Master thesis on European Politics and Society

Universitat Pompeu Fabra

Towards coherent cybersecurity in the EU? The impact of the NIS Directive implementation on the European cyberspace

Inel Shalabayev

Supervisor: Prof. Josep Ibáñez

Word count (excluding appendixes): 12642

June 2022

EPS { European
Politics
and Society

upf. Universitat
Pompeu Fabra
Barcelona

Abstract

To what extent is the EU's cybersecurity framework coherent? Coherence, defined as a shared understanding of security and institutional cooperation in the scope of this paper, has been a vital objective in developing European cybersecurity. Even though the EU has placed significant emphasis on the development of coherence in its cyber domain to ensure a consistent response between national actors during cross-border attacks, few studies have attempted to evaluate the coherence of the policy area. Moreover, few to none have focused on the Directive on security of network and information systems (NIS Directive), the first and only EU-level legislation intended to improve national capabilities and enhance cross-border collaboration. In light of this, the purpose of this study is to fill a gap in the academic literature by focusing on the implementation of the NIS Directive by the Member States and studying its effect on the coherence of European cybersecurity. To do so, it employs qualitative content analysis to examine the impact of national cybersecurity strategies and operators of essential services as part of the Directive's implementation on the shared understanding of security and institutional cooperation. The research finds that while most Member States tend to have a shared understanding of cybersecurity, the flexibility of the Directive has led to inconsistencies between the Member States, weakening institutional cooperation and coherence of European cybersecurity. In light of the ongoing development of the NIS2 Directive, this paper urges policymakers to address the flexibility in the new version to ensure institutional cooperation between Member States in the protection of networks and information systems.

Table of Contents

1. Introduction

Coherence has always been an essential objective in the European Union (henceforth, EU). Today, references to the concept can be found in many EU-related works. For instance, the Council concluded in 2000 that "reinforcing the coherence of the Union's external action and realising its policy objectives are priorities if the Union is to pull its full weight in international affairs" (Council, 2000, p. 7). In addition, the European Security Strategy of 2003 highlighted the need for greater coherence between EU institutions and among the external activities of individual Member States for successful policymaking (Council, 2003). The European Commission further emphasised the need for greater coherence in the EU to defend fundamental values and interests, advance critical political objectives, avert crises, and contribute to framing consistent policies (European Commission and HREU, 2013b).

The development of coherence has been especially prominent in European cybersecurity. Acknowledging that the cyber sector has become the cornerstone of European society, the EU has made coherent cybersecurity a top priority (Carrapico and Barrinha, 2017). Coherent interactions are critical in the sector because cyberspace requires coordinating multiple institutions, agencies, and Member States to address even a single incident. In this light, this paper aims to evaluate coherence in the context of European cybersecurity. The assessment is critical, as very few scholars have previously analysed the coherence of cybersecurity in the Union. Some argued that EU cyberspace is inconsistent due to insufficient financial resources and the underlying nature of the European cybersecurity policy (Christou, 2016; Carrapico and Barrinha, 2017). However, few to no studies have examined the impact of the Directive on the security of network and information systems (henceforth, NIS Directive) on the coherence in the cyber domain. The Directive, adopted in 2016, is the first piece of EU-wide cybersecurity legislation. Its purpose is to promote advanced preparedness and coherent interaction between the Member States in the cyber domain (Markopoulou, Papakonstantinou and Hert, 2019). In this light, assessing the Directive implementation by the Member States helps evaluate coherence within European cybersecurity, as the legislation is viewed as one of the most significant steps taken by the EU to establish cross-border collaboration against cyber threats.

The NIS Directive requires Member States to adopt national strategies on network and information security and identify operators of essential services according to the legislation (Directive (EU) 2016/1148, 2016). However, the Directive also permits national actors to consider domestic circumstances when enforcing security obligations, which could lead to variations within the EU (Markopoulou, Papakonstantinou and Hert, 2019). As a result, only 11 member states complied with the requirements of the NIS Directive before the deadline (Irwin, 2018). The diverging compliance begs the following research question: how does the implementation of the NIS Directive affect the coherence of the European cybersecurity?

The paper seeks to contribute to both the coherence and cybersecurity literature. Where the first is concerned, the paper contributes by offering a dual definition of coherence as a shared understanding of security and institutional cooperation and operationalising the term as a research object. Regarding the latter, the paper provides the first comprehensive analysis of the implementation of the NIS Directive and its impact on coherence within the context of European cybersecurity. In addition, the paper provides a comprehensive theoretical framework for evaluating European cybersecurity by introducing securitisation and liberal intergovernmentalism as complementary theories to explain the evolution of EU cyberspace in the context of coherence. The paper argues that the flexibility provided by the NIS Directive has resulted in the uneven implementation of cybersecurity policies by the Member States, weakening the coherence of the European regulation of cyberspace.

The structure of the paper is composed of three main sections. The first section examines coherence and its conceptualisation in the context of EU cyberspace. The second section explores securitisation and liberal intergovernmentalism as explanatory frameworks for evolving European cybersecurity in the context of coherence. The third section employs qualitative content analysis to analyse the implementation of the NIS Directive and its effect on the coherence of European cybersecurity. The paper's conclusion urges policymakers to evaluate flexibility in drafting the NIS2 Directive.

2. Conceptualising Coherence in the Context of Cybersecurity

Coherence has been the subject of lengthy scholarly and policy debates in the framework of the EU. Despite the broad usage of the term in the literature and political discourse, the concept of coherence is arguably one of the most commonly misunderstood and misinterpreted terms in EU foreign policy (Gebhard, 2011). Until the 1970s, the term was primarily used in conjunction with the concept of cohesion to describe political unity and the potential advantages of government cooperation on international matters (Gebhard, 2011). With the establishment of European Political Cooperation, coherence has been increasingly defined as "the ambition and necessity to bring together different strands of the EU's external relations, both strategically and procedurally" (Gebhard, 2011, p. 105). While the notion of coherence has been a source of contention for over four decades, the definition of the term remains intrinsically vague to this day. Some scholars have previously equated the term with efficiency (Hill, 1993). On the other hand, Portela and Raube (2011) have equated coherence with the absence of contradictions between policies. Others have also defined coherence as consistency, arguing that separating the two concepts ultimately results in "linguistic pedantry" (Nuttall, 2005, p. 93). This view contrasts with that of Missiroli (2001), who argued that coherence and consistency have distinct meanings, with the latter often serving as a necessary component of the former.

The literature has also recognised different types of coherence in the context of the EU. According to Gebhard, there are four primary forms of coherence: vertical, horizontal, internal/intra-institutional, and external/inter-organisational coherence. "Vertical coherence" examines the interaction between the EU and its member states (Gebhard, 2017, p. 109). "Horizontal coherence" examines the link between intergovernmental and supranational actors at the EU level (Gebhard, 2017, p. 110). "Internal or intra-institutional coherence" is linked with the EU's management of its foreign relations (Gebhard, 2017, p. 111). Finally, "external or inter-organisational coherence" concerns the EU's interaction with other parties, such as the United Nations and NATO (Gebhard, 2017, p. 112).

Although the definitional discourse is necessary, this work does not intend to enter the conceptualisation discussion. In the framework of this research, the essay will adhere to the definition in the EU documents. The decision is supported by the objective of this paper, which is to evaluate the European coherence as a cybersecurity actor by analysing its own proposed objectives and policies. According to the European Commission (2006), greater coherence is accomplished through the establishment of a "political agreement among the Member States on the goals to be achieved through the EU" (p. 5). In other words, a shared understanding of the cybersecurity objectives is necessary for coherent interaction. In addition, the European Commission's (2006) document emphasises the necessity of clearly defined "roles and responsibilities of the EU institutions and legal environment" (p. 6). Thus, a coherent framework further requires consistent institutional interaction. Carrapico and Barrinha (2017), who evaluated the coherence of European cybersecurity, used a similar dual definition of the concept as a shared understanding of security and institutional cooperation. A twofold definition of coherence is useful for this paper because it enables the concept to be operationalised effectively by providing two distinct variables. Therefore, employing the definition outlined by the EU and the literature, this paper offers a twofold definition of coherence as a shared understanding of security and institutional cooperation. Furthermore, since the study concentrates on the connection between the Member States and the EU in cyberspace, the article will primarily examine vertical coherence.

2.1. Shared understanding of security

Coherence within a shared understanding of security entails examining how various actors, particularly Member States, define security and identify the risks to address them with appropriate and coherent policy measures (Carrapico and Barrinha, 2017). In this regard, coherence, in the context of European cybersecurity, is one in which the Member States share similar views on security and threats in the cyber sphere. In the past, Member States have already made significant progress in developing a shared understanding of security to counter human trafficking and terrorism (Calderoni, 2010). While less progress has been made in the cybersecurity policy area, the EU has still made concerted efforts to foster a shared awareness of cyber threats over the years. An example is the establishment of non-binding agreements, such as the "eEurope 2002 - Action Plan", aimed at increasing Member States' awareness of the cyber threat at the EU level (Carrapico and Barrinha, 2017, p. 1259). Additionally, legally binding instruments were adopted, such as the "Council Framework Decision on Attacks against Information Systems", intending to reinforce a shared understanding of security as a critical component of efficiency in defending the EU against cyber-attacks (Carrapico and Barrinha, 2017, p. 1260).

