapest Convention on Cybercrime, 2001).

## 1.2 Problem formulation

This project sets out to assess EU Member States' approximation to the ambitions of the EU's Cybersecurity Strategy from 2013:

- *What impact does the concept of Europeanisation have on Member States' cybersecurity strategies?*

# Chapter 2: Methodology

The assessment of the EU's cybersecurity strategy being effects on regulatory changes in the EU Member States requires academic considerations regarding the methods and research design used to answer the problem formulation. These considerations take into account the methodological challenges in European Studies that arise from a research tradition of being dichotomies. The complexity of EU affairs calls for the development of innovation in the form of more cross- or transdisciplinary research designs with research methods derived from across the social sciences and international relations (IR) to ensure European studies' quality. EU affairs should be compared with domestic affairs within legal and political matters, thus deviating from the definition of an international organization (Lynggaard, Löfgren, & Manners, 2015, pp. 3-4). However, the EU should not be recognized as a nation-state either, but as a supranational Union with common values and political interest. This definition results from 55 years of integration processes that have formed the EU Members States' identity and supranational cooperation.

***(n=1 problem)***

In the effort of analyzing integration processes, attention is drawn to the fact that there can be many variables associated with too few cases (n=1 problem). This project's conclusion is not the ultimate truth of the observed reality because the tracked mechanisms are only a few variables that have caused the outcome. The project is an empirical addition to EU affairs research, which generates updated theories about European integration. Other research approaches that attempt to link cybersecurity legislation to Europeanization concepts may conclude differently due to other variables and research design. The flexible approach provides the basis for innovative research design, aiming to form European studies to an independent research object deviating from social science (Ibid, p. 5). Europeanisation occurs without the EU's policymaking about the cybersecurity legal framework. Simultaneously, cybersecurity policymaking may be shaped by variables other than what is illuminated in this research approach.

## 2.1 Methodological perspectives

In the interplay between the methods, ontological and epistemological assumptions arise in the considerations of the methodology. The study concerns the logic and procedure of the scientific inquiry behind the structure and philosophical principles of research designs in discussing European studies

(Rosamond, 2015, p. 18). Analysis of Europeanization occurs at the *meso-level*; the methodological framework is based on the interaction between groups of people, institutions and states internally in the EU (Lynggaard, Löfgren, & Manners, 2015).

### 2.1.1 Ontology

The European studies desire to define its research approaches open up for new ontological perspectives on 'what there is to know' towards the subject. To do so, Scholars over the last two decades trying to bring the *'rationalists'* and '*constructivists'* ontological positions closer to each other (Kratochvíl & Tulmets, 2010, p. 22). This has been done gradually regarding Europeanisation as *"domestic adaptation to European regional integration"* (Vink & Graziano, 2013, p. 37). This project approaches the ontological position of Constructivism: In the social sciences are Phenomena in constant revision, and therefore the researcher experiences and analyzes a specific version of social reality (Bryman, 2012, p. 33). However, the analysis processes may influence the ontology by exploration the actors with statements and arguments that challenge this position. In other words, the research strategy does not directly attempt to bridge-building the two ontological positions but does not rule out that rationalism may include useful assumptions as well (Kratochvíl & Tulmets, 2010, p. 23).

### 2.1.2 Epistemology

The considerations regarding acknowledging research objects are, in principle, a discussion on the methods to explore the limitations and practices of the Europeanisation process. According to The *'pluralistic'* position, the study of EU politics benefits from including varied epistemological standpoints methodological standpoints, while the *'mainstream'* position thinks opposed. In this project, the epistemological approach how to acknowledges that cybersecurity's legal framework generates Europeanisation processes in the EU member states. The inclusion of cybersecurity is to find phenomena and aspects within the social sciences that can add or reject explanatory theories over time or duplicate conceptual constructions of EU affairs into the research framework (Wach, 2015, s. 18).

## 2.2 Inductive Research Design

The research design has an inductive character due to the relationship between the collected data and theory. For this project, it makes the most sense to collect the data in a structured analysis in order to provide a general picture of the observed reality. A part of the reason is the limitation of cybersecurity combined with European integration cases, which challenge a deductive approach. The methods start with a structured analysis, which collects and uses empirical data to generate new theoretical perspectives. The inductive approach examines whether the EU Member States' regulatory policy changes in cybersecurity can conclude something general about the development of Europeanisation.

As mentioned, the scholar, European Studies, needs innovative solutions to explain EU Affairs development, whereby a deductive approach through a discussion of adapting traditional theories to new political issues is not understood as an innovative solution. However, this does not mean that there are deductive elements, as the interplay between empire and theory throughout the analysis can entail a modicum of deduction. The purpose is not to test existing theories, but developing the theoretical perspective of Europeanization (Bryman, 2012, p. 26).

### 2.2.1 Theory-building Process-tracing

The relevant research question to develop the understanding of the concept of Europeanization is: "*what has the EU caused at the domestic level, and how can we isolate the effect from other parallel processes?"* (Exadaktylos & Radaelli, 2015, p. 207). By introducing formula $Y = F(X)$, as a guideline for the design, the analysis framework can isolate the independent variable (X) and dependent variable (Y) from other processes and assess a functional link between the variables (F) (Ibid.). In other words, the purpose is to find "*a plausible hypothetical causal mechanism"* that links X to Y (Beach & Pedersen, 2013, p. 16). In this case, the dependent variable (Y) is the domestic regulatory changes adapting to the EU CSS because the changes are the political response. X is the EU cybersecurity policy legal framework because the regulatory changes as they are experienced cannot exist without the EU's political decisions. It means that JHA affairs, defense cooperation and institutional structure are a prerequisite for political change to occur at all. Now, what makes the design theory-building the ambition of linking Y to X (X-Y-centric) (Ibid., p. 21).

### 2.2.2 Assuming by Indicators

This approach tracks down *'alternative factors'* that emboldens a given degree of convergence in regulatory regimes by using the concept of *approximation* into the research of the Europeanization process to establish indicators of the causes (Calderoni, Organized Crime Legislation in the European Union, 2010a, p. 47). The tracking process has a historical dimension identifying major historical trajectories of institutions' integration that have implicated cyber legislative matters and an institutional dimension tracking approximation (vertical) indicators. The pinning of historical matters and the investing of indicators can evaluate how the member States' adapting to regional integration, feedbacking to the theoretical consideration of integration theories in the research in Europeanization. It adds knowledge about who empowers from the cybersecurity strategical policymaking. The indicators are highlighted in the analysis is based on a rational approach. As the intention is for Member States to approximate to EU CSS, the logic is that it is on the basis of the EU's strategy and legislation that the indicators arise. (Exadaktylos & Radaelli, 2015, p. 215).

### 2.2.3 Comparative case study

This design's comparative nature lies in comparing the different indicators of Europeanization for approximating the EU's cybersecurity strategy. The analysis goes through nine member states' cyber securities and comparing them with the indicators from the EU CSS. The collected nations are picked to cover different geographical areas of Europe: Austria, Belgium, Croatia, The Czech Republic, Denmark, Finland, France, Germany, Ireland. If indicators from the Member States turn out to distance itself from the EU's cybersecurity approach, Europeanisation effects have not explained the regulatory changes. One risk is that some Member States are moving closer to the EU, while other states pursue other strategies, leading to national strategies and policy decisions harmonizing between the Member States. National Political decisions can well harmonize without approximating EU decisions (Calderoni, 2010a, p. 52). The effects of Europeanisation depend on the extent to which the 'goodness of fit' indicators is similar in the countries. If a particular incumbent is higher prioritized in one country and not others, it may be due to national political agenda or interest in alternative cybersecurity interests. If the Indicators are very different from Member State to Member State, then it is a matter of Europeanisation not affecting

regulatory changes, which must be seen as an expression that there is no institutional adaptational on national decision-makers.

Furthermore, the inclusion of both the GDPR and the NIS Directive may have comparative elements in the method because there are two different types of EU legislation within the same political issue. Where the regulation must meet the EU legal framework, the directive can follow the legal framework. This statement provides insight into which actors have gain power within the decision process and how it has been formed. The research method attempts to examine Member States' willingness to upload preferences and willingness to adapt to the EU level by comparing the GDPR and the NIS directive's regulatory changes.

### 2.2.4 Qualitative data collection method

The analysis is exclusively a document analysis based on a systematic procedure by collecting documents, interpreting the content, and conceptualizing theoretical perspectives. The process is vital in establishing indicators, as the primary sources' contents are a prerequisite for selecting indicators (Bryman, 2012, p. 384). The primary sources are public documents like cybersecurity strategies, treaties, press releases, legal documents from EU institutions, agencies and national ministries, and the secondary sources are reports and articles from researchers and journals. This analysis uses ENISA's collection of EU Member States' National cybersecurity strategies (NCSS) and webpages from official homepages of both the EU and national levels to cover the objects. The language is limited to only English sources. The method is carried out by systematically reviewing the documents to determine approximation in the cybersecurity strategies and the domestic legal framework.

#### *2.2.4.1 The empirical challenges*

The inclusion of academic literature addresses European integration differently in classical disciplines such as economics, sociology, law, and international relations, but examining new political issues in the EU needs interdisciplinary research designs to explain the integration process's development. In terms of legal structure, the revisions of treaties illustrate how the EU's institutional changes have expanded jurisdiction and competence in EU institutions to overcome political issues like climate change by combining disciplines. Furthermore, it shows how actors and institutions on both supranational and national levels become vulnerable or strengthen due to the demand for political action on new political

issues and the massive institutional changes. With the introduction of the n=1 problem into empirical concerns, the argument is that previous reports and publications underestimate or naively ignore the complexity of the EU's policy process by having too narrow research approaches to the subjects. This constitutes an empirical challenge, as there is a risk that previous research methods do not match the EU processes and cannot enlighten the political developments in the formation of cybersecurity legislation (Exadaktylos & Radaelli, 2015, p. 6).

***Cyber Issues***

The concept of *'cyber'* is, to a greater extent, connected to the empirical insights of research in software development rather than research in European studies. In itself, the implementation of a technological research area strengthens the idea of more interdisciplinary research design, but on the other hand, it complicates the data collection method and application of the concept. The empirical challenge occurs in the search and interpretation of the concept. In searching for academic material to compose concepts such as cyber-attacks, cyberspace and information operations with Europeanization, the risk of including impressionable or inoperable content appears. A large part of the data collection method takes place by understanding software development principles and "translating" it into words that are more suitable for EU affairs and realizing which area. Although there are publications that compose international laws and policymaking with cyberspace, such combinations are relatively new hotspots empirically. Because this is a relatively new area in both the school of social science and computer technology, there is increased competition in publishing scientific articles that explain interdisciplinary concepts and the development of phenomena. Overall, the number of researchers, their research approaches, and lack of experience on the subject limit this social literature field. These barriers will disappear in line with political awareness on the subject, linking Europeanization with cybersecurity as a grey zone.

