ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act

Sandra Schmitz-Berndt Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg, ORCID: 0000-0001-9443-9206

Mark D. Cole Faculty of Law, Economics and Finance, Department of Law, University of Luxembourg, Luxembourg, ORCID: 0000-0003-4382-8791

Abstract

Cybersecurity regulation in the EU has long been implemented in a piecemeal fashion resulting in a fragmented regulatory landscape. Recent developments triggered the EU to review its approach which has not resulted in the envisaged high level of cyber resilience across the Union. The paper addresses the EU's limited mandate to regulate cybersecurity and outlines how the internal market rationale serves as a basis to harmonise cybersecurity legislation in the EU Member States. In that regard, the recent Proposal for a NIS 2.0 Directive (adopted by the European Parliament in November 2022) and the Proposal for a Cyber Resilience Act (published in September 2022) highlight how the EU seeks to align legislation and reduce complexity between different, often sectoral regulatory approaches to cybersecurity, while at the same time extending regulation in a view to achieve a high level of cybersecurity across the EU. As regards the latter, the paper also outlines how the Cyber Resilience Act will complement the NIS 2.0 Directive in order to close existing regulatory gaps.

Keywords

Cyber Resilience Act, cybersecurity, EU legislative framework, NIS 2.0 directive

Received: 07.11.2022
Accepted: 05.12.2022
Published: 08.12.2022

Cite this article as:
S. Schmitz-Berndt, M.D. Cole, "Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act," ACIG, vol. 1, no. 1, 2022, DOI: 10.5604/01.3001.0016.1323

Corresponding author:
Sandra Schmitz-Berndt, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, 6, avenue de la Fonte, L-4363 Esch-sur-Alzette, Luxembourg; ORCID: 0000-0001-9443-9206; E-mail: sandra.schmitz@uni.lu

1. Introduction

Cybersecurity threats concern every legal entity and every natural person in our society. With digital transformation and interconnectedness of society, network and information systems (NIS) have developed into an essential commodity in everyday life. The COVID-19 pandemic triggered a shift to remote working with a surge in connections from private to corporate systems and an unprecedented adoption of telecommuting and video conferencing. With telework becoming the norm in many sectors and industries, many corporate networks became more vulnerable to cyberattacks. At the same time, physical and digital infrastructures are increasingly interconnected and interdependent. Also, different services and sectors of our economies are interconnected and are growing more dependent on NIS than ever before. Apart from the economic aspect, the speedy digital transformation also means that our society is more interconnected.

The unprecedented digital dependencies that we see today mean that there is to an increased attack surface posing numerous challenges of managing cybersecurity [1]. The steady increase in the number of users and connections also creates new vulnerabilities [2]. New opportunities arise for cyber-dependent crime. Not surprisingly, within the last months, a notable increase in the number of cyberattacks on citizens, businesses and critical infrastructures has been reported [2] including for instance ransomware attacks on health services [3, 4], and on public administration [5]. In 2021, Germany faced a 360% increase of such ransomware attacks [4]. Cyberattacks also targeted a range of EU institutions, including the European Commission, the European Medicines Agency and the European Banking Authority [6]. Earlier large scale cyber espionage campaigns on agencies and ministries across the European states targeted for instance the Norwegian Parliament [7], the German Parliament and the federal government's internal communications network [8], and a French software form which supplies the French Ministry of Justice [9]. There is sufficient evidence that the number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and that this presents a major threat to the functioning of network and information systems (NIS). A disruption in one state can have cascading effects with ramifications in numerous other states.

Furthermore, renewed geopolitical tension between the West, Russia and China, and ultimately Russia's war of aggression against Ukraine have proven that the resilience of EU critical infrastructures is at risk from both physical and cyber threats [10]. This has only recently been highlighted by for instance the sabotage of the Nord Stream gas pipelines [11], the German rail network [12] and the cyberattack on the U.S. telecommunications company Viasat which was launched in parallel to the physical invasion of Ukraine and that affected customers across Europe [13].

Against that background, states and also the EU are becoming very active to strengthen the physical and cyber resilience with the latest effort being a Proposal for a Commission Recommendation to strengthen the resilience of critical infrastructures [14] in October 2022. Also, in June 2022, a political agreement [15] has been reached on the Proposal for Directive on the resilience of critical entities [16], which seeks to revise the current approach to critical infrastructure protection taken under the European Critical Infrastructures Directive[1]. Apart from legislative activities in the area of physical security, in the area of cybersecurity, the EU Commission [10] stresses the need for the application of an updated and comprehensive legal framework to be accelerated in order to strengthen cyber resilience, while at the same time striving to become a leader in cybersecurity [17]. As such, cybersecurity has been a top priority of the EU Commission since the first cybersecurity strategy in 2013 [18], which marked the formal establishment of 'cybersecurity' as a new policy area; followed by the Digital Single Market Strategy for Europe [19], where the digitalisation of the internal market is characterised by a high degree of trust, security, safety and choice for consumers. In 2022, significant steps have been taken to advance the regulation of cybersecurity: most importantly, following a political agreement [20] on the Proposal for a new NIS Directive (NIS 2.0 Proposal) [21] in May 2022[2],

[1] Council Directive 2008/114/EC of 08.12.2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75. The ECI Directive only applies to the energy and transport sectors.

[2] The NIS 2.0 Proposal mirrors the approach taken by the aforementioned Proposal for a CER Directive for the cyber dimension of the services covered; matters covered by the NIS 2.0 Directive will be excluded from the scope of the CER Directive.

the European Parliament adopted a consolidated text of the Proposal [22] in a first reading on 10 November 2022. The NIS 2.0 Directive will replace the existing 2016 NIS Directive[3]. In the same parliamentary session, the European Parliament adopted a consolidated text for a Regulation on digital operational resilience for the financial sector (DORA Regulation) [23], which seeks to strengthen the IT security of financial entities. Cybersecurity is also subject to two proposals aiming to boost cybersecurity and information security in EU institutions, bodies, offices and agencies [24, 25][4] of March 2022, and the Proposal for a Cyber Resilience Act (CRA Proposal) [26] of September 2022.