The publishing of the first EU Cybersecurity Strategy (henceforth, EUCSS) in 2013 was one of the most committed and deliberate efforts to foster coherence as a shared understanding of security (Fuster and Jasmontaite, 2020). The strategy, which recognised cybersecurity as a new policy area, resulted from a collaborative effort between the European Commission and High Representative Catherine Ashton (Carrapico and Barrinha, 2017). The EUCSS aimed to bring together disparate policy areas of European cyberspace to establish a shared framework with common directions and principles (European Commission and HREU, 2013a). In other words, the strategy aimed to foster a shared understanding of cybersecurity across the Member States to secure and sustain the resilience and efficiency of the European digital space. The EUCSS further recognised the importance of the private sector in the cyber domain, calling Member States to establish a framework protecting the network and information security (NIS), paving the way for the adoption of the NIS Directive.

The 2013 EUCSS vision is based on five major strategic priorities that establish a common framework of understanding across the EU's cyber domain. The first priority, "achieving cyber resilience," emphasises the development of capacities for effective collaboration in countering cyber risks and threats on a transnational level (European Commission and HREU, 2013a, p. 5). Furthermore, the priority outlines cybersecurity as a shared responsibility for the Member State by calling for establishing "common minimum requirements for NIS at national level" through the adoption of national cybersecurity strategies (European Commission and HREU, 2013a, p. 5). The second priority, "drastically reducing cybercrime", focuses on effective laws to combat cybercrime, most notably by urging Member States to ratify the Council of Europe's Convention on Cybercrime (European Commission and HREU, 2013a, p. 9). The third priority, "developing cyberdefence policy and capabilities related to the Common Security and Defence Policy", emphasises the need to foster a shared understanding of roles and responsibilities between civilian and military approaches to safeguard critical cyber assets (European Commission and HREU, 2013a, p. 11). The fourth priority, "develop the industrial and technological resources for cybersecurity", aims to foster the adoption of common NIS standards in both public and private sectors to maintain the security of the supply chain in vital economic sectors (European Commission and HREU, 2013a, pp. 12-13). Finally, the fifth priority, "establish a coherent international cyberspace policy for the EU and promote core EU values", highlights the importance of a consistent EU international cyberspace policy by establishing a common understanding of cybersecurity between the EU actors, including the Commission, the High Representative, and Member States (European Commission and HREU, 2013a, p. 14). The priority further emphasised the need for collaboration and shared understanding among NIS competent authorities to ensure coherent international cyberspace (European Commission and HREU, 2013a, p. 16).

To further strengthen the shared understanding of cybersecurity, the EU revised its 2013 EUCSS in 2017. The revision came due to the growing number of cyber incidents, pushing the EU further to bolster its cyber resilience (Cerulus, 2020). The updated strategy focused on strengthening Europe's NIS while further elaborating on a common ground of understanding between EU actors (Bendiek, Bossong and Schulze, 2017). Notably, the strategy called for the full implementation of the NIS Directive by the Member States to ensure a prudent cybersecurity system across the EU (European Commission and HREU, 2017). With the 2013 EUCSS remaining in place, the revised 2017 version outlined three new priorities to foster a better understanding of security threats. In brief, the updated strategy emphasises the need for

(1) “building EU resilience to cyber-attacks”, (2) “creating effective EU cyber deterrence”, and (3) “strengthening international cooperation on cybersecurity” (European Commission and HREU, 2017, pp. 3-18) Although neither version of EUCSS is legally binding, the strategies play an essential role in establishing a common ground of understanding between the Member States. In addition, the strategies elaborate the role of EU agencies, such as the European Union Agency for Cybersecurity (ENISA), thereby facilitating the establishment of shared responsibilities among EU institutions and actors (Fuster and Jasmontaite, 2020).

The EU also presented its latest strategy in December 2020, elaborating additional grounds for a shared understanding of cybersecurity. The 2020 EUCSS reflected “an ambitious plan on increasing coherence within the policy” while emphasising EU cooperation in cyberspace with the rest of the world (Kasper and Vernygora, 2021, p. 34). In brief, the EU outlined three main dimensions in its latest cybersecurity strategy. The first dimension, “resilience, technological sovereignty, and leadership,” emphasises the need for additional legislation to decrease discrepancies throughout the EU in cyber defence (European Commission and HREU, 2020, p. 5). More importantly, the strategy called for the revision of the NIS Directive “to increase the level of cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society” (European Commission and HREU, 2020, p. 5). Additionally, the dimension advocates for establishing a “European Cyber Shield”, allowing for more coherent information exchange between actors to ensure timely response against cyber threats (European Commission and HREU, 2020, p. 6). The second dimension, “building operational capacity to prevent, deter, and respond”, recognises the critical nature of establishing a Joint Cyber Unit, serving as a platform for collaboration between cybersecurity communities (European Commission and HREU, 2020, p. 13). The third and final dimension of the revised strategy, “advancing a global and open cyberspace”, highlights the role of the EU as a global leader in its vision of cyberspace (European Commission and HREU, 2020, pp. 19-20). The dimension further emphasises the significance of expanding cyber capabilities across the Member States through the “EU External Capacity Building Agenda” to establish a shared understanding of security and tackle growing challenges in the cyber domain (European Commission and HREU, 2020, p. 22).

Given that the European cybersecurity policy space is inherently complex and fragmented, the framing of the strategies at the EU level is regarded as a significant step in fostering a shared understanding of security. In other words, the development of the EU strategies can be understood as an attempt to unify diverse policy fields, including cyber defence, global cyberspace, cybercrime, and cyber resilience, under the umbrella term cybersecurity (Fuster and Jasmontaite, 2020). While the European Cybersecurity Strategies have played a significant role in defining the cyber domain, implementing a cyber security policy at the national level is especially important in promoting a shared understanding of security (Stitilis, Pakutinskas and Malinauskaite, 2016). However, due to inherent differences at the national level, it is deemed more difficult to develop a shared understanding among the Member States. Several reports in the past have indicated variation in cybersecurity policies at the national level. For instance, according to BSA (2015), "considerable discrepancies exist between Member States' cybersecurity policies," resulting in cybersecurity gaps throughout the EU (p. 1). Several scholars explained the differences in national cybersecurity strategies due to states' varying levels of development in the cyber domain (Sabillon, Cavaller and Cano, 2016). Others explained the disparities to the lack of EU-level coordination (Stitilis, Pakutinskas and Malinauskaite, 2016). Although variations at the national level have been documented, few to no studies have compared the most recent national strategies of Member States since the adoption of the NIS Directive. It is vital to compare national strategies after the Directive's adoption, as the legislation sought to bridge the gap between national actors to establish a common network and information system security framework. Moreover, none compared the most recent national cybersecurity strategies for the presence of a shared understanding. In this light, it is crucial to examine variations in the latest national cybersecurity strategies after implementing the NIS Directive. Therefore, this paper aims to answer how the implementation of national cybersecurity strategies affects shared understanding of cybersecurity?

2.2. Institutional cooperation

Coherence within institutional cooperation entails the consistent implementation of processes, instruments, and policy outputs by actors when addressing transnational security concerns (Brattberg and Rhinard, 2012). In other words, institutional cooperation in the framework of European cybersecurity is characterised by consistent response between EU actors, particularly the Member States, when confronted with cyber-attacks. Institutional cooperation is essential in establishing coherent cyberspace, given that the EU is highly decentralised, with numerous relevant bodies, including the ENISA, the Council of Europe, the European Cybercrime Centre, and the European Defence Agency (Carrapico and Barrinha, 2017). Over the years, the EU has made significant rhetorical efforts to support the development of shared policy outcomes in the cyber domain. Cybersecurity was even recognised as the priority area in the 2016 European Global Strategy, which called for the development of cooperation between EU institutions and actors (Carrapico and Barrinha, 2017). Significantly, considerable effort has been devoted to harmonising the Member States' infrastructure and capabilities to ensure consistent cooperation between the private and public sectors (Carrapico and Barrinha, 2017).

The adoption of the NIS Directive in July 2016 marked a turning point in the pursuit of institutional cooperation. The Directive aimed to set a baseline of legally binding security standards for protecting network and information systems in the Member States (Ducuing, 2021). Often referred to as the "EU's first cybersecurity law", the NIS Directive is the first EU-level horizontal legislation that covers the protection of a wide range of critical infrastructure (Ducuing, 2021, p. 1). Structurally, it is comprised of 27 articles. The first six articles establish the scope and primary definition. Articles 7 to 10 outline the requirements for the Member States to establish national frameworks for network and information systems security. The collaboration mechanism between EU actors is outlined in articles 11–13. Articles 14 to 18 specify the security criteria for operators of essential services and digital service providers. Articles 19 and 20 address the establishment of standards and the method of voluntary notice. The final seven articles include the concluding provisions of the Directive (Directive (EU) 2016/1148, 2016).

The primary goal of the NIS Directive is to enhance the coordination and coherence between EU institutions and Member States on IT security via EU cybersecurity regulation. As means of achieving this objective, the Directive obliges "all Member States to adopt a national strategy on the security of network and information systems" (Directive (EU) 2016/1148, 2016, article 1(2)). Furthermore, Member States must designate a national single point of contact to guarantee cross-border collaboration (Directive (EU) 2016/1148, 2016). The legislation additionally emphasises the need to (1) take the necessary technological and organisational steps to manage risks to NIS and (2) inform the authorities without undue delay of any serious security incident to maintain the continuity of essential services and prevent widespread blackouts (Directive (EU) 2016/1148, 2016, article 14(1)(3)).