# Chapter 3: Theoretical aspects of Europeanization

Indicators of approximation are based on theoretical considerations of Europeanisation. In order to limit the parallel processes for the development of regulatory change, the research design has had to select specific theory frameworks. The theory is chosen based on the researcher's previous research experience and a subjective notion of what may have a decisive factor in the member states' development of cybersecurity policy. It is a wonder why cybersecurity policymaking is taking place at the EU-level, which has created the idea that Europeanisation can add new or reconstruct theoretical considerations. One can even see Europeanization as a process that can be explained by theories. However, not a theory in itself, making Europeanisation flexible in understanding the integration processes and goes beyond the discussion of liberal governmentalism and neo-functionalism on European integration. The theoretical added value. The need to generalize mechanisms adds theoretical value to Europeanization by examining the effects of the EU political agenda, strategies, and institutions on domestic political changes (Vink & Graziano, 2013, p. 39).

## 3.1. New Institutionalism

Rather than positioning a particular categorization of European integration as liberal govermentalism and neo-functionalism, the focus is on the continuity and change in new institutional. The perspectives of new institutionalism incorporate a useful understanding of the Europeanization processes by having historical, rational choices and sociological and discursive approaches regarding the European institutions' role in the domestic political system's decision-making processes. This research design excludes, which focuses on socializing and EU institutions' culture and communication (Ibid., p. 40). Due to the empirical insights' lack of informal and internal documents, it would be challenging to establish indicators from the sociological institutionalism approach.

Rational institutionalism has traditionally been used before in European integration theories, as it argues for rational choices by opening up the political possibilities of European integration. It involves a discourse aspect of how the EU's institutional changes affect why some ideas are absorbed and others do not. The historical institutionalism analysis occurs by tracing domestic adaptations to the development of European political strategies, policies and institutions changes (Exadaktylos & Radaelli, 2015, p. 209).

The vital events in the development of Common Security and Defence Policy (CSCP) and JHA cooperation need to be tracked down to understand the regulatory changes' outcome fully.

### 3.1.1 'Goodness of fit': The baseline model

Europeanisation must be understood as a result of an 'adaptational pressure' on the member States, when the EU institutions produce policymaking or institutional changes. It creates an expectation for regional integration forward to institutional adaption. From the moment the EU policy is put into force, the domestic institutions are in a stage of precondition for Europeanization, where strategies and institutional settings are being organized to adapt the regulatory changes. The direction of change depends on how domestic actors and institutions react to adaptational pressure. Basically, the response to the adaptational pressure is a sign of if Europeanization occurs in the Member State. The degree of compatibility between European and domestic political processes, policies and institutions are indicators of approximation because it shows whether the member state's standards within a given subject can live up to EU standards: *"the lower the compatibility (…) the higher the adaptational pressure."* (Exadaktylos & Radaelli, 2015, p. 208). If the standards fit, there is not much pressure on the domestic institutes. In the work of regulations, such as the GDPR, member states can upload their preferences into a specific piece of legislation through the EU institutional structures. By picturing EU regulatory policy as a patchwork that distributes the pressure due to the member state's experience on the subject, some states are more prepared through national interest than other states. A crucial factor for this is the context and timing for a member state to upload its preferences, and the Member States cannot keep up with every regulation because of their prioritizing. It challenges the integration theory of liberal governmentalism, as it emphasizes the power relations between states. The "large" member states like Germany and France will not have to face much pressure to adapt to Europeanization's effects in this theory.

The model goes hand in hand with the new institutional rational choice approach in this project; they both see adaptational pressure as a set of new possibilities and limitations. Roughly speaking, they are taking up the fight with the usual (status quo) regarding the European process and arguments that the veto is a barrier in capacities to exploit new opportunities (Ibid., p. 209). The empowerment of national politics grows from a redistribution of EU political resources, but differential effects impact the national level both inside and outside the EU. The effects may affect the Member States differently because they

have different standards to handle political changes. Misfit occurs at a high level because some Member States cannot meet the same standard, which is the point of the baseline model (Goodness of fit) (Ibid., p. 210).

This challenges neo-functionalism and liberal-governmentalism. Respect for integration theories lies in accepting the Member States' political interest and willingness to cooperate based on the resources they have chosen but, at the same time, the acceptance that some EU political decisions affect the national political structure. The two classic integrations theories predict that the misfit of standards leads to convergence in the form of more supranational decision-making or national decision-making. In between the two extreme integration process possibilities, Europeanization predicts the regional integration looks different across the Member States due to the domestic institutions' adaption to regulatory changes on various political issues. (Vink & Graziano, 2013, p. 41).

Member States Lack of compliance of dealing with directives or agreements such as the Stability and Growth Pact (SGP) assesses as being the result of a resistance to change due to high adaptational pressure. The theory argues that weak Europeanization is a policy re-trigger mechanism that generates more integration. If a Member States does not fit the EU policy, it may be necessary to re-define the legislation that makes the situation more suitable. In this process, there is momentum for EU political actors to tighten up institutional processes and legislation to meet the domestic institutions' political expectations.

### 3.1.2 Criticism of the model

The goodness of fit model has been criticized for seeing Europeanization only as a mechanism that only happens through members' lack of institutional resources or political willingness to 'download' EU instructions. It does not take into account the EU's lack of guidelines or bad strategies and communication. EU institutes structures are the ultimate template for domestic institutes. The baseline model takes into account that it requires different resources to meet the standards of the EU institutions, but it does not take into account whether it is the best structures for the Member States' alignment with EU legislation (Exadaktylos & Radaelli, 2015, p. 211). The model underestimates the European Council's role, which negotiates and makes political decisions based on national interests and governmental diversity structures across member states. The problem with tracking effects from EU policy to a

domestic level is that it can be challenging to confirm a regulatory change that happened due to EU adoption pressure or whether it is a change in Domestic politics that has been underway before EU policy came into force. It happens because the member state can be ahead of the EU institutes in policymaking on the given area.

## 3.2 Bottom-up vs. Top-down

The critique of the baseline model leads to two positions where the classic view of Europeanization can be seen as top-down processes because it is the Member States that adapt to the EU, never alternative models perceive the processes as bottom-up (Vink & Graziano, 2013, p. 37). In these approaches, Europeanization can be understood differently from actor to actor, in which the discourse of institutionalism plays a role in analyzing how specific actors construct and define the influence of EU institutions' settings on domestic regulatory change. The perception of Europeanisation is thus seen in the light of the actor's perspectives, which form a certain discourse from the experiential context. This model traces important episodes within the political system overtime at the domestic level, where the purpose is to identify the episodes' causes. If there is evidence that EU institutions develop at the expense of domestic episodes, it is Europeanization.

Theoretically, it is the EU that adapts to domestic institutional changes. As can be seen, some selected publications in the section of the Literature review go beyond European definition and define domestic adaptation to regional integration. This project considers both perspectives and possibly finds that Europeanisation is an adaptation at both the domestic and EU levels, which hopefully can help re-define the cycle of EU Policy and implement flexible solutions (Exadaktylos & Radaelli, 2015, p. 212). It attempts to narrow the gap between the EU level and the domestic level through a holistic perspective, where intertwined processes are present. With this argument, the thermotical framework allows us to examine not only the classic *"EU to member-state and versa,* but through indicators of interactions among external actors and officials in the EU and domestic institutions to find the fitting mechanisms (Ibid., p.213).

## 3.3 The theoretical challenges

Given the acknowledgment of the EU's position as a supranational Union, policymaking within the legal framework of national and European affairs, the theoretical framework does not differentiate between national and international practices. The selection of theory is not limited by disciplines but open for selecting theoretical literature that covers the empirical literature from the analysis's mythological perspectives. The theoretical perspectives challenge is an extension of empirical challenges, as theories are formed from the experiences described through documentation. If the documentation is not sufficiently present within the problem field, the theories are based on other bases and objects than this analysis. That is why there is a demand for academic projects that combine international relations with information warfare and cyber law. The existing theories within this topic are thus built up of monodisciplinary approaches, and it is the project's methodological task to overcome these barriers. The technical development occurs in EU decision-making processes, giving rise to new aspects of democracy that the theoretical literature on governance does not cover well enough (Ibid. p. 7).

# Chapter 4: Literature Review

This chapter discusses previous reports and research articles whose topics, methods, or theories have relevance toward this project's academic framework. The literature belongs mainly to the scholars of Social Science and International Relations, Historical Science and Computer Science. These are academic sources with different approaches that can be linked with European integration within the topic of Europeanization, cybersecurity, or EU Institutions within sectors of common security and defense operations or JHA Council. However, the literature does not necessarily contain a link between cybersecurity and defense and the EU's criminal policy. The goal is to bring up literature that can support or challenge the idea of tracing down indicators, showing that cybersecurity policy in the EU Member States, as it stands, is due to a particular integration process beyond the classic integration theories. The selection of the literature is justified in the attempt to connect Europeanization with cybersecurity policy, as mentioned earlier, is a gray zone. However, it is not impossible:

## 4.1 Combination of Cybersecurity and Europeanisation

In Ido Sivan-Sevilla's article *Europeanisation on demand: the EU cybersecurity certification regime between market integration and core state powers (1997–2019)* shows through process-tracking how EU politicians' promises of "fundamental changes" within cybersecurity over two decades end up being limited political action (Sivan-Sevilla, 2020). The report's conclusion is the clarification of one of the "Europeanization on-Demand" model, which allows Member States to take control of their cybersecurity strategies because the EU Commission has the opportunity to draw on its internal market powers without having to regulate too much in the already existing policy. Regulatory changes are minimal in the Member States because they are governed by national interests (Ibid. 27). Overall, a well-performed analysis with good evidence forms the framework for an innovative model that succeeds in going beyond the classical integration theories' dichotomies.

Also, there is a university thesis from Leiden University, the Netherlands by Max Balder called *The cybersecurity landscape of the European Union,* which uses new institutionalism approaches to answer how EU cybersecurity institutionalization between 2001-2018 develops (Balde, 2018). The project seeks (tracks) evidence (indicators) in public documents from the EU Commission and other redundant initiatives. In many ways, this report can be compared to this thesis regarding method and

purpose. However, it lacks theoretical considerations where the classical theories are not included, and it has a uniform top-down perspective.

## 4.2 Approximation

The idea is inspired by professor Francesco Calderoni's book *Organized Crime Legislation in the European Union: Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight Against Organized Crime* (Calderoni, Organized Crime Legislation in the European Union, 2010a). The book is of great relevance, first and foremost, because it assumes EU member states degree of compliance with EU's criminal laws legal framework. It examines European integration horizontally between the Member States and vertically to the EU's JHA political issues. It uses a comparative case study, which systematically cross-compares the Member States, which provides an opportunity to examine the complexity of EU Affairs. The reason why this project avoids harmonizing is that it is not theoretically part of Europeanization. It is recognized that a horizontal analysis of EU Member States' cybersecurity strategies will assess whether the EU lacks aspects of cybersecurity that interest national governments in national security. Furthermore, Calderoni covers cybersecurity in the chapter *The European legal framework on cybercrime: striving for an effective implementation* of the book *Crime, Law and Social Change Vol. 54* (Calderoni, 2010b). The article argues that the international instruments that the EU has put in place do not play a major role in the national cybercrime legal framework because robust cybersecurity is a national interest and popular public opinion.

