Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age

Eyup Kun

Abstract

The rapid evolution of the digital landscape has increased cybersecurity challenges, necessitating legal interventions to protect critical infrastructure and essential services across the European Union (EU). The EU's Network and Information Systems (NIS 1) Directive (2016/1148) marked the first cross-sectoral legislative effort to address cybersecurity, focusing on essential services such as energy, transport, and banking. However, the Directive's scope and implementation revealed significant gaps, including inconsistent application across Member States and inadequate coverage of newly critical sectors. Recognizing these shortcomings, the EU adopted the NIS 2 Directive (2022/2555), which introduces substantial enhancements to strengthen the cybersecurity framework.

This paper examines the evolution from NIS 1 to NIS 2, highlighting the latter's broader scope, harmonized cybersecurity requirements, improved reporting mechanisms, and stronger supervision and enforcement. While setting minimum harmonization standards, it allows Member States the flexibility to adopt stricter measures aligned with EU law. The NIS 2 Directive also emphasizes cooperative frameworks at national and EU levels to enhance collective resilience against cyber threats.

This Chapter addresses the scope, objectives, and stakeholder responsibilities under NIS 2, including obligations for Member States, public and private entities, and their coordination mechanisms.

1. Introduction: evolution from the NIS Directive to NIS 2 Directive

As the digital landscape evolves, so does the complexity of cyber threats, which pose a significant risk to stability and security across the European Union (EU). Cyber disruptions can lead to substantial repercussions across Member States, thereby requiring EU-level interventions to safeguard the robustness of digital systems (Jacobs, 2023). Recognising the imperative

need to manage cybersecurity, the EU has been at the forefront of establishing comprehensive frameworks to protect its cybersecurity (Carrapico and Barrinha, 2017; Odermatt, 2018).

Nevertheless, cybersecurity, as a relatively nascent field, is not delineated as specific policy area under the EU law. The EU's competence is interpreted in relation to different policy areas (Jacobs, 2023). It falls under shared competence, allowing Member States to create legislation in this field unless the EU itself has already taken action (Jacobs, 2023). Therefore, any legal intervention taken by the EU must follow the principles of proportionality and subsidiarity, which means that the measures should be necessary and more efficiently implemented at the EU, rather than national, level. Moreover, the increasing significance of national security and technological sovereignty adds complexity to this framework, as these matters are primarily under the control of Member States (Chiara, 2024; Liebetrau, 2024). This overlap emphasises the difficulties in expanding the internal market ground of Article (Art.) 114 of the Treaty on the Functioning of the European Union (TFEU) to encompass complex cybersecurity issues, which are increasingly connected with fundamental rights, physical safety, and national security, rather than solely the operation of the internal market (Brandão and Camisão, 2022; Chiara, 2024; Liebetrau, 2024). Thus, although the EU has the competence to create laws, as per Art. 114, the extent and speed at which it can regulate are naturally constrained by these factors.

Considering these challenges, the EU adopted the Network and Information Systems (NIS 1) Directive (2016/1148) to increase the level of cybersecurity. It was the first cross-sectoral legislation aimed at enhancing cybersecurity across the EU. The NIS 1 Directive focused on cybersecurity in such essential services as energy, transport, and banking (enumerated under Annex II of the NIS Directive), which are crucial for the functioning of the economy, society, and digital service providers (namely online marketplaces, online search engines, and cloud computing service providers) under Annex III of the NIS 1 Directive.

In the realm of the rapid expansion of digitalisation and the increasing reliance on information technologies, it became apparent that the NIS 1 Directive needed a substantial update to address emerging challenges and technological dependencies (European Commission, 2020). It became evident that the scope of the NIS 1 Directive did not sufficiently cover all of the sectors now deemed critical due to advanced digitalisation and greater interconnectedness. This was a significant concern as the dependency on

digital platforms and services had escalated, necessitating a broader scope encompassing more sectors and entities (discussed in Section 2.1.). Moreover, the implementation of the NIS 1 Directive revealed inconsistencies across Member States due to varying interpretations of the Directive's criteria for determining responsible actors within it (European Commission, 2020). This resulted in a fragmented approach to cybersecurity, with some critical sectors being under-regulated in certain countries. For instance, significant disparities were noted in the inclusion of healthcare providers and major railway operators under the Directive's scope, leading to an uneven security state across the EU (European Commission, 2020, p. 14)

Considering these changes, the EU adopted the NIS 2 Directive (2022/2555), which, compared to its predecessor, is more comprehensive. It addresses the shortcomings identified in the initial implementation phase of the NIS 1 Directive into the national laws of Member States.

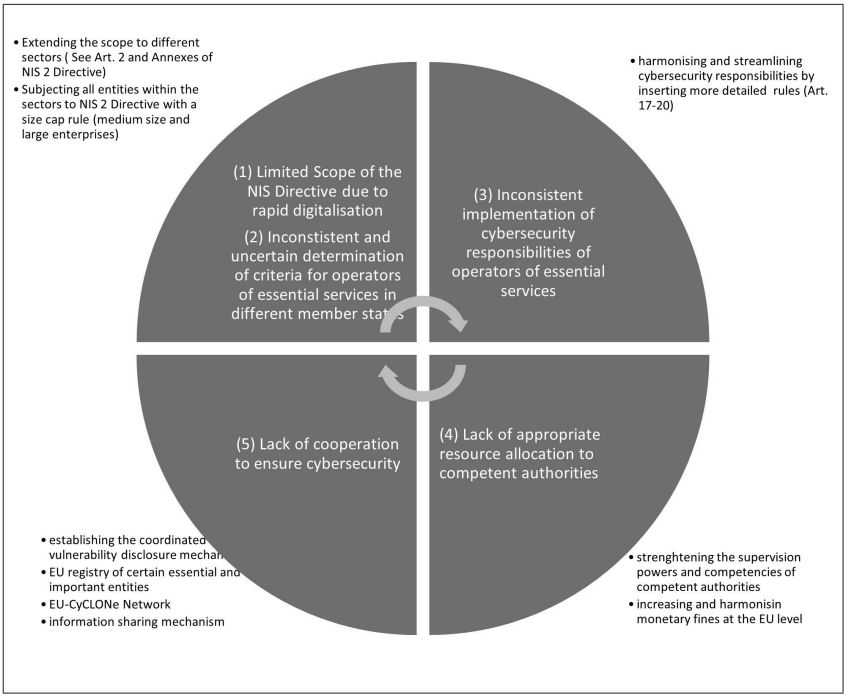

Figure 1: Overview of Challenges of NIS Directive and its Responses in NIS 2 Directive (Source: author)

As illustrated in Figure 1, the evaluation of the NIS 1 Directive underscored the need for systemic and structural changes, prompting the NIS 2 Directive. The NIS 2 Directive introduces several key enhancements aimed at strengthening the EU's cybersecurity framework (Vandezande, 2024). Firstly, it expands the scope to include a broader array of sectors and enterprises, reflecting the current digital reality and the critical nature of various services (Sievers, 2021, p. 2). This adjustment ensures that more entities are covered under the Directive, thereby enhancing the Union's overall security landscape. Secondly, the NIS 2 Directive aims to harmonise the cybersecurity requirements across Member States (Art. 21 NIS 2 Directive). It establishes clearer guidelines and criteria, aimed at minimising the previous ambiguities that led to inconsistent implementations of the NIS 1 Directive (Michels and Walden, 2018; Didenko, 2020). Thirdly, the NIS 2 Directive more strongly emphasises reporting incidents by providing more detailed requirements in such reports (Schmitz-Berndt, 2023). Thus, it requires more stringent and detailed obligations for entities, thus enhancing the resilience and response strategies against cyber threats. Fourthly, the Directive also aims to improve the mechanisms for cooperation both at national and EU levels, ensuring closer coordination when handling cyber incidents and crises. Fifthly, it strengthens the supervision and enforcement mechanisms of competent authorities, among others, by setting administrative fines for the breach of cybersecurity obligations imposed upon private and public actors.