At its core, the NIS Directive is primarily concerned with the security of two broad categories: digital service providers (henceforth, DSPs) and operators of essential services (henceforth, OES) (Directive (EU) 2016/1148, 2016). The former, DSPs, include "any legal person that provides a digital service" (Directive (EU) 2016/1148, 2016, article 4 (6)). More specifically, DSPs fall into three broad subcategories: online market place, online search engine, and cloud computing service (Directive (EU) 2016/1148, 2016, article 4 (17)(18)(19)). The first subcategory, the online market place, allows consumers and traders to finalise online sales or service contracts via the online website of the marketplace. The second subcategory, the online search engine, enables users to search across all websites per the query. Finally, the third category, cloud computing services, provides access to a shared pool of scalable and elastic computing resources (Directive (EU) 2016/1148, 2016). To ensure a uniform approach among national actors, the NIS Directive does not require the Member States to identify DPSs further, as all three subcategories are explicitly outlined in the legislation (Markopoulou, Papakonstantinou and Hert, 2019). DPSs are a critical component of network and information security since many organisations rely on these providers to supply their services. As a result, an interruption of the DPSs may negatively affect the vital economic and social operations of the EU.

The second category, OES, is defined as any public or private entity that "provides a service which is essential for the maintenance of critical societal and/or economic activities" (Directive (EU) 2016/1148, 2016, article 5(2)). Annex II of the Directive outlines a list of sectors and subsectors that must be classified as OES.[1] However, contrary to the catch-all approach in the identification process of DPSs, not all OES fall under the NIS Directive. Member States can classify additional services as OES if (1) they deem the entity to be "essential for the maintenance of critical societal and/or economic activities", (2) "provision of that service depends on network and information systems", and (3) "an incident would have significant disruptive effects on the provision of that service" (Directive (EU) 2016/1148, 2016, article 5(2)). As a result, the categorisation and designation of OES are delegated to the Member States (Markopoulou, Papakonstantinou and Hert, 2019). All critical entities under the definition outlined by the Directive must adhere to the security and notification requirements. Once an entity has been classified, the Member States must conduct an identification procedure and implement national measures (Directive (EU) 2016/1148, 2016). The first deadline was set by November 9, 2018, in which the Member States were required to identify the operators of essential services for each sector and subsector. The Member States must update this list of designated operators of essential services at least every two years to ensure accuracy in the changes in the market (Markopoulou, Papakonstantinou and Hert, 2019).

The flexibility afforded to the Member States in identifying OES is one of the shortcomings of the NIS Directive, which may compromise institutional cooperation. According to the article

[1] The following sectors (and subsectors) are outlined: energy (electricity, oil and gas), transport (air, rail, water, and road transport), banking, financial market infrastructure, health sector (health care settings), drinking water supply and distribution, and digital infrastructure ((Directive (EU) 2016/1148, 2016, Annex II).

1 (7) of the NIS Directive, Member States are required to ensure the protection of OES and to notify incidents, “provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive” (Directive (EU) 2016/1148, 2016, Article 1(7)). In other words, the Directive is regarded as les generalis because it simply outlines a legal minimum security standard (Ducuing, 2021). Consequently, the precise procedures and standards for recognising OES are the sole responsibility of each Member State. The flexibility is especially problematic because, in contrast to DPSs, which are subject to the NIS Directive upon transposition of the legislation into national law by the Member States, OES are not subject to the regime of the NIS Directive until they are designated as such by the respective countries (Ducuing, 2021). As such, a lack of uniformity across the Member States in designating OES may eventually lead to poor institutional cooperation and a lack of coherence when addressing cyber events affecting the security of network and information systems.

The EU has implicitly acknowledged shortcomings in the NIS Directive by proposing the NIS2 Directive in December 2020, only four years after the adoption of the initial proposal (Dragomir, 2021). A year later, in December 2021, the Council approved a draft of the revised Directive, reaching an agreement on steps for a high, unified level of cybersecurity throughout the EU (O’Donoghue, 2022). The NIS2 Directive intends to replace its predecessor to address the rising dangers presented by growing digitalisation (Karniyevich, 2021). One of the most significant changes in the new Directive is an expansion of the reach of the previous legislation, as it aims to extend the number of critical entities covered. For instance, the revised Directive plans to include the public administration and the production of medical equipment as operators of essential services (O’Donoghue, 2022). In this regard, the NIS2 Directive can be viewed as an evolution of the current Directive, as it maintains the same fundamental structure while expanding the scope of the law. However, simply expanding the scope of the Directive without addressing the flexibility of the law may not resolve potential uniformity problems between the Member States in identifying OES. Thus, it is essential to determine if national actors’ current identification of OES hinders institutional cooperation. The assessment is especially relevant given that the NIS2 Directive is still in the drafting process. Thus, it is essential to investigate the shortcomings in the current Directive to prevent them from being included in the revised version. In this light, it is critical to explore how the Member States’ identification of OES affects institutional cooperation in cybersecurity?

3. Analysing Cybersecurity Coherence through Theory

Little to no literature has offered a comprehensive theoretical framework for assessing the coherence of European cybersecurity. The lack of theoretical explanation is particularly problematic, as scholars have been divided in evaluating the coherence of the EU cyberspace. On the one hand, several scholars have argued that the EU policies in cyberspace are becoming more coherent. For instance, Wolff and Ladi (2020) suggest that the COVID-2019 pandemic, characterised by a surge in misinformation and cyberattacks, reaffirmed the ideation continuity of current cybersecurity measures. Additionally, over the past years, the EU has expanded its efforts to close the gap in the human dimension of cybersecurity, allowing for a more consistent framework of collaboration across organisations within the EU (Blazic, 2021). On the contrary, others have argued about the lack of coherence of the EU cybersecurity policy. Christou (2016), for example, asserts that the EU's cybersecurity policy suffers inconsistencies due to inadequate financial resources, unclear division of work, and a shortage of personnel. Carrapico and Barrinha (2017) bolster this argument further by claiming that, although the EU expressly advocates for cohesive cyberspace, its reach is severely constrained by Member State reluctance and the underlying nature of the EU's cybersecurity policy.

Given that the literature differs in evaluating the coherence of European cybersecurity, it is crucial to provide comprehensive theoretical frameworks to evaluate the policy area. This paper proposes to examine European cybersecurity from two theoretical perspectives: securitisation and liberal intergovernmentalism. While both theories serve distinct purposes in the context of European cybersecurity, they are viewed as complementary in the scope of this research. On the one hand, securitisation theory helps understand the development of shared understanding at the EU and national levels as a result of securitisation in the cyber domain. On the other hand, liberal intergovernmentalism theory is essential in explaining cybersecurity integration, particularly in adopting the NIS Directive and its impact on institutional cooperation.

3.1. Securitisation theory

The securitisation theory of the Copenhagen School, originally developed by Ole Waever in the late 1980s, is described as a socially constructed process of "labelling something a security issue that it becomes one" (Waever, 2004, p. 13). Before defining the term, it is essential to elaborate on several concepts often used in discussing the securitisation theory. The first is the "securitising actor", who initiates securitisation; the second is the "referent object" that the securitising actor deems to require securitisation; and the third is the "audience", which must be persuaded of the vulnerability of the referent object and the need for extraordinary actions to safeguard it (Balzacq, 2011, p. 3). The term "securitisation" itself is often defined as "the discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the treat" (Buzan and Waever, 2003, p. 491). In other words, by asserting that the existence of a specific referent object is threatened, a securitising actor asserts the right to take extraordinary steps to ensure the survival of the referent object (Taureck, 2006). According to this perspective, there is no separation between a "real threat" and a "perceived threat"; instead, there is simply an intersubjective understanding of a threat (Hjalmarsson, 2013, p. 3). From this perspective, securitisation is inherently a socially constructed process.

The securitisation theory appears to provide an ideal foundation for comprehending European cybersecurity. Notably, at the EU level, the Union is perceived as a securitising actor due to its growing efforts to address cyber threats. According to Christou, one of the major catalysts in the securitisation process of cybersecurity was the Russian-sourced distributed denial of service attacks on Estonian infrastructure and institutions in spring 2007. Several high-profile cyberattacks followed on the EU institutions, including the European Commission, the European External Action Service, and the European Parliament (Christou, 2018). In addition, there has been a continuous growth in daily cyber breaches and cyber-disruptive technologies over the last decade (ENISA, 2016a). While no single event sparked the securitisation process, it nonetheless arose as a response to identified external forces compelling the EU to promote a shared understanding of security (Christou, 2018). Through the lens of securitisation theory, one could argue that the EU has sought to develop an intersubjective understanding of security, treating cyber incidents as an existential threat. As a result, the Union was able to take comprehensive measures to protect the cyber domain.

Continuous rhetoric over the increasing number of cyber-attacks has dominated the EU, prompting the securitisation of cybersecurity. According to Strizel (2007), the speech act is one of the essential tools for establishing security. Similarly, many EU representatives have referred to the urgency of action necessitated by an existential threat in the cyber domain through performative speech. One example is the statement made in 2017 by the rapporteur of the European Parliament, Elissavet Vozemberg-Vrionidi, who characterised cyberattacks as an existential concern that risks destroying democratic nations. The rapporteur advocated for increased cooperation between EU institutions and Member States to address shortcomings in the ability of the Union to combat cyber-attacks (European Parliament, 2017). Another example is Caterina Chinnici, a member of the European Parliament, who stated that cyber-attacks are the greatest risks the Union faces and called for a coherent legislative framework in Europe to effectively detect cybercrimes and combat threats (European Parliament, 2017). Julian King, the former European Commissioner for the Security Union, has also expressed alarm about the rising number of cyber-attacks and advocated for the strengthening of collaboration to overcome cyber vulnerability within the EU (Singh, 2017). Similarly, the former president of the European Commission, Jean-Claude Juncker, has brought attention to the lack of capacity in cyber defence of the EU. Juncker has further emphasised the risk posed by cyber-attacks to stability and democracy, advocating for harmonisation and coherence between the Member States in cybersecurity (European Commission, 2017). Altogether, it is evident that the EU representatives have continuously developed a securitisation narrative, calling for a shared understanding of cybersecurity.