## 4.3. criticism critique of the literature

A fair critical point to evaluate Calderoni and Sivan-Sevilla's approaches is their empirical lack of covering GDPR. Calderoni's lack is because of GDPR was not even under development in 2010, but Sivan-Sevilla's does not consider the Member State's institutional changes formatted by the development of GDPR, going from directive to regulation. The right to data production was a major challenge for the users of the internet-facing system, and it needs to be on the research agenda's attention to truly understand the EU cybersecurity legal framework's impact on member states.

The literature will be expanded to more GDPR related reports if one searches for the concept of 'entrepreneurship' of EU cybersecurity policy. This concept is in the previously mentioned publications and refers to the fact that the EU (especially the Commission) has been good at taking ownership of cybersecurity policy at the right time (Schünemann, 2017). It seemed that empirical insights regarding the GDPR are mainly examined from a macro level in European studies, where the NIS Directive is an object being examined as an intergovernmental perspective (Kańciak, 2017). It is due to the legal framework for regulation and a directive. However, this project wonders about not finding literature that tries to find similarities in the development of the two cyber laws; and whether there is a future chance that the NIS-directive will become a regulation because of neo-functional mechanisms.

# Chapter 5: Analysis

This analysis is divided into four sections, each of which helps form an overall conclusion corresponding to the problem formulation. In respect of European studies on innovative research design, this project attempts to combine variants of new institutionalism with the use of a process-tracking method to implement the concept of approximation in a comparative case study.

The analysis starts with a historical institutionalist approach, showing evidence of institutional changes in the EU institutions that have impacted the cybersecurity legal framework. It is followed by a process-tracking analysis of the cyber-attack campaign against Estonia in 2007 to assess if the episode is a possible cause for the EU's political responses toward its first cyberthreat. With the first two analysis parts, where one proves the institutional structure and the other part documents the reasons why the European Commission agenda begins to prioritize cybersecurity, the third analysis goes into the content of the EU cybersecurity strategy to establish indicators of Europeanization. The indicators are used in a comparative analysis based on whether Member States to assess whether Europeanisation is a factor in the implementation of the EU's cybersecurity policy.

## 5.1 Historical institutionalism

The past forms the present's reality – Without knowledge of the EU's previous experience of cooperation on criminal laws in Europe, it will be challenging to identify indicators that say enough about the EU and its Member States effort in the fight against cyber threats. This section contains highlights from the history of European Integration and institutional changes on a European level to find the causes that lead to the processes of EU Member States' cybersecurity strategies. It includes political highlights on an EU-level and excludes national legislation and law enforcement regarding cybercrime unless they directly impact the EU's recommendations on cybersecurity strategies. Studying the historical circumstances, which explain the context's framework, is a part of the argumentation for the logic behind the consideration of the problem formulation. Since the end of World War 2 (WWII), the discussion about European integration has not been about having a single market and political cooperation or not, but about how cohesive it should be and what that implies. Roughly speaking, the debate had two positions: While representatives from The European Communities (EC) and political leaders from typically West-Germany and France expressed enthusiasm for a supranational government and even ideas for a

European federal state, the British expressed enthusiasm for an intergovernmental partnership (Bunyan, 1993, p. 1). Fighting crime and defending national security has traditionally been the responsibility of the nation-state to maintain. The processes that have led to supranational cooperation of topics within the JHA and security and defense policy explain to some extent, European integration. In this case, the study tries to examine institutional indicators that might have affected national cybersecurity strategies through the political cooperation that occurs in the JHA and CSDP and sectors.

### 5.1.1. EC's Trevi Group

The first traces of an official European intergovernmental cooperation on law enforcement emerged in Luxemburg, 1976, after the then British Foreign Secretary James Callaghan's proposal for a joint special working group to combat terrorism, during a Council of Ministers meeting in Rome in 1975 was approved. The agreement was signed by the Interior Ministers of the Member States of the European Community (EC), and that became to the beginning of the Trevi group. The Trevi group's purpose was to discuss experiences and share national security strategies between the Interior Ministers. The institutional structure divided the Trevi Group into three levels: Ministerial, the Trevi Senior Officials and five working groups. The Council of Ministers meetings had now senior police and security officials (Trevi Senior Officials) in the meeting to advise on the cooperation in criminal matters. The working groups worked on different issues, but only three out of the five working groups were active:

- Trevi 1 operated on Counter-Terrorism.
- Trevi 2 operated Public Order and hooliganism.
- Trevi 3 Operated on combating Organized crime.

In 1985, Trevi 3 became active after re-defined its target of civilian air travel security and organized crime. Shortly, the process was: Trevi senior officials approved reports, prepared by the working groups, and presented it at the meetings of the Interior Ministers (Bunyan, 1993, p. 2). At the time of the fall of the Berlin Wall, the idea of more integrated security and police cooperation is being discussed between the ministers, who choose to implement the Trevi 92 working group. Trevi 92 undertakes the task of reporting opportunities for the implementation of law enforcement cooperation until other institutional structures are established in European cooperation (Ibid., p.4)

### 5.1.2 Maastricht Treaty (TEU)

In 1992, The Maastricht Treaty, also known as the Treaty on the European Union (TEU), established the European Union with expectations of uniting Europe by creating common provisions concerning political and economic matters (TEU, 1992). The instituting of the EU originated from the diplomatic work of the EC. The European Parliament (EP) and the European Commission demanded a supranational structure regarding a single institutional to govern European issues. (Chalmers, Davies, & Monti, 2010, p. 24). In a legal sense, the affairs of these EU bodies were divided into three groups classified as EU's three Pillars:

- The European Communities (EC); (first pillar).
- The common foreign and security policy (CFSP); (second pillar).
- The cooperation in the fields of Justice and Home Affairs (JHA); (third pillar).

The first pillar was on a supranational level, while the second pillar and the third pillar were operating on an intergovernmental level (The European Parlement, 2019). ***Section 5.5.2*** is only covering the matters of the third pillar, which matters are to find in Article K of TEU: *"Cooperation in the fields of justice and home affairs shall be governed by the following provisions"* (TEU, 1992, pp. 131, Art. k). This is of great relevance to the integration process and institutional changes because article K brings together law enforcement cooperation into one institution.

> *"police cooperation for the purposes of preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime, including if necessary certain aspects of customs cooperation, in connection with the organization of a Union-wide system for exchanging information within a European Police Office (Europol)" (TEU, 1992, pp. 132, Art. k.1(9)).*

By putting the Treaty into force in November 1993, the EC States approved to reinforce the intergovernmental work on combating international criminal issues, including the replacement of Trevi 92 with Europol. The plan was that it should continue to focus on information sharing, but in a meeting with Trevi Ministers on Europol in 1989, the Commission: *"power to act within the Member States would be granted"* (Bunyan, 1993, p. 6). it had the right to share initiatives on the criminal areas. The

European Commission had no power in the decision making; nevertheless, according to TEU Art. K.4 *"2. The Commission shall be fully associated with the work in the areas referred to in this Title"* (TEU, 1992, pp. 133, Art. k.4). The lack of protection of citizens in member states of the risks that come with having a single market that formed the EC-level policing body. Observations showed that it was easy for criminals to be under the radar of domestic law enforcement whose institutional structures did not adapt to supranational cooperation. The European Parliament's role in the implementation of Europol was consulting the JHA council and the European Commission. The EP was introduced to support the work of the provision and methods, so Europol's implementation became more transparent in the process (Chalmers, Davies, & Monti, 2010).

#### *5.1.2.1 The start of Europol*

During the period between the signing of TEU and TEU's practical execution, Ad Hoc working Groups of Europol were introduced to implementing Trevi 92 objects into Europol's intuitional structure. The Ad Hoc on Europol's purpose was to create the content of the Ministerial agreement on Europol and provisions of the European Drugs Unit (EDU) while monitoring the development of Europol was in collaboration with the Trevi Senior Officials (Bunyan, 1993, p. 7). The AC Hoc group carried out the preparation on Europol. It aimed to form a European police force inspired by the same methods as the United States of America's (The US) Federal Bureau of Investigation (FBI) and Interpol used.

In 1994, One of the preparations was to let the agency start limited operations as the European Drugs Unit (EDU) (Bunyan, 1993, p. 7). Practically, The AC Hoc group on Organized crime was less active but collected knowledge on trafficking and Money laundering issues. Europol was officially founded on the 1st of October 1998, and it the first law enforcement agency working on the EU-level. It followed the Europol Convention's legal framework signed by the JHA Council in 1995 based on Article k.3 of the TEU (The JHA Council, 1995).

#### *5.1.2.2 Schengen Information System (SIS)*

In June 1900, the Schengen Convention was signed by the five EC States: West-Germany, the Netherlands, Belgium, France and Luxembourg. It reaffirmed the Schengen agreement's content 1985 regarding the free movement of citizens and agreement gradually abolishment of internal borders in the Schengen Area by providing concrete provisions on specific cases of abolition, processes and Uniform Schengen Visas (USV). Although the Schengen agreement was in place, it was first physically accomplished on the 26th of March 1995, by seven of the nine Schengen countries shutting down their border controls. Italy, Spain and Portugal joined the Schengen agreement before accomplishment and several countries joined the Schengen area over time (Schengen Visa Info, 2019). More central to the matter of cybersecurity strategies was that the Schengen Information System (SIS) was introduced. It is a database containing information about criminals, unwanted foreigners, missing persons, witnesses and persons under discreet surveillance in the Schengen Area by national police in each country.

.

### 5.1.3 The Treaty of Amsterdam (ToA)

The Treaty of Amsterdam (ToA) entered into force on the 1st of November 1999 after The EU Member States signed it in 1997. ToA was an updated version of TEU, and it increased the power of the EU supranational institution (I pillar). It incorporated the Schengen acquis into the EU framework: "*CONFIRMING that the provisions of the Schengen acquis are applicable only if and as far as they are compatible with the European Union and Community law,"* (ToA, 1997, p. 93) . In the JHA matter, ToA included significant changes as new legal instrument and precise police and judicial cooperation tasks on civil matters to tighten up the cooperation. The European Community (first pillar) adopted more responsibility on these issues by excluding the JHA council option to act independently without a proposal from the EU Commission and took over immigration and asylum issues. The changes were agreed to take place over five years. The TOA clearly illustrates how JHA affairs are entrusted to decision-making processes by the European Commission.