However, it should be borne in mind that the Directive aims for minimum harmonisation in the realm of the EU's cybersecurity (Art. 5), meaning that Member States are given the flexibility to develop or maintain cybersecurity measures that exceed the established minimum requirements of the NIS 2 Directive, provided these enhanced measures are consistent with other obligations under EU law. This approach acknowledges the diverse cybersecurity needs and capabilities of different Member States while ensuring a foundational level of security that supports the collective resilience of the EU's digital sphere.

Due to its very nature (i.e., a Directive), the NIS 2 needs to be transposed to the domestic law of Member States. According to Art. 41, EU Member States are required to adopt and publish any necessary compliance measures by 17 October, 2024, and must begin implementing these measures the following day. Once done, Member States are obliged to notify the European Commission (EC) as soon as possible. In addition, any legislative

or regulatory actions taken by Member States to comply with the Directive must specify that they are referencing it explicitly.

Following this brief overview, the remainder of this Chapter seeks to examine the scope, objective, and responsibilities of different stakeholders (Member States, private and public actors, and the coordination between them at the EU level). For this purpose, Section 2 provides an analysis of the scope and purpose of the NIS 2 Directive. Section 3 analyses the obligations of Member States and the frameworks for cooperation at both national and European levels. Section 4 examines the obligations of the private and public actors recognised as essential and important entities. Finally, Section 5 offers certain conclusions.

2. The scope and objective of the NIS 2 Directive

This section explores four key areas: personal, jurisdictional, and material scope of the NIS 2 Directive, as well as the Directive's underlying aim. Personal scope refers to those who are responsible under the NIS 2 Directive, while jurisdictional scope pertains to how the jurisdictions of Member States are determined, and the material scope concerns what responsibilities the Directive imposes to ensure cybersecurity.

2.1 Personal scope of the NIS 2 Directive

The NIS 2 Directive applies to public and private entities in a sector referred to in Annexes I and II, which are qualified as medium-sized enterprises or those which exceed the threshold for such companies (i.e., those with over 250 employees, an annual turnover of more than 50 million EUR, and/or an annual balance sheet total of over 43 million EUR).

However, there are exceptions to this rule determining the scope. For instance, the NIS 2 Directive applies to entities regardless of the size specified in Annex I (Sectors of High Criticality) and Annex II (Other Critical Sectors), such as providers of public electronic communications networks or of publicly available electronic communications services, trust service providers, top-level domain name registries, and domain name system service providers (Art. 2(2)). This exception arises due to the criticality of the availability of these services for the operations of digital services, regardless of their categorisation as medium-size enterprises.

Moreover, Art.2(6)–(8) provides exceptions for the Directive's application to entities concerned with national security. This exception is due to the EU's lack of competence in relation to national security.

2.1.1 Bifurcation of entities under the NIS 2 Directive: Essential and important entities

Entities covered by the NIS 2 Directive are classified into two categories, "essential" and "important," based on their impact and criticality within their respective sectors (Art. 3). This distinction allows for a nuanced and risk-based approach to cybersecurity, ensuring that entities with the highest impact on cybersecurity are subject to more stringent security measures.

By defining these categories, the NIS 2 Directive not only prioritises where stringent cybersecurity measures are most needed, but also supports a broader goal of fostering a secure, resilient, and EU-wide digital environment. This approach ensures that the most critical services are subject to stringent supervision, while still maintaining a protective stance over other significant sectors. The classification of entities as either essential or important allows for a risk-based approach to their supervision.

Essential entities are those identified as critical to the infrastructure of societal and economic activities. According to Art. 3(1), essential entities include those which exceed the size of medium enterprises and operate within such crucial sectors as transport and digital infrastructure (Annex I). For example, the transport sector covers entities including air carriers, airport managing bodies, and railway undertakings – all of which are crucial for maintaining both freight and passenger mobility across (inter)national boundaries. As another example, digital infrastructure consists of internet exchange point providers, Domain Name System (DNS) service providers, and cloud computing service providers, reflecting the critical nature of maintaining robust digital services and infrastructure.

Important entities, while presumably not on the same critical scale as essential entities, still play significant roles within their sectors. Art. 3(2) (Annexes I and II) outline the scope of sectors which fall into this category. These entities are integral to supporting the functionality of broader societal and economic systems, but may have presumably a lesser direct impact on the availability of the critical services in society. Examples of these include postal and courier services, waste management, the manufacturing sector, and digital providers (online marketplaces, social networking services platforms, and online search engines).

According to recent estimates, the NIS 2 Directive is set to impact over 100,000 entities across the EU (EY, 2023). To establish the list of essential and important entities according to Art. 3(3)–(4), Member States must require those entities to submit specific information to the competent authorities. This includes the entity's name, its address, and current contact details, such as email, IP ranges, and telephone numbers. Additionally, entities must provide details about the relevant sector and subsector to which they belong (Annexes I and II), if applicable. This list shall be established by 17 April, 2025.

2.1.2 The different supervision and enforcement regime for essential and important entities

Indeed, under Arts. 21–24, essential and important entities share the same responsibilities (as discussed in Section 4). The categorisation of essential and important entities under the Directive is relevant for the supervision regime to which these entities are subject. While essential entities are subject to a fully-fledged supervision and enforcement regime (both ex-ante and ex-post), important entities shall be subject to a light ex-post supervisory framework.

Fully-fledged supervision means that competent authorities shall exercise their supervision and enforcement powers regardless of any indication of non-compliance of essential entities under Art. 32. In other words, without any indication of a cybersecurity incident, competent authorities can initiate random checks and on-site inspections for essential entities (Art. 32(a)).

In contrast, ex-post supervision and enforcement means that ex-post supervision by competent authorities may be initiated for important entities upon any indication on the probable non-compliance of those entities brought to the attention of competent authorities (Art. 33).

The underlying objective of this differentiation can be found in Recital 16 of the NIS 2 Directive. According to this Recital, which has an interpretative value despite its non-binding nature, the different supervision regimes to essential and important entities are based on the risk-based approaches and resource-allocation methods of the competent authorities. This approach implies that the risk of cybersecurity incidents occurring in the operations of important entities presumably cause comparably less harm to society than those of essential entities. Regarding the resource allocation of the competent authorities, more can be allocated to the full-fledged supervision and enforcement of essential entities.

2.2 Jurisdictional scope of Member States under the NIS 2 Directive

Art. 26 establishes jurisdictional scope of the Directive. As a main rule, important and essential entities fall within the jurisdiction of the Member States where they were established. However, there are three exceptions for this rule.

The first relates to entities that provide public electronic communication or publicly available electronic communication services. The second concerns digital services, and considers their intrinsic borderless nature. As per Art. 26(1)(b), among others, these entities include a variety of digital service providers, such as DNS providers, cloud computing services, and social media platforms. These entities are subject to the jurisdiction of the Member States where they have their "main establishment".

The definition of "main establishment" is further clarified in Art. 26(2) as the location where key decisions regarding cybersecurity risk management are made. If such a location cannot be determined, the main establishment is where cybersecurity operations are conducted or, failing that, to the establishment with the highest number of employees within the Union. This multi-tiered approach ensures that an entity cannot evade supervision by fragmenting operations across multiple locations. The third exception relates to public administration entities, placing them under the jurisdiction of the Member State that established them, thus aligning with traditional principles of governmental jurisdiction.

The NIS 2 Directive is also applicable entities that were not established in the EU but offer services within it (Art. 26(3)). Such entities must designate a representative in the EU, with jurisdiction falling to the Member State where this representative is located. This provision ensures that entities affecting EU citizens are accountable, even if based outside the Union.

2.3 Material scope of the NIS 2 Directive: data and availability of services as proxies to protect individuals and society

Cybersecurity is defined as the activities required to secure network and information systems, their users, and other people affected by cyber threats under Art. 2(1) of the Cybersecurity Act (EU) 2019/881. Article 6(3) of the NIS 2 Directive borrows the cybersecurity definition from the Cybersecurity Act.

