The ‘Soft’ Europeanization of EU Member States Cybersecurity Strategies

von der Brelie, Fee-Marie

Universiteit Leiden

The 'Soft' Europeanization of EU Member States Cybersecurity Strategies

MA International Relations, Global Conflict in the Modern Era

Supervisor: *Dr. L.* ***Milevski***

Student: *Fee-Marie* ***von der Brelie***

26 January 2023

Master Thesis

Word Count: 14 998

Declaration of originality

By submitting this assignment, I certify that:

✓ this work has been drafted by me without any assistance from others (not applicable to group work);

✓ I have not copied submitted work from other students

✓ I have not used sources that are not allowed by the course instructors, and I have clearly referenced all sources (either from a printed source, internet or any other source) used in the work in accordance with the course requirements and the indications of the course instructors;

✓ this work has not been previously used for other courses in the programme or for course of another programme or university unless explicitly allowed by the course instructors.

I understand that any false claim in respect to this work will result in disciplinary action in accordance with university regulations and the programme regulations, and that any false claim will be reported to the Board of Examiners. Disciplinary measures can result in exclusion from the course and/or the programme.

I understand that my work may be checked for plagiarism, by the use of plagiarism detection software as well as through other measures taken by the university to prevent and check on fraud and plagiarism.

I understand and endorse the significance of the prevention of fraud and I acknowledge that in case of (gross) fraud the Board of Examiners could declare the examination invalid, which may have consequences for all students.

Name: Fee-Marie von der Brelie 

Date: 26 January 2023

Abstract

Disruptions to the routine operations of ICTs in conflict situations have made cybersecurity come to ascend a prominent position in the legal and political decision-makeing of the EU. Europeanization has been used to describe the processes by which EU decision-makeing manifests itself in the logic of, for example, national policy outcomes of those processes (see Radaelli, 2012, p. 1 as cited by Fererro & Ackrill, 2016, p.880). The literature has pointed to the significant amount of soft law which the EU has issued to regulate cybersecurity. However, per definition EU member states are not legally obliged to implement soft law. Accordingly, by utilizing Europeanization as a conceptual frame, this thesis has sought to answer the question: *To what extent has non-legally binding EU soft law on cybersecurity influenced the making of the national cybersecurity policies of its MS over time*? To address the research, question the thesis has taken a small-scale empirical mixed-method approach by analyzing the extent to which specifically, Germany's and Slovakia's national cybersecurity strategies have harmonized over time toward the 2020 EU cybersecurity strategy (EUCSS) as a consequence of using the soft law document in their stagey-making. The analysis suggest that the EU cybersecurity strategy did influence the national strategy-making, but that the degree of harmonization depended on the extent to which the EUCSS aligned with national ambitions and priorities.

Key Words: European Union; Member States; Europeanization; Soft Law; Cybersecurity; Harmonization

Table of Contents

List of Figures

List of Abbreviations and Acronyms

BKA	German Federal Criminal Police Office
BSI	German Federal Office for Information Security
CSU/CSU	German Christian Democratic Party
CEE	Central Eastern European
dpa	German Press-Agency
Cybersecurity Act	Regulation on ENISA & ICT cybersecurity certification
DDoS	Distributed denial of service
ENISA	European Network and Information Security Agency
EU	European Union
EUCSS	Cybersecurity Strategy of the European Union
ICT	Information and Communications Technology
MS	Member State
NATO	North Atlantic Treaty Organization
NBU	Slovakian National Security Authority
NCSS	National Cyber Security Strategy
NIS Directive	Network and Information Security Directive
OL'aNO	Slovak Ordinary People and Independent Personalities Party
OSCE	Organization for Security and Co-operation in Europe
RAN	Radio Access Network
SMER-SD	Slovakian Social Democrat Party
SPD	German Social Democratic Party
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations

Introduction

In a world that is becoming increasingly dependent on the routine operations and developments of information and communication technologies (ICTs) and services, fast-evolving and complex cyber incidents have come to present a challenging security concern. Distributed denial-of-service (DDoS) attacks, data theft, and cyber extortion, to name a few, have become an undeniable daily reality of ICT users and, as the recent Russia-Ukraine conflict demonstrates, are an integral part of geopolitical conflicts. Consequently, it is no surprise that cybersecurity has become an issue of strategic importance for many countries. In Europe, high-profile cases such as the cyber-attacks against European Union (EU) member state (MS) Estonia in 2007 (Davis, 2007) or EU institutions (EMA, 2020) had far-reaching financial, societal, and political consequences. As such, it is no surprise that over the past years, cybersecurity has quickly come to ascend a prominent position also in the legal and political decision-making of the EU.

That said, scholars have commonly used the term *'Europeanization'* to describe both the *processes* by which EU decision-making manifests itself in the logic of, for example, national discourse, identities, and behavior and the policy *outcomes* of those processes (see Radaelli, 2012, p. 1 as cited by Fererro & Ackrill, 2016, p.880). In this respect, Europeanization has served as a useful concept in International Relations (IR) studies to refer to the impacts of (potential) EU membership on the political behavior of MS or candidate countries. For example, in the context of cybersecurity, prevalent research has extensively focused on Europeanization by examining the transmission, adoption, implementation, and compliance of MS, neighboring countries, or the private sector with EU hard law, like the 2016 Directive on security of network and information systems (the NIS Directive), the 2019 Regulation on the European Union Agency for Cybersecurity (ENISA) or Regulation 2019/881, the Cybersecurity Act (Ripoll Servent, 2017; Cantero Gamito, 2018; Sivan-Sevilla, 2021).

However, thus far, scholars have failed to acknowledge that next to hard law, the EU has heavily relied on *soft law* instruments as alternative decision-making tools to influence MS domestic political behavior and regulate cybersecurity. In fact, over the past two decades, the EU has produced more soft law to address the issues arising from private and public information and communications technology (ICTs) than hard rules (see Saurugger & Terpan, 2019, p. 15). In essence, soft law may be understood as rules of conduct which (1) are laid down in non-legally binding, non-obligatory instruments; (2) are articulated and adopted

outside the margins of common legislative processes and jurisdictional control, (3) have no (direct) legal effects but nonetheless are aimed at and may produce practical effects (Snyder, 1994, p.198; Senden. 2004, p.112). The lack of soft laws' legal bindingness raises a question which so far has been overlooked by Europeanization scholars and, thus, this thesis aims to answer, namely: *To what extent has non-legally binding EU soft law on cybersecurity influenced the making of the national cybersecurity policies of its MS over time?*

In light of the importance of soft law as an EU decision-making tool in the cybersecurity policy domain, the aim is to analyze the extent to which national cybersecurity strategies (NCSS) have been Europeanized. The thesis will address the research question by taking a small-scale empirical approach. Firstly, since the *harmonization* of national and EU policies are a potential consequence of Europeanization (e.g., Radaelli, 2003, p.36) the thesis will quantitatively measure the extent to which specifically Germany's and Slovakia's NCSSs - which form an integral part of their national cybersecurity policy - have become more similar over time to the recent main EU cybersecurity soft law instrument, namely the 2020 EU Cybersecurity Strategy (EUCSS) and to each other. Secondly, it will investigate whether the results on the extent of harmonization are indeed soft law induced by utilizing qualitative method 'process tracing.' In particular, it will trace Germany's and Slovakia's national policymaking processes utilizing interviews conducted with three national policy-makers, national and EU cyber-security policy documents, and media reports that address either EU or MS-specific political developments. This way the thesis will provide insights into Europeanization through soft law, in terms of both outcomes and processes (Radaelli, 2003, p. 30)

The empirical focus of this thesis on the case of Germany and Slovakia and their NCSS, as a representative example of EU MS and their cybersecurity policies, is based on several interrelated premises which will be elaborated in more detail below: Firstly, despite small-scale, the selection of Germany constitutes a representative example of a 'newer', i.e., post-1995 (Slovakia) and an 'older' MS (Germany), a 'western' and 'eastern' MS. Moreover, the countries differ in their political systems and in their understanding of cybersecurity. These distinctions matter since they not only allow to disaggregate the data (e.g., by country or length of EU membership) but can also make for explanatory factors for the extent to which and how the ECSS may affect their NCSSs. In other words, they can offer potential explanations as to why EU cybersecurity soft law can affect MS cybersecurity policymaking in either similar or different ways.

Overall, such an exploratory inquiry into the extent of EU soft law-driven

Europeanization, specifically in the policy field of cybersecurity, is of particular importance as it will contribute to three main bodies of literature Europeanization, soft law, and cybersecurity. Whereas the first two are concerned, the thesis will add to the current explanations as to when, how, and to what extent Europeanization affects MS political behavior by looking for evidence about how soft law, despite its lack of legal bindingness, functions as an alternative channel that can facilitate Europeanization. Moreover, by utilizing a mixed-method, the thesis makes an important contribution to the plethora of literature that is concerned with the measurement of Europeanization (e.g., Ladrech, 2002; Exadaktylos & Radaelli 2009; Bache & Jordan, 2006; Töller, 2010). Where cybersecurity is concerned, it should be stressed that one of the EU's goals has been to align member states' approaches to cybersecurity (Helmbrecht et al., 2014). This is because fragmented approaches to cybersecurity in the EU are unlikely to be effective due to the cross-border nature of cyber and related threats. By seeking evidence of change and harmonization of national cybersecurity policy because of Europeanization, the thesis will make it possible to assess whether and EU achieved this goal and how soft law may have contributed to it.

The thesis proceeds as follows: The first chapter sets the scene, introducing cybersecurity as a new policy field and outlining relevant literature on its regulation on the EU level through soft law. It will introduce Europeanization as an illustrative framework through which it is possible to make sense of the influence of this alternative decision-making on the MS level, specifically when it comes to their national cybersecurity policymaking. Further, a methodological approach to analyze specifically the extent of Europeanization of Germany's and Slovakia's NCSS through the EU soft law instrument, the EUCSS, both in terms of process and outcomes, will be introduced. Chapters two and three present, respectively, the quantitative and qualitative analysis's empirical findings. The thesis concludes by discussing the findings and their implications in light of the theoretical expectations and suggesting future research directions.

Chapter 1: From Soft Regulation to Soft Europeanization

To fully explore the extent to which the EU soft law approach to regulate cybersecurity has influenced the (making of) cybersecurity policies of its MS requires robustness in terms of conceptual and theoretical underpinnings and clarity on previous research. This chapter will provide precisely that. It is divided into two parts and proceeds as follows: The first section provides a literature review of the specific policy field addressed here, i.e., cybersecurity, and elaborates on how the EU cybersecurity decision-making, specifically through soft law instruments, are positioned within it. Fuhrer it will introduce and reflect on the academic literature on Europeanization as an illustrative conceptual framework through which it is possible to assess the influence of EU soft law on MS cybersecurity policymaking. The second section will lay out the methodology through which the extent of Europeanization of Germany's and Slovakia's NCSS through EU soft law may be assessed.

1.1 Literature Review

1.1.1 EU's 'soft' regulatory approach to cybersecurity

Over the past decades, cyberspace, related ICTs, networks, and the world wide web have become of growing importance and brought many benefits to all social, political, and economic players. However, as geopoliticals conflicts, like Russia's recent invasion of Ukraine, demonstrate, they have also brought many different, and continuously progressing cyber threats and risks. The importance of cybersecurity in conflict situations has made cybersecurity a prominent point on many countries and organizations political and legal agendas, including the EU.

Early accounts of EU cybersecurity date back to the early 1980s (Carrapico & Farrand, 2020, p.1114). However, at that point, 'cybersecurity' mainly consisted of economic ad hoc mechanisms evoked by the EU to protect the internal market in the context of emerging ICTs (p. 1114). However, as the DDoS attacks against Estonia's public and private networks and systems in 2007 made clear, cybersecurity extends the realm of the internal market. Thus, today, the EU's conceptions of *cybersecurity* extend the internal market. It more widely signifies *"[...] the* ***protection of information, information systems****, infrastructure and the* ***applications*** *that run on top of it* ***from those threats that are associated with a globally***

connected environment."[1] (Helmbrecht et al., 2012, p. 13). These days cybersecurity is its own fully realized policy domain with a distinguished internal rationale, agenda, regulatory and institutional framework, and an impact on most other EU policy areas (Carrapico & Farrand, 2020, pp.1114-1116).

Moreover, over the years, there has been a general recognition that cyber threats are a cross-border phenomenon and are becoming more diverse in terms of actors and objectives. Hence, the EU quickly recognized that individual approaches to cybersecurity by MS are unlikely to be effective (Christou, 2016; Coman, 2017; Odermatt, 2018). Unsurprisingly, scholars have noted that a characteristic ambition of the EU in their development of cybersecurity as a policy field has been the continuous emphasis on the need to establish a unifying basis for common action (Carrapico & Barrinha, 2017, 2018; Odermatt, 2018; Wessel, 2015, 2021). As former executive director of the European Network and Information Security Agency (ENISA), Professor Udo Hambrecht and his colleagues (2012) stress: *"A truly* ***effective approach*** […] *will* ***require close collaboration*** […] ***and a corresponding alignment of approaches. […]*** *This is* ***not the case at the present time*** *[…]"*[2] (pp. 12-13). In this context, studies have pointed to the significant amount of different legally binding and non-legally binding rules, i.e., *hard and soft laws* that the EU has produced over the years to achieve this goal and to address and mitigate cybersecurity threats effectively (van der Meulen et al., 2015; Wessel, 2015, 2019, 2021).

Specifically, the establishment of *hard laws* in this respect is particularly intriguing since the legal and security responsibilities and competencies for this policy area do not remain within the jurisdiction of the EU. Put differently, since neither the Treaty of the European Union (TEU) nor the Treaty on the Function of the European Union (TFEU) mention cybersecurity as a policy field, there is, strictly speaking, no explicit and unifying legal basis for the EU to provide hard regulation on cybersecurity (Bendiek & Pander Maat, 2019, p.4; Wessel, 2021, p. 497). Rather, as cybersecurity is part of national security, MS possess the competencies to define cyber offenses, initiate law enforcement operations, and punish offenders. The EU merely holds a coordinating role for this policy field (Bendiek, 2012, p. 12). The lack of a unifying legal basis has forced the EU to formulate and justify its hard regulatory approaches to cybersecurity by linking them to policy fields that can be affected by cyber threats and for which the EU has competencies. In the past, this has primarily been the internal

[1] emphasis added
[2] emphasis added

market (Odermatt, 2018).

Scholars have noted that where the Union has not been able to connect cybersecurity issues with existing EU competencies, it has commonly pursued *soft law* measures (Wessel, 2015, p. 425; 2019, p.285; Odermatt, 2018). In essence, *soft law* refers to ***"…rules of conduct*** *that are laid down in instruments which have* ***not been attributed legally binding force*** *as such, but nevertheless* ***may have certain (indirect) legal effects,*** *and that are* ***aimed at and may produce practical effects."*** [3](Senden, 2004, p.112). Soft law is comparatively easy to enact since it does not involve the difficulties and challenges which are usually involved in the EU's formal decision-making process (Slominski & Trauner, 2020, p.98). Its unbinding nature makes its adoption by the EU and MS much easier and faster. Moreover, in principle, it is exempt from strict legal protection and scrutiny (Consolidated version of the TFEU, 2012, Article 263; Article 265; Article 26). Accordingly, soft law is deemed particularly suitable to deal with rapidly evolving policy areas like cybersecurity (Terpan, 2015; Andone & Coman-Kund, 2022).