This paper will first provide an introduction into the regulation of cybersecurity in the EU in general, in particular into the EU mandate to regulate cybersecurity (section 2), before it will address in detail how the NIS 2.0 Directive and the CRA seek to improve the overall cybersecurity across the EU (section 3.). The focus on the NIS 2.0 Directive and the CRA is owed to the fact that both instruments regulate cyber aspects of ICT horizontally instead of introducing different, sectoral regulatory approaches to cybersecurity: the NIS 2.0 Directive addresses specific services based on digital infrastructures, while the CRA addresses the underlying technology of digital products and ancillary services. Section 3 also addresses how the NIS 2.0 Directive and the CRA reflect a risk-based approach to technology regulation and how they complement each other.

2. Cybersecurity Regulation in the EU in General

2.1. Cybersecurity as a EU Policy Field

The EU's approach to cybersecurity policy is mainly addressed in the EU Cybersecurity Strategies. The first EU Cybersecurity Strategy [18] of February 2013 represented the EU's comprehensive vision on how to best prevent and respond to cyber disruptions and attacks while at the same time furthering European values of freedom and democracy and ensuring the digital economy can safely grow. The Strategy also provided – although only in a footnote – a definition of cybersecurity as cybersecurity commonly referring 'to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure' [18]. Accordingly, the primary objectives of cybersecurity were identified as preserving 'the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein' [18][5].

As outlined in the introduction, with increased interconnection new challenges arose accompanied by growing concerns about the privacy and security of businesses and individuals in cyberspace. The WannaCry, Petya and NotPetya ransomware attacks in 2017 proved that cyberattacks are the new reality, and perfectly highlighted the cascading effects that may affect more entities than anticipated [27]. In response to the attack, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a new Cybersecurity Strategy [28] in 2017. The 2017 Cybersecurity Strategy highlighted the need for measures that would allow building greater EU resilience to cyberattacks, facilitating their detection, and strengthening international cooperation on cybersecurity. The two Cybersecurity Strategies resulted in legislation, namely the NIS Directive in 2016 (as a result of the 2013 Cybersecurity Strategy), which was the first EU-wide legislation on cybersecurity, and the Cybersecurity Act (CSA)[6] in 2019 (as a result of the 2017 Cybersecurity Strategy), which strengthens the role and mandate of the European Union Agency for Network and Information Security (ENISA) and introduces the legal basis to adopt an EU-wide cybersecurity certification scheme for ICT products. Several soft law instruments complemented these regulatory initiatives, for instance a Recommendation on the cybersecurity of 5G networks [29]. Also, strategic investments in digital capacity and infrastructure building took place. With reducing cybercrime also being a policy aim of the Cybersecurity Strategies, legislative and policy measures were

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 06.07.2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.07.2016, p. 1.

[4] The Proposal for a Regulation laying down measures on a high level of cybersecurity at the institutions, bodies, offices and agencies of the Union will put in place a framework for governance, risk management and control in the cybersecurity field. The Regulation will also extend the mandate of CERT-EU. The Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union will create a minimum set of information security rules and standards for all EU institutions, bodies, offices and agencies to ensure an enhanced and consistent protection against evolving threats.

[5] This definition deviated to some extent from a previous suggestion by ENISA, see on this [27].

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17.04.2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 07.06.2019, p. 15.

taken forward in judicial and law enforcement matters, for instance the Directive on Attacks against Information Systems[7]. Cybersecurity has also been a driver for security and defence integration in the EU [30].

Building on the Commission Communication Shaping Europe's digital future [31] and the EU Security Union Strategy [32], the European Commission published a new Cybersecurity Strategy [33] in 2020 accompanied by a Proposal for a NIS 2.0 Directive [21] and a Proposal for Directive on the resilience of critical entities [16]. The 2020 Strategy pays regard to the speed of digital transformation in a complex threat environment, which is compounded by geopolitical tensions over the global and open Internet and over control of technologies across the supply chain. The main objectives of the Strategy are (1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace. The short interval between the 2017 and 2020 Strategies reflects the political acquis that there is an urgent need for action; as already addressed in the introduction, the speed of regulatory action is accelerating.

2.2. The EU's Limited Mandate to Regulate Cybersecurity

A fundamental principle of EU law is the principle of conferral under which the EU acts only within the limits of the competences conferred upon it by the Member States. In general, the EU can legislate in areas where it is more appropriate for the EU to act than for the Member States individually. The introduction of any regulatory measure at EU level requires a legal basis. For cybersecurity, the EU Treaties do not provide such a unifying legal basis. Moreover, if one considers cybersecurity as part of national security, Article 4(2) TFEU provides that national security remains the sole responsibility of each Member State. Cyber policy, especially in the context of the protection of critical infrastructures has a national security dimension [34]. However, the cybersecurity dimension goes beyond national security, cybersecurity also has cross-border effects. What is more, not all cybersecurity aspects fall outside the scope of EU law: there are policy domains which are affected by cyber threats and in which the Treaties do confer powers upon the EU.

The EU's regulatory approach towards internet and cyberspace has long been focusing on economic growth under the single market rationale. Under this rationale, the EU deploys its political and legal mandate to regulate the internal market to issue common policies and legislation on cybersecurity. The legal basis for this is Article 114 TFEU[8], which provides a very versatile legislative basis for the issuance of legislation that serves the aim of smoothening the functioning of the internal market. By establishing a link between cybersecurity and the smooth functioning of the internal market, the European Commission provided a justification for acquiring competence to legislate in the cybersecurity field: the Proposal for a NIS Directive [35] outlines the cascading effects across borders resulting from the intrinsic transnational dimension of NIS that a disruption of NIS may have and which affect the cross-border movement of goods, services and people. The 'disparities resulting from uneven NIS national capabilities, policies and level of protection across the Member States' are recognized as a barrier to the functioning of the internal market, and hence justifying EU action [35].