This definition consists of two main components: the activities (1) and the security of network and information systems, their users, and people affected by cyber threats (2).

(1) Activities: There is no specific definition of the activities stipulated under the Cybersecurity Act. Instead, I here use the general definition of "activities". Activities mean actions conducted. More specifically, in the context of cybersecurity, these are all types of actions required to ensure the security of network information. Papakonstantinou (2022) coined the term of "cybersecurity as *praxis*" for the activities that ensure the security of networks and information systems. These measures and actions ensure that network and information systems cover organisational and technical processes for the security of network and information systems.

(2) The security of network and information systems, users, and other people affected by cyber threats: There is no definition of the security of network and information systems in the EU Cybersecurity Act. However, the NIS 2 Directive defines both of these.

Art. 6(1) of the NIS 2 Directive defines "network and information systems" as:

> (a) an electronic communications network within the meaning of Article 2, point (1), of Directive (EU) 2018/1972; (b) any device or group of interconnected or related devices, one or more of which, under a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for their operation, use, protection, and maintenance.

Additionally, Art. 6(2) states that the "security of network and information systems" means "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems". Thus, this security can be roughly defined as "being resilient to cyber threats". Cyber threats are specifically defined in Art. 4(8) of the EU Cybersecurity Act as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons". This component refers to the desired aim of cybersecurity, which is to ensure the security of network and information systems and its impact on its users and natural persons.

Neither the EU Cybersecurity Act nor the NIS 2 Directive clearly define users and other people. However, it is worth mentioning that the users of network and information systems include not only natural persons, but also legal ones, which is one of the ways of differentiating the scope of cybersecurity from data protection.

Cybersecurity is not a goal in and of itself, but rather aims to protect a variety of public and private interests. In so doing, the NIS 2 Directive uses data as proxies to protect these interests. The definition of "cybersecurity" in the EU Cybersecurity Act, in conjunction with the definition of security of network and information systems under the NIS 2 Directive, refers to the protection of data (both personal and non-personal) and the availability of services as proxies for protecting those interests (Brinker, 2024). The inclusion of personal data within the scope of cybersecurity responsibilities, as evidenced by the coordination framework under Art. 35 of the NIS 2 Directive with data protection authorities in addition to the inclusion of personal data into the definition of network and information systems, underscores the dual need to prevent data breaches and mitigate their consequences. Non-personal data are defined as the opposite of personal data, which is any information related to a natural person (Art. 4(1) of the General Data Protection Regulation (EU) 2016/679).[1] Non-personal data, while not directly linked to individual identities, hold significant value for the functioning of services and the broader economy (Pałka, 2023). This data type, encompassing everything from operational data in industrial systems to anonymised datasets used for big-data analytics, is critical for the operational continuity of services across the EU. The NIS 2 Directive's coverage of non-personal data reflects an understanding that the security of such data is important to preventing disruptions and maintaining trust in digital services.

Under the scope of the NIS 2 Directive, both personal and non-personal data play a critical role in cybersecurity. Personal data include such information as customer names, contact details, payment information, and browsing history held by online marketplaces. Such data are directly tied to individuals and must be protected to prevent identity theft, fraud, and privacy violations. On the other hand, non-personal data cover such operational information as product inventories, anonymised user behaviour analytics, pricing algorithms, and logistical information within these mar-

1 For more information about the GDPR, see Chapter 14 'EU Data Protection Law in Action: Introducing the GDPR' by Julia Krämer.

ketplaces. Although these data are not linked to specific individuals, their protection is essential for maintaining the efficiency and continuity of marketplace operations. The disruption or manipulation of non-personal data could lead to supply chain issues, distorted market information, or loss of trust in digital services. Therefore, the NIS 2 Directive's inclusion of both types of data reflects its broad approach to safeguarding critical digital ecosystems.

By imposing uniform cybersecurity responsibilities on all entities within its scope, the NIS 2 Directives minimises the variations in national implementations that previously led to disparities in cybersecurity readiness and response across the EU. This uniformity is crucial for creating a level playing field, ensuring that all critical sectors maintain high standards of data security, thereby enhancing collective cyber defences. The NIS 2 Directive also plays a significant role in bolstering trust among market participants and the public sector regarding cross-border data processing. By clarifying the security obligations for data, the NIS 2 Directive strengthens legal clarity for entities engaged in data processing and outsourcing, particularly in transnational contexts. This clarity is vital for entities relying on digital services that cross national boundaries, as it assures them of the continuous protection of their data under a unified EU-wide cybersecurity regime. Moreover, by encompassing all data types in its cybersecurity mandate, the Directive indirectly discourages data localisation practices that are often adopted as proxies for data security, which aligns with the Free Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807).

The availability of services is used as another proxy, which is mentioned as part of the security of network information systems under Art. 6(2) of the NIS 2 Directive. This shows the Directive's aim to make available those services that are minimally affected by cyber threats. All in all, the material scope of the Directive is not only the protection of data processed by essential and important entities, but also the continuity of the critical services they provide.

2.4 Objective of the NIS 2 Directive: solving underinvestment problem in cybersecurity

The objective of the NIS 2 Directive, similar to its predecessor (NIS 1), is to incentivise the investment in cybersecurity by private and public actors. There is an underlying assumption of the legal rules for cybersecurity that

more investment means a more secure digital environment. This assumption is predicated on the observation that, without a legal requirement, there is a dearth of investment in cybersecurity (discussed below in terms of underinvestment).

Threats from cyberspace can endanger society and citizens' security or safety (Taddeo, 2013). Significantly, the increased interconnectedness of various devices and systems across industries broadens the scope of cybersecurity policy problems (Lin and Saebeler, 2019). Due to how cybersecurity threats can harm individuals and society rather than organisations themselves, and the ways in which the harm may be dispersed, the firms or entities that use these information systems must take precautions to reduce the risk of cyber incidents. Taking action, on the other hand, has costs. When businesses make decisions, it is believed that they do so based on cost-benefit analyses due to the profit-making nature of their activities (Gordon, Loeb and Lucyshyn, 2014). These analyses are often conducted based on the costs likely to be incurred in the event of a security breach, such as actual harm caused by the breach and reputational damage in the event of exposure (Bauer and van Eeten, 2009). Underinvestment in cybersecurity results from failing to account for negative externalities, such as the costs suffered by other people or enterprises (Frye, 2002). The following statement by the executive of Sony Pictures illustrates the underinvestment issue in the cybersecurity context. The former executive director of Sony Pictures was quoted as saying, "[I]t's a reasonable business decision to take the risk of a security breach", and, in 2015, refused to invest $10 million to avert a possible 1$ million loss (Kostadinov, 2015). In another example, Cortez and Dekker (2022) held semi-structured interviews with 11 Chief (Information) Security Officers in the Benelux region, finding that firms' practises in relation to underinvesting in cybersecurity may be shifting, at least on the margins due to digitalisation during COVID-19 and the increased awareness amongst corporate stakeholders that cybersecurity is a key enabler (and disabler) of business continuity and resilience.

To fix this underinvestment issue, governments should make businesses responsible for reducing the security risks they pose (Clark-Ginsberg and Slayton, 2019). The NIS 2 Directive is a response to this problem as it requires public and private actors to ensure the security of network and information systems during their activities. If they are not compliant with these responsibilities, they can be faced with monetary fines or other sanctions.