As Saurugger and Terpan (2019) have shown, even though the utilization of hard law to regulate cybersecurity has increased, over the last years, the employment of soft law has constituted the largest portion of EU activity in the cybersecurity policy domain (p. 15). The most prominent soft law documents that the EU has issued in the cybersecurity policy domain are the various Commission communications. The latter commonly fulfill either an informative, interpretative, decisional, or steering function (see Senden, 2004, p.123). Important Commission communications are the "EU Cybersecurity Strategys" (EUCSS). Due to the ever-changing cyber domain, the EU has already published three EUCSSs, its latest one in 2020. EUCSSs are particularly important EU soft law instruments since they set out and clarify the general EU principles and objectives and intend to guide national cybersecurity policymaking.

Despite the prominence of soft law in EU cybersecurity regulation, considering the absence of legal bindingness, one still might be inclined to believe that the significance of such instruments must be rather limited: How can these instruments possibly influence MS in such a way that they contribute to common action and the alignment of MS cybersecurity approaches? To answer this question, it is useful to turn to the research on Europeanization. Over the past three decades, the latter has brought forward significant evidence of the different (indirect) legal and practical effects that EU soft law can have on MS level.

[3] emphasis added

1.1.2 'Soft' Europeanization

While emerging in the 1970s, only in the early 2000s, academic attention on Europeanization has come to the fore. As a comparatively young concept, to this day, no scientifically stringent definition or single theoretical approach or methodology of Europeanisation can be found in the literature (Dyson, 2002, p. 3). A common opinion, however, is that Europeanization can be used to understand the influence and effect of EU integration, enlargement, and decision-making on MS, neighboring countries, candidate states, and private actors.

Early works like the one from Heritier et al. (2001) defined *Europeanization* as *"the process of influence deriving from European decisions and impacting member states' policies and political and administrative structures"* (p.3). Similarly, Börzel (2002) defines it simply as a *"process whereby domestic policy areas become increasingly subject to European policy making"* (p.6). The main problem with these definitions is that they facilitate a rather simplistic view of Europeanization. By viewing Europeanization solely as a process through which EU integration, enlargement, and decision-making penetrates and, under certain circumstances, brings about adjustment and change of polities, politics, and policies at the domestic level, they portray Europeanization merely as a one-way street. Moreover, these definitions make it easy to confuse Europeanization with the sources of domestic change - EU integration, enlargement, and decision-making.

Addressing these criticisms, Radaelli (2003) has provided a more comprehensive view of Europeanization and thus provides a definition of Europeanization that this thesis will adopt. Drawing on Ladrech (1994), for Radaelli (2003), Europeanization signifies a ***"processes of (a) construction (b) diffusion and (c) institutionalization of formal and informal rules,*** *procedures, policy paradigms, styles, "ways of doing things" and shared beliefs and norms which are* ***first defined and consolidated in the making of EU decisions*** *and* ***then incorporated in the logic of domestic discourse, identities, political structures and public policies****"* and which „***can be more or less incremental"*** (p. 30). In contrast to earlier definitions, for Radaelli (2012, p. 1), Europeanization does not only signify one process but multiple processes as well as the outcomes of these processes. For example, Radaelli (2003) recognizes that Europeanization processes can have consequences for national politics, policies, and, or polities, such as their potential *convergence* or *harmonization* (p.36). However, he also recognized that this does not always have to be the case (p.33). Europeanization can also produce *divergence, convergence limited to a country,* or lead to

diversity, intense competition, or *distortions of competitions* (Héritier & Knill, 2001; Montpetit, 2000).

Radaelli's (2003) definition helps to move past the simplistic view of Europeanization and the plethora of studies that have conceptualized Europeanization as mere one-way, *vertical top-down processes* where Europeanization simply happens to countries due to pressures from the EU level (see next to Ladrech, 1994; Heritier et al. 2001; Boerzel, 2002 also Schmidt, 2009). By considering the making of EU decisions in his definition, he reflects upon the complexities of the EU and its decision-making process and acknowledges the multiple roles MS can have within them. He specifically argues that in practice, Europeanization describes as much vertical, top-down as it describes *bottom-up, horizontal processes:* On the one hand, EU policies and laws are being adopted and essentially *'downloaded'* by MS into their domestic structures (vertical, top-down). On the other hand, MS participate in the EU policy and law-making, interact with each other, and *'upload'* their ideas to the EU level (bottom-up, horizontal) (Radaelli, 2004). Thus, Europeanization has to be seen as a complex, more circular process that is happening in multiple directions (see Figure 1).

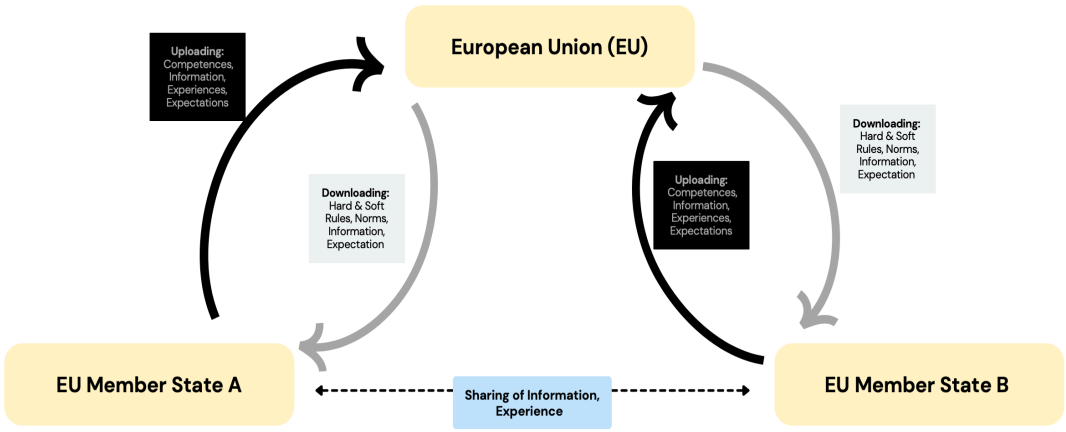

Figure 1: Europeanization as complex, circular process (derived from Graziano & Vink, 2013, p.47).

Over the years, scholars have produced a wide variety of research on the different individual mechanisms that may facilitate Europeanization processes and the outcomes thereof. For example, Olsen (1996), argued that Europeanization is facilitated through *"the objective characteristics of the contemporary context, in history, and in the purposes, reason and power of identifiable political agents"* (p.248). In contrast, Börzel (1999) and Cowles et al. (2001) argued that Europeanization depends on the degree of institutional compatibility between domestic and European processes, policies, and institutions, i.e., the goodness of fit. Börzel and Risse (2003) explain: *"The bigger the fit between European and domestic processes,*

policies, and institutions, the lower the adaptational pressure" (p.61). For Knill and Lehmkuhl (2002), Europeanization is the result of *"institutional compliance, changing domestic opportunity structures, and framing domestic beliefs and expectations"* (p. 256).

Radaelli (2003) differentiates between *vertical and horizontal mechanisms* of Europeanization (pp.40-44). Vertical mechanisms of Europeanization involve pressure to conform with EU decisions. In contrast, horizontal mechanisms involve the absence of such adaptational pressures and are instead, for example, induced by the internal market or the diffusion of ideas and discourses about the notion of good policy and best practice (p.41). Radaelli (2003) recognizes that commonly adaptational "pressure implies coercion," and the latter is typically based on hard law such as directives or decisions. Conversely, horizontal mechanisms of Europeanization are based on *"soft framing mechanisms"* (pp.42-43). In this context, Radaelli (2003) specifically emphasized the role of the Open Method of Coordination (OMC) which has been intrinsic to the development of various policies on the EU and MS level (p.43). The OMC is an EU-specific governance architecture based on soft law instruments and the social exchange of ideas (Tholoniat, 2010).

Since Radaelli's (2003) argumentation for soft law as potential instruments of Europeanization, much research has been conducted on how they may contribute to Europeanization in the form of policy reforms and changes in MS. Europeanization scholars have predominantly identified four distinct soft law instrument-induced mechanisms that can help explain Europeanization. For example, soft law can facilitate *'discursive transformations'* that stimulate policy change (Trubek & Trubek, 2005, p. 92). Soft law frames, for example, objectives, instruments, frameworks, benchmarks, or introduce EU-level concepts (Radaelli, 2003, p. 43; López-Santana, 2006). Due to the instruments' interpretative, explanatory, and steering character, they are adapted by domestic policymakers and consequently may cause a policy shift. In addition, research has found that by opening the decision-making process also to non-state actors, EU soft law instruments and architectures like the OMC can enhance democratic participation and accountability (Zeitlin, 2005). In turn, they facilitate information exchange, networking, or dialogue between different stakeholders, contribute to the *learning* about desirable policies and thus indirectly cause potential (re)formulation of national policy (Checkel, 2001; Scott, 2011; Polak, 2015). Moreover, by setting out behavioral norms, soft law generates feelings that a rule, either politically, socially, or morally ought to be obeyed (Stefan et al., 2018, p.26). In turn, these feelings may lead to *'naming and shaming'* and *'peer pressure'* towards national-policy makers who are underperforming with regard to the non-binding rules (Hodson, 2004). Consequently, national policymakers pursue the policy change according to

EU soft law to avoid 'naming and shaming' and 'peer pressure' (Trubek & Trubek, 2005; Heidenreich & Bischoff, 2008; Stefan et al., 2019).

In sum, Europeanization literature shows that Europeanization processes and outcomes can as much be the result of the objective characteristics of the contemporary context or history, good reasons, and power by the EU (Olsen, 1996); the degree of misfit between EU and MS policies (Börzel, 1999; Cowles et al., 2001; Börzel & Risse, 2003) or the institutional compliance, changing domestic opportunity structures (Knill & Lehmkuhl, 2002) as it can be the result of soft law. What follows from this is that while soft law may be only one explanation for Europeanization, Europeanization makes for an illustrative framework through which it is possible to assess the influence of EU soft law on domestic cybersecurity policymaking. That said, while research has been conducted on the Europeanization facilitated through soft law in various policy fields (e.g., López-Santana, 2007; Brooks, 2012; Ferrero & Ackrill, 2016), there are merely a few studies on Europeanization through soft law in the cybersecurity policy domain. This is particularly concerning considering the importance of soft law for the EU regulation of the cybersecurity domain and, by extent, for the EU's objective to align cybersecurity approaches. Thus, to address this gap and get an insight into the influence of EU's non-legally binding soft law on MS cybersecurity policy, this thesis will assess the extent to which EU soft law has led to Europeanization processes that are, for example, reflected in the harmonization of MS cybersecurity policymaking.

1.2 Methodology: Measuring Soft Europeanization

Whether Europeanization is considered a vertical top-down or horizontal bottom-up processes or facilitated by hard or soft law, scholars who want to determine the extent of Europeanization are confronted with multiple questions: How is it possible to assess if, when, and how much Europeanization has happened, and what exactly is affected by Europeanization? (Ferrero & Ackrill, 2016, p. 881; López-Santana, 2007, p.4). Since the prerequisites for implementation and reform are not required for soft law, their influence cannot be measured as easily (López-Santana, 2007). While, due to the breadth of the concept, there is no widespread consensus on how to operationalize or measure Europeanization, there are some recognizable trends to which this thesis connects.

For instance, Europeanization literature has commonly operationalized and measured the extent of Europeanization by qualitatively analyzing the extent to which national politics, policies, or polities have harmonized over time utilizing specific case studies (e.g., Falkner et

al., 2005; Ackrill & Ferrero, 2016). Thereby harmonization is understood as *"the regulatory requirements or governmental policies of different jurisdictions"* becoming *"more identical or at least more similar"* over time (Majone, 2014, p.4). Moreover, while the importance of developing quantitative approaches to measure Europeanization has been acknowledged, they are rare since research commonly must rely on text-based sources without spoiling their essence and meaning (Töller, 2010; Ferrero & Ackrill, 2016). Moreover, quantitative approaches are usually avoided because they only allow to evaluate Europeanization as a dichotomous outcome (i.e., harmonization of policy content occurs/does not occur). Thus, alone they do not allow to provide useful insights into the different shades and modes of the Europeanization processes and its outcomes (López-Santana, 2007).

To address these difficulties and contribute to Europeanization research, this thesis suggests a mixed-method approach and a small-empirical case design to gain insight into the extent of Europeanization of MS cybersecurity policymaking, through EU soft law. Specifically, to answer the question to which extent the EU soft law approach to regulate cybersecurity has influenced the cybersecurity policymaking of its MS, the thesis will quantitatively and qualitatively assess the extent to which Germany's and Slovakia's NCSS have Europeanized through the non-binding 2020 EUCSS.

1.2.1 Overview of Case Selection

The empirical focus of this thesis is put on the 2020 EUCSS as a potential soft law instrument that may have Europeanized national cybersecurity policymaking because it is currently the main soft law instrument that the EU has published in the cyber security policy area. By setting out the EU objectives when it comes to cybersecurity, it builds a reference for all other EU cybersecurity soft law instruments. Moreover, aiming to guide national cybersecurity policymaking, its prime intention is to deliver policy change at the MS level. Similarly, the empirical focus on NCSSs, are justified through the fact that NCSSs are an important part of MS national cybersecurity policy. They provide a key framework to meet a nation's basic cybersecurity needs and concerns and elaborate on ways to address these. In this way, they set the benchmark for all other policies in the domain. Thus, if indicators for Europeanization of NCSS can be found, other policies in the domain will likely show signs of Europeanization as well.

That said, the specific selection of Germany and Slovakia and their NCSS as representative examples is based on three interrelated premises: First, despite small-scale,

Germany's and Slovakia's selection constitutes a representative example of a 'newer', i.e., post-1995 and ‘eastern’(Slovakia) and an 'older', ‘western’ MS (Germany) EU MS. Research has found, that until today the conditions EU membership have created an impetus for new MS like Slovakia to 'catch-up' with the old. Thus, their approach to EU specific political, economic, and legal decisions is, compared to old MS, often characterized by compliance and rapid domestic political changes (Toshkov, 2012). Second, the MS differ in their political systems. Whereas Germany has a federal- Slovakia has a unitary political system. This affects their policymaking process. While in a unitary system, the power to make authoritative decisions is located at the central government level, in a federally structured political systems the power to make authoritative decisions is shared between the federal and constituent state levels. As a result, political decision- and policymaking are said to be more difficult and slower than in a unitary system (Kaiser et al., 2012, p.1). Third, the MS have different understandings of cybersecurity: Slovakia highlight the provision, availability, integrity, and confidentiality of information in the widest sense, not just mere information stored in cyberspace (Hriciková & Kaska, 2015; Tumkevič, 2017). In contrast, Germany understands cybersecurity more as protecting, maintaining, and restoring ICT devices, services, systems, and networks. While this also includes the information stored within these systems and networks, it is not Germany's prime focus (Cymutta, 2015).