While in the internal market, the so-called first pillar, there is a rather broad legislative competence to regulate, this is not the case in the three other pillars, namely the Area of Freedom, Security and Justice (AFSJ), the Common Security and Defence Policy (CSDP) and the Common Foreign and Security Policy (CFSP)[9]. Legislation in the AFSJ is under Art. 83(1) TFEU mainly restricted to law enforcement [36], while in the CSDP the realization of a common cyber defence policy is presented with institutional challenges and national sovereignty concerns [36]. The adoption of legislation based on the CFSP is legally excluded; accordingly, Council decisions are the most tangible instrument in this pillar.

2.3. Focus Internal Market: Sector-Specific Regulation

The afore outlined limited mandate of the EU to regulate cybersecurity resulted in a multitude of different European and national regulations as well as sector-specific

[7] Directive 2013/40/EU of the European Parliament and of the Council of 12.08.2013 on attacks against information systems and replacing Council Framework decision 2005/222/JHA, OJ L 218, 14.08.2013, p. 8.

[8] Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47. Under Art. 114 TFEU, the EU can adopt 'measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market'.

[9] Addressing these three pillars in detail would go beyond the scope of this paper which focuses on the internal market.

standards that address different aspects of cybersecurity. Similar to general security aspects, cybersecurity was primarily addressed in sector-specific regulations that paid respect to sector specificities. For instance in the energy sector, the Electricity Regulation[10] requires the European Commission to develop a network code on cybersecurity of cross-border electricity flows[11].

Various sector-specific legislation introduced rules on the prevention and mitigation of security incidents. For instance, in the telecommunication sector, the EU Telecoms Framework[12], which had been amended by Telecoms Package[13], introduced rules on the prevention and mitigation of data breaches as well as notification obligations in the e-Privacy Directive[14], and added rules on security breaches in the Framework Directive[15]. The convergence of the telecommunications, media and information technology sectors resulted in the European Electronic Communications Code (EECC)[16] which covers all electronic communications networks and services by a single legal act and requires the implementation of technical (and organisational) security measures following a risk-based approach as well as the notification of security incidents of a certain quality[17].

In the financial sector, the Payment Services Directive 2 (PSD2)[18] introduced provisions on operational and security incidents affecting in particular electronic payments enabled by payment services providers.

Similar to the EECC in the telecoms sector, the DORA Proposal [37] aims to establish a single European legislation restricted to ICT and cybersecurity for all financial institutions by introducing a more harmonised and comprehensive framework that spells out requirements to address and mitigate ICT and cyber risks at the level of the financial sector.

Legislative action also targeted the (cyber)security of particular assets, as for instance mandatory security measures to ensure security of personal data[19].

3. Horizontal Approach to Regulating Cyber Aspects: NIS Directive and CRA

3.1. A Cross-Sectoral Approach Addressing Cybersecurity

While the legal measures and initiatives outlined in section 2.3. constitute sector-specific regulation, the NIS Directives and the CRA Proposal reflect a new approach in regulating cyber aspects by introducing rules on the underlying ICT infrastructure, hardware and software.

The first horizontal instrument, i.e. a cross-sectoral instrument, to regulate cybersecurity at EU level is the NIS Directive which entered into force in August 2016. The NIS Directive will soon be replaced by a NIS 2.0 Directive for which a Proposal was published along the 2020 Cybersecurity Strategy highlighting again the expedited speed of cybersecurity regulation since the NIS 2.0 Proposal was published six months ahead of the completion of the original foreseen first periodic review of the NIS Directive. Political agreement on a new Directive was reached in May 2022. Work on a CRA also intensified recently following the announcement of such a legislative action in the Commission 2022 work programme; a CRA Proposal was published in September 2022.

Similar to the NIS Directive, the NIS 2.0 Directive and the CRA follow a horizontal approach that addresses the underlying technology. While introducing provisions to make digital products more secure, the CRA will complement the NIS 2.0 Directive by also addressing manufacturers of tangible and intangible digital products and ancillary services. Previously, regulation has been aimed primarily at operators of ICT with the NIS Directive imposing obligations upon operators of essential services and digital service providers, and, for instance, the GDPR demanding state of the art security mechanisms to protect personal data.

[10] Regulation (EU) 2019/943 of the European Parliament and of the Council of 05.06.2019 on the internal market for electricity (recast) (Electricity Regulation), OJ L 158, 14.06.2019, p. 54.

[11] Art. 59(2)(e) Electricity Regulation.

[12] The EU Telecoms Framework consisted of Directive 2002/19/EC (Access Directive), Directive 2002/20/EC (Authorisation Directive), Directive 2002/21/EC (Framework Directive), Directive 2002/22/EC (Universal Service Directive), Directive 2002/58/EC (e-Privacy Directive).

[13] The EU Telecoms Package consisted of Directive 2009/140/EC (Better Regulation Directive), which amended the Framework, Authorisation and Access Directive, Directive 2009/136/EC (Citizens' Rights Directive), which amended the Universal services and e-Privacy Directive and Regulation No 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC).

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12.07.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), OJ L 201, 31.07.2002, p. 37. See Art. 4 e-Privacy Directive. Art. 4(2) provides for an obligation to inform the subscribers of a particular risk of a breach of the security of the network.

[15] Directive 2002/21/EC of the European Parliament and of the Council of 07.03.2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.04.2002, p. 33.

[16] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11.12.2018 establishing the European Electronic Communications Code (Recast), OJ L 321, 17.12.2018, p. 36.