The European Cybersecurity Strategies constitute one of the EU's most extensive efforts to secure the cyber domain. The underlying rationale for adopting the 2013 EUCSS is evident from a statement by the European Commission, which prompted the development of the strategy. Specifically, the Commission stressed the importance of internet and digital technologies for the EU economies and society and the increased vulnerability of the policy area towards the growing number of cyber assaults (European Commission, 2011, p. 2). In other words, the perceived "existential threat" posed by cyberattacks prompted the EU to securitise its cyber domain via the 2013 EUCSS that aimed to establish a single framework of intersubjective understanding of security and threats. The introduction of the second and third European Cybersecurity Strategies, the EUCSS 2017 and the EUCSS 2020, respectively, has further acknowledged the growing threat in the cyber realm, requiring coordinated action from national governments to prevent cyberattacks. All three strategies have also recognised the significance of EU-level engagement by outlining the roles and responsibilities of EU bodies, including the European Commission and ENISA (Christou, 2018; Dutton et al., 2022). Consequently, the EU Cybersecurity Strategies urged the securitisation of both Member States and EU institutions by identifying intersubjective understanding of security against existential threats in the cyber realm.

Adopting the NIS Directive was another critical step in securitising cybersecurity at the EU level. The European Commission (2013) framed the Directive as a critical tool to enable shared protection of network and information systems in the rapidly changing landscape of threats.

Specifically, the Commission highlighted that the existing situation in the EU, reflecting the exclusively voluntary approach, is insufficient to protect against NIS breaches throughout the EU. As a result, the institution called for a step-change in the European approach toward NIS protection, particularly by calling for regulatory requirements to level the playing field and address the legislative loopholes (European Commission and HREU, 2013a). In other words, in the context of securitisation theory, the framing of NIS incidents as an existential threat enabled the EU to call for exceptional measures and advocate for mandatory reporting of cyber incidents by the Member States.

While cybersecurity has been extensively securitised at the EU level, the consistent securitisation process at the national level is deemed more complex. The EU-level approach to securitisation is frequently initiated by influential institutional players, such as the European Parliament and European Commission, in response to a growing perception of threat and insecurity (Christou, 2018). On the other hand, at the national level, Member States are frequently susceptible to varying perceptions of threats in the cyber domain, compromising consistent securitisation (Tumkevic, 2017). Consequently, some Member States, such as Estonia, which experienced widespread data breaches in 2007, view cyberattacks as an existential threat to national security, resulting in a high level of cybersecurity securitisation. In contrast, the other Member States, such as Hungary, which has not experienced a comparable cyberattack, view cyber incidents as a security risk only for specific industries (Tumkevic, 2017). Due to differences in the perception of cyberthreats, varying levels of national securitisation may compromise Member States' shared understanding of security. Lack of understanding between the Member States is problematic because securitisation at the EU level necessitates the development of an intersubjective understanding to effectively protect NIS across Europe. Since national strategies reflect the Member States' security understanding, this paper hypothesises that national cybersecurity strategies target diverse objectives, weakening a shared understanding of security.

3.2. Liberal Intergovernmentalism theory

Liberal intergovernmentalism (henceforth, LI) theory, developed in the early 1990s by Andrew Moravcsik, has been one of the most dominant interpretations of the European integration process. LI rests on the idea that effective European integration is positively related to economic interests, credible commitments, and relative power of Member States as long as they maintain liberal orientation (Moravcsik, 1998). Schimmelfennig (2015) expands on this idea, arguing that international cooperation between actors occurs in three stages: first, states define preferences; second, substantive agreements are negotiated; and third, institutions are established (or adjusted) to secure the outcomes despite future uncertainty on the political arena. Similarly, Hooghe and Marks (2019) argue that LI regards institutional outcome as a functional response to the cooperation problem, assuming that the Member States would delegate just enough capacity to guarantee that national governments find it in their self-interest to comply with the agreement. An important assumption within LI theory is that the EU Member States preserve a liberal outlook toward the European togetherness when such an exercise is necessary. Arguing, negotiating, and being unsatisfied are all characteristics of the LI paradigm (Schimmelfennig, 2015).

LI rests on two central premises of international relations. The first premise is that countries are the crucial players in international anarchy. However, contrary to a realist perspective, LI does not view state authority as dependent on coercive power by marginalising institutions (Moravcsik, 1993). LI argues that countries strive to accomplish goals primarily via intergovernmental dialogue and bargaining instead of a centralised authority that creates and enforces political decisions (Moravcsik and Schimmelfennig, 2018). LI sees the European Community as an "international regime for policy coordination" (Moravcsik, 1993, p. 480). LI further admits that in making EU institutions, Member States often are the "masters of the treaty" with primary decision-making authority and political credibility (Moravcsik and Schimmelfennig, 2018, p. 66). The second fundamental premise of LI is that states are rational actors (Moravcsik and Schimmelfennig, 2018). In this regard, individual states weigh the utility of different courses of action and select the one that maximises their value in the given circumstances. According to LI, collective outcomes are explained as the interaction between individual actors based on the efficient pursuit of preference optimisation (Moravcsik and Schimmelfennig, 2018). LI views collaboration and formation of international institutions between actors as a collective result of rational and interdependent choices reached via intergovernmental dialogue.

LI is crucial for evaluating EU cybersecurity since it is a vivid example of European integration. In particular, the adoption of the NIS Directive marked a turning point in the integration of cybersecurity, as it institutionalised for the first time at the EU level the mandatory reporting and protection of network and information systems. The Directive was regarded as a contentious topic, which took over forty months for the European Parliament and the European Council to adopt (Ivanova, 2021). During the preparation of the Directive, the European

Parliament supported an increase in Member State responsibility for security breaches in critical sectors, including energy, health, banking, transportation, and internet services. However, these developments confronted opposition from the EU Council, which feared the threat to the sovereignty of the member states. Consequently, the Council scaled down to the bare minimum the mechanism for interstate information sharing (Kasper and Vernygora, 2020). The domination of national interests resulted in unbalanced developments, including only mandatory control on information transfers between the corporate and public sectors but voluntary collaboration between the Member States. Furthermore, the Council initially failed to endorse the Directive during the drafting process because the several Member States, including Ireland, Sweden, and France, strongly opposed mandatory incident reporting for large non-European corporations (Papademetriou, 2015). The official statement of the Council stated that the majority of Member States have pushed for greater flexibility, restricting the implementation of binding regulations at the EU level to critical and fundamental requirements to be complemented by optional measures (Kasper and Vernygora, 2020). In other words, through the lens of LI theory, one could argue that the pursuit of preference optimisation by the Member States limited the ambitions of the Commission and the Parliament in drafting the Directive.

The pursuit of preference optimisation by national actors in cybersecurity integration produced variations in implementing a uniform European cyber framework. One of the fundamental challenges stems from the reluctance of Member States to delegate authority to the EU (Carrapico and Barrinha, 2017). Consequently, this results in the unwillingness of Member States to commit themselves, particularly when it comes to information sharing (Carrapico and Barrinha, 2017). The challenges are especially significant in intra-EU collaboration since some nations favour sub-regional cooperation over cooperation at the EU level. One of the most visible instances is the development of the Central European Cyber Security Platform, which fosters cybersecurity collaboration only among Visegrad nations and Austria. This stance starkly contrasts with that of countries such as Germany, Italy, and Estonia, which advocate for further collaboration in the European cyberspace (Carrapico and Barrinha, 2017). Variations in framing cybersecurity policies are also evident when looking at implementing cybersecurity requirements on network and information systems. Specifically, sixteen Member States failed to comply with the deadline of the NIS Directive, which was set on 9 May 2018 (Irwin, 2018). All in all, the inconsistencies in the implementation of European cybersecurity policies are problematic, as they may impede institutional cooperation within the EU.

The intergovernmental dialogue in the formulation of the NIS Directive has granted the flexibility to the Member States, potentially weakening institutional cooperation in network and information security. Specifically, substantial compromises were made during the drafting of the legislation to ensure the independence of national security at the expense of the Directive's functionality. For example, although the NIS Directive mandates the publication of national cybersecurity strategies at the EU level, Member States have the autonomy to disguise elements of their strategies if they deem such elements too sensitive to be revealed at the European level (Brun and Bellanova, 2018). Another example is the requirement of the Directive to establish a national Computer Security Incident Response Team (CSIRT) to ensure institutional cooperation at the EU level between different national CSIRTs during cross-border cyberattacks (Directive (EU) 2016/1148, 2016). However, the NIS Directive does not specify the organisational structure of CSIRT, leaving a great deal of implementation autonomy to Member States (Brun and Bellanova, 2018). In this regard, one could argue that the intergovernmental nature of cybersecurity integration allowed Member States to maintain sovereignty by placing national needs above EU priorities during the NIS Directive drafting process. Even though the EU refers to the NIS Directive as "the child of consensus" between EU institutions and national actors, many Member States continue to interpret cybersecurity in terms of national interests (Brun and Bellanova, 2018, p. 26). Prevalence of national interests in implementing the Directive is especially problematic in the identification process of operators of essential services. While the Directive mandates identifying OES at the national level, Member States are not required to notify the European institutions of the precise list of essential services. In addition, Member States are granted autonomy to take national circumstances into account during the OES identification process (Brun and Bellanova, 2018). A lack of uniformity in identifying OES between the Member States is problematic, as it may impede the ability of national actors to interact coherently during transnational cyberattacks. Therefore, this paper hypothesises that uneven identification of OES by the Member States undermines institutional cooperation across the EU.