### *5.1.4 The Treaty of Lisbon (TFEU)*

The institutional structures of the whole EC were formed into the European Union. Thus, the three pillars were melted into one institutional body, which has great significance for the JHA policy in the Member States (TFEU, 2007, pp. Art. 63-69). The Justice and Home Affairs Council became one of the Councils of the European Union, each covering their own political areas. The TFEU formed the beginning of a new era, which included *'the ordinary legislative procedure'*, in which the EU Commission has a monopoly on introducing legislative proposals. The JHA Council has no legal function in the EU but has the task of meeting every six months to develop guidelines, goals, and strategies representing the Member States' interests, which the Commission can use in the legislative process's initial process. This legislative proposal must then be voted for or against by the European Parliament; if it has a majority, the European Council must approve the vote and the proposal (Chalmers, Davies, & Monti, 2010, p. 129).

**Europol after the Treaty of Lisbon**

Europol came under EU competence, which means that the agency's legal framework is set by the legislative procedure system that came with the introduction of TFEU. A Council Decision in the TFEU replaced the Convention on Europol and reformed Europol to a fully integrated EU agency. The JHA council has the responsibility of keeping control and creating the guidance of Europol's work (European Commission, 2020a). In cooperation with the European parliament, the JHA Council approves Europol's budget and appointing the Executive Director. Besides that, the JHA Council handover a report regarding Europol to the European Parliament (Europol, 2020).

### 5.1.5 Sup-Conclusion

Section 5.1 shows that the main features of those institutional changes the JHA council and law enforcement agency (Europol) have been through. This analysis part could well have gone more in-depth and be a larger analysis, which had tracked processes of the implementation of Europol and examined in detail what compromises the Member States should consider in Europol's establishment. In this sub-analysis, the funnels and the establishment of Europol indicate that the supranational JHA cooperation should have a desire for better control of the single market's back.

## 5.2 Estonia cyberattack 2007

Cyber operations received international attention at a conference held at the United States Naval War College (US NWC) for the first time in 1999. At that time, the international community was aware of attacks on individuals and public institutions and private companies, and political action was also addressed to it. However, due to other security political issues like transnational terrorism, it was not a high priority. It changed when Europe's awareness of cybersecurity's importance heightened after a cyberattack campaign hit Estonia's for 22 days in the spring of 2007. Other attacks against digital infrastructures have also been recorded, such as activists attacking Georgia during the Russo-Georgian War in August 2008 (Schmitt, 2013, p. 2). This section focuses only on the attack against Estonia because it is the case that has the most significant impact on the EU's cybersecurity strategies. Roughly speaking, the case is the digital version of the 9/11 terror attack in the way this crisis formed international cyberlaw and defense cooperation afterward. It was the first coordinated cyberattack against a European country, and it showed how damaging the conquests could be to national infrastructures (Ottis, 2008, p. 1). The mainstream media and politicians of the Western World define the cyberattacks against Estonia as politically motivated by the Russian authorities, even though it has not been possible for officials to prove the culprits' identities.

### 5.2.1 New Tools In An old Conflict

The majority of sources associate the cyberattacks to the dissatisfaction from a minority of Russians living in Estonia and Russian politicians regarding the Estonian government's decision to relocate the Bronze Soldier of Tallinn, a WWII Soviet Monument, on the 26$^{th}$ of April 2007. The monument was a focal point of tension in the center of Tallinn between pro-Kremlin and Estonian Nationalists, which was the argument for relocating to a military cemetery outside the city. According to The New Your Times, Sergey Lavrov, the Russian foreign minister, had the following statement regarding the decision: *"This is blasphemous, and will have serious consequences for our relations with Estonia"* (Myers, Estonia removes Soviet-era war memorial after a night of violence, 2007). The night before removing the monument, a confrontation between around 1.000 Estonians, mostly of Russian

descent, and the Tallinn law enforcement took place in the area. One man named Dmitri Ganin died, and 156 people were injured (McGuinness, 2017).

The day after the removal, the 27th of April 2007, Estonia's public- and private sectors were under cyberattacks, mostly Charred as Denial of Service (DoS) and Distributed Denial of Service (DDoS), which cost temporary degradation, leaking e-mails and loss of online service. On a typical day, an average public website would handle 1.000 hits a day, but during the campaign was attacked by 2.000 hits per second (Herzog, 2017, p. 68). Other attacks were complex hacking cases where example, the method SQL injection was used to retrieve confidential data. Mainly, non-critical attacks targeted services like websites of the ministries, the parliament and newspapers, but severe attacks on the online banking system or personal data database also appeared (Ottis, 2008, p. 2). At the time, Estonia was one of the most developed EU Member states within information and communication technology (ICT), making them a vulnerable target. 60% of the population was daily internet users, 97% of all banking was done electronically (Herzog, 2017, p. 67), and the country also had *"the first online parliamentary elections in the world"* (Czosseck, Ottis, & Talihärm, 2011, s. 1).

The investigation of the cyberattack campaign against Estonia proved to be challenging. The number of single attacks was incredible, and they were carried out by a larger group of individuals with different IP-addresses, mainly from Russia. Some of them were tracked down to computers in the Russian public sector. Due to encryption and foreign IP-address, these traces led the investigation into dead ends or became foreign authorities' responsibility. An investigation showed that the attackers' location came from 178 countries (Delerue, 2020, p. 68). Tallinn, the European Commission and NATO were only able to gather enough evidence to arrest one cyber attacker in January 2008 because he operated within Estonia's borderline. A 20-year old ethical Russian student named Dmitri Galuškevitš, who lived in Tallinn, was found guilty of committing a DDoS attack on the Estonian Reform Party. Two other individuals were charged with participation, but lack of evidence stopped further prosecution (Ibid., p. 84). Mr. Galuškevitš's unwilling to cooperate with Estonian law enforcement made it not possible to gain more information about the culprits behind the attacks (Ibid., p 147). According to several newspapers and books, he was fined with 17.500 krooni for his actions (Herzog, 2017, p. 71).

Tallinn tried with international diplomacy to overcome the barriers mentioned above by involving the Mutual Legal Assistance Treaty (MLAT) between Russia and Estonia and sending *"a formal investigation assistance request"* to the Russian Federation's Supreme Procuratorate (RFSS) in May

2007. Russia rejected Tallinn's request because the RFSS argued that the actual MLAT did not cover the Estonian foreign ministry's proposed investigative processes. The Russian argument is that cyberattacks tracked to Russian IP-addresses were not enough evidence to open an investigation (Ottis, 2008, p. 3). It is a case that illustrates the issues international law is facing when it comes to cybersecurity and cyberattacks. The MLAT does not mention aspects of digital platforms and internet technology so that the national governments can interpret in favor of their interests.

Meanwhile, the Estonian internet system was under tremendous pressure, the Estonian embassy in Moscow was facing well-organized protests by Pro-Kremlin youth groups. It escalated on the 2nd of May 2007, when the then Estonian Ambassador to Russia, Marina Kaljurand, was attacked during a press conference (Ministry of Foreign Affairs of Estonia, 2007). The protests were reactions to Dmitri Ganin's death during the mass riots in Tallinn. Another case where a commercial truck blocking a border bridge near Narva was also considered protests to the events in Tallin (Myers, 2007a). Some sources see this as a clear sign of the Russian government's involvement since no authorities tried to stop it.

In May 2008, Konstantin Goloskokov, a' Commissar of the pro-Kremlin youth movement, Nashi, was the first and so far only one to claim responsibility for some of the first cyberattacks of the campaign (Delerue, 2020, p. 306). However, there is no concrete evidence to prove his statement, and experts and the Estonian government are questioning his motive to announce his actions. It is assumed to be a window-dressing strategy to promote the movement (Keating, 2010). The article '*Who was behind the Estonia cyber attacks?'* by Joshua Keating uses content from an anonymous source leaked on Wikileaks. The document is classified by the American Ambassador in Estonia, Ambassador Dave Phillips. Nevertheless, François Delerue's '*Cyber Operations and International Law'* from 2020, mentoring the same information, but from an interview with Mr. Goloskokov in Financial Times by Charles Clover (Delerue, 2020, p. 146). Furthermore, a Russian parliament member confirmed that an assistant took part in the cyber operations, but the investigating stopped due to dead ends (Ibid., 306).

### 5.2.2 The "invisible" attacker's causes

Rain Ottis' analysis from 2008 brings up three hypotheses about who may have been behind the attacks: the first hypothesis is more well-developed, where the two others are opportunities if the first turns out not to be true. The analysis is based on qualitative documents, as it was not possible to collect reliable

quantitative data. Interpretation and specific selection of documents are the used methods through text analysis and argumentations. It outlines the most likely scenario. However, this thesis does not conclude that the qualitative analysis outcome is the ultimate truth, but it approaches reality based on the arguments and facts he presented. Ottis clarifies the same statement by concluding that his "*conclusion is considered plausible"* (Ottis, 2008, p. 6).

The first hypothesis argues that the Russian government was politically motivated to disturb the Estonian authorities' actions. The motivation can be found in a combination of punishment of the political resistance, weaken Estonia's tie to the EU by pressuring the economy, and trying out methods to gain international power (Herzog, 2017, p. 69). The Russian government waged information warfare (IW) against Estonia in 2007 through an *information operation* using elements of Mao Tze Dong's classic military strategy,' *people's war'* into modern warfare. Essentially, the purpose of this strategy is to mislead the enemy away from their supplies and maintain the State's anonymity by giving the population resources to start small impulsive attacks that take the attention away from the actual attacks against the State. Implementing *people's war* into IW was introduced in 1995 by The Chinese general, Pu Feng Wang (Wu, 2004, p. 179). Chris Wu outlines IW's development in the context of China's military strategies, but it can be relative to other nations too (Ibid., p. 173). General Wang argued that civilians would be more likely to participate in this type of warfare, as the consequents of performing cyberattacks are less damaging for the individual than performing warfare types like Guerrilla warfare. The main force would be IW-experts employed by the government to anonymously supply civil attackers and find the right time windows to perform more significant information operations on the opponent's digital Infrastructure (Ibid., p. 181).

Hypothetically, it makes sense that the Russian government was behind the attacks against Estonia using the People's war. First, the attacks ranged from very simple to advanced types from many IP addresses. By making the ill-coordinated attacks like DDOS, the more complex attacks would be harder to trace. The 'new people's war strategy uses a concept called 'loot the burning house' where hackers pretend to be businessmen or students - Dmitri Galuškevitš was a student, hacking internet-facing information systems. Next, the Russian population, or a group of the population, was offended by the Estonian government. It gives them an external motivation to carry out the attacks, which is also supported by the attacks' content, which mainly had Russian political messages. The 3rd and final factor is whether it can be shown that the Russian government has invested and supported the hackers. It has

not been possible, and that is where this hypothesis starts to lack. Tallinn admits the lack of evidence to continue further investigation (Delerue, 2020, p. 305).