The differences in their length of EU membership, their political systems, and their understanding of cybersecurity affect the approach that the MS take in their NCSSs. Thus, they are potential explanatory factors for the extent to which and how the ECSS may affect (i.e., Europeanized) their NCSSs. Put differently, they can offer potential explanations as to why EU cybersecurity soft law can affect MS cybersecurity policymaking in either similar or different ways.

1.2.2 Data Set and Research Design

To answer to what extent the Unions soft law approach to regulate cybersecurity has influenced MS cybersecurity policymaking, the thesis will assess the extent to which Germany's and Slovakia's NCSS have Europeanized through the non-binding 2020 EUCSS. To this end, Europeanization is operationalized and measured as harmonization since the main goal of the EU in the cybersecurity domain has been the 'alignment' of approaches (Helmbrecht et al., 2012).

The thesis utilized a mixed method approach. Firstly, it will determine the extent of harmonization by assessing the quantitative extent to which Germany's and Slovakia's NCSS have changed to adapt the key components identified in the main EU cybersecurity soft law document, the 2020 EUCSS. Accordingly, it will employ a primary data set namely, Germany's and Slovakia's current and former NCSSs, issued respectively in 2016 and 2015, and in 2021 and the current EUCSS issued in 2020. The NCSSs were retrieved from the official ENISA website, which provides the full text of all existing EU MS NCSSs. The EUCSS was retrieved from EUR-lex, the official website of EU law, and other EU public documents. The documents share a similar length, have been published in English, thus, ensuring a coherent and systemic analysis. To perform the quantitative analysis, first, the "Evaluation Framework for NCSS" proposed by ENISA (2014) has been utilized to identify key components, covering the strategies suggested (1) objectives, (2) action points, (3) inputs, (4) direct outputs, (5) long-term outcomes & impact, (6) evaluation processes which (see ANNEX 2). In a next step, itwas quantitatively assessed how many key components of the EUCSS are also present in the respective NCSSs, as well as the extent to which key components of the German NCSSs are also present in the ones from Slovakia. This is done through the application of a binary score – one if a key component is present, zero if not. To avoid potential subjective evaluations, no range of zero to one was adopted (Giner, 1995). Values were obtained for each key component, then aggregated and converted to an overall percentage for each NCSS. This way, it is possible to determine an in- or decrease in similarity and thus to make a statement about the extent of harmonization not only between the national policies and the EU soft law instrument but also solely between national policies.

By quantitatively determining the extent of harmonization, this thesis makes an important contribution to the Europeanization literature, which usually avoids such approaches. As indicated above, such a quantitative analysis only allows to make a claim about the extent of Europeanization of NCSSs. It does, however, not provide sufficient insight to the question to what extent the non-binding EUCSS played a role in the (potential) Europeanization of the NCSS. Hence, to get an insight into the latter, the thesis will secondly utilize the qualitative method 'process tracing .'Process tracing *"attempts to identify the intervening [...] causal mechanism between an independent variable [...] and the outcome of the dependent variable"* (George & Bennett, 2005, p. 206). In the case at hand, the dependent variable is Germany's and Slovakia's recent NCSS, and the independent variable is the EUCSS. For the process tracing, a *'bottom-up'* approach which starts and ends on the national level and surveys *"if, when, and how the EU provides a change"* is used. Usually, with a bottom-up approach, the analysis

considers the policy systems at hand, so the *"actors, ideas, problems, rules styles and outcomes at the domestic level [...]"* and "*then it process-traces the system over the years"* (Radaelli & Pasquier, 2007, p. 41). Thus, the bottom-up approach uses temporal sequences as starting points to identify turning points and critical moments in national policymaking. The thesis will investigate the period from January 2020 to December 2021 and trace whether and how EUCSS played a role in Germany's and Slovakia's recent NCSS-making. This way it is traced whether the extent of harmonization between the MS NCSS and between the latter and the EUCSS are indeed 'EUCSS-induced' or caused at the national level (Radaelli, 2004, p. 4; Exadaktylos & Radaelli, 2009, p. 510). Accordingly, it is ensured that also factors other than the EU soft law instrument are considered as explanations for possible harmonization of the NCSS.

To conduct the process tracing, the thesis will utilize a set of primary sources namely: Germany's and Slovakia's previous and recent NCSS and other national policies, EU legal measures and policies, media reports retrieved from the official websites and data established from semi-structured interviews which have been conducted between April 2022 and September 2022 with two German national cybersecurity policymakers and one Slovakian national cybersecurity policymaker. The interview questions have been established by employing the interview template provided by Eliantonio et al. (2021, p.12-14), which conducted a similar research on the utilization of EU soft law in MS and the effects thereof (ANNEX 1). A semi-structured approach has been used to cover all relevant themes while giving interviewees the space to further expand on topics that they consider relevant. Most interviews were held online due to geographical restrictions, through the platforms Zoom and Webex, and lasted between 30 and 60 min. With the prior consent of the participants all interviews were recorded and then directly transcribed. The recordings were then immediately deleted to avoid unnecessary storage of sensitive data. While making the transcripts, any information that could reveal the identity of the participants was anonymized.

The interviews, and the other primary sources, will be coded following Moumoutzis and Zartaloudis (2015, pp.346-348). They argue that to 'process trace' a national policymaking process, scholars must focus on three dimensions: First, *how the national-policy makers have defined cybersecurity policy problems and objectives*. Thereby, in the analysis attention is being put on explanations that suggest distinct EUCSS-induced causal mechanisms that can help explain Europeanization, such as discursive transformations, learning, peer pressure, or naming and shaming (p.347). Second, it will be identified *whether alternative courses of actions to the ones proposed by the EU in their EUCSS have been considered by the national policymakers* (p.347). Thirdly, it is established *whether there is evidence that policymakers*

calculated the cost and benefits of the alternatives and if so, the type of costs and benefits that they calculated (p.348).

Chapter 2: Outcomes of 'Soft' Europeanization: Quantitative Analysis of the Extent of Harmonization between Germany's and Slovakia's NCSS and the EUCSS

The following chapter presents the quantitative findings on the extent of harmonization between the German and Slovakian NCSS and the current EUCSS over time, as well as the harmonization between the MS NCSS. This is done to provide an insight into the *outcome* of Europeanization; that is, the extent of Europeanization of Germany's and Slovakia's NCSS through EU soft law, like the EUCSS 2020. Overall, by utilizing ENISA's Evaluation Framework (2014), a total of 344 key components were identified and quantitatively compared between the 2020 EUCSS (nEU20=65) and Germany's (nGER16=63; nGER21=83) as well as Slovakia's (nSLO15=60; nSLO21=73) former and recent NCSS. The chapter is divided into five sections. The first section presents the findings on the general extent of similarity between the NCSS and between the NCSS and the EUCSS over time. To contextualize these general findings further, the following three subsections elaborate on the extent of the quantitative harmonization first, between Slovakia's and the EU's CSS; second, between Germany's and the EU's CSS; and third, between Slovakia's and Germany's NCSS, by clustering the data according to key components covering respectively the strategies suggested (1) objectives, (2) action points, (3) inputs, (4) direct outputs, (5) long-term outcomes and impact, (6) evaluation processes. Finally, the chapter will draw a short conclusion on the extent of harmonization.

2.1 General Results

The quantitative analysis reveals evidence that Germany's and Slovakia's indeed adjusted their NCSS-making, with the key components suggested in their NCSS becoming more similar to the ones advocated in the 2020 EUCSS over time. While in 2015, Slovakia's NCSS only covered around 54% of the key components laid down in the 2020 EUCSS, in 2021, its NCSS shows similarity to around 69% of the key components suggested in the 2020 EUCSS. Likewise, Germany also adapted its NCSS to reflect more of the key components of the 2020 EUCSS. While in 2016, its NCSS included around 69% of the key components, in 2021, its NCSS incorporated around 77%. What is further striking is that even the NCSS published

before the 2020 EUCSS cover a significant amount of its suggested key components. This indicates that the MS early NCSS profoundly reflected what would later be picked up in the 2020 EUCSS.

In relation to the latter, specific attention should be, for example, given to Germany, whose 2016 NCSS already incorporated 69% of the key components, which later have been suggested in the 2020 EUCSS. Moreover, noticeably Germany's NCSSs were and have become more aligned with the 2020 EUCSS than those issued by Slovakia. However, compared to Germany's NCSSs, the Slovakian NCSSs show a larger alignment concerning the key components suggested in the 2020 EUCSS over time. Slovakia adjusted its 2021 NCSS to include 15% more key components identified in the EUCSS 2020 compared to the NCSS it published in 2015. Germany covered only 8% more key components proposed in the EUCSS 2020 in its NCSS 2021 than in its NCSS 2016. These findings indicate that an 'eastern' and 'new' MS, like Slovakia, whose former NCSS, in comparison, did not align much with the EUCSS, has responded with greater adjustments, resulting in a more considerable harmonization over time, compared to a 'west,' 'older' MS, like Germany, whose former NCSS did already greatly align with the key components suggested in the EUCSS.

Overall, this increase in similarity suggests harmonization towards the sixty-five key components of the 2020 EUCSS by the German and Slovakian NCSS. However, this result may be explained by the fact that half of the analyzed NCSSs were published before the 2020 EUCSS. Therefore, the similarity increase of the NCSSs with the 2020 EUCSS over time can be expected. However, the fact that quantitative evidence of harmonization also between Germany's and Slovakia's NCSSs challenges this argument: The quantitative analysis also reveals a reduction of deviating key components between Germany's and Slovakia's NCSS over time. Whereas in 2016, Germany's NCSS showed similarity to 68% of the key components suggested in Slovakia's 2015 NCSS, in 2021, the similarity between the MS NCSSs increased by about 10%. In 2021 Germany's NCSS changed to cover around 78% of the key components, which can also be found in Slovakia's 2021 NCSS.

Altogether, the general increase in similarity between Germany's and Slovakia's NCSSs with the 2020 EUCSS and the increase in similarity between the MS NCSS indicates harmonization of CSSs. To better understand these general results and test their robustness, and derive a potential explanation for them, the following sections will investigate the similarity between the NCSSs as well as the NCSSs and the 2020 EUCSS in more detail by clustering the data on key components, which cover respectively the strategies suggested (1)

objectives, (2) action points, (3) inputs, (4) outputs, (5) outcomes and impact, (6) evaluation processes.

2.1.1 Quantitative Harmonization between Slovakia's NCSS and the EUCSS over time

In its 2020 EUCSS, the Union presents a total of three *objectives*: First, to achieve resilience, technological sovereignty, and leadership. Second, to build operational capacity to prevent, deter and respond. Third, to advance a global and open cyberspace through increased cooperation. The quantitative analysis revealed that the objectives Slovakia presented in its 2015 NCSS were only similar to 67% of those in terms of their content. This changed in 2021 when its NCSS covered all the objectives presented in the EUCSS 2020. Being 100% consistent with proposed EUCSS objectives in 2021 resulted in an increase of similarity between the Slovakian NCSS with the EUCSS of 32%. The reason for this major shift can be explained by the fact that only in 2021 Slovakia started to fully consider 'resilience' and 'deterrence' in their strategic objectives.

A slightly different picture presents itself regarding the *action points.* In general, regardless if issued by the EU or the MS, most of the key components presented in the different CSSs covered action points. That said, the 2020 EUCSS advocates thirty-five action points. Most of them suggest to develop, reform, amend, implement or promote either EU or (inter)national standards, norms, legislation, or policies. This is, for example, the case concerning network and information security, the general cybersecurity of products and services of the internal market; crisis-, defense-, deterrence- or operative- management; cybercrime, and state behavior in cyberspace. While Slovakia's 2015 NCSS covers only 31% of the action points the Union suggested in 2020, in 2021, Slovakia's NCSS referred to 49%. This correlates to an 18% increase in similarity.

In total, the EU suggests nine different types of resources for implementing CSS (*inputs*). As expected from the action points laid out in EUCSS 2020, most of the inputs the Union suggested are legal or policy measures. Prominent are also process and coordination structures or organizational components. The inputs proposed in the Slovakian 2015 NCSS showed a similarity of 89% to those presented in the 2020 EUCSS. In 2021 Slovakia's NCSS, the inputs are identical to the ones suggested by the EU in 2020. This correlates to an increase in similarity of 11%.

In relation to the inputs, a total of five *output*s can be derived from the 2020 EUCSS: (1) improved regulatory frameworks; (2) improved capabilities; (3) an increase in (public-

private) partnerships, (4) more research and development; and (5) increased international cooperation. Even though it covers slightly different objectives, action points, and inputs, also Slovakia's 2015 NCSS covers all of these. Moreover, on top of the five outputs that can be derived from the 2020 EUCSS, Slovakia's 2015 NCSS also suggests 'warning systems and measures' aimed at stopping the escalation of crisis situations as outputs. While this changed in its 2021 NCSS, all the other outputs stressed by the EUCSS are covered. In short, in its 2015 and 2021 NCSS, Slovakia covered 100% of the outputs mentioned in the 2020 EUCSS. As elaborated in more detail below, Germany presents an almost identical case. The fact that the number of inputs and outputs is comparatively low suggests that the EU and its MS not only have a preferred but presumably also limited set of resources and means available to them to achieve their strategic objectives, which limits the type of outputs they achieve.

That said, twelve *outcomes and impacts* can be derived from the 2020 EUCSS strategy. The ones derived from Slovakia's 2015 NCSS show similarity to 67% of the latter. In contrast, the ones that can be derived from its 2021 NCSS resemble 92% of the outcomes and impacts that can be derived from the 2020 EUCSS. This resembles an increase of 25% and can be explained through the fact that specifically in its objectives and action points, Slovakia has aligned towards the ones the EU has put forward.

Finally, moving to the *evaluation processes*: The EU suggests that MS publish regular progress reports on the success of their NCSS. Slovakia complies with this proposal in both of its NCSSs, thus being 100% in line with the EU. It describes but does not define the evaluation process through progress reports in a separate document, the so-called 'Action Plan'.

2.1.2 Quantitative Harmonization of Germany's NCSS and the EUCSS over time

As indicated above, Germany's NCSSs show an overall higher similarity to the 2020 EUCSS than those issued by Slovakia. Like Slovakia, Germany has never used the exact wording as the EU to describe its *objectives*. However, similarly to Slovakia, at least in terms of content, the objectives formulated by Germany in both its 2016 and 2021 NCSS cover those proposed in the EUCSS 2020 by 100%. The resemblance results from the fact that Germany did not change its objectives over time. Moreover, the fact that Slovakia adjusted its objectives, whereas Germany did not, points to the difference in the formulation of the objectives: Whereas Germany has arguably formulated general long-term goals, so goals that apply and remain useful across disciplines, Slovakia formulated short-term objectives, which are of limited and discipline-specific value.