[17] See Art. 40 EECC.

[18] Directive 2015/2366/EU of the Parliament and of the Council of 25.11.2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35.

[19] See Art. 32 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), OJ L 119, 04.05.2016, p. 1.

The following section outlines how the NIS 2.0 Directive and CRA seek to improve cybersecurity and how they complement each other.

3.2. From NIS 1.0 to NIS 2.0: Imposing Obligations Upon Certain Operators of NIS

The NIS Directive: The original NIS Directive is a cornerstone of EU policy on cybersecurity laying down the foundations for a EU cybersecurity framework. The Proposal rooted in the Communication [38] released by the Commission in 2009 on critical information infrastructure protection from large scale cyberattacks[20] and the NIS Directive became a concrete deliverable of 2013 the Cybersecurity Strategy[21]. The choice of the legal instrument of a 'directive' means that the NIS Directive is not directly applicable in the EU Member States but binds the Member States as to the results to be achieved. The Member States have to transpose the Directive into the national legal framework leaving them a margin for manoeuvre as to the form and means of implementation. In the case of the NIS Directive, ENISA was tasked to assist MS to implement the Directive and support the strengthening of cybersecurity capabilities at EU level[22].

The NIS Directive lays down measures with a view to achieve a high common level of NIS security within the Union so as to improve the functioning of the internal market. To that end, the Directive covers capacity building and planning requirements, exchange of information, cooperation and common security and incident notification requirements for operators of essential services (OESs) and digital service providers (DSPs). The Directive only applies to entities identified by Member States as OESs in the sectors energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure[23]; DSPs under the scope of the Directive are only those listed in Annex III to the Directive, namely, online marketplaces, online search engines, and cloud computing services.

As regards OESs, the Directive only requires a minimum level of harmonisation[24], recognising that the legal systems in some EU Member States had already set higher standards, or may aim for higher standards than those required by the Directive[25]. In contrast, as regards DSPs, the Directive employs a maximum harmonisation approach[26], meaning that Member States may not introduce rules that are stricter than those set in the Directive.

With the 2013 Cybersecurity calling for effective EU-wide cooperation, including between authorities, public and private sectors, the NIS Directive introduced several cooperation mechanisms. In particular, two new fora were created: the NIS Cooperation Group[27] (to support and facilitate the strategic cooperation and exchange of information among Member States) and a network of Computer Incident Response Teams[28] (CSIRTs) (to improve the handling of cross-border incidents, share information about risks and coordinate responses to specific incidents). Further, Member States are required to designate a single national central contact point (SPOC) as liaison office for supranational cooperation[29].

Article 7 NIS Directive also required Member States to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining the desired high level of cybersecurity.

Deficits of NIS Directive: The review process of the NIS Directive that was conducted in 2021 identified limitations as well as deficiencies that are deemed to have prevented the NIS Directive from unlocking its initially foreseen full potential.

First of all, a weakness of NIS Directive is its limited scope of application, since the Directive only applies to certain DSPs and OESs; the latter restricted to the

[20] In recognition of the economic and societal role of ICT infrastructures, the Communication noted that there is a clear need to rapidly put in place the necessary elements to build a framework that will feed into the future strategy for network and information security.

[21] A political agreement on the Directive was reached in 2015 after three years of negotiations between the co-legislators.

[22] In that regard, ENISA's mandate was further strengthened by the CSA.

[23] See Annex II.

[24] See Art. 3 NIS Directive.

[25] In fact, various Member States have decided to include additional sectors (e.g. public administrations, postal sector, food sector, chemical and nuclear industry) and expand obligations for the sectors covered.

[26] See Art. 16(10) NIS Directive.

[27] The NIS Cooperation Group was established by Art. 11 NIS Directive with the aim to ensure strategic cooperation and information exchange among EU Member States.

[28] See Art. 12 NIS Directive. The national CSIRTs collaborate in the CSIRTs Network 'to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation'.

[29] Art. 8(3) NIS 1.0.

sectors energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure[30]. As a result, the NIS Directive fails to sufficiently address the increased interconnectedness and interdependencies in sectors outside its scope [39] . This potentially results in companies outside the scope of the Directive not sufficiently investing in cybersecurity because they are not legally obliged to fulfil a certain standard; however, the protection of these companies may be of similar importance, e.g. in the pharma industry or logistics, or because they are an important supplier of ICT to an OES or DSP [39]. A significant weakness of the Directive is also the broad discretion given to the Member States in defining the de facto scope of the Directive [39] as well as the vagueness of provisions and resulting unclear requirements [40]. This ultimately led to divergences across Member States in the implementation of the Directive and thus, a fragmented regulatory policy landscape. For instance, the leeway given to Member States in identifying OESs in the sectors encompassed by the NIS Directive resulted in national identification methodologies that differ significantly in terms of which types of services national authorities deem to be essential [40]. The way national thresholds are applied also varies across the EU [40][31]. As a consequence, similar entities are not treated consistently across the Union.

Information sharing is a central element of the NIS Directive; however, in practice, the information sharing about incidents and vulnerabilities remains limited[32], although national competent authorities report improvements [41].

In order to increase the cyber resilience of OESs and DSPs, the NIS Directive foresees the implementation of security measures (following a risk-based approach) and introduces an obligation to report significant incidents[33]. As with the OES identification procedure, the transposition of the respective articles into national law varies significantly [39]. Without an obligation to ensure coherence with certification schemes[34], some Member States introduced detailed security requirements, while others provide no guidance at all.

Different approaches in the transposition and in some cases pre-existing legislation[35], are one reason why security measures and incident reporting requirements are currently inconsistent across Member States. Another reason is that there is no common set of criteria as to what is considered an appropriate security measure in view of the risk posed and what is considered an incident [42]. Adding to uncertainties for reporting entities is the fragmented supervisory landscape [39].