Concerning the underinvestment problem and its relation with the adoption of the NIS 1 Directive, Porcedda (2018) described underinvestment as a root cause for the NIS 1 Directive's reason to impose cybersecurity responsibility upon certain private actors. To determine how the NIS 1 Directive (as the predecessor to the NIS 2 Directive) incentivised these actors to invest in cybersecurity, the European Network and Information Security Agency (ENISA) published reports on network and information systems investments in 2020 (ENISA, 2020). According to the report, the average expenditure on network and information system security by operators subject to the NIS 1 Directive was 40% lower than that of their US counterparts. The ENISA also issued a follow-up report in 2021, encompassing all 27 EU Member States and providing new insights into the allocation of network and information system budgets of the operators of essential services (OES)/ digital service providers (DSP) (ENISA, 2021). A survey of 947 organisations designated as OES/DSP across the 27 Member States was used to obtain data. In this second version of the report, in addition to covering all Member States, additional and supplementary questions were asked of the organisations assessed. Overall, 48.9% of the organisations polled said the NIS 1 Directive had a very significant or major impact on their cybersecurity. The fourth version, which included data collected from 1,080 OES/DSPs across all 27 EU Member States, affirmed the role of the NIS 1 Directive in cybersecurity investment in the EU (ENISA, 2023). As the NIS 2 Directive replaces the NIS 1 Directive, the objective to solve the underinvestment problem is still relevant for the former.

3. Responsibilities of Member States and cooperation structures for cybersecurity

This section consists of two parts. The first deals with the roles and responsibilities of Member States under the NIS 2 Directive for cybersecurity. The second concerns cooperation and collaboration within the realm of cybersecurity.

3.1 Responsibilities of Member States

State responsibilities in the realm of cybersecurity reflect the growing recognition that digital infrastructure is as vital to the security as physical

infrastructure. As discussed below, the adoption of cybersecurity strategies by Member States delineates the scope of proactive measures that states foresee to take. Cybersecurity is no longer merely a technical issue, but rather a matter of national resilience, where States play a role in creating protective frameworks. As another role of fostering collaboration between public and private actors to deal with cybersecurity incidents, Member States are tasked with establishing computer security incidents response teams and national cyber crisis management frameworks. These frameworks help States prepare for future cybersecurity incidents and form coordinated responses. A central aspect of state responsibility in cybersecurity is the enforcement of cybersecurity responsibilities by different public and private actors (see Section 4). This implementation is only possible by establishing competent authorities with appropriate enforcement power and competences.

3.1.1 Cybersecurity strategies

First, under Art. 7 of the NIS 2 Directive, each Member State is required to develop a national cybersecurity strategy that clearly outlines the strategic objectives and priorities, especially targeting critical sectors identified in the annexes of the Directive. The strategy must detail the necessary resources and a variety of policy and regulatory measures aimed at achieving and maintaining a robust level of cybersecurity. This includes a comprehensive governance framework to ensure the achievement of these objectives, which involves clear definitions of the roles and responsibilities of key stakeholders, such as national competent authorities, single points of contact, and Computer Security Incident Response Teams (CSIRTs).

The strategy shall establish effective cooperation and coordination both at the national level and with sector-specific authorities. Furthermore, the strategy must feature mechanisms for identifying key assets and assessing risks, policies for improving incident preparedness, response, and recovery, and cooperation between the public and private sectors. It should also list all authorities and stakeholders involved and establish a policy framework for information sharing on cyber and non-cyber risks and incidents among competent authorities.

Raising public awareness about cybersecurity is another critical component, aimed at enhancing the general cybersecurity knowledge of citizens. The strategy is also expected to cover policies related to cybersecurity in ICT supply chains, the inclusion of cybersecurity standards in public

procurement, and the management of vulnerabilities, including promoting coordinated vulnerability disclosure (Art. 12). Additionally, it must address the protection of the public core of the internet, promote the use of advanced cybersecurity technologies, and enhance cybersecurity education, training, and research. The strategy should support voluntary information sharing in accordance with Union law, strengthen cyber resilience and hygiene, particularly in small and medium-sized enterprises, and promote active cyber protection measures.

Member States must notify the EC of their adopted strategies within three months, keeping certain national security information confidential if necessary. They are also obliged to regularly assess and update their strategies at least every five years based on key performance indicators, with support available from the ENISA to ensure alignment with the Directive's requirements and obligations.

3.1.2 National cyber crisis management frameworks

The second requirement is to establish national cyber crisis management frameworks, outlined under Art. 9 of the NIS 2 Directive. These frameworks should be designed so as to handle large-scale cybersecurity incidents and crises effectively. Each Member State is required to designate or establish one or more competent authorities tasked with this critical role. These authorities, known as cyber crisis management authorities, must be equipped with adequate resources to perform their duties efficiently and effectively (Art. 9(1)). To ensure a unified approach to cyber crisis management, these frameworks must align with existing national crisis management systems. When multiple cyber crisis management authorities are established, a clear delineation of responsibilities is necessary, including the designation of a lead authority to coordinate the response to significant cybersecurity incidents and crises (Art. 9(2)). These authorities are also responsible for identifying necessary capabilities, assets, and procedures that can be mobilised in a crisis. Furthermore, each Member State must develop a comprehensive response plan for large-scale cybersecurity incidents and crises. This plan should outline the objectives of national preparedness measures, detail the responsibilities of the cyber crisis management authorities, and describe the procedures for managing cyber crises, including their integration into broader national crisis management frameworks and communication channels (Art. 9(4)). The plan should also include preparedness measures, such as regular exercises and training, and delineate

the roles of relevant public and private stakeholders. Within three months of establishing a cyber crisis management authority, Member States must notify the EC and the European cyber crisis liaison organisation network (EU-CyCLONe) of the authority's identity and any changes thereafter, as well as provide details of their national response plans, while maintaining the necessary discretion for national security reasons.

3.1.3 Establishment of competent authorities and single points of contact for cybersecurity

Under Art. 8 of the NIS 2 Directive, each Member State is mandated to designate or establish one or more competent authorities responsible for overseeing cybersecurity and performing supervisory duties. These authorities play a pivotal role in monitoring the implementation of the Directive at the national level.

Additionally, each Member State is required to designate a single point of contact to streamline communications and enhance cooperation. In cases where a Member State establishes only one competent authority, this entity also assumes the role of the single point of contact. The single point of contact is crucial for ensuring effective liaison functions, facilitating cross-border cooperation with authorities from other Member States, and engaging with the ENISA and EC. This role also extends to fostering cross-sectoral cooperation within the Member State, thus ensuring a cohesive approach to national cybersecurity efforts.

Member States must ensure that their designated competent authorities and single points of contact are equipped with sufficient resources to efficiently and effectively conduct their assigned tasks, thereby achieving the objectives outlined in the Directive. Member States are also required to promptly notify the Commission of the identity of these designated authorities and any changes to their roles or responsibilities. The identity of each competent authority is to be made public, and the EC is tasked with maintaining and publishing a list of all single points of contact to facilitate transparency and accessibility.

3.1.4 Computer Security Incident Response Teams (CSIRTS)

Under the NIS 2 Directive, each Member State is mandated to designate or establish one or more CSIRTs tasked with specific cybersecurity respon-

sibilities. These teams play a crucial role in managing and responding to cybersecurity incidents on a national level, and the scope of their competence must cover at least the sectors, subsectors, and types of entities listed in Annexes I and II of the Directive (Kamara and van den Boom, 2022).

To ensure effective operations under Art. 11, CSIRTs are required to comply with stringent requirements, including maintaining secure and resilient communication and information infrastructures to facilitate robust information exchanges with key stakeholders. CSIRTs' responsibilities include monitoring and analysing cybersecurity threats, vulnerabilities, and incidents within their jurisdictions. They are also tasked with providing timely warnings, alerts, and the dissemination of critical information to relevant entities and stakeholders, aiding in the (near) real-time monitoring of network and information systems (Art. 11(3)(a)). Additionally, CSIRTs respond to incidents and offer necessary assistance to affected entities, undertake forensic data analyses, and contribute to dynamic risk assessments and situational awareness concerning cybersecurity (Art. 11(3)(d)). Furthermore, CSIRTs are pivotal in the proactive scanning of networks to detect vulnerabilities, thus playing a proactive role in securing national and cross-border cyber infrastructures (Art. 11(3)(e)).