4. Evaluating Implementation of the NIS Directive by the Member States

Given the complexity of coherence as a concept, its operationalisation is often challenging. According to Thaler (2020), it is inherently complex, if not impossible, to evaluate the coherence or incoherence of the outcome of a set of policies because EU documents fail to offer sufficient quantitative or qualitative standards against which reality may be evaluated. One of the solutions for the operationalisation is offered by Wunderlig (2013), who argues that coherence becomes evident when the policy execution produces a minimum of inconsistencies with the policy's key objectives. In this perspective, coherent cybersecurity becomes tangible when implementing the NIS Directive provides a shared understanding of security and institutional cooperation between the Member States. On the other hand, the implementation of the Directive is examined through the analysis of national cybersecurity strategies and OES implementation. In other words, national strategies and OES are treated as explanatory variables within the scope of this paper.

Since this research aims to analyse the impact of Member States' implementation of the NIS Directive on coherence, a case study of all the current 27 EU countries is conducted. The primary method of the paper is qualitative content analysis. According to Hsieh and Shannon (2005), qualitative content analysis is a method for "the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (p. 1278). The method is mainly used to analyse complex text data by focusing on the contextual meaning and content (Tesch, 1995). In this light, qualitative content analysis is particularly useful for evaluating national cybersecurity strategies, which are frequently complex and lengthy legal documents requiring a systematic assessment approach. The primary empirical data used in this research are national cybersecurity strategies and the 2019 European Commission report. The paper also relies on additional secondary sources to complement the data, including the NIS implementation tracker, expert reviews, and official documents.

The ENISA database is employed to collect national cybersecurity strategies (ENISA, 2022). Since most of the Member States have published multiple strategies throughout the years, only the most recent strategies are selected for the analysis, as they represent the current status of cybersecurity development.[2] Several Member States were excluded from the analysis because the assessment of the strategies is limited to the English language only. Specifically, the evaluation did not include the latest national strategies of Bulgaria, Cyprus, Greece, Hungary, Latvia, and Romania.

[2] Finland is an exception. The country's latest 2019 Cybersecurity Strategy is based on the general principles of the 2013 Strategy. Therefore, both strategies of the country are evaluated.

The national cybersecurity strategies are systematically evaluated using the National Cybersecurity Strategies Evaluation Tool (ENISA, 2018). ENISA created the tool, which consists of fifteen objectives, to assist the Member States in the evaluation process of national cybersecurity strategies (see Appendix A). ENISA first introduced and outlined all the objectives in its 2016 great practice guide (ENISA, 2016b). Consequently, the guide is also used in the analysis to evaluate and identify the objectives of respective national strategies effectively. The ENISA evaluation tool objectives are instrumental, as they allow to determine whether or not Member States adhere to a similar understanding of cybersecurity development (ENISA, 2016b). In addition, the application of the evaluation tool is useful for the content analysis, provided that the Member States have vastly different strategies, necessitating a set of indicators for effective comparison. Therefore, within the scope of this study, national cybersecurity strategies are analysed for the presence of these objectives to determine systematically whether the Member States adhere to a shared understanding of security in the cyber domain.

The scope of OES identification across the Member States is mainly evaluated using the 2019 report from the European Commission. The report is based on information directly obtained from the Member States, interviews and group meetings (European Commission, 2019). Since, at the time of the report publication, not all Member States had contributed the required information on OES identification, alternative sources, such as the NIS implementation tracker and expert reviews, are also used in the analysis (DigitalEurope, 2019; Bird&Bird, 2018). Furthermore, Annex II of the NIS Directive, which provides information on sectors and subsectors of OES, is used in the analysis to effectively compare the scope of OES implementation in the EU countries (Directive (EU) 2016/1148, 2016). Consequently, in the context of this research, OES implementation across the Member States is evaluated to determine its effect on institutional cooperation in cybersecurity.

4.1 National cybersecurity strategies

According to the evaluation, only three nations fully complied with the ENISA assessment tool objectives. Specifically Spain, Italy, and Slovakia (see table 1). All three countries presented comprehensive national cybersecurity policies that included details on the fifteen objectives specified by ENISA. The latest Italian cybersecurity strategy, published in 2017 and replaced the 2013 strategy, extensively outlined the course of action to strengthen the network and information security of the country. For instance, the strategy committed to collaborating closely with the ministry of defence and advocated for the establishment of a “Joint Command for Cyber Operations” to ensure the protection of all national assets in the cybersphere.[3] In addition, the Italian strategy established the “Cyber Security Management Board” to monitor cyber events at the national level and offer coordination between public entities.[4] In a similar vein, the most recent Spanish cybersecurity strategy, published in 2019 and replaced the 2013 version, included several extensive legislative efforts aimed at safeguarding national networks and information systems. The introduction of cybersecurity solutions into the Spanish legislative framework and the expansion of the capabilities of the agency responsible for prosecuting cybercrime are two of the most significant advancements in the Spanish strategy.[5] The most recent Slovakian cybersecurity strategy, published in 2021, is already the country’s third national strategy in cyberspace. The strategy is committed to assisting both the corporate and public sectors in implementing the necessary security measures against cyberattacks to protect operators of essential services. [6] The strategy further highlighted the need for “political cooperation in the field of cybersecurity”.[7]

The identification procedure revealed that Malta, the Netherlands, and Croatia have the least comprehensive national cybersecurity strategies. Malta’s latest and only cybersecurity strategy, published in 2016, addressed just six of fifteen objectives of the ENISA assessment tool. Notably, the strategy did not specify detailed guidance for critical information infrastructure security. The strategy only vaguely indicated that the “measures of preparedness, response and recovery, … are particularly necessary to protect national critical information infrastructure”.[8] However, the strategy lacked details about the specific measures to secure the critical information infrastructure. In the Netherlands, the 2018 Dutch national cybersecurity strategy is the country’s third and latest strategy. The strategy only delivered seven of fifteen objectives. While the strategy targeted the development of incident response capabilities through the “National Cyber Security Centre” and “Defence Computer Emergency Response Team” to protect against cyberattacks, it failed to establish comprehensive incident reporting mechanisms.[9] The most recent and only Croatian cybersecurity strategy was issued in 2015, one year prior to the adoption of the NIS Directive. The country’s strategy defined only nine

[3] ‘The Italian Cybersecurity Action Plan’ (2017), p. 12. Collected from ENISA (2022).

[4] Ibid, p. 11.

[5] ‘National Cybersecurity Strategy’ (2019). Collected from ENISA (2022).

[6] ‘The National Cybersecurity Strategy 2021-2025’ (2021). Collected from ENISA (2022).

[7] Ibid, p. 22.

[8] ‘Malta Cyber Security Strategy 2016’ (2016), p. 17. Collected from ENISA (2022).

[9] ‘National Cyber Security Agenda: A cyber secure Netherlands’ (2018), p. 20. Collected from ENISA (2022).

of the fifteen goals of the evaluation tool. While the strategy did not achieve all of the ENISA criteria, it introduced the “Act on Critical Infrastructure”, marking a significant step toward the protection of the country’s critical infrastructure.[10]

Table 1: Number of identified objectives in National Cybersecurity Strategies

Country	Number of identified objectives (out of 15)
Austria	13
Belgium	11
Croatia	9
Czech Republic	14
Denmark	12
Estonia	14
Finland	14
France	13
Germany	10
Ireland	14
Italy	15
Lithuania	11
Luxembourg	13
Malta	6
Netherlands	7
Poland	13
Portugal	13
Slovakia	15
Slovenia	10
Spain	15
Sweden	10
Country Average	**12**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Alarmingly, only Finland and Ireland, in addition to Italy, Slovakia, and Spain, addressed “incentives for the private sector to invest in security measures”[11] in their national cybersecurity strategies (see Appendix B). The Finnish cybersecurity strategy, which comprises both the 2013 strategy and its 2019 implementation programme, tasked the “Cyber

[10] ‘The National Cyber Security Strategy of the Republic of Croatia’ (2015), p. 13. Collected from ENISA (2022).

[11] One of the objectives of the ENISA evaluation tool (ENISA, 2018).