In comparison to Slovakia, Germany's NCSSs do not only show a higher similarity regarding objectives but also regarding *action points* that are proposed in the 2020 EUCSS. Germany's 2016 NCSS already covered 51% of the action points that were later proposed in the 2020 EUCSS. In 2021 this number increased to around 63%. This is an increase in similarity of 12%. Compared to the EU, however, most of the action points Germany mentioned did not focus on developing, reforming, amending, implementing, or promoting EU or international standards, norms, legislation, or policies. Instead, most of the action points in Germany's NCSS focus on capability building.

The latter is reflected in the *inputs* Germany suggests in its NCSSs. Like the EU, in 2016 and 2021, next to legal measures, most of the inputs Germany introduced in its NCSS concern new process and coordination structures and new tools and organizational components. As indicated above, the inputs the EU suggests in its 2020 EUCSS and Germany presents in its 2016, and 2021 NCSS are 100% the same. The fact that no change happened over time confirms the above-mentioned assumption that MS and the EU rely on a preferred and limited variety of resources and means to achieve their strategic objectives. Moreover, the case of Germany shows that generally speaking, over time, objectives can remain the same. However, the courses of action and resources, so how the objectives can be reached, can and/or must change.

Moving to *outputs*: Like Slovakia's NCSSs also, Germany's NCSSs show no change regarding outputs over time – they remain 100% the same compared to the ones derived from the 2020 EUCSS. The only difference to the 2020 EUCSS is that both of Germany's NCSSs, on top of the five outputs that can be derived from the EUCSS, also suggest 'warning systems and measures' as outputs. This finding confirms that a limited variety of resources and means has direct consequences for potential outputs. Moreover, the fact that Slovakia and Germany exceeded the outputs that can be derived from the EUCSS suggests that both MS had to (or, in Germany's case: have to) 'catch up' - likely with the warning systems and measures in place.

Like Slovakia, the *outcomes and impacts* that can be derived from Germany's NCSSs over time show a high similarity to those derived from the 2020 EUCSS: In 2016, Germany's NCSS covered around 75% of the outcomes and impacts of those that can be derived from the 2020 EUCSS. In comparison, its 2021 NCSS covers around 83%. This corresponds to an 8% increase in similarity. Noteworthy as potential outcomes and impacts that can be derived from the 2020 EUCSS and the MS NCSS are, for example, an increased awareness and a culture of cybersecurity or improved capabilities to protect critical information infrastructures, communication networks, and services.

Finally, also Germany fully complies with the *evaluation process* suggested in the 2020

EUCSS. Thus, its NCSS show 100% similarity to the 2020 EUCSS. However, on top, of the annual progress reports by the responsible ministries, the German NCSSs also include provisions for additional regular reviews of the technology landscape and regular meetings of a Cyber Security Council as part of the evaluation process. Further, unlike Slovakia, especially in its 2021 NCSS, Germany outlines the methodology it applies to evaluate the implementation and progress of specified objectives, ensuring transparency and accountability vis-à-vis the public.

2.1.3 Quantitative Harmonization between Germany's and Slovakia's NCSS over time

Next to an increase in similarity between the NCSS and the EUCSS is the increase in similarity between the NCSS. As mentioned above, from 2015 to 2021, the similarity between Germany's and Slovakia's NCSS increased by 10%. While in 2016, Germany's NCSS covered around 43% of the *objectives* that Slovakia introduced in its 2015 NCSS, in 2021, the objectives Germany introduced in its NCSS shared a similarity of 57% to the ones presented in Slovakia. This correlates to an increase of similarity of 14%. The initial similarity-difference between the MS strategic objectives may be explained through different national circumstances, which have given rise to different priorities. The increase in similarity, however, can not only be explained through the fact that Germany did not change its objectives over time but may also be explained through the fact that learning and adoption have taken place on the Slovakian level, for example, from the other MS or the EUCSS 2020.

In 2016 Germany's NCSS shared seventeen *action points* with Slovakia's 2015 NCSS, which correlates to a similarity of around 65%. In 2021 this number increased to twenty-five similarity action points in 2021, which correlates to 71% comparability and, therefore, an increase in similarity of 6%. It should be mentioned that also on MS level most of the action points that have been identified cover the development, implementation, or promotion of EU or (inter)national standards, norms, legislation, or policies.

This has a direct consequence for suggested *inputs* and *outputs,* which can be derived from the four different NCSS. In 2016 and 2021, Germany's and Slovakia's NCSS showed 100% compatibility regarding their suggested inputs and outputs. Considering that most action points in the NCSS relate to the development, implementation, or promotion of EU or (inter)national standards, norms, legislation, or policies, it is unsurprising that the establishment of legal measures is the preferred means (input) in both MS to achieve their strategic objectives. Accordingly, the main output that can be derived from the NCSS is the

improvement of regulatory frameworks. The fact that for both MS legal means remain a preferred way and/or resource over time suggests that they presumably proved to be most effective to achieve the strategic objectives.

The *outcomes and impacts* that can be derived from Germany's 2016 NCSS match those that can be derived from Slovakia's 2015 NCSS by 50%. The number increases drastically in 2021 when outcomes and impacts that can be derived from Germany's NCSS match 78% of those presented in Slovakia's NCSS. This corresponds to an increase in the alignment of outcomes and impacts of 28% over time. This significant increase in similarity can be explained through the alignment of objectives and action points.

Finally, regarding the *evaluation processes*: In all of the issued NCSSs, Germany and Slovakia include a provision that mentions regular progress reports as part of their evaluation process to measure the success of their NCSS. As such, they are 100% alike. However, as indicated above, on top of progress reports, Germany's evaluation process further includes regular review as well as regular meetings of its Cyber Security Council.

2.2 Harmonization or Fragmentation?

Overall, the quantitative analysis reveals that key components covering the (1) objectives, (2) action points, (3) inputs, (4) outputs, (5) outcomes and impact, (6) evaluation processes have, over time, either remained the same or increased in their similarity. This is the case not only between the NCSSs but also between the NCSSs and the 2020 EUCSS. The fact that for MS, an extreme increase in alignment was found for some key components, whereas for others, no increase in alignment was detected because they already shared a high degree of similarity indicates that certain conditions already exited in the MS and that presumably learning on the national level had been taking place for example from the EUCSS 2020. If the latter was indeed the case, the 2020 EUCSS did not simply formalize what already existed but arguably, introduced an even wider range of measures and principles towards which the MS had to work, and which caused them to adapt their NCSS, becoming more similar to the EUCSS 2020 and thus also more similar to each other over time. That said, the quantitative evidence of an increase in similarity between the NCSS and the NCSS with the 2020 EUCSS indicate that harmonization has been taking place, which is, in turn, at the very least, suggestive of Europeanization. The following chapter will discuss whether the latter is truly facilitated through the utilization of and learning from the 2020 EUCSS soft law document rather than the result of specific national circumstances and developments.

Chapter 3: Processes of ‘Soft’ Europeanization: Qualitative Analysis of EUCSS role in Germany’s and Slovakia’s NCSS-making

While the quantitative analysis revealed evidence of harmonization and, thus, Europeanization of Germanys and Slovakia NCSS, the question remains to what extent the latter is indeed the result of the utilization of the 2020 EUCSS by the MS. The thesis utilized the qualitative method 'process tracing' to explore the latter and provide insights into the *processes* that lay behind the outcomes of Europeanization. The following chapter preset the result of the qualitative analysis and is divided into three parts: First, the results of Slovakia's 2021 NCSS-making are presented. Second, the results of Germany's 2021 NCSS-making are introduced. The chapter will conclude with a short discussion of the quantitative and qualitative results.

3.1 Slovakia's 2021 NCSS-making

Cybersecurity has been embraced as one of the fundamental aspects to ensure Slovakia's security for some time. However, due to recurring regulatory and organizational shortfalls, it took Slovakia up to the beginning of 2019 to establish a solid and robust legal and institutional framework for cybersecurity with the implementation of Act No. 69/2018 Coll. This is why the national policymaker sees Slovakia as "*a young country in this field*" (I-3, 2022). Despite this, Slovakia's ambitions are high: The country is determined to reach the same digital economic growth level as major players like Sweden and Estonia (Hathaway et al., 2019, p.8) This may also explain why the increase in harmonization between the 2020 EUCSS and Slovakia’s 2021 NCSS is higher than between the 2020 EUCSS and Germany’s 2021 NCSS.

Not only due to the outbreak of Covid-19 and the corresponding increase in cyber-attacks but also due to the parliamentary elections on the 29th of February 2020, the year 2020 brought noticeable political attention to cybersecurity. During the election, the left-wing populist party SMER-SD, which had been ruling the country since 2006, lost its governmental mandate to the center-right wing populist party OL'aNO (Haughton et al., 2022). After its election and under the leadership of Igor Matovič, OL'aNO adopted a generally conservative outlook, resulting in national cybersecurity policy changes, which also affected Slovakia's 2021 NCSS-making.

In this context, three strategic changes deserve more detailed attention: First, from 2020 until the end of 2021, a shift in Slovakia's attitude towards China and Russia was noticeable.

This is arguably the result of the OL'aNO program document, the latter set as a goal a return to consensus on the course of Slovakia's foreign policy, stressing its commitments to Euro-Atlantic values and institutions. It further mentions EU MS and the US as sole key strategic partners. This stands in contrast to the previous government, which, although not uniformly, embraced next to a pro-EU and -US, also a pro-Russia and -China attitude. OL'aNO's newly established consensus to focus primarily on Euro/EU-Atlantic political relations resulted in the fact that Slovakia, together with more than ten other Central and Eastern European (CEE) countries, signed a memorandum with the US on the security of 5G networks while leaving a similar proposal from China unanswered (Pleschová, 2022, p.108). Moreover, it led to the exclusion of employing equipment from the Chinese provider of ICT infrastructure and smart devices Huawei, at least in the radio access network (RAN) component of the 5G (Pleschová, 2022, p.108). Further, reoccurring reports from, Globsec, a prominent Slovakian security think tank, pointed to Russia and China as significant sources of attacks, hybrid threats, propaganda, and disinformation (Milo et al., 2018; Hathaway et al., 2019). These developments led to a hardening of the pro-Euro/EU-Atlantic attitude and ultimately translated into policy documents like Slovakia's 2021 NCSS. In fact, its 2021 NCSS dedicates a whole chapter to this matter, declaring the EU, United Nations (UN), the North Atlantic Treaty Organization (NATO), and the Organization for Security and Cooperation in Europe (OSCE) as its main foreign political partners. It further announced that it wants to achieve its key strategic vision of creating an 'open, free and secure cyberspace' – by closely cooperating with the latter in cyber defense.

Second, since the pandemic caused a massive transfer of activities to the online space, it caused an increase in cyber-attacks in and against Slovakia, warnings about Slovakia's lack of cybersecurity experts, especially in public administration, increased in 2020. In 2020, a report on cybersecurity prepared by Slovakia's National Security Authority (NBU) indicated that a lack of cybersecurity experts is most likely related to a lack of awareness among the operators and the comparatively low level of digital education and training (2020). The Ministry of Education, Science, Research and Sport reacted with a digital education strategy for school and higher education (2020). The latter aimed to modernize the digital infrastructure, invest in access to digital educational content, and improve teaching staff's competencies - points which later reappeared at even greater length in Slovakia's 2021 NCSS. Compared to its former NCSS, Slovakia's 2021 NCSS has as its central objective to make cybersecurity an essential part of public administration through raising awareness initiatives and professional capacity building, which in turn relies on the education and training of professionals.

Thirdly, at the beginning of 2021, cybercrime, a topic that was not even addressed in

Slovakia's former NCSS, gained increased political attention. The reason for this was that the country came under pressure since it made headlines because of its comparatively limp approach to money laundering occurring around or in relation to cybercrimes (Council of Europe, 2020). The effective detection of cybercrime became a 'hot topic' and was ultimately adopted as an objective in the 2021 NCSS. To achieve this objective, Slovakia proposed increasing investments in intelligence, operational, and personnel structures to improve the collection of evidence and tracing of criminal assets. Moreover, it stressed the closer cooperation with EU MS.

Based on these three points, one could get the impression that the 2020 EUCSS did not play a great role in these strategic changes. Rather, they appear to be the direct result of exceptional international circumstances like the pandemic and national events, like the 2020 elections and the resulting politics thereof. However, as the interview with a Slovakian national-policy maker suggests, the picture was more complex. According to him and a report by the NBU, Slovakia already started 2020 to develop a working group comprised of experts from specific sectors and the responsible Ministries (I-3, 2022; NBU, 2020). As the interviewee indicates: "[…] *they put their specific issue on the table and, ahm, after that process, we started to create our national strategy. Because many of these experts are also representing Slovak Republic at the European level. And, ahm, there is some, ahm, connection with, ahm, Cyberstrategy at the European level* […]" (I-3, 2022). According to interviewee I-3, the EUCSS 2020 was particularly useful in the national "*preparation process*" of Slovakia's 2020 NCSS as it was, at least in part, developed at the same time as the 2020 EUCSS. Interviewee I-3 that the 2020 EUCSS "*frames*" issues, suggests potential "*methodologies*" and provides "*guidelines*." Through it prevents ambiguity among MS because generally, the national actors feel a "[…] *need to also respect the soft law.*" Generally, when it comes to soft law the interviewee stresses: "*we use many aspects of the past documents in the future* […] *continuance is very important aspect in that way*." (I-3, 2022). According to the interviewee, as such, the 2021 NCSS is "*based on the EU policies*" like the 2020 EUCSS. However, the interviewee also emphasized that in the making of their NCSS, they were generally cautious regarding documents like the EUCSS because sometimes "*they bite with the national security*." The interviewee indicates that in those cases, an EU MS like Slovakia has to make a cost-benefit analysis about what (not) to adopt (I-3, 2022).

Overall, these findings suggest that Slovakias 2021 NCSS-making was primarily influenced by national political circumstances and preferences, like the election in 2020 that changed the cybersecurity policy landscape and the Covid-19 pandemic, which made

cybersecurity an even more important and prominent topic. However, the interviewee confirmed that the 2020 EUCSS had at least in part impacts on the 2021 Slovakian NCSS-making and thus may partly be responsible for the harmonization of the NCSS with the EUCSS. While indeed discussions on Slovakia's 2021 NCSS started on the national level, national strategic questions, and issues, concerning, for example, strategic relations, the lack of cybersecurity experts in public administration and cybercrime were also brought forward on the EU level, and considered in relation to the 2020 EUCSS. This confirms the findings by Checkel (2001), Scott (2011), and Polak (2015), which were addressed earlier: By providing information and soft law supports learning about desirable policies and thus indirectly causes potential (re)formulation of national policy. It gave Slovakian NCSS-makers a clear indication of what to expect on the EU level and thus about to include or leave out. The interview with the Slovakian-national policy maker also showed that the MS always has the final word since cybersecurity is considered a clear national competence. That is to say that, even though national policy-makers learn, for example, about the strategies that the EU desires through the 2020 EUCSS, it does not mean that they will also follow it. Soft documents can be disregarded when they do not align with national legal, institutional, and political priorities.