Also, the review process identified different approaches to enforcement, inter alia in terms of regime of sanctions and penalties [39][36].

Besides the magnitude of obligations imposed on Member States, an impact assessment [43] in 2020 identified inter alia a low level of cyber resilience of businesses operating in the EU as well as inconsistent resilience across Member States and sectors.

The NIS 2.0 Proposal[37]: The NIS 2.0 Directive replaces the existing NIS Directive. A key change of the Proposal relates to its scope with new sectors being added and the Directive abolishing the differentiation between OESs and DSPs by introducing the concept of essential entities (EEs) and important entities (IEs). EEs are entities that operate in the sectors and sub-sectors listed in Annex I[38] or are of a type listed in Article 2(2)(a) NIS 2.0 Proposal. IEs are entities that operate in the sectors and sub-sectors listed in Annex II[39]. The Proposal tremendously extends the scope of application of the Directive by adding new sectors (inter alia include waste water, public administration entities, space and chemicals manufacture), amending existing sectors and also by setting a size-threshold. Member States will no longer be required to carry out an identification process to determine which entities meet the criteria to qualify as relevant operators. In order to eliminate the wide divergences among Member States in that regard, and

[30] See Annex II NIS Directive.

[31] Preliminary evidence from the review process also suggests that the divergence between Member States may be related to two factors: the delegation of the identification process to sectoral authorities (e.g. ministries, agencies) and the top-down versus bottom-up (self-identification) identification procedure.

[32] Operational information sharing focused on cross-border incidents, whereas the need to share information on vulnerabilities across the Member States to ensure more robust risk management is hardly addressed.

[33] Cf. Arts. 14 and 16 NIS Directive.

[34] As for instance set out in the CSA.

[35] Such as for instance the German IT security Act (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)), which has only recently been extended by the IT-Sicherheitsgesetz 2.0 (IT Security Act 2.0).

[36] For the significant variation of the penalty levels see [52].

[37] All references in the section relate to the consolidated text adopted by the European Parliament in November 2022 [22].

[38] Annex I lists as 'sectors of high criticality': energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT-service management (B2), public administration entities excluding the judiciary, parliaments and central banks, and space.

[39] Annex II lists as so called 'other critical sectors': postal and courier services, waste management, manufacture, production and distribution of chemicals, food production, processing and distribution, manufacturing, digital providers, and research.

to ensure legal certainty for risk management requirements and reporting obligations, a uniform size-cap rule is introduced whereby all medium and large entities (as defined by Commission Recommendation 2003/361/EC[40]), that operate within the sectors or provide the services covered by the Directive, fall within its scope. The Proposal replicates the minimum harmonisation approach under the existing Directive and extends this to all types of service providers[41].

The Proposal also replicates the obligation for Member States to adopt a national cybersecurity strategy[42]. In contrast to the existing Directive, Article 7 NIS 2.0 Proposal (consolidated text of November 2022) not only concretises the issues to be addressed but also provides a list of policies that Member States will have to adopt including, inter alia, a policy addressing cybersecurity in the supply chain for ICT products and services used by EEs and IEs, and a policy on the management of vulnerabilities.

As regards vulnerabilities disclosure, the NIS 2.0 Directive establishes a framework for so called coordinated vulnerability disclosure, where designated CSIRTs act as trusted intermediaries and thereby facilitate the interaction between reporting entities and manufacturers or providers of ICT products and services[43]. The confidential reporting of a vulnerability will also be possible for any natural or legal person[44]. Further, a European vulnerability database is set-up to which all interested parties shall have access[45].

At national level, Member States are required to have a national cybersecurity crisis management framework in place, inter alia by designating national competent authorities responsible for the management of large-scale cybersecurity incidents and crises[46].

Similar to the status quo, Member States are required to designate one or more national competent cybersecurity authorities for the Directive's supervisory tasks and a national single point of contact (SPOC) to exercise a liaison function in cross-border cooperation. The requirement to designate at least one CSIRT remains[47]. In contrast to the NIS Directive, the NIS 2.0 Proposal sets out an extensive catalogue of tasks for CSIRTs for the performance of which sufficient resources have to be allocated to the CSIRTs[48].

As regards cooperation at national level, the operative part of the NIS Directive only addressed cooperation between competent NIS authorities, the SPOC and the CSIRT(s) of the same Member State. The NIS 2.0 Proposal also addresses cooperation between these actors and law enforcement authorities, data protection authorities and further authorities[49]. The same actors are now also addressed in terms of cooperation at EU level in direct response to the perceived limited cooperation in practice[50].

Furthermore the tasks of the existing NIS Cooperation Group and the CSIRTs network are extended[51]. In order to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies, the NIS 2.0 Proposal also establishes the European Cyber Crises Liaison Organisation Network (EU-CyCLONe)[52]. Ultimately, in the field of cooperation, the Union is mandated to conclude international agreements in accordance with Article 218 TFEU with third countries or international organisations to allow and organise their participation in some activities of the NIS cooperation fora[53].

As a further new mechanism in the field of cooperation, the Proposal establishes a voluntary peer-review system with a view to, inter alia, learn from shared experiences, and strengthen mutual trust[54].

Cybersecurity risk management and reporting obligations remain a central element of the Directive. The Proposal requires Member States to provide that management bodies of the entities encompassed approve and oversee the cybersecurity risk

[40] Commission Recommendation 2003/361/EC of 06.05.2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124, 20.05.2003, p. 36.

[41] See Art. 5 NIS 2.0 Proposal (consolidated text of November 2022).

[42] Art. 7 NIS 2.0 Proposal (consolidated text of November 2022). This requirement was previously referred to as 'national strategy on the security of network and information systems' (Art. 7 NIS Directive).