For example, under Art. 11 of the NIS 2 Directive, a national CSIRT might work closely with a large online marketplace, such as an e-commerce platform, to maintain secure communication channels. If the marketplace detects unusual activity indicative of a potential cyberattack, such as unauthorised access to customer data, the team would provide immediate support by analysing the incident and offering technical assistance. They would also issue timely alerts to other stakeholders, such as payment processors or logistics providers, to mitigate the broader impact. Additionally, the CSIRT might proactively scan the marketplace's network for vulnerabilities, such as weaknesses in payment gateways or customer databases, and provide guidance on how to strengthen its defences to prevent future incidents.

To bolster their effectiveness, CSIRTs are encouraged to engage in international cooperation and establish cooperative relationships with their counterparts in other countries. This global networking aims to enhance their capability to manage cyber threats more effectively and share critical information under secured protocols, including the traffic light protocol. They also participate in the CSIRTs network, providing mutual assistance and sharing best practices and technologies, thus further strengthening their response to cybersecurity challenges (Art. 11(3)(f)). The Directive also emphasises the importance providing these teams with sufficient resources

and access to secure working environments and redundant systems to ensure the continuity of their services (Art. 11(2)). Moreover, each Member State is required to designate one of its CSIRTS as a coordinator for vulnerability disclosure (Art. 11(3)(g)).

3.1.5 Cooperation at the national level

Under Art. 13 of the NIS 2 Directive, national-level cooperation among various cybersecurity bodies within Member States is crucial. Competent authorities, single points of contact, and CSIRTs are required to work collaboratively to fulfil the Directive's obligations. This includes the sharing and handling of notifications regarding significant incidents, cyber threats, and near misses. It also mandates that these entities not only cooperate internally, but also engage with law enforcement, data protection authorities, and other relevant national regulatory authorities. This integrated approach ensures that all notifications are effectively managed and that consistent information flow is maintained across different regulatory frameworks, thereby enhancing the level of national cybersecurity.

3.2 European vulnerability database and EU-level cooperation

This section discusses two main areas: the European vulnerability database and the EU-level cooperation structures designed in the NIS 2 Directive.

3.2.1 European vulnerability database

Art. 12 of the NIS 2 Directive requires coordinated vulnerability disclosure, achieved through the establishment of a European vulnerability database. The ENISA is tasked with developing and maintaining this database, which will serve as a central resource for registering publicly known vulnerabilities on a voluntary basis, providing access to all stakeholders. It is designed to enhance the security and integrity of ICT systems by including detailed information about each vulnerability, the affected products or services, the severity of the vulnerability, available patches, and, where patches are not available, guidance on mitigating risks. This structured approach to vulnerability disclosure and the centralisation of vulnerability information is aimed at strengthening cybersecurity across the EU by ensuring the timely

and effective communication and management of vulnerabilities, thereby reducing the risk of exploitation and enhancing the overall resilience of ICT infrastructures.

The focus on Art. 12's mandate for a European vulnerability database underscores the EU's commitment to transparency and security in managing ICT vulnerabilities. This database will play a pivotal role in centralising information on known vulnerabilities, thereby facilitating timely access to essential details for stakeholders across the EU. While the database's voluntary nature aims to encourage wide participation, this could be a double-edged sword, as it may limit comprehensive data collection if some stakeholders choose not to participate. Nonetheless, the overall goal is to create a more resilient and secure digital ecosystem by fostering coordinated vulnerability disclosure and information sharing.

3.2.2 EU-level cooperation

The NIS 2 Directive establishes a sophisticated structure for cooperation at both the EU and international levels to enhance the overall cybersecurity posture across Member States. This is articulated through the establishment of the Cooperation Group, the CSIRTs network, and the EU-CyCLONe, each playing a crucial role in facilitating strategic cooperation, information exchange, and coordinated response to cybersecurity incidents and vulnerabilities.

According to Art. 14, the Cooperation Group serves as a platform for strategic cooperation among Member States, fostering the trust and confidence necessary for effective cybersecurity governance. Comprised of representatives from Member States, the EC, and ENISA, the group is tasked with a wide array of responsibilities.

These include providing guidance on the transposition and implementation of the Directive (Art. 14(4)(a)), developing and implementing policies on coordinated vulnerability disclosure (Art. 14(4)(b)), exchanging best practices, and collaborating on emerging cybersecurity policy initiatives (Art. 14(4)(o)). The Group operates under biennial work programmes and includes a variety of participants, including the European External Action Service as an observer, which ensures a comprehensive approach to addressing cybersecurity issues (Art. 14(3)).

The Cooperation Group, through its strategic role, aims to harmonise the Directive's implementation across Member States, promoting a sense of unity in addressing cybersecurity challenges. The challenge here lies in bal-

ancing national interests with EU-level goals, especially in an environment that demands both trust and transparency among the Member States.

The network of national CSIRTs under Art. 15 is a critical component of the EU's cybersecurity infrastructure, promoting swift and effective operational cooperation among Member States. Moreover, it facilitates the exchange of information regarding capabilities, incidents, cyber threats, and vulnerabilities, and also plays a key role in coordinating responses to cross-border cyber incidents. ENISA provides the secretariat for the CSIRTs network, enhancing the support for cooperation among teams (Art. 15(2)). This network ensures that Member States are both informed and prepared to manage and mitigate cybersecurity incidents effectively.

As per Art. 16, EU-CyCLONe is aimed at improving the coordination of large-scale cybersecurity incidents and crises at the operational level. It helps in developing a shared situational awareness and supports decision-making processes during such crises. Composed of representatives from Member States' cyber crisis management authorities and the EC, EU-CyCLONe assesses the impact of large-scale incidents and proposes mitigation measures.

This organisation plays a crucial role in ensuring that Member States are prepared for, and can effectively manage, significant cybersecurity challenges. Under the Directive, EU-CyCLONe's tasks allow for a robust interaction between different cybersecurity bodies within the EU (Art. 16(3)). This includes regular meetings, joint exercises, and continuous information sharing that spans technical details to strategic policies. By fostering an environment where Member States can request assistance, share operational practices, and partake in joint supervisory actions, the Directive ensures that cybersecurity measures are not only unified across the EU, but also adaptable to the evolving nature of cyber threats.

Art. 19 introduces a voluntary peer review system, facilitated by the Cooperation Group with support from the EC, ENISA, and the CSIRTs network.

The system aims to promote shared learning, strengthen mutual trust, and enhance cybersecurity across Member States. The reviews focus on various aspects of cybersecurity, including risk management measures, reporting obligations, competent authorities' capabilities, operational capabilities of CSIRTs, mutual assistance, information-sharing arrangements, and cross-border or sector-specific issues. The methodology and review process are objective, non-discriminatory, transparent, and fair, incorporates both virtual and physical assessments, and ensure that information exchanges

adhere to confidentiality standards and national security protection. The experts are obligated to maintain the confidentiality of sensitive information and disclose any findings to third parties.

Post-review, the experts draft a report summarising their findings and conclusions, including recommendations for improvements. The reviewed Member State can comment on this draft, which is appended to the final report.

Recital 75 of the NIS 2 Directive emphasises that peer reviews should complement existing mechanisms, such as the CSIRTs network peer review system, avoiding the duplication and leveraging of past results. This framework supports the improvement of individual Member States' cybersecurity and fosters a collaborative environment where best practices are shared and collective cybersecurity resilience is bolstered.

4. Responsibilities of important and essential entities for cybersecurity under the NIS 2 Directive

The responsibility for ensuring cybersecurity rests largely with essential and important entities. There are three main responsibilities which these entities must bear. The first directs the managerial board to be personally involved in cybersecurity. The second is risk management responsibility, aimed at mitigating cyber risks arising from the operations of these entities. The third is the reporting of cybersecurity incidents to the competent authorities or CSIRTS, to recipients of their services, as well as to the public, where appropriate. In addition to these responsibilities, the NIS 2 Directive introduces a voluntary information-sharing framework on cybersecurity among these entities. This section analyses these responsibilities and this framework.

4.1 Responsibilities of managerial boards

The NIS 2 Directive addresses concerns related to the involvement of management boards in cybersecurity within essential and important entities. Recognising the limitations in management boards' engagement with cybersecurity issues, the Directive imposes new responsibilities to enhance this engagement and address the identified deficiencies.