3.2 Germany's 2021 NCSS-making

In contrast to Slovakia, not 2020 but 2021 was an election year for Germany. Next to the federal elections, state elections and regional elections were held in five out of the sixteen different provinces of Germany. Accordingly, 2020 was shaped by political preparations for the latter. Interviews with two German cybersecurity policy-makers confirmed that these circumstances also had implications on Germany's 2021 NCSS-making. In 2018, the in 2020 still governing parties, CDU/CSU (center-right) and SPD (center-left), outlined a few prime fields for strategic action concerning the research and development as well as the security of IT products in their coalition government treaty: (1) to increase the responsibilities of manufacturers and providers of IT products beyond the area of critical infrastructure through expanding existing IT security law; (2) increase investments in research in the field of IT products and security (3) to develop minimum IT security standards for internet-connected products in cooperation with industry; (4) to introduce a quality label indicating the security level of IT products for consumers. Moreover, it aimed to (5) to make secure electronic identification and end-to-end encryption solutions more easily accessible to citizens; (6) set up competence centers; (7) strengthen the role of the Federal Office for Information Security (BSI), and (8) to improve cooperation

between private and public authorities (Schallbruch & Skierka, 2018, p. 12). Considering the upcoming federal elections, CDU/CSU and the SPD party and its members sitting in the Ministry of Interior - the Ministry that is also responsible for issuing the NCSS - were under pressure and eager to publish the 2021 NCSS still during their governance and corresponding to their ideas. Indeed, Germany's NCSS 2021 strategy picked up all these action points. As interviewee I-1 stressed: "[…] *we just made it, ahm, in the end, to bring this strategy 'through the door*' […]" (2022).

Further, in 2020 and 2021, increased national attention was put on cybercrime and research and development in cybercrime. Two incidents are particularly noteworthy since they confirmed the course that the national political coalition was planning to take in their 2021 NCSS regarding cybercrime and cybersecurity at that time: First, in April 2021, hackers attacked the IT-network of the retail grocery chain Tegut. As a response, the IT-network systems had to be shut down and taken offline. Among other things, this affected merchandise management programs, which usually controlled scheduling in the logistics. The result was a shortage of goods. On top, the attackers published sensitive company files and customer contact information, like the address, e-mail, and telephone numbers on the darknet (DER SPIEGEL, 2021). Further, right before the federal elections, in July 2021, a cyberattack on the district of Anhalt-Bitterfeld in the state of Saxony-Anhalt made national news after it had declared disaster and the BSI called the incident Germany's first "cyber-catastrophe." The attack affected the entire range of district services, leaving it, for example, unable to pay out welfare benefits (DW, 2021). Both of these incidents did not happen in isolation. In May 2020, the German Federal Criminal Police Office (BKA) stated in its annual federal situation report 'cybercrime' that the number of reordered criminal cyberattacks rose by 7.9% to 108,474 cases alone in 2020, especially against businesses and public institutions that have been relevant in the fight against the pandemic increased. Moreover, as a reaction to the incidents and the report former German Interior Minister Horst Seehofer (CDU) admitted in an interview with the German Press-Agency (dpa) that there was still a lot to do in cybersecurity and cybercrime. Moreover, he stressed the importance of strengthening the role of the BSI. Similarly, CDU General-Secretary Paul Ziemak stated as a reaction that more research and development in the area of cybersecurity are necessary (FR, 2021).

All these matters indicate that, similarly to Slovakia, also the making of the German 2021 NCSS was primarily a national concern, highly influenced by the exceptional condition created through the pandemic and motivated by the ambitions of national politics. However, important to note the development and discussions on its own NCSS started when Germany

took over the presidency of the Council of the EU from July until December 2020. During this time, also the 2020 EUCSS was in its final stages of development. The interviews with two national-policy makers confirm, while generally, the German and the EU strategy-making follow two different processes, even in its development "*The EU Cybersecurity Strategy has* […] *the character of a roadmap* […], *it gives us an indication what to prepare for and what are the main action points at European level*" (I-2, 2022). Moreover, it gave "*good hints*" on "*how to implement* […] *how to come to the measures*" (I-1, 2022), and it usually "*triggers a discussion process among the member states*" (I-2, 2022). As interviewee I-1 elaborates, in the 2021 NCSS making, policymakers had " *a* […] *look whether our own measures are following and are satisfying what the* [EU] *strategy says*." (2022). However, similarly to Slovakia, interviewee I-2 stresses that "*cybersecurity is a clear national competence*" (2022). In this way, it was generally evaluated on the national level to what extent the 2020 EUCSS "[…] *affects our own work and where do we want to take over things* […]" (I-1, 2022). In the end, it was a national "*political decision*," on what to adopt so, "*we do a bit of cherry-picking, indeed*." (I-1, 2022). For example, interviewee I-2 mentions: "*we in Germany have always put a lot of emphasis to strengthen our national agency, the BSI,*" a point that was indeed included in Germany's 2021 NCSS but as indicated above, was a national decision (2022).

This confirms the finding that was made in the Slovakian case. While ultimately, it was a national political decision about what Germany included in its 2021 NCSS, the interviews confirm that the EUCSS 2020 was used as an inspiration and an indication for potential (legally binding) measures coming up on EU level which affect national conditions. Hence the 2020 EUCSS supported MS *learning* about desirable policies. Next to providing inspiration, the interviewees indicates that soft law like the 2020 EUCSS also facilitated a dialogue process among MS and thus leading next to learning process also to *'peer pressure.'* As such Germany further confirm the findings by Hodson (2004), Trubek and Trubek (2005), Heidenreich and Bischoff (2008) and Stefan et al., 2019: MS not only learn from the EU about desirable policy's but also form their *'peers.'* Arguably, by learning from other MS which aspects they are going to adopt from the 2020 EUCSS must have contributed to an increase of social and moral pressure in Germany to not underperform with regard to the non-binding rules and facilitated and alignment and thus harmonization of the NCSS.

That said, another finding is striking: During its presidency a central topic for Germany was 'EU's digital sovereignty' (EU2020.de, 2020). As such, Germany, amongst other points, was seeking to (1) to accelerate the deployment of gigabit networks, including 5G across the EU; (2) contribute in and facilitate more EU and international cooperation with regards to the

effective detection and resolution of cybercrime; (3) increase the development, employment, expansion of the cyber diplomacy. All these points were discussed among EU MS and were ultimately not only picked up in Germany's 2021 NCSS but also in the 2020 EUCSS. This indicates that national policymaking are also directly involved in discussions on soft law documents like the 2020EUCSS. In turn, this may have also influenced Germany's willingness to take over key components laid out in the 2020 EUCSS. This may also explain the overall greater alignment to the 2020 EUCSS. To say it in the words of interviewee I-2: "*on the one side member states trying to reach a higher level of their own cybersecurity and at the same time the Commission is trying to harmonize it […] The European Strategy paved the road. But I think that in the end, both sides are affecting each other in one way or the other […]*" (2022).

3.3 Europeanization through soft law?

In sum, the 'process tracing' of Germany's and Slovakia's 2021 NCSS-making indicates that the quantitative harmonization that was detected between the MS NCSS and the 2020 EUCSS is, at the very least, partly the result of the utilization of the soft law document on the national level. The soft law document facilitated a learning process on the national level about desired policies. It provided, for example, inspiration on potential ways and means on how to achieve strategic objectives. Moreover, it led to discussion among MS, which facilitated social peer pressure to align with 2020 EUCSS components. Further, since MS are usually directly involved in the making process of EU soft law like the 2020 EUCSS, it directly influenced MS's willingness to (not) take over certain points. As such, it is possible to argue that a Europeanization process through soft law was taking place, with MS cybersecurity policies, like Germany's and Slovakia's NCSS key components aligning with each other and laid down in the 2020 EUCSS. However, it should be stressed that from the qualitative analysis, it becomes evident that steps towards harmonization for both MS were a conscious decision: The EU soft law document 'Europeanized' Germany's and Slovakia's 2021 NCSS, however only to the extent to which it also aligned with national ambitions and priorities.

Conclusion

Disruptions to the routine operations of ICTs in conflict situations have made cybersecurity come to ascend a prominent position in the legal and political decision-makeing of the EU. Scholars have used the concept Europeanization to describe the processes by which EU decision-makeing manifests itself in the logic of, for example, national policy outcomes of those processes (see Radaelli, 2012, p. 1 as cited by Fererro & Ackrill, 2016, p.880). The literature has pointed to the significant amount of soft law that the EU has issued to address potential threats arising from the active use of ICTs and to facilitate uniformity across MS cybersecurity policies. While soft law is intended to deliver policy change at the national level (e.g., alignment of MS cybersecurity policy), by definition, there is no legal obligation for MS to implement soft law. Accordingly, by utilizing Europeanization as a conceptual frame, this thesis has sought to answer the question: To what extent has non-legally binding EU soft law on cybersecurity influenced the making of the national cybersecurity policies of its MS over time?

By taking a small-scale empirical approach, the thesis essentially aimed to establish the extent to which specifically Germany's and Slovakia's main national cybersecurity policies, namely, their 2021 NCSSs, have been 'Europeanized' through the main EU soft law document issued in the policy domain of cybersecurity, namely the 2020 EUCCS. Therefore, the thesis has utilized a mixed-methods approach and first quantitatively analyze the extent to which Germany's and Slovakia's recent NCSS have become more similar (i.e., harmonized) with each other and the recent EUCSS over time as an outcome of Europeanization processes. To shed light on the Europeanization processes through soft law itself, the thesis has secondly qualitatively' process traced' whether and how the extent of harmonization between Germany's and Slovakia's NCSS and the EUCSS was indeed influenced through the EU soft law instrument.

The thesis found evidence that the MS NCSS key components indeed became indeed more similar (i.e., harmonized) to each other and to the ones laid down in the EU over time. It was identified that in 2021 Germany's and Slovakia's NCSS shared 10% more similar key components than their previous ones. Similarly, it was found that an 'eastern' and 'new' MS, like Slovakia, whose former NCSS, in comparison, did not align much with the EUCSS, has responded with greater adjustments, resulting in a considerable alignment over time. Slovakia's current NCSS shows 15% more similarity to the 2020 EUCSS than its previous one. In comparison, a 'west,' 'older' MS, like Germany, whose former NCSS did already greatly align

with the key components suggested in the EUCSS, did not respond which such great adjustments. Germany's current NCSS shows only 8% more similarity to the 2020 EUCSS than its former ones.

The qualitative analysis reveals that this evidence of harmonization and, thus, Europeanization of the MS NCSS was, at the very least, partially the outcome of the deployment of the soft law document on a national level during their NCSS-making. While it became clear that cybersecurity is understood as a national competence and the NCSS-making followed primarily national prerogatives as well as a response to international circumstances like the Covid-19 pandemic, evidence was found that the 2020 EUCSS in addition, for example, contributed to a learning process about preferred national policies. It gave ideas for possible methods and means to accomplish strategic goals and indicated what can be expected on EU-level that may have potential consequences on the national level. Further, it sparked debates among the EU MS, which in turn increased peer pressure to adhere to the 2020 EUCSS key components. Moreover, evidence was found that the fact that EU MS were involved in the 2020 EUCSS-making also affected their willingness to comply with the 2020 EUCSS in their own NCSS. That Slovakia's NCSSs more closely aligned with the 2020 EUCSS than over time can be explained by the fact that Slovakia is considered a young country in the cybersecurity field. As a new MS, it actively seeks to 'catch-up,' and its political system offers the best conditions to do so. Likewise, the fact that Germany's NCSS codes are more closely aligned with the 2020 EUCSS however, in a similar fashion did not show a great increase in alignment with the 2020 EUCSS over time indicates that Germany, a 'west' and 'old' MS had next to long-term strategic goals also different preconditions than Slovakia. Thus, Germany did not have to actively strive to 'Europeanize' its NCSS.

Overall, based on these findings, it is possible to conclude that the EU soft law document 'Europeanized' Germany's and Slovakia's 2021 NCSS, however, only to the extent to which it also played into national ambitions and priorities. Moreover, these findings offer an interesting observation into the Europeanization process, namely that MS (can) actively strive to 'Europeanize' their NCSS. Finally, the harmonization of NCSS indicates that the EU is achieving its aim of aligning approaches to cybersecurity in the EU and is an indicator that the EU has the potential to establish itself as a strong cybersecurity actor in the international environment. That said, future research should test the generalizability of these findings. Thereby future research can address and develop several issues and limitations that have not been addressed here: First, concerning the methodological approach: While the thesis presents a qualitative way to measure the extent of Europeanization, this approach remains novel. Future

research should test the applicability of this approach also in other policy areas. Further, the investigation period presented here for the process training is comparatively short, and the case selection is small. With the development and increasing importance of the cybersecurity field, future research should consider a longer investigation period and more cases. Regarding Europeanization through soft law: Since this thesis focuses on cybersecurity policymaking, future research could find ways to analyze, in greater detail, how EU cybersecurity soft law is implemented, monitored, and enforced. While this thesis has made a first step to improve the comprehension of Europeanization through soft law in the cybersecurity domain, further research is needed to explore these avenues.

Bibliography

Primary Sources

List of Legislation

EU hard law

Consolidated version of the Treaty on the Functioning of the European Union (TFEU). (2012, October 26). *Official Journal of the European Union*, C326/47-390.

Consolidated version of the Treaty on the European Union (TEU). (2012, October 26). *Official Journal of the European Union*, C326/13-45.

European Parliament & Council of the European Union. (2013, May 21). Regulation (EU) Regulation (EU) concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. *Official Journal of the European Union*, L165/41.