Security Centre" with incentivising authorities and actors in the private sector in the implementation of security measures and management against cyberattacks.[12] Furthermore, the Finnish strategy addressed nearly all of the fifteen objectives, apart from the institutionalisation of public agency cooperation. The Irish cybersecurity strategy, published in 2019 and replaced the 2013 strategy, also addressed fourteen out of fifteen objectives. In order to incentivise the private sector to invest in security measures, the strategy tasked the "Computer Security Incident Response Team" with assisting private enterprises in fostering cooperation and managing cyberattacks.[13] Some national strategies, such as the most recent Estonian cybersecurity strategy for 2019, attempted to encourage the private sector to invest in security measures by "offering technical information streams, organising joint exercises, and involving the private sector... in legislative drafting and strategic planning processes".[14] However, the strategy failed to build a comprehensive framework to incentivise the private sector in developing its cybersecurity capabilities. Overall, it is concerning that only five of the twenty-one examined countries addressed the private sector in national cybersecurity strategies to incentivise security. The vast majority of network and information systems are privately operated (Directive (EU) 2016/1148, 2016). As a result, Member States risk the security of the critical infrastructure if the private sector is not adequately incentivised to secure its infrastructure.

Nevertheless, most countries provided relatively comprehensive frameworks in their national strategies, with Member States addressing, on average, twelve of the fifteen objectives of the ENISA evaluation tool. Four out of twenty-one analysed nations met fourteen of fifteen objectives, including the Czech Republic, Estonia, Finland, and Ireland. Additional five countries, Austria, France, Luxembourg, Poland, and Portugal, incorporated thirteen objectives of the ENISA evaluation tool. Notably, except for Malta, all analysed countries pledged to comprehensively protect their critical information infrastructure. In other words, nearly all examined Member States have fully defined and identified critical sectors in their national strategies with the ENISA (2016b) good practice guide. In addition, all twenty-one countries are committed to engaging in international cooperation in their national strategies. According to the ENISA guide, international cooperation entails the commitment of Member States to combat cybercrime on a transnational level and the development of a shared understanding of

[12] 'Finland´s Cyber security Strategy' (2013), p. 24. Collected from ENISA (2022).
[13] 'National Cyber Security Strategy 2019-2024' (2019), p. 21. Collected from ENISA (2022).
[14] 'Cybersecurity Strategy. Republic of Estonia' (2019), p. 17. Collected from ENISA (2022).

security between EU Members (ENISA, 2016b). In this regard, it can be argued that, on paper, the majority of the Member States recognise the cyber domain as a transnational issue requiring the development of a shared understanding of security to combat threats effectively.

4.2. OES implementation

According to the evaluation, except for the Netherlands, all current Member States fulfilled the NIS Directive's criteria on the scope of OES identification (see table 2). On the other hand, the Netherlands, which transposed its administrative decree specifying the list of operators of essential services in 2018, did not meet all the conditions established in Annex II of the Directive. In particular, the country failed to include the health sector as an essential service in its decree (DigitalEurope, 2019). In turn, this contradicts article 3 of the NIS Directive, which requires the Member States to "adopt or maintain provisions with a view to achieving a higher level of security of network and information systems" (Directive (EU) 2016/1148, 2016, article 3). Thus, while the Directive permits Member States to go beyond the scope of Annex II, it prohibits omitting the specified essential sectors. Failure to correctly identify the health sector is especially problematic, considering the ongoing pandemic, making the protection of the health infrastructure critical against cyberattacks. In addition, the Dutch administrative decree simplified the identification process in transport and financial market infrastructure, potentially weakening the cyber resilience of the two sectors (Kalis, 2018).

The analysis also revealed that many Member States covered sectors not included in Annex II of the NIS Directive. Specifically, thirteen out of twenty-seven countries have gone beyond the NIS Directive criteria and identified additional sectors under the scope of OES. In general, this can be viewed as a positive development since it potentially strengthens the cyber resilience of Member States against attacks. However, it also raises concerns about the scope of Annex II in the Directive, as nearly fifty per cent of nations chose to add additional sectors. In this regard, it is clear that the current NIS Directive fails to cover all sectors that may be deemed essential to the functioning of the economy and society by the Member States. Some Member States have added only several sectors as operators of essential services. For instance, Slovenia has identified two additional sectors as OES, particularly environmental protection industries and the food supply sector (Bird&Bird, 2018). On the other hand, other countries have identified numerous additional sectors as OES. Slovakia has identified seven additional sectors, including public administration, pharmaceutical industry, chemical industry, postal service, electronic communication, metallurgical industry, and even intelligent industry (DigitalEurope, 2019).

Some countries such as Cyprus, Spain, and France have identified seventeen, eighteen, and twenty additional sectors, respectively, as OES (European Commission, 2019). Some of the additional sectors included the wastewater industry, government and emergency services, food sector, space research, and military activities (Bird&Bird, 2018; DigitalEurope, 2019).

Table 2: Scope of OES in Member States

Country	Does the OES scope meet the NIS Directive's criteria?	Are there additional sectors?
Austria	Yes	No
Belgium	Yes	No
Bulgaria	Yes	Yes
Croatia	Yes	Yes
Cyprus	Yes	Yes
Czech Republic	Yes	Yes
Denmark	Yes	Yes
Estonia	Yes	Yes
Finland	Yes	Yes
France	Yes	Yes
Germany	Yes	Yes
Greece	Yes	No
Hungary	Yes	No
Ireland	Yes	No
Italy	Yes	No
Latvia	Yes	No
Lithuania	Yes	No
Luxembourg	Yes	No
Malta	Yes	Yes
Netherlands	No	No
Poland	Yes	No
Portugal	Yes	No
Romania	Yes	No
Slovakia	Yes	Yes
Slovenia	Yes	Yes
Spain	Yes	Yes
Sweden	Yes	No

Source: Report from the Commission to the European Parliament and the Council (European Commission, 2019); NIS Implementation Tracker (DigitalEurope, 2019); NISD Tracker (Bird&Bird, 2018); compiled by the author

The analysis has further shown that Member States have identified a varying number of services as OES, although nearly all nations have complied with the NIS Directive in identifying OES, and many have even beyond the minimum requirements. The flexibility of the NIS Directive, which allows varying methodologies for identifying essential services by the Member States, contributes to variation. As a result, in the electricity subsector, nations such as Hungary have opted for a highly general methodology that permits the identification of virtually any operator they consider vital for the subsector. On the other hand, nations such as Romania, Italy, and Belgium, have chosen a more granular method (European Commission, 2019). As a result, the inconsistencies between the Member States potentially weaken institutional collaboration. The existence of inconsistencies is indicated in table 3. It is important to mention that the five countries have been chosen for demonstrative purposes to illustrate how different identification of services might lead to inconsistencies among the Member States. As shown in the table, Romania has provided a very granular and comprehensive list of services under electricity subsectors, ranging from "production of electricity" to "operation of the power system". On the other hand, Hungary has only included one general service, "electricity", allowing the government to identify different types of services as OES within the electricity subsector. While the Netherlands has likewise only listed one type of service under the electricity subsector, it focuses solely on "transmission and distribution of electricity". As a result, Dutch services do not cover operationalisation, production, and electricity supply in the subsector, leading to inter-state inconsistencies. In a similar vein, the Italian and Belgian identified services do not cover the operation of "centralised electricity markets" and "power system" in the electricity subsector. The Belgian electricity subsector also fails to cover services associated with electricity supply.

Inconsistencies in the electricity sector extend beyond Romania, Italy, Belgium, the Netherlands, and Hungary. Similar dynamics exist among all EU Member States, with some countries opting for a more general methodology and others for a more granular identification method. Similar trends can be further observed in other OES sectors and subsectors (European Commission, 2019). As a result, the number of services identified as OES varies significantly between nations, with Cyprus identifying only 20 services and Finland identifying 10897 services (see Appendix C). The problem is exacerbated by the fact that the NIS Directive does not require national authorities to reveal specific information on the identification methodology, resulting in a lack of transparency and potentially even more significant discrepancies (European Commission, 2019). Lack of inter-state cooperation is problematic, as inconsistencies between the Member States during cross-border cyberattacks puts the critical infrastructure of the Union at a greater risk. Consequently, it can be argued that the Directive’s flexibility in allowing the Member States to protect the security of their network and information systems, as long as it is similar to the standards outlined in the Directive, has led to varying identification of services under OES. As a result of the variations, institutional cooperation between the Member States is compromised, leading to poor transnational cyber resilience.

Table 3: Identified services in the electricity subsector

Romania	Italy	Belgium	Netherlands	Hungary
Production of electricity	Generation	Production, transport and distribution companies	*inconsistency*	Electricity
Supply of electricity to consumers	Trading	*inconsistency*		
Operation of centralized electricity markets	*inconsistency*			
Transport of electricity	Transmission	Electricity transport	Transmission and Distribution of Electricity	
Distribution of electricity	Distribution	Electricity distribution		
Operation of the power system	*inconsistency*	*inconsistency*	*inconsistency*	

Source: Report from the Commission to the European Parliament and the Council (European Commission, 2019); compiled by the author

5. Conclusion

The key conclusion of the paper is that the flexibility of the NIS Directive has resulted in inconsistent implementation of the legislation by the Member States, thereby weakening the coherence of European cybersecurity. In particular, the collected evidence indicates that the Member States’ autonomy in defining essential services has led to inconsistent identification of OES, thereby undermining institutional cooperation at the EU level. Cooperation is compromised because some services covered by some EU countries are not covered by others, leaving the network and information systems vulnerable to transnational cyberattacks. For instance, in the electricity subsector, Hungary opted for a highly general methodology that permits the identification of virtually any operator deemed essential. In contrast, the Netherlands only listed one type of service that focuses solely on the transmission and distribution of electricity, thus failing to cover its operationalisation, production, and supply. The consistency issue extends beyond the electricity subsector, resulting in inconsistent identification across all national OES. Lack of consistency, in turn, weakens institutional cooperation between the Member States, increasing the risk to the EU's critical infrastructure. The risk is exacerbated by the NIS Directive's flexibility, which does not require the Member States to share information on identification methodologies, resulting in a lack of interstate transparency and cooperation. Through the lens of LI theory, one could argue that the domination of an intergovernmental dialogue in the preparation of the NIS Directive has granted autonomy to the Member States, jeopardising institutional cooperation and coherence at the EU level in network and information security. Overall, the presented evidence corroborates the second hypothesis of the paper, which states that the uneven identification of OES by the Member States undermines institutional cooperation throughout the EU.