The two other hypotheses suggest who the culprits can be if it is not Russian authorities. The second hypothesis introduces the concept of *'False Flag Operation',* and the third introduces the concept of '*grass-root response'* - The difference is whom to blame for the attacks. The *false flag operation* believes that the culprits' strategy was to make the campaign look like a Russian interest by camouflaged themselves behind IP address encryption. Although this hypothesis is not impossible, it is difficult to assuming or concluding the motive besides damaging Russia's international relations. The *Grass-root response* perspective is that independent individuals who protested online by damaging the digital Infrastructure in Estonia due to their political disagreement with Russia have the responsibility. What makes it less likely is the well-structured pattern and the attacks; it is organized to be independent of each other. Ottis argues that both scenarios are most likely, not the case. The way Russia acted as a silent state supporter by not responding to Tallinn's request for investigative cooperation and their reactions to the relocation of the Soviet monument point Russia out as the main suspect (Ottis, 2008, p. 5). NATO officials publicly concluded that attacks were beyond non-state actor capacities (Delerue, 2020, p. 69).

### 5.2.3 The Political Aftermaths

The attacks have subsequently had a significant impact on Estonia's security policy and international relations. After the cyberattack campaign calmed down, the government acted fast and approved an Action Plan to Fight Cyber-attacks in June 2007. Three months later, it was approved that The Estonia information Society Strategy 2013 (MoEAC, 2007) should include an Implementation Plan managing digital emergency by building a better critical information infrastructure. The Estonian cyber crisis was a horror scenario for all European countries, and therefore it was natural that the EU prioritized cybersecurity on the agenda for security and law enforcement. Instantly, the EU Member States' lack of National cybersecurity strategies (CCS) became a hot political issue. Tallinn's experiences and motivation for protecting the internet-facing information systems made them the leading cybersecurity EU Member State and one of the first nations, globally, to publish a CCS in May 2008. The CCS is the first one out of three exiting – the last document covers the period 2019-2022 (Ministry of Economic Affairs and Communication of Estonia, 2018, p. 7).

The legal framework of digital information security covers all aspects of society, making the implementation essential for various agencies and ministries. To achieve the goals of the implementation plan, the government formed a cybersecurity council with various representatives of professional groups for transparent cooperation between institutions. The advice from the Council led, for example, to the protection of vital services from digital attacks; it helped shape policies that ensure the military's build defensive cyberwarfare capabilities to support Estonia's Computer emergency response team (CERT) and support the information authorities in finding vulnerable software systems. Besides the state capacity, the private sector contributed to the implementation - The voluntary organization Estonian Defense League (EDL) established the Cyber Defense League (CDL) to support the military to defend the nation's sovereignty. (Herzog, 2017, p. 70). All related provisions to cybercrime in the Penal Code of Estonia were revised, so the legal framework would not be limited by *"interference with computer data,(…)"illegal obtaining of access to computer systems."* (Ibid., p. 71). It integrated new computer-related criminal offenses as disseminating spyware and malware, and it got into the fight against terrorism by dividing cyber attacks against infrastructure and ordinary computer crime. In addition to being better prepared and protecting for a similar attack, there was undoubtedly a desire to make the execution of these attacks far more punishable. At the time, EU Member States were following the guidelines of Directive 95/46/EC regarding Data protection. Nevertheless, Estonia's Personal Data Protection Act from 2007 introduced data protection of personal data when private or public users were collecting or using them digitally (Czosseck, Ottis, & Talihärm, 2011, s. 4).

#### *5.2.3.1 Shaping international cyberlaw*

The whole case shows that it is difficult for victims to identify criminals without international cooperation. The internet does not depend on borders or physical environment, which challenges the theoretical framework of geopolitics perspectives on warfare and undermining enforcement laws. National Security needs international laws and actions to overcome investigative barriers regarding cybercrime operations or cyber warfare. During the attacks, Estonia's actions were in cooperation with its NATO allies, and on the 28$^{th}$ of May 2008, NATO founded its Cooperative Cyber Defense Center of Excellence (CCDCOE) located in Tallinn. The center's main tasks are researching and exchanging data on cybersecurity, a great new force to support the work of NATO's Cyber Defense Management

Authority (CDMA). The report *Tallinn Manual on the International Law Applicable to Cyber Warfare* is one of the most recognized publications in the academical development of connecting International law with cyberwarfare. It is developed by an *'independent expert group"* invited by CCDCOE (Schmitt, 2013, p. 1).

The role and size of The EU's Network and Information Security Agency (ENISA) in the EU in the aftermath of the 2007 cyber attacks. Cybercrime was on the dashboard of ENISA, mainly because of the Council of Europe Convention on Cyber Crime (Council of Europe, 2001) and the Council Framework Decision 2005/222/JHA (Council of Europe, 2005). These documents have been renewed by regulation but is seen as the cornerstone of EU common legislation on information security issues. However, ENISA received far more resources from the EU budget for capacity building and awareness-raising regarding the topics associated with the **use** of internet-facing information systems. The agency became a major player in building the EU cybersecurity strategy and supporting other EU Member States defense strategies. In 2012, the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security, and Justice (EU-LISA) was established in Tallinn. It is an interoperation database functioning so authorities can smoothly access to collected data from the EU agencies, bodies, and external cooperation like the Schengen information system (SIS) and Interpol (EU-LISA, 2019).

### 5.2.4 Sub-conclusion

The cyber attacks on Estonia in 2007 and subsequent political interest from the EU and the rest of the world are a clear sign of Europeanisation's bottom-up approach. It is seen how an "episode" in a member state becomes a political issue that the EU will have to react to in order to show solidity with Estonia, but also because the EU's own interests are that it does not happen against the Union itself or for other States in it. The likely possibility that the Russian government is responsible also means that the EU must be ready for defense. It became a high priority for member states because the Estonia case shows how it can harm national security. The aftermath shows that Estonia is turning a crisis into something useful by becoming a leader in cybersecurity. They have shown that by mastering crisis management in new political issues, one can gain international influence.

## 5.3 The statistical framework of a digital European Union

The third part of the analysis identifies "indicators" for Europeanisation in EU CSS. The indicators must be strategic goals that can be applied at the domestic level in order to be able to assess the approximation of Member States to the EU objectives. A basic indicator is whether the Member State has adapted to the EU legal framework, but this section only looks for National Cyber Security Strategies (NCSS) indicators.

### 5.3.1 The EU's Cybersecurity strategy

Document JOIN (2013 1 final (EU CSS 2013) is the European Commission's Communication on a *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, and it was published the 7th of February 2013. According to the EU cybersecurity strategy, The internet is a "*powerful instrument for global progress without governmental oversight or regulation"* which in some cases can turn in to be a severe threat to EU citizens, Members States and institutions overall security (European Commission, 2013, p. 3). The beginning of Section 2 (Strategic priorities and actions) covers the context of this comparative case analysis by mentioning: *"The EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance.*" (Ibid, p. 4).

The European Commission acknowledges the member States' sovereignty on laws of criminal matters but setting an agenda on the national cybersecurity by including EU's values "*fundamental rights, freedom of expression, personal data and privacy"* to gain powerful influence globally. Aiming to do so, the EU CCS has five priority points to ensure overall cybersecurity in the EU and the Member States.

The five priorities are used in the next analysis part as indicators of the EU Member States' approximation to the EU cybersecurity strategy to conclude if Europeanization impacts the member states adapting to cybersecurity. The priorities that the Eu tries to achieve will be illuminated in the next part sections.

#### *5.3.1.1 Achieving cyber resilience*

To ensure internal security within the EU, the private sector and the public sector must work together to collect experience and data to build resilience. It ensures that the consequences of cyber-attacks are reduced by being prepared and disseminating the information on a cross-border dimension. National capabilities, private sector involvement emergency knowledge spanning were on the agenda of cyber resilience and became parts of a proposal involving the EU Network and Information Security Directive (NIS). Three years later, The proposal was adopted by the EP and the Council, which made it the first EU-wide cybersecurity legislation, Directive (EU) 2016/1148. It means that the EU member states now must implement the legal framework of Directive (EU) 2016/1148 into their national legislation. The dateline for the national transposition of Directive (EU) 2016/1148 was 2018 the 9th of May, 2018 (ENISA, 2020). Creating directives is a sign of increasing harmonization between The EU member States because the national laws adapt to the directive and, at the same time, force it to get EU member states to approximate the Commission's cybersecurity strategy.

Back to the content of Document JOIN (2013 1 final, One of the strategy's collaborative elements was the National NIS competent authorities' role, which is recommended to collaborate and exchange information with other regulatory bodies, especially to personal data protection authorities. That the European Commission mention personal data protection authorities matters because, at that time, The EU was working on updating the European Data Protection Directive (Directive 95/46/EC) into what we today know as the General Data Protection Regulation (Regulation (EU) 2016/679). It was based on a proposal from the European Commission on the 25th of January 2012, aiming to make a *"comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy*" (European Data Protection Supervisor, 2020).

The plan is for competent national authorities to issue warnings regarding on-going accidents and risks and update coordinated responses. The cooperation between the public and private sectors should remain voluntary and not be replaced or stopped due to legal obligations to increase security, best practices and exchanging information (European Commission, 2013, p. 7). ENISA has an essential role in the development of The EU Member States' cyber capabilities by assisting in building expertise on security and manages the program of pan-European exercise (Cyber-Europe), which are simulated incidents of large-scale cybersecurity. The Commission raised awareness by inviting the EU Member-

States to organize a yearly cybersecurity month with the US and introducing NIS and GDPR into the education and training programs (Ibid, p.8.).

#### *5.3.1.2 Drastically reducing cybercrime.*

The Budapest convention forms the framework of national cybercrime legislation. In 2011, the EU replaced Decision 2004/68/JHA with Directive 2011/93/EU, and the legislation concerns the matter of combating sexual exploitation of children child pornography (Council of Europe, 2001). The replacement happened because the old legislation did not cover such actions over the internet. It shows how replacing EU legislation implements new legislation on cybercrime to adapt to the changes in society. The EU legislation regarding cybersecurity has, until the NIS directive, been produced because they were an update to other policy areas which got adopted the TEU and ToA negotiations. The section of '*Drastically reducing cybercrime'* underlines the Commission's action on combating Child sexual abuse online and working with non-EU countries on the subject.

European Cybercrime Centre (EC3) is a key factor when it comes to reducing cybercrime**.** Its tasks are to provide intelligence and analysis, create communication channels for the competent national authorities, and gradually implement instruments to combat cybercrime into law enforcement. It supports the EU Member States with disrupting cybercrime networks (Europol, 2020a). The strategy contains a suggestion to Eurojust regarding judicial cooperation in the field of reducing cybercrime. Cybercrime concepts build on globalization, and the criminals do not have to be European citizens or even operate in the EU. Providing support for judicial strategies and investigation can reduce the number of cybercriminals worldwide, which would reduce cyberattacks against the EU. Including Third Countries can be a sign of trying to gain normative power as it experienced in the case of the GDPR Directive by how example, Australia and Canada were adopting elements of the GDPR in their national legislation.