[43] Art. 12(1) NIS 2.0 Proposal (consolidated text of November 2022).

[44] Ibid.

[45] Art. 12(2) NIS 2.0 Proposal (consolidated text of November 2022).

[46] Art. 9 NIS 2.0 Proposal (consolidated text of November 2022).

[47] Art. 10 NIS 2.0 Proposal (consolidated text of November 2022).

[48] Art. 11 NIS 2.0 Proposal (consolidated text of November 2022).

[49] Art. 13(4) NIS 2.0 Proposal (consolidated text of November 2022).

[50] Cf. Recital 107, which states that in relation to serious criminal activities, it is desirable that the European Cybercrime Centre and ENISA facilitate coordination.

[51] Arts. 14 and 15 NIS 2.0 Proposal (consolidated text of November 2022).

[52] Art. 16 NIS 2.0 Proposal (consolidated text of November 2022).

[53] Art. 17 NIS 2.0 Proposal (consolidated text of November 2022).

[54] Art. 19 NIS 2.0 Proposal (consolidated text of November 2022).

management measures taken by the respective entities and to follow specific cybersecurity-related training[55]. The management may be personally liable for non-compliance with these obligations[56]. In terms of cybersecurity risk management, similar to the NIS Directive, Member States are required to ensure that entities encompassed take appropriate and proportionate technical, operational and organisational measures to manage the cybersecurity risks posed to the security of NIS[57]. In addition, the entities will in the future also be required to prevent or minimise the impact of incidents on recipients of their services and on other services[58]. The measures shall be based on an 'all-hazards approach' and the minimum measures are now outlined in the Directive. These include, inter alia, supply chain security, human resources security and business continuity measures[59]. The entities encompassed will also have to notify the national competent authorities or the CSIRTs of any cybersecurity incident having a significant impact on the provision of the service they provide. In order to demonstrate compliance with certain security requirements, Member States may require entities to use ICT products, services and process that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 CSA[60]. Member States shall also encourage the use of European or internationally accepted standards and specifications[61].

In terms of critical supply chains[62], the Proposal introduces a requirement for the NIS Cooperation Group to conduct coordinated sectoral supply chain security assessments for particular technologies mirroring the risk assessment foreseen for 5G networks by the Commission Recommendation on Cybersecurity of 5G networks (EU) 2019/534[63]. The assessment shall take into account both technical and, where relevant[64], non-technical factors including those applied to 5G networks[65].

For the purpose of contributing to the security, stability and resilience of the DNS, TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data[66].

While the NIS Directive requires OESs and DSPs to report incidents which have resulted in actual harm, the Proposal expands the reporting obligation to incidents that have caused or are 'capable of causing severe operational disruption of the service or financial losses for the entity concerned', as well as incidents that have affected or are 'capable of affecting other natural or legal persons by causing considerable material or non-material damage'[67]. As regards the reporting procedure, the Proposal lays down a three-stage approach[68] in order to strike a balance between swift reporting that helps to mitigate a potential spread of an incident, and in-depth reporting that draws lessons from incidents and improves the future resilience of NIS[69]. Where entities become aware of an incident, they will have to submit an initial warning within 24 hours, followed by an initial notification within 72 hours updating the information and indicating an initial assessment of the incident; a final report has to be submitted not later than one month thereafter, or where the incident is still on-going, a progress report and a final report one month after the incident has been handled[70].

In terms of jurisdiction, EEs and IEs will be under the jurisdiction of the Member State where they are established[71]. Providers of public electronic communication networks and providers of publicly available electronic communications services are excluded from this general rule; these entities are deemed to fall under the jurisdiction of the Member State in which they provide their services[72]. For certain types of entities[73], jurisdiction is established at the place of their main establishment[74].

Since the review of the NIS Directive revealed a reluctance to share information on cybersecurity threats and incidents, the NIS 2.0 Proposal introduces a separate chapter on information sharing. Chapter VI provides a legal basis for the voluntary sharing of relevant cybersecurity information. First of all, Member States shall provide rules enabling entities to engage in cybersecurity-related information

[55] Art. 20 NIS 2.0 Proposal (consolidated text of November 2022).

[56] See ibid. Similarly, any natural person responsible for or acting as a representative of an EE on the basis of the power to represent it will be held liable for breach of their duties to ensure compliance with the obligations laid down in the Directive, see Art. 32(6) NIS 2.0 Proposal (consolidated text of November 2022.

[57] Art. 21(1) NIS 2.0 Proposal (consolidated text of November 2022).
[58] Ibid.
[59] Art. 21(2) NIS 2.0 Proposal (consolidated text of November 2022).
[60] Art. 24 NIS 2.0 Proposal (consolidated text of November 2022).
[61] Art. 25 NIS 2.0 Proposal (consolidated text of November 2022).

[62] To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which EEs and IEs use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities (Recital 47 NIS 2.0 Proposal).

[63] Commission Recommendation (EU) 2019/534 of 26.03.2019, Cybersecurity of 5G networks, OJ L 88, 29.03.2019, p. 42.

[64] Art. 22 NIS 2.0 Proposal (consolidated text of November 2022). Already in 2021, the German legislator introduced a trustworthiness assessment of the manufacturer of critical components that mirrors the coordinated risk assessment for critical supply chains.

[65] See Recital 90 NIS 2.0 Proposal (consolidated text of November 2022).
[66] Art. 28 NIS 2.0 Proposal (consolidated text of November 2022). Furthermore, such entities are required to provide efficient access to domain registration data for legitimate access seekers.
[67] Art. 23(3) NIS 2.0 Proposal (consolidated text of November 2022).
[68] The original Commission Proposal foresaw a two-stage reporting process.
[69] Cf. Recital 101 NIS 2.0 Proposal (consolidated text of November 2022).
[70] Art. 23(4) NIS 2.0 Proposal (consolidated text of November 2022).
[71] Recital 113 and Art. 26(1) NIS 2.0 Proposal (consolidated text of November 2022).
[72] Art. 26(1)(a) NIS 2.0 Proposal (consolidated text of November 2022).