European Parliament & Council of the European Union. (2016, July 7). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1

European Parliament & Council of the European Union. (2019, April 17). Regulation (EU) 2019/88 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union,* L 151/15

EU soft law

High Representative of the European Union for Foreign Affairs and Security Policy, European Commission. (2020). Joint Communication - The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18). Author. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN

List of National Law

Slovakia

National Council of Slovak Republic (2018). Act on Cybersecurity and on Amendments and Supplements to certain Acts. Act No. 69/2018 Coll. https://www.sk-cert/wp-content/uploads /2018/03/2018_69-Act-on-Cybersecurity.pdf

List of National Policy and Reports

Germany

Federal Criminal Police Office. (2020). Bundeslagebild Cybercrime 2020. Retrieved January 8th, 2023, from https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/210507_BLBCyber.html

Federal Ministry of the Interior, Building and Community. (2016). The Cyber Security Strategy for Germany 2016. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

Federal Ministry of the Interior, Building and Community. (2021). The Cyber Security Strategy for Germany 2021.https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

Slovakia

Ministry of Education, Science, Research and Sport. (2020). *Digital education strategy for school and higher education.* Retrieved January 8th, 2023, from www.minedu.sk/informatizacia-a-digitalizia-skolstva/

National Security Authority. (2020). *Report on the Cybersecurity of the Slovak Republic in 2020.* Retrieved January 8th, 2023, from https://www.nbu.gov.sk/wp-content/uploads/ENG/Cybersecurity-report-2020.pdf

National Security Authority. (2021). *The National Cybersecurity Strategy 2021-2025.* Retrieved January 8th, 2023, from https://www.enisa.europa.eu/topics/national-cyber security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Slovakia

National Security Authority, National Agency for Network and Electronic Services, & Government Office. (2015). *Cyber Security Concept of the Slovak Republic 2015 2020.* Retrieved January 8th, 2023, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss map/national-cyber-security-strategies-interactive-map?selected=Slovakia

OL'aNO. **(2020).** *The Programme Document of the Slovak Government.* Retrieved December 22, 2022, from https://www.teraz .sk/download/135/programove-vyhlasenie-vlady.pdf

United States–Slovak Republic (23 October 2020). Joint Declaration on 5G Security.Retrieved December 22, 2022, from https://2017-2021.state.gov/unitedstates-slovak-republic-joint-declaration-on-5g -security/index.html

List of Interviews

Germany

von der Brelie, F.M (2022, April 21) Personal Interview [I-1]

von der Brelie, F.M (2022, June 24) Personal Interview [I-2]

Slovakia

von der Brelie, F.M (2022, May 22) Personal Interview [I-1]

News Articles

Council of Europe. (2020a, October, 30). *Slovakia should prosecute money laundering with more determination.* Retrieved January 8th, 2023, from https://www.coe.int/en/web/portal/-/slovakia-should-prosecute-money-laundering-with-more-determination

DER SPIEGEL. (2021, May 28). Erpresser erhöhen den Druck auf Supermarktkette Tegut. Retrieved January 15th, 2023, from https://www.spiegel.de/netzwelt/web/tegut-nach-hackerangriff-tauchen-interne-daten-im-darknet-auf-a-06d52a1a-b5df-4601-b7a6-c295d1cd9e8a

Deutsche Welle (DW). (2021, July, 10). Rural German district declares disaster after cyberattack. RetrievedJanuary 15th, 2023, from http://www.dw.com/en/rural-german-district-declares-disaster-after-cyberattack/a-58227484

Frankfurter Rundschau (FR). (2021, May 10). Cybercrime nimmt zu: Angreifer-Interesse an Impfstoff. Retrieved January 15th, 2023, from https://www.fr.de/panorama/cybercrime-nimmt-zu-angreifer.intresse-an-inmpfstoff-zr-90530258.html

Websites

EU2020.de. (2020). Expanding the EU's digital sovereignty. Germany's Presidency of the Council of the European Union. Retrieved January 20th, 2023, from https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828

Secondary Sources

Andone, C., & Coman-Kund, F. (2022). Persuasive rather than 'binding' EU soft law? An argumentative perspective on the European Commission's soft law instruments in times of crisis. *The Theory and Practice of Legislation*, *10*(1), 22–47.

Bache, I. & Jordan, A. (2006). Europeanization and Domestic Change In Bache, I. & Jordan, A. (Eds.), *The Europeanization of British Politic* (pp.17-33). Palgrave Macmillan.

Benediek, A. (2012). *European Cyber Security Policy*. German Institute for International and Security Affairs (SWP). Retrieved October 10, 2022, from https://www.swp-berlin.org/publications/products/research_papers/2012_RP13_bdk.pdf

Benediek, A. & Pander Maat, E. (2019). *The EU's regulatory approach to cybersecurity*. German Institute for International and Security Affairs (SWP) Working Paper No. 2. Retrieved October 10, 2022, from https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf

Börzel, T. (1999). Towards Convergence in Europe? Institutional Adaptation to Europeanisation in Germany and Spain. *Journal of Common Market Studies*, *39*(4), 573–96.

Brooks, E. (2012). Europeanisation through soft law: the future of EU health policy?. *Political Perspectives, 6*(1), 86-104.

Cantero Gamito, M. (2018). Europeanization through Standardization: ICT and Telecommunications. *Yearbook of European Law*, *37*, 395–423.

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272.

Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, *19*(3), 299–303.

Carrapico, H. & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126.

Checkel, J. (2001). Why Comply? Social Learning and European Identity Change. *International Organization, 55*(3), 553-588.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Palgrave Macmillan.

Coman, I. (2017). Cross-border cyber-attacks and critical infrastructure protection. *International Journal of Information Security and Cybercrime, 6*(2), 47-52.

Cowles, M. G., Caporaso, J., & Risse, T. (2001). *Transforming Europe: Europeanization and Domestic Change*. Cornell University Press.

Cymutta, S. (2015). *National Cyber Security Organization: Germany.* NATO Cooperative Cyber Defence Centre of Excellence. Retrieved November 11, 2022, from https://ccdcoe.org/uploads/2020/12/Country_Report_DEU.pdf

Dyson, K. (2002). Introduction: EMU as Integration, Europeanization and Convergence. In Dyson, K. (Eds.), *European States and the Euro* (pp. 1-27). Oxford University Press.

Eliantonio, M., Korkea-aho, E., & Stefan, O. (2021). *EU Soft Law in the Member States: Theoretical Findings and Empirical Evidence*. Bloomsbury Publishing.

Exadaktylos, T. & Radaelli, C. (2009). Research Design in European Studies: The Case of Europeanization. *Journal of Common Market Studies, 47*(3), 507-530.

Falkner, G., Treib, O., Hartlapp, M. & Leiber, S. (2005). *Complying with Europe: EU Harmonisation and Soft Law in the Member States.* Cambridge University Press.

Ferrero, I., & Ackrill, R. (2016). Europeanization and the Soft Law Process of EU Corporate Governance: How has the 2003 Action Plan Impacted on National Corporate Governance Codes? *JCMS: Journal of Common Market Studies*, *54*(4), 878–895.

George, A.L. & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences.* MIT Press

Giner, B. (1995). *La divulgación de información financiera: Una investigación empírica* (Madrid: Instituto de Contabilidad y Auditoría de Cuentas)

Graziano, P. R. & Vink, M. (2013). Europeanization: Concept, Theory, and Methods In Bulmer & S. Lesquene *The Member States of the European Union*, (2nd ed., pp. 31 54). Oxford University Press

Hathaway, M., Spidalieri, F., & Kaushik, A. (2019). *Slovak Republic Cyber Readiness at Glance*. GLOBSEC. Retrieved December 22, 2022, from https://www.potomacinstitute.org/images/CRI/CRI_Slovakia_Profile-Digital.pdf

Haughton, T., Rybář, M., & Deegan-Krause, K. (2022). Corruption, Campaigning, and Novelty: The 2020 Parliamentary Elections and the Evolving Patterns of Party Politics in Slovakia. *East European Politics and Societies*, *36*(3), 728-752. https://doi.org/10.1177/08883254211012765

Heidenreich, M. & Bischoff, G. (2008). The Open Method of Co-ordination: A Way to the Europeanization of Social and Employment Policies?. *Journal of Common Market Studies, 46*(3), 497–532.

Helmbrecht, U., Purser, S. & Ritter Kleijnstrup, M. (2012). *Cyber security: future challenges and opportunities (ENISA Report).* Retrieved October 10, 2022, from *https://btg.org/wp-content/uploads/2012/01/ENISA-Cyber-Security-Report-2011.pdf*

Héritier, A. & Knill, C. (2001). Differential Responses to European Policies: A Comparison, In A. Héritier, D. Kerwer, C. Knill, D., Lehmkuhl, M. Teutsch, and A. C. Douillet (Eds.). *Differential Europe: The European Union Impact on National Policymaking*, (pp. 257–94). Rowman and Littlefield.

Hodson, D. (2004). Macroeconomic Co-ordination in the Euro Area: The Scope and Limits of the Open Method. *Journal of European Public Policy, 11*(2), 231–48.

Hricikóvá, L. & Kaska, K. (2015). *National Cyber Security Organization: Slovakia.* NATO Cooperative Cyber Defence Centre of Excellence. Retrieved November 11, 2022, from https://ccdcoe.org/uploads/2018/10/CS_organisation_SLOVAKIA_042015.pdf

Kaiser, A. D., Biela, J., & Hennl, A. (2012). *Policy Making in Multilevel Systems: Federalism, Decentralisation, and Performance in the OECD Countries (ECPR Monographs)*. ECPR Press.

Knill, C., & Lehmkuhl, D. (2002). The national impact of European Union regulatory policy: Three Europeanization mechanisms. *European Journal of Political Research*, *41*(2), 255–280.

Ladrech, R. (1994). Europeanization of Domestic Politics and Institutions: The Case of France. *Journal of Common Market Studies, (32)*1, 69-88.

Ladrech, R. (2002). Europeanization and Political Parties: Towards a Framework for Analysis. *Party Politics*, *8*(4), 389–403.

López-Santana, M. (2006). The domestic implications of European soft law: framing and transmitting change in employment policy. *Journal of European Public Policy*, *13*(4), 481–499.

López-Santana, M. (2007). *Soft Europeanization? How the Soft Pressure from Above Affects the Bottom (Differently): The Belgian, Spanish and Swedish Experience* (European University Institute Working Paper No.10).

Majone, G. (2014). Policy Harmonization: Limits and Alternatives. *Journal of Comparative Policy Analysis: Research and Practice*, *16*(1), 4–21. https://doi.org/10.1080/13876988.2013.873191

Milo, D. et al. (2018). *Mapovanie zraniteľnosti SR v oblasti hybridných hrozieb (Mapping of Vulnerabilities of the Slovak Republic in the Field of Hybrid Threats).* GLOBSEC. Retrieved December 22, 2022, from https://www.politicalcapital.hu/pc-admin/source/documents/authoritarian_shadows_in_the_eu_2020_09.pdf

Montpetit, E. (2000). Europeanisation and Domestic Politics: Europe and the Development of a French Environmental Policy for the Agricultural Sector. *Journal of European Public Policy, 7*(4), 576–92.

Moumoutzis, K., & Zartaloudis, S. (2015). Europeanization Mechanisms and Process Tracing: A Template for Empirical Research. *JCMS: Journal of Common Market Studies*, *54*(2), 337–352.

Odermatt, J. (2018). *The European Union as a Cybersecurity Actor*. University of Copenhagen Faculty of Law Research Paper No. 2018-52. Retrieved October 10, 2022, from https://ssrn.com/abstract=3144257

Olsen, J. P. (1996). Europeanization and Nation-State Dynamics. In: Gustavsson, S. & Leif; L. (Eds.), *The Future of the Nation State. Essays on Cultural Pluralism and Political Integration*, (pp.245-285). Routledge.

Pleschová,, G. (2022). Chapter 6: Significant conversations on Slovakias cybersecurity: China, Huawei and the struggle for the countries political orientation. Pleschová, G. (Eds.), *China in Central Europe. Seeking Allies, Creating Tensions* (1st ed., pp.106-127). Edward Elgar Publishing. http://doi.org/10.4337/9781800371859

Polak, J. (2015). *What works to make EU law work? An analysis of the usefulness of national, transnational, and supranational compliance instruments*, PhD Maastricht University.

Radaelli, C. (2003). The Europeanization of Public Policy. In Featherstone, K. & Radaelli, C. (Eds.), *The Politics of Europeanization,* (pp. 27-57). Oxford University Press.

Radaelli, C.(2004). Europeanisation: solution or problem? *European Integration Online Papers (EIoP)*, *8*(16), 1-23.

Radaelli, C. & Pasquier, R. (2007). Conceptual Issues. In: Graziano, P. & Vink, M. P. (Eds.), *Europeanization. New Research Agendas*, (pp. 35-45). Palgrave.

Radaelli, C. (2012). Europeanization: The Challenge of Establishing Causality. In Exadaktylos, T. and Radaelli, C. (Eds.), *Research Design in European Studies: Establishing Causality in Europeanization,* (pp. 1-16). Palgrave.

Ripoll Servent, A. (2017). Protecting or Processing? Recasting EU Data Norms. In Schünemann, W.O & Baumann, M.O (Eds.), *Privacy, Data Protection and Cybersecurity in Europe* (pp.115-130). Springer.

Saurugger, S., & Terpan, F. (2019, May). *Explaining the transformation of law. The cases of economic governance, migration and cybersecurity*. EUSA Conference, Denver.

Schallbruch, M. & Skierka, I. (2018). *Cybersecurity in Germany*. Springer.

Schmidt, V.A. (2009). The EU and its Member States: From Bottom-Up to Top-Down', in: Phinnemore D., Warleigh-Lack A. (Eds.), *Reflections on European Integration*, (pp.194-211). Palgrave.

Scott, J. (2011). In legal limbo: Post-legislative guidance as a challenge for European administrative law. *Common Market Law Review*, *48*(2), 329–355. Retrieved May 15, 2021 from https://ssrn.com/abstract=1783557

Senden, L. (2004). *Soft law in European Community law*. Hart Publishing.

Sivan-Sevilla, I. (2021). Europeanisation on demand: The EU cybersecurity certification regime between market integration and core state powers (1997-2019). *Journal of Public Policy, 41*(3), 600-631.

Slominski, P., & Trauner, F. (2020). Reforming me softly – how soft law has changed EU return policy since the migration crisis. *West European Politics*, *44*(1), 93–113.

Stefan, O., Avbelj, M., Eliantonio, M., Hartlapp, M., Korkea-Aho & Rubio, N. (2019). *EU Soft Law in the EU Legal Order:A Literature Review* (SoLaR Working Paper No. 1). Soft Law Research Network. Retrieved May 15, 2021 from https://www.solar-network.eu/wp-content/uploads/2018/11/SoLaR-A-Literature-Review.pdf

Terpan, F. (2015). Soft law in the European Union – the changing nature of EU Law, *European Law Journal, 21*(1), 68-96.

Tholoniat, L. (2010). The Career of the Open Method of Coordination: Lessons from a 'Soft' EU Instrument. *West European Politics*, *33*(1), 93–117.

Töller, A., E. (2010). Measuring and Comparing Europeanization of National Legislation: A Research Note. *Journal of Common Market Studies, 48*(2), 417-444.

Toshkov, D. (2012). Compliance with EU Law in Central and Eastern Europe: The Disaster that Didn't Happen (Yet). *L'Europe en Formation*, 364, 91-109.

Trubek, D.M. & Trubek, L.G. (2005). Hard and Soft Law in the Construction of Social Europe: the Role of the Open Method of Co-ordination. *European Law Journal, 11*(3), 343–64.

Tumkevič, A. (2017). Cybersecurity in Central Eastern Europe: Form Identifying Risks to Countering Threats. *Baltic Journal of Political Science*, *5*(5), 73.

Van der Meulen N., Eun A. J. & Soesanto, S. (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses (RAND Europe). Retrieved October 10, 2022, from https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

Wessel, R.A. (2015). 19.Towards EU cybersecurity law: Regulating a new policy field In Tsagourias, N. & Buchan, R. (Eds.), *Research Handbook on International Law and Cyberspace*. (pp.403-425). Edward Elgar Publishing.

Wessel, R.A. (2019). Cybersecurity in the European Union: Resilience through Regulation? in E. Conde, Yaneva, Z., Scopelli, M. (Eds.), *Routledge Handbook of EU Security Law and Policy* (pp.283-301). Routledge.

Wessel, R.A. (2021). Chapter 23: European law and cyberspace. InTsagourias, N. & Buchan, R. (Eds.), *Research Handbook on International Law and Cyberspace* (pp.491-508). Edward Elgar Publishing.