#### *5.3.1.3 Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)*

The developing of CSDP's cyber defense strategy has some relevance to answering the problem formulation as it involves decision- and policy making on a supranational level. However, the analysis is not investigating indicators as budgets or decisions of the CSDP regarding military cyber defense

missions or warfare; the relevance to the problem formulation comes in light of European integration where CSDP is defined as a supranational EU body. The rationale of the project means that topics in the EU's cybersecurity strategy, to which the Commission attaches to CSDP, are understood as a neo-functionalist trait. The EU can legally determine future military strategy guidelines, as the Member States share common foreign and security policy. It does not directly apply to Denmark, which did not want to be part of the common European Defense by voting against the TEU proposal in 1993; the outcome of Denmark's cybersecurity strategy concerning the development of a cyber defense has no official barriers from the EU (TEU, 1992, p. 194).

#### *5.3.1.4 Develop the industrial and technological resources for cybersecurity*

This point covers the products and tools that people use every day while diving into cyberspace. The ICT industry has evolved to be one of the world's largest industries, and most of the production happens outside the EU's external borders. (Statista, 2020). The Commission argues that security solutions concerning privacy and data protection on ICT products are also developed on other continents, making it less trustworthy and secure because they do not follow the requirements of the GDPR.

According to the Commission, the private sector has a significant role in promoting a single market on ICT-products and ensuring safety quality. The Commission suggests making cybersecurity a priority for the companies: *"Labels indicating adequate cybersecurity performance will enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge"* (European Commission, 2013, p. 12). The mentioned obligations from the proposed directive on NIS should also play a legal role in business competitiveness by creating a judicial framework, which would benefit the European ICT- Manufacturers. The Member States are invited to use public administrations' purchasing power to ensure ICT products' security and services it with Research and development (R & D) technological innovations.

The cooperation regarding security in ICT products has to be transparent. Public and private Stakeholders are asked to develop *harmonized metrics for calculating risk premiums* so companies that invested in ICP security can benefit from lower risk premiums.

#### *5.3.1.5 Establish a coherent international cyberspace policy for the European Union and promote core EU values.*

This section describes the EU's responsibility for the global challenge of cybercrime, in which openness and freedom is a European value that must remain in the 'legislation of international cyberspace policy. The same legal framework as the EU legislation will also be included in how the EU tries to guide in cyber issues legislation. It is seen how the normative power used by talking about values such as the maintenance of human rights and democracy must be implemented in the use of cyberspace**.** *"In cooperation with the Member States, the Commission and the High Representative will: Work towards a coherent EU International cyberspace policy to increase engagement with key international partners and organisations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues;"* (Ibid., p. 16). From a theoretical point of view, this statement represents a willingness to include handling cyber issues in CFSP, which is interesting because it interprets because the Commission was wanting more power in the EU on the subject. Thus, 'mainstream cyber issues' go from being a problem for the EU Member States legislating to supranational legislation because of the joint defense initiative founded in TEU's wok.

### 5.3.2 Coordination

The responsibility of cybersecurity in the EU is divided into national and EU levels into three areas: Network and Information security, Law enforcement, Defense. At the national level, distribution of information and creating networks of relevant stakeholders go to selected CERTs (emergency response groups) and NIS competent authorities. Reporting cybercrime is done in the same way as reporting other criminal activities; the national law enforcement takes care of it through Cybercrime Units. The national defense authorities must have established departments that prepare cybersecurity for military strategy and risk assessments. The EU Defense agency supports the national defense to managing and reporting on cyber Defense strategies while bringing it up to the EU level by sharing experiences with the other member States and the European Union External Action (EEAS). They are also focusing on the external policy framework. The European law enforcement agency Europol and epically its unit EC3 is the active linkage from the NIS directive to the implantation of law enforcement (Ibid. p. 16).

## 5.4 National cybersecurity strategies

In the EU cybersecurity strategy, the Commission recommends that the Member States make their national cybersecurity strategies to accommodate the population and the government's interests. There is an understanding of the EU's part about the complexity and that each state has its own needs. Furthermore, domestic strategies are important in emergency situations, as the Member State itself has the main responsibility for its own national security (Ibid. 17).

### 5.4.1 Austria

| **Member State: Austria** | **Title:** *Austrian Cyber Security Strategy* (Chancellery of the Republic of Austria, 2013) | **Dato:** the 20th of March, 2013 |
|---|---|---|
| **Strategy assessment:** | **Top-down approach** | Bottom-up or neutral approach |
| **indicators** | - The strategy mentions that future legislation must be based on European solidarity.<br>- A desire for cybersecurity to meet the high standards – Guarantee *"human rights, in particular privacy and data protection"* (Ibid., p 7)<br>- Austria transposed Nis-directive In time (High compatibility).<br>- Implemented a Single point of contact: Federal Ministry of the Interior of Austria | |
| **1. Achieving cyber resilience**<br>. | - Positive for resilience critical infrastructures.<br>- Plan of implementing cybersecurity into the Austrian Programme for Critical Infrastructure Protection. | |
| **2. Drastically reducing cybercrime** | | - The strategy has Minus on a strategic plan on reducing cybercrime. |

| | | |
|---|---|---|
| | | - It does not mention of Europol or EC3. |
| **3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)** | | - No strategic insight. |
| **4. Develop the industrial and technological resources for cybersecurity** | - EU Security programs must prioritize research on cybersecurity | |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - *"Austria will make a substantial contribution to the development and implementation of an EU Cyber Security Strategy. It will fully participate in the strategic and operational work of the EU"* (Austria, 2013, p. 13) | |

Austria's cybersecurity has not been updated since the 20th of March, 2013, a month after the EU's first cybersecurity strategy. It is a signal that Austria has been aware of cybercrime issues and has been working on improving a cybersecurity strategy. In 2015 Austria published a cybersecurity platform, and in the spring of 2018, they implemented a cybersecurity team to transpose the NIS-directive (Chancellery of the Republic of Austria, 2013). However, it is problematic in order to form a national plan on the cyber legislation that has been in force since.

### 5.4.2 Croatia

| | | |
|---|---|---|
| **Member State:** Croatia | **Title:** *The national cyber security strategy of the Republic of Croatia* (Government of the Republic of Croatia,, 2015). | **Date:** 7th of October 2020 |
| **Strategy assessment:** | Top-down approach | Bottom-up or neutral approach |
| **direct indicators** | - Croatia wants to improve standard single-factor authentication and other qualified electronic signatures *"in accordance with the EU requirements"* (Government of the Republic of Croatia,, 2015, p. 12) | |

| | | |
|---|---|---|
| | - Croatia Transposed the NIS-directive in time (High compatibility).<br><br>- Croatia Implemented a single point of contact: . | |
| **1. Achieving cyber resilience**<br>. | - *"Strengthening cooperation in the area of risk management for European critical infrastructures"* | |
| **2. Drastically reducing cybercrime** | - Sharing information over Europol and Eurojust.<br>- A Detailed plan of reducing cybercrime (section 5.3) (Ibid. p. 16) | |
| **3. Developing cyberdefence policy and capabilities related to the CSDP** | - Desire for international regulation on cyberlaw from both EU and NATO<br>- Croatia's cybersecurity crisis management needs to harmonize with EU and NATO' standards. | |
| **4. Develop the industrial and technological resources for cybersecurity** | | - Lack of develop strategy in the industrial area of cybersecurity. |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - *"requires close cooperation of the EU and NATO Member States"* (Ibid. 17)<br>- Wants improvement of the implementation of the Council of Europe's Convention on cybercrime | |

Croatia's cybersecurity strategy meets all points to be indicators of wanting to achieve European transparency and standards. Compared to Austria, which had a more confident attitude toward cybersecurity strategy, Croatia's strategy is that they are trying to live up to standards and not set them. The adaptational pressure emerges, but not that it can be seen to a great extent (Ibid., p.22).The strategy does not come with specific numbers or statements about which goals require intense prioritization - just what needs to be strengthened to achieve goals. The strategy is published approx. one and a half years after the EU strategy from 2013, and as mentioned, strategic considerations regarding industrial development are lacking (European Commission, 2020b).

### 5.4.3 The Czech Republic

| | | |
|---|---|---|
| **Member State:** The Czech Republic | **Title:** *National Cyber Security Strategy Of the Czech Republic for the Period From 2015 to 2020* (Czech Republic National Cyber Security Centre, 2015). | **Dato:** 16/02/2015 |
| **Strategy assessment:** | Top-down | Bottom-up or neutral approach |
| **Other indicators:** | - Following EU and NATO.<br>- The Czech Republic is adapting to international laws.<br>- Domestic Changes.<br>- The Czech Republic transposed Nis-directive in time (High compatibility).<br>- Implemented a national CSIRT: The Czech republic's national cyber and information security agency | |
| **1. Achieving cyber resilience**<br>. | | - Weak strategy: no plan<br>- The only goal for gaining resilience to stop DDos/Dos attacks - Not how to achieve cyber residence. |
| **2. Drastically reducing cybercrime** | - *"To support international cooperation in information sharing and training in the field of cybercrime"* (Ibid. p. 20). | - The NCSS not mention EU agencies. |
| **3. Developing cyberdefence policy and capabilities related to the CSDP** | - Point 13: ICT development in the hands of the Czech Republic's defence forces. *"Information and communication technologies are increasingly present in the state defence forces' systems (…)(for instance, military vehicles or aircraft)"* (Ibid. p.14).<br>- Update according to EU and NATO requests. | |
| **4. Develop the industrial and technological resources for cybersecurity** | - Point E(1): Participating in European projects concerning cybersecurity.<br>- Experimental research across EU borders. | |

| | | |
|---|---|---|
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - Principles: Respecting data protection privacy rights before the complication of the GDPR | |

The Czech Republic is adapting to the international system; however, it is difficult to conclude whether there is a base model understanding of Europeanisation, as no pressure is seen to appear in the strategy. The NIS-directive is "transposed", which indicates that the action plan has been implemented (European Commission, 2020c).