[73] DNS service providers, TLD name registries, providers of domain name registration services, cloud computing service providers, data centre providers, managed service providers, managed security service providers, content delivery network providers, as well as certain digital providers, and public administration entities.

[74] Art. 26(1)(b) NIS 2.0 Proposal (consolidated text of November 2022). According to Art. 26(2) the main establishment is where the decisions related to the cybersecurity risk management measures are predominantly taken, or, if this cannot be determined, the place where cybersecurity operations are carried out.

sharing within the framework of specific cybersecurity information-sharing arrangements[75]. In addition, Member States shall allow EEs and IEs to report, on a voluntary basis, cyber threats, near misses and relevant incidents that do not meet the reporting thresholds for mandatory reporting[76]. Furthermore, entities outside the scope of this Directive shall be able to report, on a voluntary basis, significant incidents, cyber threats, or near misses[77].

Although the NIS Directive required Member States to ensure that the competent authorities have the necessary powers and means to assess the compliance with the security and notification requirements, the supervision and enforcement regime of the NIS Directive has proven ineffective [21]. Accordingly, the NIS 2.0 Proposal seeks to strengthen supervisory powers via a minimum list of actions and means for competent authorities. The new means include, inter alia, on-site inspections and off-site supervision, and regular targeted security audits[78]. While EEs will be subject to a full ex-ante supervisory regime, a lighter, ex-post only, approach will apply to IEs, mirroring the so-called 'light-touch' approach applied to DSPs under the NIS Directive [44]. Member States must ensure that the competent authorities, where exercising their enforcement powers have certain powers including the power to issue warning and binding instructions as well as the power to impose administrative fines[79]. Besides the sanctioning regime with administrative fines of a maximum of at least EUR 10,000,000 or 2 % of the total worldwide annual turnover[80], the Proposal also establishes responsibilities and sanctions directed at natural persons exercising managerial functions[81].

In line with the new permanent, and moreover extended, mandate for ENISA under the CSA[82], the NIS 2.0 Proposal foresees additional action areas for ENISA. These include the development and maintenance of a European vulnerability database[83], the provision of the secretariat of the EU-CyCLONe[84], a biennial report on the state of cybersecurity in the EU[85], the support in the organisation of Member State peer reviews[86], the collection of aggregated incident data from Member States and the provision of technical guidance for comparable information[87], as well as the creation and maintenance of a registry of entities providing certain cross-border services[88].

3.3. The CRA Proposal: Imposing Obligations Upon Manufacturers of Products with Digital Elements

The CRA Proposal supplements the CSA and aims to make digital products and ancillary services more secure. In order to achieve this aim, the CRA, similar to the NIS Directive, introduces horizontal cybersecurity rules. These rules apply to industry stakeholders, namely manufacturers, importers and distributors of tangible and intangible products with digital elements. The European Commission [45] notes four specific objectives of the CRA: (1) to ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole lifecycle; (2) to ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers; (3) to enhance the transparency of security properties of products with digital elements, and (4) to enable businesses and consumers to use products with digital elements securely. As a Regulation, the CRA will become directly applicable in the EU Member States on its entry into force.

The CRA follows the so-called 'New Legislative Framework' (NLF)[89], which aims to improve the internal market for goods by improving market surveillance and boosting the quality of conformity assessments. The NLF inter alia sets out requirements for accreditation of conformity assessment bodies, and the market surveillance of products. A central principle are high-level essential requirements in terms of health and safety that products have to meet before they can be placed on the Internal Market; these requirements are then detailed by harmonised technical standards drafted by European Standardisation Organisations[90].

[75] Art. 29 NIS 2.0 Proposal (consolidated text of November 2022).

[76] Art. 30(1)(a) NIS 2.0 Proposal (consolidated text of November 2022).

[77] Art. 30(1)(b) NIS 2.0 Proposal (consolidated text of November 2022).

[78] Cf. Art. 32(2) NIS 2.0 Proposal (consolidated text of November 2022)in relation to EEs, and Art. 33(2) in relation to IEs.

[79] Cf. Art. 32(4) and (5) NIS 2.0 Proposal (consolidated text of November 2022) in relation to EEs, and Art. 33(4) and (5) in relation to IEs.

[80] Art. 34(4) NIS 2.0 Proposal (consolidated text of November 2022), applying to EEs; IEs are subject to administrative fines of a maximum of at least EUR 7,000,000 or 1.4% of the total worldwide annual turnover of the undertaking, see Art. 34(5).

[81] Art. 32(5)(b) and (6) NIS 2.0 Proposal (consolidated text of November 2022) in relation to EEs, and Art. 33(5) in connection with Art. 32(6) in relation to IEs. This does not extend to criminal or civil liability (cf. Recital 128)

[82] Under the extended mandate ENISA is tasked to assist the Member States and the Commission in the implementation of the revised NIS Directive.

[83] Art. 12(2) NIS 2.0 Proposal (consolidated text of November 2022).

[84] Art. 16 (2) NIS 2.0 Proposal (consolidated text of November 2022).

[85] Art. 18 NIS 2.0 Proposal (consolidated text of November 2022).

[86] Art. 19 NIS 2.0 Proposal (consolidated text of November 2022).

[87] Art. 23(9) NIS 2.0 Proposal (consolidated text of November 2022).

[88] Art. 27 NIS 2.0 Proposal (consolidated text of November 2022).

[89] The 'NLF' consists of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 09.07.2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.08.2008, p. 30; Decision 768/2008 of the European Parliament and of the Council of 09.07.2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, OJ L 218, 13.08.2008, p. 82; and Regulation (EU) No 2019/1020 of the European Parliament and of the Council of 20.06.2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.06.2019, p. 1.