Historically, senior management figures, such as chief executive officers (CEOs), chief financial officers (CFOs), and chief information officers

(CIOs) have been primarily responsible for overseeing a firm's cybersecurity strategies, which include assessing and mitigating security breaches. Research has indicated that IT expertise within the board is positively associated with a company's preparedness for cybersecurity incidents (Hartmann and Carmenate, 2021). Studies have shown that CEOs with IT expertise are more likely to detect and report breaches, and the presence of such IT executives as CIOs on the management team correlates with a reduced likelihood of security breaches and better overall preparedness (Haislip et al, 2017). Despite these positive associations, corporate boards continue to be general unprepared to handle cybersecurity incidents. A survey conducted by Cheng et al, (2021) revealed that only a minority of directors have an above-average or excellent awareness of their cybersecurity processes, highlighting a significant gap in effective cybersecurity management at the board level. This ineffectiveness is often compounded by a lack of necessary expertise and inadequate involvement in proactive cybersecurity management, which leads to cybersecurity being treated as a lower priority issue that is often delegated to lower operational levels.

The NIS 2 Directive aims to rectify these shortcomings by explicitly requiring management boards to approve and oversee the cybersecurity risk management measures of their entities. Art. 20(1) mandates that Member States ensure that management bodies of essential and important entities not only approve, but also actively oversee, these risk management measures. Furthermore, to address the expertise gap, Art. 20(2) stipulates that board members must undergo training to enhance their understanding of cybersecurity risks, which should also be regularly encouraged for all employees. Additionally, the Directive strengthens accountability by providing enforcement powers to hold management boards liable for non-compliance with their cybersecurity obligations. According to Arts. 32(6) and 33(5), respectively, natural persons acting as representatives of essential and important entities (likely including members of the management board) can be held personally liable for breaches of the Directive's responsibilities. The specifics of this liability are determined by individual Member States, but the inclusion of such measures underscores the Directive's serious commitment to ensuring management boards' active and knowledgeable involvement in cybersecurity.

In sum, the NIS 2 Directive introduces targeted measures to significantly enhance the role of management boards in cybersecurity, addressing well-documented gaps in involvement and expertise. By mandating direct oversight and accountability of management boards in cybersecurity matters,

coupled with required training for board members, the Directive aims to elevate the strategic importance of cybersecurity within corporate governance structures and ensure a more robust and proactive management of cybersecurity risks.

4.2 Risk management responsibility

The NIS 2 Directive revises the risk management framework established by its predecessor, focusing on enhancing and clarifying the responsibilities of essential and important entities rather than introducing substantial structural changes.

The NIS 2 Directive delineates several key areas of adjustment, primarily aimed at providing a more comprehensive and nuanced understanding of cybersecurity risks and management. First, the NIS 2 Directive modifies the terminology used in its predecessor, changing "Security Requirements" to "Cybersecurity Risk Management Measures". This change, reflected in Art. 21 of the NIS 2 Directive, aims to encapsulate a broader definition of cybersecurity, not only ensuring the security of network and information systems, but also safeguarding the users and other parties impacted by cyber threats (Papakonstantinou, 2022; Biasin and Kamenjasevic, 2022). This aligns with the definitions provided in the EU Cybersecurity Act, which include activities necessary to secure both networks and the broader digital environment from cyber threats.

Article 21(1) of the NIS 2 Directive stipulates that entities must adopt appropriate and proportionate technical, operational, and organisational measures to manage risks to network and information systems. These measures are crucial for maintaining the integrity and security of operations and minimising the impact of any incidents on service recipients and other services. While the emphasis on network and information system security continues from NIS Directive 1, its successor introduces clearer language and requirements, specifically addressing the broader impacts of cybersecurity incidents.

A significant aspect of the Directive involves specific requirements across organisational, technical, and operational measures. Entities are mandated to establish robust governance frameworks that clearly define cybersecurity responsibilities and ensure regular staff training. Additionally, they must develop incident response plans and effectively manage risks associated with third-party service providers. Technical measures require entities to

maintain system security through state-of-the-art technology, enforce strict access control, and engage in continuous monitoring to detect and respond to threats promptly. Operational measures under the NIS 2 Directive include conducting regular risk assessments and developing business continuity plans to ensure resilience in the face of disruptions. It also mandates the regular testing and auditing of cybersecurity measures to ascertain their effectiveness. Furthermore, the Directive encourages entities to adopt cyber hygiene practices, which are vital for mitigating risks from social engineering and other cyber threats.

Art. 21 of the NIS 2 Directive also emphasises the importance of proportional measures in cybersecurity. Moreover, Art. 18(1) specifically considers the costs of implementation, the entity's exposure to risks, and the potential societal and economic impacts of incidents when assessing the proportionality of security measures. This ensures that, while the cybersecurity measures should be robust, they should not necessarily aim for perfection, but rather be proportionate to the risks involved. Furthermore, the Directive aligns with international and European standards, such as ISO 27001, which advocates for an all-hazards approach to security, which is specifically mentioned in Recital 79 of the NIS 2 Directive. This approach is not limited to cyber threats, but also includes other potential risks, such as natural disasters or operational disruptions, thus ensuring comprehensive protection across various scenarios.

Upon conducting a statutory interpretation of the NIS 2 Directive and analysing the cyber kill chain model, Ferguson (2023) observed that the cybersecurity risk management measures outlined in the Directive may have significant limitations in effectively mitigating cyberattacks targeting essential and important entities within EU Member States. This limited efficacy was mainly attributed to the restricted extent of the measures, which notably lack specific methods for targeting the reconnaissance phases of cyberattacks. The Directive does not mandate such key security practices as denial, vulnerability scanning, or threat modelling during reconnaissance phases, which are crucial for anticipating threat actor's tactics (Ferguson, 2023). This leaves essential and important entities at risk of losing information superiority as they prepare for future attack phases, especially the weaponisation phase (Ferguson, 2023). Despite access to threat intelligence, essential and important entities are not required to leverage it effectively, potentially compromising their mitigation capacities.

Regarding risk management responsibility, the EC adopted Implementing Regulation (2024/2690) on cybersecurity measures of the NIS 2 Di-

rective for a variety of important and essential entities (including cloud computing service providers and online marketplaces), according to the mandate given in Art. 21(5) of the Directive. The Implementing Regulation, which is directly applicable and does not need to be implemented in national laws, along with its Annex, establishes comprehensive requirements for cybersecurity measures under Art. 21 of the NIS 2 Directive. The purpose of the Implementing Regulation is to establish uniform cybersecurity standards for digital entities across all Member States. Notably, its Annex, spanning 26 pages, exceeds the length of the Regulation itself. It offers a thorough and detailed explanation of key policies, including the security of network and information systems outlined in Art. 21(2)(a) of the NIS 2 Directive, as well as the incident handling policy specified in Art. 21(2)(b).

In conclusion, compared to its predecessor, the NIS 2 Directive's adjustments primarily function to clarify and slightly extend the responsibilities and requirements for cybersecurity risk management. By emphasising a balanced approach that includes robust protection mechanisms and practical, proportionate measures, the Directive aims to enhance the resilience of network and information systems across the EU. The integration of clearer requirements and the expansion of the scope of risk management reflect a concerted effort to foster a safer and more secure digital environment across Europe.

4.3 Reporting responsibility of essential and important entities

In the NIS 2 Directive, there are three different notification responsibilities imposed upon essential and important entities. These are notifications to competent authorities or CSIRTs, the recipients of the services, and to the public.

4.3.1 Notification to CSIRT or competent authorities

According to Art. 23(1) of the NIS 2 Directive, notification to competent authorities or CSIRT is required for any incident having a significant impact on their services. Not all incidents trigger notification responsibility, but those with severe operational disruption or financial losses for the entity concerned are subject to notification. The parameters of an incident having a significant impact include references to not only organisational harm, but

also to considerable material or non-material losses of legal and natural persons, as per Art. 23(3).