Another conclusion of the paper is that majority of the Member States offered comprehensive national strategies, resulting in, at least on paper, a shared understanding of cybersecurity. In particular, the analysis revealed that Member States have addressed, on average, twelve of fifteen ENISA evaluation tool objectives in their national cybersecurity strategies. Even though several outliers, including the Maltese and Dutch cybersecurity strategies, failed to meet even half of the objectives, twelve out of twenty-one evaluated countries met at least thirteen out of fifteen objectives. In addition, except for the Netherlands, all current Member States have fully complied with the NIS Directive in the identification process of OES. Moreover, thirteen out of twenty-seven Member States have exceeded the NIS Directive's scope and identified additional services as OES. Notably, except for Malta, all evaluated countries pledged to protect comprehensively critical information infrastructure. Thus, through the perspective of the securitisation theory, it is reasonable to argue that an overall extensive securitisation occurred at both the EU and national levels, identifying cyber incidents as an existential threat. In this regard, the presented evidence fails to support the first hypothesis of the paper, which states that national cybersecurity strategies pursue diverse objectives, thereby eroding a shared understanding of security.

The findings of this study have significantly contributed to academic literature and policy development. Where the first is concerned, the paper provided the first comprehensive analysis of the impact of the NIS Directive implementation on coherence within the context of European cybersecurity. While several scholars have previously analysed the coherence of the EU cyberspace (Carrapico and Barrinha, 2017; Blazic, 2021; Wolff and Ladi, 2020; Christou, 2016), none have assessed it exclusively through the framework of the NIS Directive. More importantly, little to no offered a comprehensive theoretical framework to evaluate the policy area. In this regard, this study contributed to the body of knowledge by introducing securitisation and liberal intergovernmentalism as complementary theories to explain the development of European cybersecurity in the context of coherence. Moreover, the paper contributed to the literature on coherence by providing a dual definition and operationalising the term as a research object. Regarding the contribution to the policy area, the analysis offered an extensive assessment of the NIS Directive. The evaluation is especially relevant given that the NIS2 Directive is still being developed. In light of this, policymakers must address the flexibility in the new version to ensure consistent institutional cooperation between Member States in protecting networks and information systems. Significantly, the scope of the research extends beyond European cybersecurity, as it reveals potential flaws in other EU-level legislation that grant Member States excessive autonomy due to the dominance of intergovernmental dialogue. As a result, policymakers should be aware of the potential constraints that flexible legislation poses to institutional cooperation among national actors.

References

Bibliography

Balzacq, T. (2011). *Securitization theory: how security problems emerge and dissolve*. London: Routledge.

Bendiek, A., Bossong, R., and Schulze, M. (2017). The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges, *SWP Comments 47, November 2017.*

Bird&Bird. (2018). *NISD Tracker*. [online] Available at: https://www.twobirds.com/en/trending-topics/cybersecurity/nisd-tracker [Accessed 7 May 2022]

Blazic, B. (2021). Cybersecurity Skills in EU: New Educational Concept for Closing the Missing Workforce Gap. *Cybersecurity Threats with New Perspectives*. doi:10.5772/intechopen.97094.

Brattberg, E. and Rhinard, M. (2012). The EU as a global counter-terrorism actor in the making. *European Security*, 21(4), pp.557–577. doi:10.1080/09662839.2012.688809.

Brun, L., and Bellanova, R. (2018). The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity. *Université catholique de Louvain*.

BSA (2015). EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace [online], Available at: https://cybersecurity.bsa.org/ [Accessed May 19, 2022].

Buzan, B. and Waever, O. (2003). *Regions and powers: the structure of international security*. Cambridge: Cambridge University Press.

Calderoni, F. (2010). *Organised Crime Legislation in the European Union: Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight Against Organised Crime*, New York: Springer, London.

Carrapico, H. and Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, 55(6), pp.1254–1272. doi:10.1111/jcms.12575.

Cerulus (2020). *EU bolsters defenses against cyberattacks: new strategy and laws aim to stop hacks of key assets and information*. [online] Politico. Available at: https://www.politico.eu/article/eu-bolsters-defenses-against-cyberattacks/?fbclid=IwAR3_Gi-I9ITIm3nER_EiCZcF82VmXI7qnBs89CZWdy6enQ577gOKr0MQe4g [Accessed May 20 2022].

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Basingstoke; New York: Palgrave Macmillan.

Christou, G. (2018). The collective securitisation of cyberspace in the European Union. *West European Politics*, 42(2), pp.278–301. doi:10.1080/01402382.2018.1510195.

DigitalEurope. (2019). *NIS Implementation Tracker*. [online] Available at: https://www.digitaleurope.org/resources/nis-implementation-tracker/ [Accessed 4 May 2022].

Dragomir, A. V. (2021) What's new in the NIS 2 Directive proposal compared to the old NIS Directive. *SEA - Practical Application of Science, Romanian Foundation for Business Intelligence, Editorial Department*, 27, pp. 155-162.

Ducuing, C. (2021). Understanding the rule of prevalence in the NIS directive: C-ITS as a case study. *Computer Law & Security Review*, 40, p.1-11. doi:10.1016/j.clsr.2020.105514.

Dutton, W.H., Creese, S., Esteve-Gonzalez, P., Goldsmith, M. and Weisser Harris, C. (2022). Next Steps for the EU: Building on the Paris Call and EU Cybersecurity Strategy. *SSRN Electronic Journal*. doi:10.2139/ssrn.4052728.

Fuster, G. G., & Jasmontaite, L. (2020). ‘Cybersecurity regulation in the European union: the digital, the critical and fundamental rights’, in *The Ethics of Cybersecurity.* Springer, Cham, pp. 97-115.

Gebhard, C. (2011). ‘The Problem of Coherence in the European Union's International Relations’, in Hill, C., Smith, M., and Vanhoonacker, S. (eds) *International Relations and the European Union*. Oxford University Press, pp.101-127.

Gebhard, C. (2017). The problem of coherence in the EU's international relations. *International relations and the European Union*, pp.102-130.

Hill, C. (1993). The Capability-Expectations Gap, or Conceptualizing Europe’s International Role. *JCMS: Journal of Common Market Studies*, 31(3), pp.305–328.

Hjalmarsson, O. (2013). The Securitization of Cyberspace. *Lund University, Department of Political Science.*

Hooghe, L. and Marks, G. (2019). Grand theories of European integration in the twenty-first century. *Journal of European Public Policy*, 26(8), pp.1–21.

Hsieh, H.F. and Shannon, S.E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9), pp.1277–1288. doi:10.1177/1049732305276687.

Irwin, L. (2018). *Majority of EU member states missed NIS Directive deadline*. [online] IT Governance Blog En. Available at: https://www.itgovernance.eu/blog/en/majority-of-eu-member-states-missed-nis-directive-deadline [Accessed 6 May 2022].

Ivanova, M. (2021). 'Explaining European Integration in Cybersecurity', PhD thesis, Ludwig Maximilian University, Munich.

Kalis, P. (2018). *NIS Directive – update for the Netherlands*. [online] Leidenlawblog. Available at: https://leidenlawblog.nl/articles/nis-directive-update-for-the-netherlands#:~:text=According%20to%20the%20Directive%2C%20there [Accessed 31 May 2022].

Karniyevich, N. (2021). *Cybersecurity: Council adopts its position on the NIS2 Directive*. [online] Bird&Bird. Available at: https://www.twobirds.com/en/insights/2021/germany/cybersecurity-council-adopts-its-position-on-the-nis2-directive#:~:text=To%20recall%2C%20the%20overall%20aim,the%20surge%20in%20cyber%2Dattacks.

Kasper, A. and Vernygora, V. (2020). *Towards a 'Cyber Maastricht': two steps forward, one step back*. [online] University of Malta. Institute for European Studies. Available at: https://www.um.edu.mt/library/oar/handle/123456789/52310 [Accessed 15 May 2022].

Kasper, A. and Vernygora, V. (2021). The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? *Cuadernos Europeos de Deusto*, (65), pp.29–71.

Markopoulou, D., Papakonstantinou, V. and Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection

Regulation. *Computer Law & Security Review*, 35(6), p.1-11. doi:10.1016/j.clsr.2019.06.007.

Missiroli, A. (2001). European Security Policy: The Challenge of Coherence. *European Foreign Affairs Review*, 6(2), pp.177–196. doi:10.54648/356609.

Moravcsik, A. (1993). Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach. *JCMS: Journal of Common Market Studies*, 31(4), pp.473–524. doi:10.1111/j.1468-5965.1993.tb00477.x.

Moravcsik, A. (1998). *The choice for Europe: social purpose and state power from Messina to Maastricht*. New York: Cornell University Press.

Moravcsik, A. and Schimmelfennig, F. (2018). 4. Liberal Intergovernmentalism. *European Integration Theory*, pp.64–84. doi:10.1093/hepl/9780198737315.003.0004.