Zeitlin, J. (2005). The Open Method of Coordination in Action In Zeitlin, J., Pochet, P., Magnusson, L.(Eds.), *The Open Method of Coordination In Action: the European Employment and Social Inclusion Strategies* (pp.19-33). P.I.E. – Peter Lang S.A.

ANNEX 1: Interview-Template following the example provided by Eliantonio et al. (2021, p.12-14)

Interview Outline

1. **Prelude**

1.1 Short Introduction

- About Myself: My name is Fee-Marie von der Brelie, I'm currently trying to obtain a Master of Arts degree at Leiden University in International Relations.
- About my Research: To obtain the Master of Arts degree in International Relations, I'm currently conducting research on the Europeanization of German and Slovakian main cybersecurity policies through European Union soft law. In the literature there is no agreed upon meaning of soft law; in the following when I talk about soft law, I shall refer to all types of EU instruments issued by the European Parliament, Commission, Council or the High Representative of the EU for Foreign Affairs and Security policy that are non-legally binding. Specific emphasis in the Interview will be for example put on the soft law instruments such as the the 2013 Joint Communication "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"[4]; the revised version published in 2017 by the European Commission called "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[5] and the 2020 Joint Communication "The EU's Cybersecurity Strategy for the Digital Decade"[6] issued by the High Representative of the EU for Foreign Affairs and Security

1.2 Why Interviewee has been selected

- Expert in the development/making of national cybersecurity policy and the implementation of national policy in the cybersecurity policy domain
- Explanation that for each country 1-3 interviews are carried out

1.3 Interview Material

- Stress that the interview will be used for scientific purposes only: Explain the conditions of the interview again. Mention specifically the use of individual sentences from the transcript of the interview and the potential use of the full name, job title, and the institute/company the interviewee works for in the final work. Stress what the interviewee has agreed to in his/her consent form
- Ask interviewee once again if he/she agrees to be recorded or talk without tape. Highlight that in the later case you will take notes manually

2. **Information on interviewee**

2.1 Could you briefly describe your professional background? Since when have you been in your current position? How do your daily tasks look like?

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:0001:FIN
[5] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450
[6] https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018

2.2 Could you briefly describe the development of the three German/Slovakian/EU Cybersecurity Strategies?

3. Usage and effects of Soft Law

3.1 How frequently do you deal with soft law instruments and in what kind of situations?

3.2 When dealing with soft law, what is your general impression of how soft law is understood in your working environment? Is it considered having relevance for political decision-making?

3.3 3.3 Now thinking specifically of the three German/Slovakian/EU Cybersecurity Strategies....

i. Do you know if policy-makers ever-make use of EU soft law instruments, like the 2013, 2017 or 2020 EU Cybersecurity strategy in the development of the national Cybersecurity Strategies?

ii. If not, why not? What are the arguments that speak against or for the use of EU soft law?

3.4 Can you describe the process that commonly leds to the decision to use/not to use these instruments?

i. ***Who decides whether to use these soft law instruments or not? What influences/motivates the usage of these instruments?***

- Need for clarification of hard law
- Easing the implementation of hard law
- Need for inspiration?
- Moving interpretation in a specific direction; which one?
- Soft law has been invoked by the parties (applicants, stakeholders, organizations etc.)
- Making sure that you are doing things right (vis-a-vis the Commission or Federal Government
- (Cross border) Peer pressure by collogues or cross boarder
- National legal or practical culture of using soft law

ii. ***Now, if you think back, hast the utilization of soft law like the strategies (by EU MS like Germany and Slovakia) changed over time?***

4. Judging Soft law

4.1 What do you think in general about the use/lack of use of EU soft law in the policy domain of cybersecurity?

- Acts as a catalyst for successful international corporation
- Is well-suited to deal with the complexity of European affairs, their diversity
- Is well-suited to regulate sensitive, cross- sectors
- Works well in situations where swift action of imperative

- Enhances discretion of some actors to the detriment of others
- Is inappropriate
- Something else?

5. Conclusion

5.1 Now that we have talked about the different aspects of EU soft law utilization is there anything I forgot to ask that is important in this context?

5.2 Are there any documents or reports you would/could recommend?

5.3 Are there other people I can talk to?

ANNEX 2: Coded Cybersecurity Strategies

EUCSS 2020

Key Components	Total: 65
Objectives *(long- and short-term goals)*	**1. Establish resilience, technological sovereignty, and leadership** **2. Establish operational capacity to prevent, deter and respond** **3. Establish advancing a global and open cyberspace**
Main Action Points *(actions that need to be taken to achieve the objectives)*	**1. <u>To establish resilience, technological sovereignty, and leadership</u>** - ***develop/reform/amend/implement/promote (EU/national/international) standards, norms, legislation and/or measures:*** • e.g., revise NIS Directive; legislation on the resilience of critical infrastructure • e.g., new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market (include duty of care norm) • the main Toolbox measures proposed in the "5G Cybersecurity Toolbox" by MS - ***capability building:*** • build a network of Security Operations Centers (SOC) across the EU & improve existing ones • deployment of a secure quantum communication infrastructure (QCI) to offer public authorities a brand-new way to transmit confidential information using an ultra-secure form of encryption and shield against cyberattacks and keep sensitive information and in turn critical infrastructure safe & deployment of a multi-orbital secure connectivity system • adoption of first Union Rolling Work Programme, under the Cybersecurity Act, in the first quarter of 2021, to allow industry, national authorities and standardization bodies to prepare in advance for future European cybersecurity certification schemes - ***protection of critical infrastructures:*** • find ways to deal with extreme scenarios affecting the integrity and availability of the global DNS [Domain Name System] root system. - ***implementation/maintenance of cybersecurity standards:***

	• encourage relevant stakeholders including EU companies, Internet Service Providers and browser vendors to adopt a DNS resolution diversification strategy • support the development of a public European DNS resolver service ('DNS4EU' initiative) • accelerate the uptake of key internet standards including IPv6 [Internet Protocol version 6] and well-established internet security standards and good practices for DNS, routing, and email security in MS and partner countries - ***research, development, and innovation & create culture of security: inform, educate, raise awareness*** • investment in Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centers (CCCN) & support, potentially with the CCCN, the development of a dedicated cybersecurity Master's program, and contribute to a common European Cybersecurity Research and Innovation Roadmap beyond 2020 • upskilling of the workforce, the development, attraction and retention of the best cybersecurity talent and investments in world class research and innovation - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • Commission, together with the EU Intellectual Property Office at Europol, ENISA, MS and the private sector, develop awareness tools and guidance to increase the resilience of EU businesses against cyber-enabled intellectual property theft **2. <u>To stablish operational capacity to prevent, deter and respond</u>** - ***develop/reform/amend/implement/promote (EU/national/international) standards, norms, legislation and/or measures:*** • complete the European cybersecurity crisis management framework • 2013 Directive on attacks against information systems by MS • implementation of the 'e-evidence package' and practical measures to provide appropriate channels and clarify rules to obtain cross-border access to electronic evidence for criminal investigations • Define EU's & MS cyber deterrence posture • update of the tools proposed in the cyber diplomacy toolbox & implementing guidelines • review of the Cyber Defense Policy Framework (CDPF) • EU "Military Vision and Strategy on Cyberspace as a Domain of Operations" for CSDP military missions and operations

	- ***capability building:***
	  • determine the process, milestones, and timeline for establishing a Joint Cyber Unit (JCU)
	  • facilitate the establishment of a MS cyber intelligence working group residing within the EU Intelligence and Situation Centre (INTCEN)
	  • development of state-of- the-art cyber defense capabilities
	- ***counter cybercrime:***
	  • *Security of Services delivered in cyberspace:* prevent abuse of domain names, including where appropriate for the distribution of illegal content, and pursue the availability of accurate registration data
	- ***research, development, and innovation:***
	  • more cyber defense research and innovation
	- ***strategic collaboration between public authorities, the private sector, academics, civil society:***
	  • support synergies between civil, defense and space industries
	- ***protection of critical infrastructures:***
	  • cybersecurity of critical space infrastructures
	
	3. <u>To establish advancing a global and open cyberspace</u>
	- ***develop/reform/amend/implement/promote (EU/national/international) standards, norms, legislation and/or measures:***
	  • the definition and promotion of a set of objectives in international standardization processes
	  • establish Strategy on the Rights of the Child
	  • strengthen and promote the Budapest Convention on Cybercrime
	  • propose an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board.
	- ***international cooperation:***
	  • establish Program of Action to Advance Responsible State Behavior in Cyberspace (PoA) in the United Nations (UN)
	  • strengthen and expand EU cyber dialogue with third countries, regional and international organizations on Internet governance and cyber norms and rules and especially NATO on cyber defense
	- ***strategic collaboration between public authorities, the private sector, academics, civil society:***
	  • reinforce the exchanges with the multi-stakeholder community, notably by regular and structured exchanges with the private sector, academia, and civil society

Inputs *(Resources made available for the implementation of the EUCSS)*	- ***tools & organizational components*** - ***legislative measures*** - ***processes & coordinating structures*** - ***plans/guidelines/information/ recommendations etc. on cyber- and information security*** - ***strategic investments*** - ***support research, development & innovation*** - ***support education, training, awareness*** - ***increasing law enforcement and judiciary capabilities*** - ***participation in international & regional cooperation***
Outputs *(Direct results of actions taken)*	- ***improved regulatory frameworks*** - ***improved capabilities*** - ***public-private partnerships*** - ***research & development*** - ***international cooperation*** - ***warning systems***
Outcomes and Impacts *(Outcomes = the short and medium-term results of strategy, while impacts = the longer term (e.g. 10+ years) results)*	- ***strengthened capabilities protecting critical information infrastructures, communication networks and services*:** - ***improved cybersecurity practices/procedures/standards:*** - ***stimulate technological capabilities and national private and academic initiatives in security and privacy*** - ***public-private relationships:*** - ***growing innovative workforce:*** - ***prevention & resilience against cyberthreats/attacks:*** - ***improved ability to counter online criminal activities:*** - ***ability to counter offensive cyber operations:*** - ***enhanced national security*** - ***international cooperation*** - ***international leading position*** - ***protection of fundamental rights and freedoms, notably the right to dignity, privacy and freedom of expression and information while guaranteeing security***
Evaluation *(provisions on a*	- **progress reports**

review and evaluation process for the strategy)	

Germany NCSS 2021

Key Components	Total: 83
Objectives *(long- and short-term goals)*	**1. Remaining safe and autonomous in a digital environment** **2. Government and private industry working together** **3. Strong and sustainable cyber security architecture for every level of government** **4. Germany's active role in European and international cyber security policy**
Main Action Points *(actions that need to be taken to achieve the objectives)*	**1. <u>To remain safe and autonomous in digital environment</u>** - ***increasing the user-friendliness of security solutions*** - ***develop/reform/amend/implement/ promote (EU/national/international) standards, norms, legislation and/or measures:*** • Expanding government measures to protect consumers in the digital world • Establishing uniform European security requirements • Guaranteeing IT security through AI and for AI - ***capability building****:* • Guaranteeing secure electronic identities • Creating the conditions for secure electronic communication and safe web offerings • Responding responsibly to vulnerabilities – promoting coordinated vulnerability disclosure - ***security of services delivered in cyberspace****:* • Protecting the authenticity and integrity of algorithms, data and documents, and the electronic identities of people and things in the broader sense • Using encryption – a prerequisite for self-determined, autonomous action – across the board

	2. <u>To achieve the government and private industry working together</u> - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • Improving cooperation between government, private industry, the research community, and civil society on matters of cyber security - ***capability building:*** • Reinforcing the coordination function of the NCSR in the cyber security landscape • Establishing a cooperative platform for government, private industry, the research community, and society to enable communication about cyber attacks • Protecting businesses in Germany • Providing IT security through quantum technology • Cyber security certification - ***strengthening Germany's digital economy*** - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation, and measures:*** • Creating a uniform European regulatory framework for businesses • Harmonizing testing and approval processes with innovation cycles (time to market) - ***research, development, and innovation:*** • Promoting research and development into more resilient, more secure IT products, services and systems for the EU single market - ***security of services delivered in cyberspace****:* • Strengthening the security of future technologies and key enabling technologies through "security by design**"*** • Securing the telecommunications infrastructure of the future - ***protection of critical infrastructures:*** • Improving the protection of critical infrastructures **3. <u>To achieve a strong and sustainable cyber security architecture for every level of government</u>** - ***capability building:*** • Developing the National Cyber Response Centre

	• Ramping up law enforcement in cyberspace • Strengthening cyber and information security in the federal administration • Expanding central skills and services of the BKA for combating cyber crime • Strengthening defense aspects of cyber security • Improving the options available to the Federal Government for threat prevention in case of cyber attacks • Equipping the technical and operational divisions of the BSI for the future and creating a network for them • Increasing the digital sovereignty of the security authorities by expanding the Central Office for Information Technology in the Security Sector • Raising the level of cyber security through increased preventive intelligence gathering • Strengthening institutionalized cooperation between the BSI and the states - ***security of services delivered in cyberspace***: • Providing security through encryption, and security despite encryption • Fostering responsible handling of zero-day vulnerabilities and exploits - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation, and/or measures:*** • Adapting telecommunications and telemedia law and other specialist legislation to technological progress - ***security of activities/actions delivered in physical world that have a cyber component*** • Stepping up cyber security associated with elections **4.Germany's active role in European and international cyber security policy** - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation, and/or measures:*** • Actively shaping effective European cyber security policy • Strengthening international law and the legislative framework for cyberspace and working towards responsible state behaviour - ***capability building:*** • Shaping cyber security and defense in NATO

	• Promoting confidence-building measures - ***international cooperation:*** • Strengthening bilateral and regional support and cooperation for cyber capacity building • Strengthening international law enforcement cooperation and combating international cyber crime • Working jointly in the EU on innovative solutions for combating crime more effectively
Inputs *(Resources made available for the implementation of the NCSS)*	- ***support education, training, awareness*** - ***plans/guidelines/information on cyber- and information security*** - ***tools & organizational components*** - ***strategic investments*** - ***support research, development & innovation*** - ***process & coordinating structures*** - ***legislative measures*** - ***increasing law enforcement and judiciary capabilities*** - ***participation in international and regional cooperation***
Outputs *(Direct results of actions taken)*	- **improved capabilities** - **research & development** - **improved regulatory frameworks** - **public-private partnerships** - **warning systems** - **international cooperation**
Outcomes and Impacts *(Outcomes = the short and medium-term results of strategy, while impacts = the longer*	- **awareness and a culture of security among citizen and institutions** - **improved cybersecurity practices/procedures/standards** - **greater public trust in safety of using cyberspace** - **greater public trust in technology** - **protection of (personal) data & privacy** - **ensure confidentiality, integrity, and accessibility of electronic information and services:** - **reduction or elimination of disruptions in the normal functioning of essential services that are vital to functioning of society:**

term (e.g. 10+ years) results)	- **protection & resilience against cyber threats/attacks** - **growing innovative workforce** - **public-private relationships** - **stimulation of technological capabilities and national academic initiatives in security and privacy knowledge:** - **better coordination and greater competence of public and private actors involved on the protection of critical infrastructure** - **ability to counter online cybercrime** - **Secure democratic elections** - **a balance between privacy, fundamental rights and liberties, and access to information within the need to guarantee security** - **ability to counter offensive cyber operations** - **international cooperation** - **International leading position**
Evaluation *(provisions on a review and evaluation process for the strategy)*	- **Cyber Security Council Assessment** - **Progress Reports** - **Regular reviews**