The NIS 2 Directive provides a three-tier approach to notification, with reporting conducted at three-time intervals: an early warning, an incident notification, and final reporting. CSIRTs or competent authorities can request an intermediate report on relevant status updates between incident notification and final reporting, as per Art. 23(4)(c). This approach aims to strike a balance between swift reporting and allowing entities to seek support and draw valuable lessons to improve their resilience to cyber threats. Art. 23(4)(a) sets down the scope of an early warning, which entities must submit within 24 hours after essential and important entities become aware of the incident. Recital 102 of the NIS 2 Directive states that this early warning should not result in the diversion of resources for preparation of early warning.

Art. 23(4)(b) sets forth a second notification, called an incident notification, which must be sent within 72 hours of becoming aware of the incident. This notification should include an update on the elements of early warning, an initial assessment of its severity and impact, and indicators of compromise.

Art. 23(4)(d) outlines the submission of the final report, which includes a detailed description of the incident, its severity and impact, the type of threat or root causes, mitigation measures implemented, and its cross-border impacts. If the incident is still ongoing, essential and important entities must provide a progress (instead of a final) report.

4.3.2 Notification to the recipients of services

There are two different notifications to the recipients of the entities' services: notification of the incidents that significantly impact the provision of their services and communication of a significant cyber threat. Despite the novelty of the notification to the recipients under the NIS 2 Directive, the Directive and its Recitals are notably silent on the underlying objective of these notifications. The question is then what would be the objective of requiring entities to notify their recipients of the incident that have a likely adverse impact on the provision of services? This type of notification serves two different purposes, namely deterrence for the entities from taking inappropriate measures due to reputational damage of the incident, and the mitigation of harms caused to the recipients of services. The former is served through its exposure of the incident and possible negligence of the

entities to their clients. It serves the latter by allowing recipients of services to take appropriate measures to mitigate possible damage.

4.3.3 Notification of the incident to the recipients of services

The NIS 2 Directive outlines three conditions for notification to the recipients of the services under Article 23(1): (1) an incident meeting the requirements of a significant impact, (2) an incident likely to adversely affect the provision of the service, and (3) the notification being deemed appropriate. These recipients can be both natural and legal persons.
The scope of notification in the NIS 2 Directive should include the information to serve the objectives of deterrence and mitigation. It should include information on the extent to which recipients of services should take measures to mitigate damages, the potential impact of the incident on recipients, and the overview of technical and organisational measures to mitigate the incident's impacts.

According to Art. 23(1), notification to recipients of service shall be done without undue delay. There is no specific time limit imposed on entities for notification to recipients, but Member States can either stipulate these or provide discretionary guidelines. The time of notification serves the objective of deterrence and mitigation, ensuring that entities notify recipients as soon as possible to prevent collateral damages.

4.3.4 The communication of significant cyber threats to the recipients of services

Art. 23(2) of the NIS 2 Directive mandates Member States to impose responsibility upon essential and important entities to inform recipients of their services affected by a significant cyber threat of any measures or remedies they can take in response. It also requires entities to inform recipients of the threat itself, if applicable. A "significant" cyber threat is defined as one which could severely impact an entity's network and information systems, causing consequential (non-)material losses. The notification of such threats should be given with best efforts and not relieve entities of their obligation to take immediate measures to prevent or remedy the threat and restore the service's normal security level. The information should be free of charge and written in simple language. This responsibility is unique

to the NIS 2 Directive, as it is related not only to the incident, but also to the significant cyber threat. This type of notification can be justified based on the mitigation objective, allowing essential and important entities to inform recipients of a significant cyber threat without undue delay, thereby enabling them to take appropriate measures to mitigate potential losses.

As an illustration, according to Art. 23(2) of the NIS 2 Directive, if an online marketplace experiences a significant cyber threat, such as a vulnerability that could expose customer payment details, the marketplace must promptly inform its users about the threat. This notification would include clear instructions on steps users can take to protect themselves, such as changing their passwords or monitoring their accounts for suspicious activity. The marketplace would also need to explain the nature of the threat in simple, accessible language and provide this information free of charge. Further to informing its users, the marketplace must still take immediate action to fix the vulnerability and restore normal security levels, ensuring the protection of both the users and platform.

4.3.5 Notification to the incident to the public

The NIS 2 Directive imposes the responsibility to notify the public of cybersecurity incidents in certain circumstances. Indeed, Art. 23(7) states that, after consulting with the entities involved in a cybersecurity incident, the relevant authorities or CSIRTs from other affected Member States can inform the public. They may also require these entities to inform the public if awareness is needed to prevent or manage the incident, or if sharing the information is in the public's interest.

4.3.6 Information sharing on voluntary basis

Information-sharing practices are crucial in cybersecurity, as they help prevent, detect, respond to, or mitigate incidents by raising awareness about, and limiting the spread of, cyber threats (Cormack, 2021; Kolini and Janczewski, 2022). Art. 29 of the NIS 2 Directive requires Member States to ensure that essential and important entities exchange relevant cybersecurity information while respecting the GDPR. Recital 119 emphasises the importance of regular threat and vulnerability intelligence sharing between institutions for the effective detection and prevention strategies.

Entities should be encouraged to pool their expertise and experience at strategic, tactical, and operational levels to strengthen their capacity to analyse, monitor, defend against, and respond to cyber threats effectively. Facilitating voluntary information sharing platforms at the Union level is significant. Thus, Member States should actively promote and encourage participation by relevant entities not covered by this Directive.

Art. 29(2) foresees the conclusion of information-sharing arrangements when potentially sensitive information is exchanged, including between the cybersecurity service providers of important and essential entities. Art. 29(3) specifies the scope of these arrangements, specifying operational elements, content, and conditions of information sharing. Member States may impose conditions on information provided by competent authorities or CSIRTs. Art. 7(2)(h) of the NIS 2 Directive requires Member States to support the application of such arrangements, and essential and important entities must notify competent authorities when participating in, or withdrawing from, information-sharing arrangements (Art. 29(4)).

In addition to these, the Directive also stipulates voluntary notification of cyber threats and near misses by essential and important entities under Art. 30(1). It also opens a room for the notification of significant incidents, cyber threats, and near misses by other entities outside the Directive's scope. This provision seeks to obtain a comprehensive situational picture of cybersecurity in the EU without imposing obligations to other entities.

5. Conclusion

The NIS 2 Directive aims to strengthen cybersecurity in the EU by making structural changes to the NIS 1 Directive. It promotes investment in cybersecurity by both private and public entities, recognising that allocating resources for cybersecurity measures is essential for protecting the digital landscape.

A significant challenge for the Directive is the extension of the scope of entities responsible for ensuring cybersecurity. The new categorisation of important and essential entities eliminates the distinction between OESs and DSPs, and subjects all important and essential entities to the same provisions. However, there is a difference in the supervision and oversight regime, with essential entities being subject to full-fledged supervision and important entities only requiring demonstration of compliance ex-post.

The NIS 2 Directive takes a data agnostic approach to cybersecurity, covering all types of data processed by essential and important entities.

It also requires Member States to develop national cybersecurity strategies, outlining strategic objectives, priorities, and resources, as well as establishing effective cooperation and coordination mechanisms between public and private sectors. The Directive establishes a new cybersecurity framework, which includes coordinated vulnerability disclosure and the establishment of a European vulnerability database. The ENISA is made responsible for maintaining this database, which seeks to enhance the security and integrity of ICT systems.

The NIS 2 Directive also establishes a cooperation structure at the EU level, with the Cooperation Group, CSIRTs network, and EU-CyCLONe playing crucial roles in facilitating strategic cooperation, information exchanges, and coordinated responses to cybersecurity incidents and vulnerabilities.