Nuttall, S. (2005). 'Coherence and Consistency', in Hill, C., Smith, M., and Vanhoonacker, S. (eds) *International Relations and the European Union*. Oxford University Press, pp. 91–112.

O'Donoghue, C. (2022). *Cybersecurity 2.0: European Parliament adopts new draft directive*. [online] Technology Law Dispatch. Available at: https://www.technologylawdispatch.com/2022/01/data-cyber-security/cybersecurity-2-0-european-parliament-adopts-new-draft-directive/.

Papademetriou, T. (2015). *European Union: Member States Disagree over Proposed Cybersecurity Directive*. [online] Library of Congress. Available at: https://www.loc.gov/item/global-legal-monitor/2015-06-12/european-union-member-states-disagree-over-proposed-cybersecurity-directive/ [Accessed 20 May 2022].

Portela, C. and Raube, K. (2011). The EU Polity and Foreign Policy Coherence. *Journal of Contemporary European Research*, 8(1), pp.3–20.

Sabillon, R., Cavaller, V., and Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, 5(5), pp.67-80.

Schimmelfennig, F. (2015). Liberal intergovernmentalism and the euro area crisis. *Journal of European Public Policy*, 22(2), pp.177–195.

Singh, R. (2017). *Julian King: Bold EU action is required to address cyber vulnerabilities.* [online] The Parliament Magazine. Available at: https://www.theparliamentmagazine.eu/news/article/julian-king-bold-eu-action-is-required-to-address-cyber-vulnerabilities [Accessed 30 May 2022].

Stitilis, D., Pakutinskas, P. and Malinauskaite, I. (2016). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, 30(4), pp.1151–1168. doi:10.1057/s41284-016-0083-9.

Taureck, R. (2006). Securitization theory and securitization studies. *Journal of International Relations and Development*, 9(1), pp.53–61. doi:10.1057/palgrave.jird.1800072.

Tesch, R. (1995). *Qualitative research: analysis types and software tools*. New York; Philadelphia ; London: The Falmer Press.

Thaler, P. (2020). *Shaping EU Foreign Policy Towards Russia: Improving Coherence in External Relations*. Northampton: Edward Elgar Publishing.

Tumkevic, A. (2017). Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats. *Baltic Journal of Political Science*, 5(5), pp. 73-88. doi:10.15388/bjps.2016.5.10337.

Waever, O. (2004). “Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery”. *Montreal: ISA Conference*, March.

Wolff, S. and Ladi, S. (2020). European Union Responses to the Covid-19 Pandemic: adaptability in times of Permanent Emergency. *Journal of European Integration*, 42(8), pp.1025–1040. doi:10.1080/07036337.2020.1853120.

Wunderlich, D. (2013). Towards Coherence of EU External Migration Policy? Implementing a Complex Policy. *International Migration*, 51(6), pp.26–40. doi:10.1111/imig.12088.

Official documents and legislation

‘Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union’ (2016) *Official Journal of the European Union* L 194/1-30.

Council of the European Union (2000). ‘2294th Council Meeting – General Affairs’, Counseil/00/364, Luxembourg.

Council of the European Union (2003). ‘European Security Strategy: a Secure Europe in a Better World’, Brussels.

ENISA (2016a). ‘ENISA Threat Landscape Report 2016’, [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 [Accessed 10 May 2022].

ENISA (2016b). ‘NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies’, [online] Available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide [Accessed 29 May 2022].

ENISA (2018). ‘National Cybersecurity Strategies Evaluation Tool’, [online] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool [Accessed 27 May 2022].

ENISA (2022). ‘National Cybersecurity Strategies’, [online] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies [Accessed 17 May 2022].

European Commission (2006). ‘Communication from the Commission to the European Council of June 2006: Europe in the World- Some Practical Proposals for Greater Coherence, Effectiveness and Visibility’, COM (2006) 278 final.

European Commission (2011). ‘Proposal on a European Strategy for Internet Security’, November 2011.

European Commission (2013). ‘Proposal for a Directive of the European Parliament and the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union’, COM (2013) 48 final.

European Commission (2017). ‘State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks’. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193 [Accessed 15 May 2022].

European Commission (2019). ‘Report from the Commission to the European Parliament and the Council’, COM(2019) 546 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN [Accessed 6 May 2022].

European Commission and HREU (2013a). ‘Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’, JOIN(2013) 1 final.

European Commission and HREU (2013b). ‘Joint Communication to the European Parliament And The Council. The EU's comprehensive approach to external conflict and crises’, JOIN(2013) 30 final.

European Commission and HREU (2017). ‘Joint Communication to the European Parliament And The Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’, JOIN(2017) 450 final.

European Commission and HREU (2020). ‘Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade’, JOIN(2020) 18 final.

European Parliament (2017). ‘Report on the fight against cybercrime’, (2017/2068(INI)). Available at: https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_EN.html. [Accessed 11 May 2022].

Appendixes

Appendix A: ENISA Evaluation Tool

Objectives for the evaluation of National Cybersecurity Strategies

Objectives
Develop national cyber contingency plans
Protect critical information infrastructure
Organise cyber security exercises
Establish baseline security measures
Establish incident reporting mechanisms
Raise user awareness
Foster R&D
Strengthen training and educational programmes
Establish an incident response capability
Address cyber crime
Engage in international cooperation
Establish a public-private partnership
Balance security with privacy
Institutionalise cooperation between public agencies
Provide incentives for the private sector to invest in security measures

Source: National Cybersecurity Strategies Evaluation Tool (ENISA, 2018)

Appendix B: National Cybersecurity Strategies

Austrian National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	Are the objectives present in the strategy? Present/Absent
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Belgian National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	**Absent**
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	**Absent**
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Croatian National Cybersecurity Strategy (2015)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	**Absent**
Protect critical information infrastructure	Present
Organise cyber security exercises	**Absent**
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	**Absent**
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	**Absent**
Balance security with privacy	Present
Institutionalise cooperation between public agencies	**Absent**
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Czech National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Danish National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	**Absent**
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Estonian National Cybersecurity Strategy (2019)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Finnish National Cybersecurity Strategy (2013) and (2019)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	**Absent**
Provide incentives for the private sector to invest in security measures	Present

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

French National Cybersecurity Strategy (2015)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	**Absent**
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

German National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	**Absent**
Establish baseline security measures	Present
Establish incident reporting mechanisms	**Absent**
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	**Absent**
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Irish National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	Are the objectives present in the strategy? Present/Absent
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	**Absent**
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	Present

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Italian National Cybersecurity Strategy (2017)

Objective (ENISA evaluation tool)	Are the objectives present in the strategy? Present/Absent
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	Present

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Lithuanian National Cybersecurity Strategy (2018)

Objective (ENISA evaluation tool)	Are the objectives present in the strategy? Present/Absent
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	**Absent**
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	**Absent**
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Luxembourgish National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Maltese National Cybersecurity Strategy (2016)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	**Absent**
Protect critical information infrastructure	**Absent**
Organise cyber security exercises	**Absent**
Establish baseline security measures	**Absent**
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	**Absent**
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	**Absent**
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	**Absent**
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Dutch National Cybersecurity Strategy (2018)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	**Absent**
Protect critical information infrastructure	Present
Organise cyber security exercises	**Absent**
Establish baseline security measures	Present
Establish incident reporting mechanisms	**Absent**
Raise user awareness	**Absent**
Foster R&D	**Absent**
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	**Absent**
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Polish National Cybersecurity Strategy (2019)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Portuguese National Cybersecurity Strategy (2019)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	**Absent**
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Slovakian National Cybersecurity Strategy (2021)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	Present

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Slovenian National Cybersecurity Strategy (2016)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	**Absent**
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	**Absent**
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	**Absent**
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	**Absent**
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Spanish National Cybersecurity Strategy (2019)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	Present
Establish incident reporting mechanisms	Present
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	Present
Establish an incident response capability	Present
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	Present

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Swedish National Cybersecurity Strategy (2017)

Objective (ENISA evaluation tool)	**Are the objectives present in the strategy? Present/Absent**
Develop national cyber contingency plans	Present
Protect critical information infrastructure	Present
Organise cyber security exercises	Present
Establish baseline security measures	**Absent**
Establish incident reporting mechanisms	**Absent**
Raise user awareness	Present
Foster R&D	Present
Strengthen training and educational programmes	**Absent**
Establish an incident response capability	**Absent**
Address cyber crime	Present
Engage in international cooperation	Present
Establish a public-private partnership	Present
Balance security with privacy	Present
Institutionalise cooperation between public agencies	Present
Provide incentives for the private sector to invest in security measures	**Absent**

Source: National Cybersecurity Strategies (ENISA, 2022); compiled by the author

Appendix C: Number of identified OES

Table 1A: Number of identified services as OES

Country	Number of identified services as OES[15]
Austria	Data Missing
Belgium	Data Missing
Bulgaria	185
Croatia	85
Cyprus	20
Czech Republic	50
Denmark	128
Estonia	137
Finland	10897
France	127
Germany	573
Greece	67
Hungary	42
Ireland	64
Italy	553
Latvia	66
Lithuania	22
Luxembourg	49
Malta	36
Netherlands	42
Poland	142
Portugal	1250
Romania	86
Slovakia	273
Slovenia	Data Missing
Spain	132
Sweden	326

Source: Report from the Commission to the European Parliament and the Council (European Commission, 2019)

[15] Since not all Member States submitted information on the number of identified services as OES at the time the report was published, some of it is marked as "Data Missing."