#### 5.4.4 Denmark

| **Member State:** Denmark | **Title:** *Danish Cyber and Information Security Strategy* (Danish Ministry of Finance, 2018) | **Dato:** 01/05/2018 |
|---|---|---|
| **Strategy assessment:** | Top-down approach | Bottom-up approach |
| **Direct indicators** | - Denmark transposed NIS- directive in May 2018. (High compatibility).<br>- Denmark did institutional changes in the financial and Maritime sector.<br>- Implemented Single point of contact: *The Danish Centre for Cybersecurity* | - The second edition of the Danish cybersecurity strategy: First one was published in 2015. |
| **1. Achieving cyber resilience**<br>. | - *"The European Commission has proposed a comprehensive cyber-security package, of which the overall aim is to achieve resilience, (...) The cyber-security package continues the progress made with the EU Cybersecurity Strategy of 2013, in which the Network and Information Security Directive (NIS directive) was a key element."* (Ibid. 40) | |
| **2. Drastically reducing cybercrime** | | - NCSS does not included cybercrime directly. |

| | | |
|---|---|---|
| | | - Uses the term 'IT-related crime' or ICT crime.´<br><br>- A matter of national institutions' interest in becoming resilience. |
| **3. Developing cyberdefence policy and capabilities related to the (CSDP)** | | - Plan of establishing a working group on best possible way to fight ICT crime – participants are the ministry of defense and Ministry of Justice. |
| **4. Develop the industrial and technological resources for cybersecurity** | | - Initiative 3.9: *"At the international level, the government will identify data ethics and data protection as key focus areas for the Danish tech ambassador in Silicon Valley as a step towards improving its dialogue with major multinational tech companies"* (Ibid. 45).<br>- |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - Denmark is using common European values in the principles of the cybersecurity. | |

Denmark's cybersecurity strategy goes beyond European standards and helps to influence European cybersecurity. It is an adaptational pressure that makes domestic institutes adapt regulatory changes towards the Nis-directive, but the Danish interest in the subject makes it comply with the EU legal framework of cybersecurity.

### 5.4.5 Estonia

| **Member State: Estonia** | **Title:** *Cybersecurity Strategy Republic of Estonia* (Republic of Estonia Ministry of Economic Affairs and Communication, 2019) | **Dato:** 5/09/2019 |
|---|---|---|
| **Strategy assessment:** | Top-Down approach | Bottom-Up approach |
| **indicators** | - Acknowledge that the GDPR and the Nis-directive can not be separated into different disciplines. | - Arguments that the EU has listened to and been inspired by Estonia's first cybersecurity from 2009. |

| | | |
|---|---|---|
| | - The EU has formed to cybersecurity legal framework in the EU.<br>- Estonia transposed Nis-directive in time (High compatibility).<br>- Implemented National CSIRT*: Estonian Information System Authority* | - That the EU strategy's framework from 2013 has formed the NIS directive (Ibid., p.7).<br>- Sets the agenda for what is trending in cybersecurity. |
| **1. Achieving cyber resilience**<br>. | - NCSS maintains the development of strong technological resilience. | |
| **2. Drastically reducing cybercrime** | - Cooperation with Europol is essential to combat cybercrime.<br>- Estonia updated law enforcement institutions for better communication with Europol. | - Want to form the framework of Interagency cooperation.<br>- New initiatives. |
| **3. Developing cyberdefence policy and capabilities related to the CSDP** | | - NCSS Focus more on NATO than CSDP. |
| **4. Develop the industrial and technological resources for cybersecurity** | | - Criticism the EU Member states for being passive in the development of resources.<br>- Using instruments developed in the US: reducing European development (Ibid., p. 22). |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | | - Estonia has an internationally leading role in cybersecurity.<br>- NCSS is setting the values. |

Estonia has ownership of the European cybersecurity strategic agenda. The public does not need to make its cybersecurity strategy 2019 to 2022 a year before the EU's cybersecurity strategy 2020-2025. The alternative Bottom-Up approach of Europeanization fits this case. Estonia is trying to go beyond the European framework, but at the same time is trying to gain influence in Europe. It thus shows that the EU's "new" member states can play a more influential role in the EU by specializing in new political issues.

### 5.4.6 Finland

| **Member State:** Finland | **Title:** *Information Security Strategy for Finland* (Finnish Ministry of Transport and Communications, 2016) | **Dato:** 16.04.2016 |
|---|---|---|
| **Strategy assessment:** | Top-down approach | Bottom-up approach |
| **Indicators:** | - Finland Seeking to ensure that the domestic strategy fits the EC's trade negotiations and single market strategies.<br>- Finland Transposed the Nis-directive in time (High compatibility).<br>- Finland implemented a Single point of contact. | |
| **1. Achieving cyber resilience**<br>. | - The priority does not appear in the document. | |
| **2. Drastically reducing cybercrime** | - Establishing a working group that is open for European cooperation. | - No initiatives |
| **3. Developing cyberdefence policy and capabilities related to the CSDP** | - NCSS Supporting the activities of ENISA. | - No concrete plan. |
| **4. Develop the industrial and technological resources for cybersecurity** | - Wants to adopt a higher standard with the EU on digital goods and services. | |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - Point: 3.2 _ *"Finland will acknowledge the objectives of this strategy in the implementation of the EU's strategies for a digital single market and cyber security."* (Ibid., p.8) | |

Finland has a "transpose" NIS directive and a CERT responsible. Finland is up to date on the law, but based on their cyber security strategy, they do not contribute to the reading of cybercrime and attacks

through policy initiatives and proposals. It is their second cybersecurity strategy: it was first released on the 24th of February 2013, a month before the EU's CCS in 2013, but both have been small 11-page strategies that seems more to be a checklist. However, the older version looks similar to the EU strategy.

### 5.4.7 France

| **Member State:** France | **Title:** *French national digital security strategy* (Valls, 2015) | **Dato:** 10.10.2015 |
|---|---|---|
| **Strategy assessment:** | Top-down approach | A bottom-up approach |
| **Indicators:** | - France transposed the Nis-directive in time (High compatibility).<br>- Implemented CERT-FR | - *Along with voluntary Member States, France will be the driving force behind European strategic autonomy. It will play an active role in the promotion of a safe, stable and open cyberspace* (Ibid. 39) |
| **1. Achieving cyber resilience** | | - *"France owes it to itself to assist in reinforcing the capabilities of countries that would like to increase the resilience"* (Ibid. 40)<br>- Going for a central role |
| **2. Drastically reducing cybercrime** | - Open for European Cooperation | - Does not mention European agencies |
| **3. Developing cyber defence policy and capabilities related to the CSDP** | - Responsible for ensuring high-level crisis management cyber defence is Cert-EU and NCIRC (Computer Incidence Response Capability) in NATO (France support both with consulting).<br>- Support crisis management on EU level | |
| **4. Develop the industrial and technological resources for cybersecurity** | - French Takes full advantage of the EU's offer to support and defend French technological and industrial competencies. | - Having industrial capabilities to protect sovereign information |
| **5. Establish a coherent international cyberspace policy for the European** | - *"French or European concept of privacy or with its legal framework."* (Ibid. 20) | |

| | | |
|---|---|---|
| **Union and promote core EU values.** | | |

France is not under adaptational pressure because the compatibility is high toward the EU strategy. The strategy does not mention the EU much but uses more 'European' cooperation. Their approach can be compared with the Danish strategy, where there is an interest in creating solutions that the EU can consider implementation in the next strategy. It is (another) example that the National cyber securities are flexible as long the regulatory changes following the legal framework.

### 5.4.8 Germany

| **Member State: Germany** | **Title:** *Cyber Security Strategy for Germany 2016* (The Federal Government of Germany, 2016) | **Dato:** 07.11.2016 |
|---|---|---|
| **Strategy assessment:** | Top-down approach | Bottom-up approach |
| **Indicators** | - The GCSS expresses that European Cooperation Strengthen Germany's cybersecurity.<br>- Advising European IT security to be based on Common Criteria (CC) to measure certification<br>- Germany Transposed the Nis-directive in time (High compatibility).<br>- Implemented a Single point of contact | - *"Germany must maintain its sovereignty"* (Ibid. p. 7) |
| **1. Achieving cyber resilience**<br>. | - Action area 4: Germany wants to push the interoperable cybersecurity cooperation within the EU's competences framework. (Ibid. 29) | |
| **2. Drastically reducing cybercrime** | - Does not appear<br>- the interoperable cybersecurity cooperation applies *police and judicial cooperation* | |
| **3. Developing cyberdefence policy and capabilities related to the CSDP** | - *"applies to(...), to the Common Foreign and Security Policy and to the European IT security research network.* (Ibid., p. 29) | |

| | | |
|---|---|---|
| **4. Develop the industrial and technological resources for cybersecurity** | - The federal government wants the security authorities to use latest technological developments. | |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - Closing European work strengthens Germany's cybersecurity.<br>- Encouraging as many countries to join the Convention on Cybercrime. | |

Germany wants close European cooperation and is more supportive and content to include the EU as a decision-maker compared to France and Denmark. The German government does not express that institutional change is a problem, and the NIS Directive implementation is transposed successfully. In the fields of cybersecurity, Germany is not the member State that sets high standards. It follows the common act of the EU.

### 5.4.9 Ireland

| **Member State:** Ireland | **Title:** *National Cyber Security Strategy 2015-2017* (Irish department of communications energy and natural resources, 2015) | **Dato:** 20.07.2015 |
|---|---|---|
| **Strategy assessment:** | Top-down approach | Bottom-up approach |
| **indicators** | - Ireland Transposed the Nis-directive in time. (High compatibility).<br>- Implemented CSIRT-IE | |
| **1. Achieving cyber resilience** . | - Concerned that the EU CSS was losing ground, using the Draft Directive of the NIS- directive (2013) as a "template" for the ICSS. | |
| **2. Drastically reducing cybercrime** | - Expressing political action from the Minister for Justice and Equality to give legislative effect to the Updated Budapest Convention on cybercrime. | - |
| **3. Developing cyberdefence policy and** | - CSIRT-IE develops strong relations with ENISA and other similar organizations on a global level. | |

| | | |
|---|---|---|
| **capabilities related to the CSDP** | - The Irish Defence Forces maintain cyberdefence arrangements to prepare for a national cyber emergency. | |
| **4. Develop the industrial and technological resources for cybersecurity** | - The ICSS lacks initiatives for developing resources for cybersecurity.<br>- The ICSS appears only to mention institutional changes within Communications, Energy and Natural Resources. | |
| **5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.** | - Fostering a secured cyberculture by including cooperation with the education system and *"promoting events like the cyber security month" (Ibid., 15).* | |

Ireland's strategy sets out the priorities of the EU CSS and refers extensively to the EU institutions. It follows up on the legal framework but does not bring initiatives. It is a low level of Europeanisation because national security is in the country's interests, and since EU cooperation covers needs, it is not necessary to use many resources.

# Chapter 6: Conclusion

The quote saying: *"The more you know, the more you know you do not know"* seems to be quite suitable to the process of this thesis project. In the end, while trying to answer the problem formulation by connecting four analysis parts, the acknowledgment of the n=1 problem hit: This project is on the surface of too many variables but fails to go in-depth with the cases. The research design became too broad due to curiosity in too many directions.

The weakness of the analysis is its lack of limitation – Section 5.1 historical institutionalism, or its attempt, fails to assess the Europeanisation effects in implementing cybersecurity in the EU Member States. However, it provides an overview of European integration within justice and home affairs and the CSDP, which helped analyze indicators at the domestic level.

The case of the cyber attacks on Estonia shows an example of the bottom-up approach against the baseline model. Estonia is dominant at the EU level in terms of cybersecurity. Although it has been shown through this project that the crisis of 2007 is an alternative factor, it cannot be stated that it has a causal connection with this episode and the content of the EU Cyber Security strategy. There is not enough empirical evidence to conclude it, but enough empirical material to say that it has some influence. The assessment is that before the argument about Estonia's cyberattacks in 2007 as a Europeanisation, the effect can be empirically approved. A European or national cyber crisis must arise in an EU Member State to clarify Estonia's significance's ownership of cybersecurity and defense in European cooperation.