Germany 2016 NCSS

Key Components	**Total: 63**
Objectives *(long- and short-term goals)*	1. **Remaining safe and autonomous in a digital environment** 2. **Government and private industry working together** 3. **Strong and sustainable cyber security architecture for every level of government** 4. **Germany's active role in European and international cyber security policy**

Main Action Points *(actions that need to be taken to achieve the objectives)*	1. **<u>To remain safe and autonomous in a digital environment</u>** - ***create culture of security: inform, educate, raise awareness:*** • Promoting digital literacy among all users • Countering digital carelessness - ***research, development, and innovation:*** • Creating the conditions for secure electronic communication and safe web offerings • Advancing IT security research - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:*** • Making digitalization secure through legislative measures - ***capability building:*** • Strengthening certification and approval: Introducing a quality label for IT security • Security of services delivered in cyberspace: Creating the conditions for secure electronic communication and safe web offerings 2. **<u>To achieve government and private industry working together</u>** - ***protect critical information infrastructures:*** • Securing critical infrastructures - ***capabilities building & research, development, and innovation:*** • Protecting businesses in Germany • Strengthening Germany's IT industry - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • Creating a platform for sharing information on the basis of mutual trust **3. <u>To achieve a strong and sustainable cyber security architecture for every level of government</u>** - ***capabilities building:*** • Further developing the National Cyber Response Centre • Improving local analysis and response capability • Centre for Information Technology of Security Authorities (ZITiS) • Strengthening the defensive aspects of cyber security

	• Strengthening CERT structures in Germany • Using resources, recruiting, and developing staff - ***protection of critical infrastructures:*** • Keeping the federal administration secure - ***counter cybercrime:*** • Intensifying law enforcement in cyberspace to counter cybercrime - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • Working more closely with federal and state governments **4. <u>To achieve Germany's active role in European and international cyber security policy</u>** - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:*** • Actively shaping effective European cyber security policy • Further developing NATO's cyber defense policy - ***international cooperation*** • corporation with NATO regarding cyber defense • Bilateral and regional support and cooperation for cyber capacity building - ***capability building:*** • Shaping international cyber security • Strengthening international law enforcement
Inputs *(Resources made available for the implementation of the NCSS)*	- **support education, training, awareness** - **strategic investments** - **processes & coordinating structures** - **tools & organizational components** - **support research, development & innovation** - **legislative measures** - **increasing law enforcement and judiciary capabilities** - **plans/guidelines/ information on cyber- and information security** - **participation in international & regional cooperation**
Outputs	- **research & development**

(Direct results of actions taken)	- **improved capabilities** - **public-private partnerships** - **improved regulatory frameworks** - **international cooperation** - **warning systems**
Outcomes and Impacts *(Outcomes = the short and medium-term results of strategy, while impacts = the longer term (e.g. 10+ years) results)*	- **awareness and a culture of security among citizen and businesses:** - **confidentiality, integrity and accessibility of electronic information and services:** - **protection of (personal) data & privacy** - **greater confidence in security of IT products and services:** - **stimulate technological capabilities and national private and academic initiatives in IT security and privacy:** - **maintaining and promoting economic and social prosperity:** - **reduction of potential disruptions in the normal functioning of critical infrastructures that are vital for the functioning of society:** - **prevention & resilience of cyberthreats/attacks** - **improved ability to counter online criminal activity:** - **improved cybersecurity practices/procedures/standards:** - **enhanced national security:** - **ability to counter offensive cyber operations** - **strengthened capabilities to protect critical information infrastructures, communication networks and services** - **international cooperation:** - **international leadership position:** - **public-private relationships**
Evaluation *(provisions on a review and evaluation process for the strategy)*	- **Cyber Security Council Assessment** - **Progress Reports** - **Regular reviews**

Key Components	Total: 73
Objectives *(long- and short-term goals)*	**1. Reliable state prepared for threats** **2. Effective detection and clarification of cybercrime** **3. Resilient private sector** **4. Cybersecurity as an essential part of public administration** **5. Strong partnerships** **6. Well-educated professionals and well-educated public** **7. Building research and development capabilities in the field of cybersecurity**
Main Action Points *(actions that need to be taken to achieve the objectives)*	**1. <u>To achieve: Reliable state prepared for threats</u>** - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:*** • Creation and use of certification schemes for a wide portfolio of product types, processes, and services - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • Cooperation between the state and the citizen at the level of providing sufficient information and recommendations, and the implementation of actions that the citizen will tangibly experience as an increase in their own security and the security of the national cyberspace. - ***capability building:*** • building a sufficient professional personnel base for the information and cybersecurity governance system not only at national level but also at sectoral level. • Capability development to detect and handle cybersecurity incidents at all levels. • More improved technical, organizational and personnel security, based on the use of modern approaches to cybersecurity for detection and handling of cybersecurity incidents. • Effective cooperation of stakeholders at all levels in addressing information security and cybersecurity. • A well-configured process of technical, as well as political attribution of cybersecurity incidents.

	• systematic and continuous cybersecurity risk management across sectors. • Improving the detection of cybersecurity incidents at sectoral level, improving and simplifying the cybersecurity incident reporting not only for liable entities, but also in voluntary reporting. • Support of the competence of entities in the field of business continuity management **2. To achieve effective detection and clarification of cybercrime** - ***capability building & counter cybercrime:*** • sufficient capacities allocated to fight cybercrime, effective cooperation of stakeholders, speed of criminal proceedings as necessary detection and clarification of cybercrime • Better coordination of procedures in the field of cybercrime and their integration at international level. • Active cooperation in the field of cybercrime between stakeholders at national level and sharing of relevant information. • Specialization of prosecuting authorities in the field of cybercrime from basic departments of the police force up to the public prosecutor‘s office and courts. • More criminal acts of cybercrime reported and investigated. - ***create culture of security: inform, educate, raise awareness & counter cybercrime:*** • Development of education activities in the field of cybercrime. **3. To achieve a resilient private sector** - ***capability building:*** • sector-specific security requirements complementing the basic minimum legal requirements, ensuring high-level cybersecurity, with regard to sectoral needs and specifics. - ***create culture of security: inform, educate, raise awareness & protect critical infrastructures:*** • Cybersecurity awareness of operators of essential services and operators of critical infrastructure in the private sector as an essential part of their operation, not just as further state regulation. - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • Well-functioning public-private cooperation not only in the field of regulation, but especially in sharing of security information, experience and in further development. **4. To achieve Cybersecurity as an essential part of public administration**

	- ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:*** • **"**security by design" rule as mandatory in the design, procurement, creation, implementation and operation of the state's systems and services. - ***create culture of security: inform, educate, raise awareness:*** • A citizen must perceive that the services provided by the state, as well as their own activities, are safe. - ***capability building:*** • Risk management of cybersecurity and information security in public administration must be a viable process that minimizes risks at all stages of the system's life cycle from preparation of specification, procurement, architecture design, implementation, operation and maintenance up to decommissioning. The governance of cybersecurity and information security must be a natural part of the governance of public administration information systems. **5. To achieve strong partnerships** - ***international cooperation:*** • The Slovak Republic as a respected state with good representation abroad through professionally competent representatives at both technical and political levels. • increased involvement of the Slovak Republic in the activities of the European Cyber Security Organization (ECSO). - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • A healthy and strong partnership network established at national level between the state authorities, the state and the private sector, as well as academia and the professional public. - ***capability building:*** • A network of cybersecurity competence centers established at the European level, including the Slovak Competence and Certification Cyber Security Centre as a national representative in the Governing Board of the European Competence Centers. - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:*** • Defining the main foreign policy partners in the field of cybersecurity.

	6. To achieve well-educated professionals and well-educated public - ***create culture of security: inform, educate, raise awareness:*** • sustainable vocational higher education system and specialized trainings as forms of further education in the field of cybersecurity and information security. • The concept of basic security education at all levels of education, from primary schools to universities. • Systematic, broad-spectrum and planned situational and security awareness raising based on a reliable system that responds flexibly to changes in cyberspace. • Educated public administration staff who can safely provide services and use public administration systems without emerging cybersecurity incidents due to their low security awareness. **7.To build research and development capabilities in the field of cybersecurity** - ***research, development & innovation:*** • well-functioning and state-supported research and development in the field of cybersecurity. - ***strategic collaboration between public authorities, the private sector, academics, civil society:*** • A good communication between the public sector, the private sector and academia in the field of research and development with clear outcomes. - ***capability building:*** • An effective system of cooperation between the public sector, the private sector and academia. - ***international cooperation:*** • State support of cybersecurity projects and active state assistance in the use of European funds.
Inputs *(Resources made available for the implementation of the EUCSS)*	- ***tools & organizational components*** - ***legislative measures*** - ***processes & coordinating structures*** - ***support education, training, awareness*** - ***participation in international and regional cooperation*** - ***support research, development & innovation*** - ***strategic investment*** - ***plans/guidelines/information/recommendations etc. for cyber- and information security*** - ***increasing law enforcement and judiciary capabilities***

Outputs *(Direct results of actions taken)*	- ***Improved Capabilities*** - ***improved regulatory frameworks*** - ***public-private partnerships*** - ***Research & development*** - ***international cooperation***
Outcomes and Impacts *(Outcomes = the short and medium-term results of strategy, while impacts = the longer term (e.g. 10+ years) results)*	- **prevention & resilience against cyber threats/attacks:** - **innovative public services:** - **better coordination and greater competence and capabilities of public and private actors involved on the protection of critical (information) infrastructure:** - **greater public trust in technology:** - **improved cybersecurity practices/procedures/standards:** - **ability to counter online criminal activities:** - **international cooperation:** - **reduction and elimination of disruptions in the normal functioning of essential services that are vital for the functioning of society:** - **public- private relationships:** - **greater confidence in safety using cyberspace by citizen, business, and public sector:** - **awareness and a culture of security among citizen and institutions**: - **ability to counter offensive cyber operations** - **stimulation of technological capabilities and national academic initiatives in security and privacy knowledge:** - **international leadership position** - **enhanced national security** - **growing innovative workforce** - **strengthened capabilities protecting critical information infrastructures, communication networks and services**
Evaluation *(provisions on a review and evaluation*	- **Progress Reports**

process for the strategy)	

Slovakia 2015 NCSS

Key Components	Total: 60
Objectives *(long- and short-term goals)*	**1. Building an institutional framework for cyber security administration.** **2. Creating and adopting a legal framework for cyber security.** **3. Defining and applying basic mechanisms for securing the administration of cyber space.** **4. Supporting, preparing, and introducing a system of education in the area of cyber security.** **5. Defining and applying a risk control culture and a system of communication between the stakeholders.** **6. Active international collaboration.** **7. Supporting science and research in the area of cyber security.**
Main Action Points *(actions that need to be taken to achieve the objectives)*	**1. <u>To Build an institutional framework for cyber security administration.</u>** - ***capability building:*** • Formation of Central state administration body for cyber security • Formation of National Incident Resolution Unit (national CERT/CSIRT) • Sector oriented authority for cyber security • Incident resolution unit (government CERT/CSIRT, CERT/CSIRT XY) **2. <u>To Create and adopt a legal framework for cyber security.</u>** - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:***

	• the scope and method of the exercise of public authority in the area of cyber security by relevant central state administration bodies and other state bodies will be defined by a special law: *Cyber Security Act* • establishment of binding *terminology and standards* for the area of cyber security • issue of a *methodical guidance* for the practical application of the Act and of standards in the system of the sector's management and operation. **3. <u>To define and apply basic mechanisms for securing the administration of cyber space.</u>** - ***capability building:*** • establishment of decision-making control mechanisms • establishment of prevention mechanisms • establishment of reaction mechanisms • establishment of restoration mechanisms **4. <u>To supporting, prepare, and introduce a system of education in the area of cyber security</u>** - ***create culture of security: inform, educate, raise awareness:*** • Spreading knowledge and raising awareness. • General educational system in the Slovak Republic at the levels of: Primary education, Secondary education. • Specialized educational system at the levels of: Secondary education, University education, Experts. **5. <u>To define and apply a risk control culture and a system of communication between the stakeholders.</u>** - ***capability building:*** • To set up control and executive structures optimally, with clearly defined powers and competences

	• To implement relevant supporting information, communication and control systems as well as secure systems: exchange of information, early warning and coordinated reaction. - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures*** • To prepare and introduce relevant methodologies and standards for communication and exchnage of information between stakeholders **6. <u>For Active international collaboration</u>** - ***international cooperation:*** • joint use of information and coordination of activities with EU & NATO • develop bilateral collaboration with nations sharing identical values. - ***develop/reform/amend/promote (EU/national/international) standards, norms, legislation and/or measures:*** • drawing up international strategic and conceptual documents, international policies and standards - ***capability building:*** • build the most efficient model of cooperation, exchange and joint use of information between different CERT and CSIR-type offices. - ***create culture of security: inform, educate, raise awareness:*** • organize and participate in international cyber trainings and exercises.

	7. <u>To support science and research in the area of cyber security</u> - ***strategic collaboration between public authorities, the private sector, academics, and civil society:*** • cooperation of the public sector with the private sector and the academic institutions, - ***research, development & innovation:*** • support the development of cooperation in research projects (including qualitative and quantitative research). • support participation in national as well as European research projects and activities in the area of cyber security, stressing the use of funds from the Research and Innovations Operating Programme for the 2014 - 2020 programming period. - ***capability building:*** • support the private sector and academic institutions in the development and implementation of information and communication technologies aimed at the protection of cyber space and in the development thereof
Inputs *(Resources made available for the implementation of the NCSS)*	- **processes & coordinating structures** - **tools & organizational components** - **legislative measures** - **strategic investments** - **support education, training awareness** - **plans/guidelines/information/recommendations etc. for cyber- and information security** - **support research, development & innovation** - **participation in international and regional cooperation**
Outputs	- **improved capabilities**

(Direct results of actions taken)	- **improved regulatory framework** - **warning systems** - **international cooperation** - **research & development** - **public-private partnerships**
Outcomes and Impacts *(Outcomes = the short and medium-term results of strategy, while impacts = the longer term (e.g. 10+ years) results)*	- **prevention (& resilience) against cyber threats/ attacks** - **enhanced national security** - **improved cybersecurity practices/procedures/standards:** - **awareness and a culture of security among citizen, businesses and institutions** - **better coordination and greater competence of public and private actors involved in the protection of critical (information) infrastructure** - **public-private relationships** - **International cooperation** - **International leadership position** - **protection of fundamental rights and freedoms, notably the right to dignity, privacy and freedom of expression and information while guaranteeing security** - **growing innovative workforce**
Evaluation *(provisions on a review and evaluation process for the strategy)*	- **Progress Reports**