Essential and important entities have responsibilities for network and information system security, including involving the managerial board in cybersecurity, mitigating cyber risks, and reporting incidents to authorities. The NIS 2 Directive introduces a voluntary information-sharing framework to address limitations in engagement with cybersecurity issues. Furthermore, it aims to enhance network and information system resilience by clarifying cybersecurity risk management responsibilities and expanding the scope. It includes notification responsibilities for entities to competent authorities, recipients of services, and the public. Timely and appropriate notifications serve deterrence and mitigation purposes, and collaboration and voluntary information sharing platforms at the Union level are encouraged.

Overall, the NIS 2 Directive aims to strengthen cybersecurity in the EU by addressing the ineffectiveness of cybersecurity management, expanding the scope of entities responsible for cybersecurity, and establishing frameworks for cooperation, information sharing, and incident reporting. It emphasises the importance of investment in cybersecurity and the protection of critical sectors.

Acknowledgements

This research has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101057844 (iFLOWS Project).

References

Bauer, J.M. and van Eeten, M.J.G. (2009) 'Cybersecurity: stakeholder incentives, externalities, and policy options', *Telecommunications Policy*, 33(10–11), pp. 706–719.

Biasin, E. and Kamenjasevic, E. (2022) 'Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive Proposals', *International Cybersecurity Law Review*, 3, pp. 163-180.

Brandão, A.P. and Camisão, I. (2022) 'Playing the market card: The Commission's strategy to shape EU cybersecurity policy', *JCMS: Journal of Common Market Studies*, 60(5), pp. 1335–1355.

Brinker, N. (2024) 'Identification and demarcation – a general definition and method to address information technology in European IT security law', *Computer Law & Security Review*, 52, 105927 [Online]. Available at: https://doi.org/10.1016/j.clsr.2023.105927 (Accessed: 5 February 2025).

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.

Cheng, J.Y.-J., Groysberg, B., Healy, P. and Vijayaraghavan, R. (2021) 'directors' perceptions of board effectiveness and internal operations', *Management Science*, 67(10), pp. 6399–6420.

Chiara, P.G. (2024) 'Towards a right to cybersecurity in EU law? The challenges ahead', *Computer Law & Security Review*, 53, 105961 [Online]. Available at: https://doi.org/10.1016/j.clsr.2024.105961 (Accessed: 5 February 2025).

Clark-Ginsberg, A. and Slayton, R. (2019) 'Regulating risks within complex sociotechnical systems: evidence from critical infrastructure cybersecurity standards', *Science and Public Policy*, 46(3), pp. 339–346.

'Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (Text with EEA relevance)' (2024) *Official Journal* L [Online]. Available at: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng (Accessed: 21 January 2025).

Cormack, A. (2021) 'NISD2: a common framework for information sharing among network defenders', *SCRIPTed: A Journal of Law, Technology and Society*, 18(1), pp. 83–98.

Cortez, E.K. and Dekker, M. (2022) 'A corporate governance approach to cybersecurity risk disclosure', *European Journal of Risk Regulation*, 13(3), pp. 1–23.

Didenko, A.N. (2020) 'Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond', *Uniform Law Review*, 25(1), pp. 125–167.

'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)' (2022) *Official Journal* L 333, 27 December, pp. 80–152 [Online]. Available at: http://data.europa.eu/eli/dir/2022/2555/oj/eng (Accessed: 18 April 2024).

ENISA (2020) *NIS investments report 2020*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/nis-investments (Accessed: 7 April 2022).

ENISA (2021) *NIS investments report 2021*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/nis-investments-2021 (Accessed: 5 October 2022).

ENISA (2023) *NIS investments report 2023*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/nis-investments-2023 (Accessed: 18 April 2024).

European Commission (2020). *Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union (Accessed: 18 April 2024).

EY (2023) *Five things to know if your company falls under the scope of NIS2*. EY [Online]. Available at: https://www.ey.com/en_dk/cybersecurity/five-things-to-know-if-your-company-falls-under-the-scope-of-nis2 (Accessed: 18 April 2024).

Ferguson, D.D.S. (2023) 'The outcome efficacy of the entity risk management requirements of the NIS 2 Directive', *International Cybersecurity Law Review*, 4(4), pp. 371–386.

Frye, E. (2002) 'The tragedy of the cybercommons: overcoming fundamental vulnerabilities to critical infrastructures in a networked world', *The Business Lawyer*, 58(1), pp. 349–382.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2014) 'Cybersecurity investments in the private sector: the role of governments', *Georgetown Journal of International Affairs*, 15(SI), pp. 79–88.

Haislip, J., Lim, J.H. and Pinsker, R. (2017) 'Do the roles of the CEO and CFO differ when it comes to data security breaches?', in *AMCIS 2017 – America's Conference on Information Systems: A Tradition of Innovation* [Online]. Available at: https://scholars.ttu.edu/en/publications/do-the-roles-of-the-ceo-and-cfo-differ-when-it-comes-to-data-secu (Accessed: 16 November 2022).

Hartmann, C.C. and Carmenate, J. (2021) 'Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: implications for practice, policy, and research', *Current Issues in Auditing*, 15(2), pp. A9–A23.

Jacobs, B. (2023) 'A comparative study of EU and US regulatory approaches to cybersecurity in space', *Air and Space Law*, 48(4/5) [Online]. Available at: https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\AILA\AILA2023052.pdf (Accessed: 10 April 2024).

Kamara, I. and van den Boom, J. (2022) *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices*. Den Haag: National Cybersecurity Centre.

Kolini, F. and Janczewski, L.J. (2022) 'Exploring incentives and challenges for Cybersecurity Intelligence Sharing (CIS) across organizations: a systematic review', *Communications of the Association for Information Systems*, 50(1), pp. 86–121.

Kostadinov, D. (2015) *How harmful can a data breach be?* Infosec Resources [Online]. Available at: https://resources.infosecinstitute.com/topic/the-cost-of-a-data-breach-how-harmful-can-a-data-breach-be/ (Accessed: 4 October 2022).

Liebetrau, T. (2024) 'Problematising EU cybersecurity: exploring how the single market functions as a security practice', *JCMS: Journal of Common Market Studies*, 62(3), pp. 705–724. Available at: https://doi.org/10.1111/jcms.13523.

Lin, W.C. and Saebeler, D. (2019) 'Ris-based v. compliance-based utility cybersecurity – a false dichotomy?, *Energy Law Journal*, 40, pp. 243-282.

Michels, J.D. and Walden, I. (2018) 'How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=3297470 (Accessed: 18 April 2024).

Odermatt, J. (2018) 'The European Union as a cybersecurity actor' in *Research Handbook on the EU's Common Foreign and Security Policy*. Edward Elgar Publishing, pp. 354–373.

Pałka, P. (2023) 'Harmed while anonymous: beyond the personal/non-personal distinction in data governance', *Technology and Regulation*, 2023, pp. 22–34.

Papakonstantinou, V. (2022) 'Cybersecurity as praxis and as a state: the EU law path towards acknowledgement of a new right to cybersecurity?', *Computer Law & Security Review*, 44, 105653 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105653 (Accessed: 5 February 2025).

Porcedda, M.G. (2018) 'Patching the patchwork: appraising the EU regulatory framework on cyber security breaches', *Computer Law and Security Review*, 34(5), pp. 1077–1098.

'Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance)' (2018) *Official Journal* L 303, 28 November, pp. 59–68 [Online]. Available at: http://data.europa.eu/eli/reg/2018/1807/oj/eng (Accessed: 24 April 2024).

Schmitz-Berndt, S. (2023) 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive', *Journal of Cybersecurity*, 9(1), p.tyad009 [Online]. Available at: https://doi.org/10.1093/cybsec/tyad009 (Accessed: 5 February 2025).

Sievers, T. (2021) 'Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations', *International Cybersecurity Law Review*, 2(2), pp. 223–231.

Taddeo, M. (2013) 'Cyber security and individual rights, striking the right balance', *Philosophy & Technology*, 26, pp. 353–356.

Vandezande, N. (2024) 'Cybersecurity in the EU: how the NIS2-directive stacks up against its predecessor', *Computer Law & Security Review*, 52, p.105890. Available at: https://doi.org/10.1016/j.clsr.2023.105890.