The comparative analysis has shown that Europeanisation (the top-down approach) cannot be confirmed because the nine Member States that have been sampled have all adapted the legislation without any noticeable difficulty. It means that the member states included in **Section 5.4** have high compatibility concerning EU standards, which is equal to low Europeanisation according to Goodness of fit. There is thus no need to tighten up the legislation, as everyone follows the legislation. Next, it shows that national cybersecurity strategies have different levels of ambition. Estonia, Denmark and France set a higher standard than the rest of the nine sampled Member States on cybersecurity strategy. The standard depends on nations' interest, where some are very interested in providing a robust independent NCSS, and others basically follow up on what is necessary. The motivation for being a "cybernation" can be international prestige, fear of cyberattacks or expanding markets.

This project adheres to Ido Sivan-Sevilla's 'Europeanisation on-demand' model, saying that if there is any top-down approach in the matter of cybersecurity policymaking, it is because it is on-demand from the Member States (Sivan-Sevilla, 2020). The Member state's desire for more legislation and regulatory changes to improve the individual country's quality of cyber security will be in the interest of national and EU levels. The 'Europeanisation on-demand' model may just be temporary until the Cybersecurity becomes a more integrated political area. The prediction is that the first two decades with policymaking in cyberspace will be the two first decades out of many. **Section 5.1** showed that the integration process changes the institutional structures of Justice and home affairs before, and with the development of information system technology, it would be naïve not to prepare for new significant changes in the future.

## Bibliography

Austria, F. C. (2013). *Austrian Cyber security Stratey.* Vienna: Security Policy Affairs.

Balde, M. C. (2018). *The cybersecurity landscape of the European Union: An institutional journey of EU cybersecurity cooperation from 2001 to 2018.* Retrieved from leidenuniv.nl: https://openaccess.leidenuniv.nl/bitstream/handle/1887/75216/MA%20EUS%20Thesis%20s1288601.pdf?sequence=1

Beach, D., & Pedersen, R. B. (2013). *Process-Tracing Methods: Foundations and Guidelines.* The University of Michigan Press: Ann Arbor.

Bryman, A. (2012). *Social Research Methods.* Oxford: Oxford University Express.

Bunyan, T. (1993). *Trevi, Europol and the European state.* Retrieved from www.statewatch.org: https://www.statewatch.org/news/handbook-trevi.pdf

Calderoni, F. (2010a). *Organized Crime Legislation in the European Union.* Milano: Springer.

Calderoni, F. (2010b, December). *The European legal framework on cybercrime: Striving for an effective implementation.* Retrieved from Researchgate: https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation

Chalmers, D., Davies, G., & Monti, G. (2010). *European Union Law.* London: Cambridge University Press.

Chancellery of the Republic of Austria. (2013, March 20). *Cyber Security*. Retrieved from Chancellery of the Republic of Austria: https://www.bundeskanzleramt.gv.at/en/topics/security-policy/cyber-security?lang=en

Council of Europe. (2001, December 13). *Budapest Convention on Cybercrime.* Retrieved from Coouncil of Europe: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Council of Europe. (2005, Marts 16). *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.* Retrieved from Eur-lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN

Czech Republic National Cyber Security Centre. (2015). *National Cyber Security Strategy Of the Czech Republic for the Period From 2015 to 2020.* Prauge: National Cyber Security Centre. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.* Tallinn: CCDCOE.

Danish Ministry of Finance. (2018, May 1). Danish Cyber and Information Security Strategy. Copenhagen.

Delerue, F. (2020). *Cyber Operations and International Law.* Cambridge: Cambridge University Press.

ENISA. (2020, 04 17). *NIS Directive*. Retrieved from the European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/nis-directive

EU-LISA. (2019, January 3). *Youtube.* Retrieved from Achieving Interoperability for a Safer Europe: https://www.youtube.com/watch?time_continue=7&v=JcYk0Ld2gus&feature=emb_title

Europa Commission. (2010, November 4). *COM(2010) 609 final.* Retrieved from ec.europa.eu: http://ec.europa.eu/transparency/regdoc/rep/1/2010/EN/1-2010-609-EN-F1-1.Pdf

European Commision. (2020, October 7). *Cybersecurity*. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/cyber-security#Strategy

European Commission. (2013, 2 7). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN (2013) 1 final*. Retrieved from ec.europa.eu: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

European Commission. (2020a, October 08). *Migration and Home Affairs*. Retrieved from European Commission: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/europol_en#:~:text=Europol%20came%20under%20the%20European,agency%20on%201%20January%202010.

European Commission. (2020b, October 9). *Implementation of the NIS Directive in Croatia*. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-croatia

European Commission. (2020c, October 10). Implementation of the NIS Directive in the Czech Republic. Brussels.

European Data Protection Supervisor. (2020, 05 06). *The History of the General Data Protection Regulation*. Retrieved from edps.europa.eu: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Europol. (2020, October 13). *About Europol*. Retrieved from Europol: https://www.europol.europa.eu/about-europol

Europol. (2020a, October 6). *EUROPEAN CYBERCRIME CENTRE - EC3.* Retrieved from Europol: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Exadaktylos, T., & Radaelli, C. (2015). Europeanisation. In K. Lynggaard, I. Manners, & K. Löfgren, *Research Methods in European Union Studies* (pp. 206-220). London: Palgrave Macmillan.

Finnish Ministry of Transport and Communications. (2016, 19 April). *Information Security Strategy for Finland.* Retrieved from Valto Etusivu: https://julkaisut.valtioneuvosto.fi/handle/10024/75353

Government of the Republic of Croatia,. (2015). *The national cyber security strategy of the republic of Croatia.* Zagreb: Government of the Republic of Croatia.

Herzog, S. (2017). *Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity.* Washington: Georgetown Journal of International Affairs.

Irish department of communications energy and natural resources. (2015, August 20). *Irish National Cyber Security Strategy.* Retrieved from ENISA: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Kańciak, A. (2017, Juli 03). *In search of EU law in the domain of cyberspaceprotection – the proposal based on the Cyber-PDCA model.* Retrieved from Tandfonline: https://www.tandfonline.com/doi/full/10.1080/23742917.2017.1322854

Keating, J. (2010, December 7). *Who was behind the Estonia cyber attacks?* Retrieved from foreignpolicy (FP): https://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/

Kettunen, M. (2020). *Legitimizing European Criminal Law Justification And Restrictions Merita Kettunen.* Helsinkin: Springer.

Kratochvíl, P., & Tulmets, E. (2010). *Constructivism and Rationalism as Analytical Lenses: The Case of the European Neighbourhood Policy.* Berlin: SSOR - social science open access repository.

Lynggaard, K., Löfgren, K., & Manners, I. (2015). Crossroads in European Union Studies. In K. Lynggaard, K. Löfgren, & I. Manners, *Research Methods in European Union Studies* (pp. 3-17). London: Palgrave Macmillan.

McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia.* Retrieved from BBC New: https://www.bbc.com/news/39655415

Ministry of Economic Affairs and Communication of Estonia. (2018). *CYBERSECURITY STRATEGY - Republic of Estonia (2019-2022).* Tallinn: ministry of economic affairs and communication estonia.

Ministry of Foreign Affairs of Estonia. (2007, May 02). *Estonian Ambassador to Moscow was attacked*. Retrieved from Republic of Estonia Ministry of Foreign Affairs: https://vm.ee/en/news/estonian-ambassador-moscow-was-attacked

Myers, S. L. (2007, April 27). *Estonia removes Soviet-era war memorial after a night of violence.* Retrieved from The New Your Times: https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html

Myers, S. L. (2007a, May 03). *Friction Between Estonia and Russia Ignites Protests in Moscow*. Retrieved from The New York Times: https://www.nytimes.com/2007/05/03/world/europe/03estonia.html

Ottis, R. (2008, January). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Retrieved from https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Republic of Estonia Ministry of Economic Affairs and Communication. (2019, September 05). Cybersecurity Strategy Republic of Estonia. Tallinn.

Rosamond, B. (2015). Research Methods in European Union Studies. In K. Lynggaard, K. Löfgren, & I. Manners, *Research Methods in* (pp. 18-36). London: palgrave Macmillan.

Schengen Visa Info. (2019, October 1). *Schengen Agreement*. Retrieved from schengenvisainfo.com: https://www.schengenvisainfo.com/schengen-agreement/

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge : Cambridge University Press.

Schünemann, W. J. (2017, September). *Supranational norm entrepreneurship or uploading of high standards: the case of the European data protection regulation and the role of the European Parliament*. Retrieved from European Consortium for Political Research (ECPR) : https://ecpr.eu/Filestore/PaperProposal/94aab165-09ee-4f99-bc1e-ff6df6056d67.pdf

Sivan-Sevilla, I. (2020, Juli 4). *Artificial Intelligence.* London: Combridge University Press. Retrieved from Commissionand its priorties: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

Statista. (2020, January). *www.statista.com*. Retrieved from www.statista.com: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/

TEU. (1992, February 7). *Treaty on european union.* Retrieved from https://europa.eu/: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf

TFEU. (2007, December 13). *Treaty of Lisbon*. Retrieved from https://eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12007L%2FTXT

The European Parlement. (2019, 11). *The Maastricht and Amsterdam Treaties*. Retrieved from europarl.europa.eu: https://www.europarl.europa.eu/factsheets/en/sheet/3/the-maastricht-and-amsterdam-treaties

The Federal Government of Germany. (2016, November 07). *Cyber Security Strategy for Germany 2016.* Retrieved from ENISA: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

The JHA Council. (1995, July 26). *COUNCIL ACT of 26 July 1995*. Retrieved from drawing up the Convention based on Article K.3 of the Treaty on European Union, on the: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995F1127(01)&from=ES

ToA. (1997, November 10). *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed at Amsterdam,*. Retrieved from eur-lex.europa.eu: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_of_amsterdam_en.pdf

Valls, M. (2015, October 10). *French national digital security strategy.* Retrieved from Manuel Valls: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Vink, M., & Graziano, P. (2013, Januar). *Europeanization: Concept, Theory, and Methods.* Retrieved from Researchgate: https://www.researchgate.net/publication/303484310_Europeanization_Concept_Theory_and_Methods

Wach, K. (2015). *Conceptualizing Europeanization: Theoretical Approaches and Research Designs.* Kraków: Cracow University of Economics.

Wu, C. (2004). An Overview of the Research and Development of Information Warfare in China. In E. Halpin, P. Trevorrow, D. Webb, & S. Wright, *Cyberwar, Netwar and the Revolution in Military Affairs* (pp. 173-195). Hampshire: Palgrave MacMillan .