[90] On the alignment of the CRA with the NLF see [47].

The CRA will apply to products with digital elements (i.e. any software or hardware product and its remote data processing solutions) 'whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network'[91]. While in the initial call for evidence for an impact assessment [46], the terminology of 'digital products and ancillary services' was used, the notion of 'products with digital elements' indicates a commitment to an even broader regulation [47].

In line with the NLF requirements, several obligations need to be fulfilled before and whilst placing a product with digital elements on the market. For instance, manufacturers, importers and distributors need to ensure that the product with digital elements is accompanied with appropriate instructions and information in a language that is easy to understand in order to ensure a safe use by the user[92].

As regards further requirements, the Proposal distinguishes between two product categories; products with digital elements as the default category, and critical products with digital elements, which are subdivided into two classes. All products have to comply with the essential cybersecurity requirements laid down in section I of Annex I to the CRA Proposal. These requirements include 'security requirements relating to the properties of products with digital elements', such as the absence of any known exploitable vulnerabilities, a secure by default configuration, or the possibility to address vulnerabilities through security updates, and 'vulnerability handling requirements such as regular tests and reviews of the security of the product'[93]. Hence, the CRA will make security by design mandatory.

Products with digital elements that amount to critical products are enlisted in Annex III to the CRA Proposal. Generally speaking, a product is considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use[94]. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as secure elements, can lead to a propagation of security issues throughout the supply chain, rendering the product critical in the sense of the CRA[95]. As regards critical products, the Proposal further distinguishes between two different classes with class II representing a greater risk than class I. The Commission is empowered to adopt delegated acts supplementing the CRA to specify the product category definitions in class I and II.

In any case, before placing a product on the market, manufacturers must carry out appropriate conformity assessment procedures[96]. For the default category, manufacturers will have to self-assess conformity[97]. Products with digital elements that are certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the CSA and which has been identified by the Commission in an implementing act, shall be presumed compliant with Annex I[98]. The same applies to products with digital elements, which are in conformity with harmonised standards or parts thereof. Class I products must adhere to the application of a harmonised standard or certification scheme as set out in the CSA, or complete a third-party assessment to demonstrate compliance[99]. Class II products must always complete a third-party conformity assessment[100]. In line with the NLF, the Proposal sets out requirements for national authorities responsible for conformity assessment bodies[101].

If the compliance of the product has been demonstrated, manufacturers shall draw up an 'EU declaration of conformity' and state that the fulfilment of the applicable essential requirements has been demonstrated[102]. The EU declaration of conformity shall, inter alia, contain the elements specified in the relevant conformity assessment, and shall be continuously updated[103]. By drawing up the declaration of conformity, the manufacturer assumes responsibility for the product's compliance[104]. Further, the manufacturer can affix a CE marking to the product that indicates that it assumes responsibility for the conformity with all applicable requirements[105].

[91] Art. 2(1) CRA Proposal. Exceptions are listed in subsections (2) to (5) and mainly address situations where sectoral rules achieve the same level of protection as the one provided by the CRA. As regards the notion 'products with digital elements', the Commission departed in the Proposal from its prior terminology of 'digital products and ancillary services' used in the call for evidence for an impact assessment [46].

[92] Arts. 10(10) CRA Proposal (with regard to manufacturers), 13(2)(c) (with regard to importers), 14(2)(b) (with regard to distributors).

[93] Annex I to the CRA Proposal.

[94] Recital 25 CRA Proposal. As regards the intended use, the use in an in an industrial setting or in the context of an EE of the type referred to in Annex I to the NIS 2.0 Proposal renders a product critical since the severity of the impact of a cybersecurity incident may be more severe.

[95] Ibid.
[96] Arts. 20 and 24 CRA Proposal.
[97] Art. 24(1) CRA Proposal.
[98] Art. 24(2) and Recital 39 CRA Proposal.
[99] Ibid.
[100] Art. 24(3) CRA Proposal.
[101] Arts. 25 et seq. CRA Proposal.
[102] Art. 10 CRA Proposal.
[103] Art. 10(2) CRA Proposal.
[104] Art. 10(4) CRA Proposal.
[105] Art. 22 CRA Proposal.

The CRA will also introduce reporting obligations of manufacturers similar to those for IEs and EEs under the NIS 2.0 Proposal: manufacturers shall, without undue delay and in any event within 24 hours of becoming aware of it, notify ENISA any actively exploited vulnerability contained in products with digital elements, as well as incidents having an impact on the security of those products[106]. In order to ensure that users can react quickly to incidents having an impact on the security of their products, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly[107].

Manufacturers also have to ensure that vulnerabilities of the product are handled effectively for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter[108]. The Proposal also mandates that manufacturers are transparent on cybersecurity aspects that need to be made known to customers[109].

As regards importers, Article 13 CRA Proposal requires importers, inter alia, to ensure conformity of the manufacturer with the essential requirements set out in Annex I before placing a product on the market. When identifying a vulnerability in a product with digital elements, importers are obliged to inform the manufacturer without undue delay about that vulnerability[110]. Similar obligations apply to distributors[111].

In line with the principles of the NLF[112], a legal framework within which market surveillance can be carried out is drawn up[113]. National market surveillance authorities carry out the tasks enlisted in relation to that Member State.

Where the market surveillance authority of a Member State has sufficient reasons to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall carry out a product evaluation in respect of the product's compliance with the requirements laid down in the CRA[114]. Under certain circumstances, for instance, when there is a risk to the provision of the services by an EE, the European Commission may requires ENISA to carry out the evaluation[115]. The market surveillance authority has the power to impose or request the imposition of administrative fines. In that regard, the CRA Proposal establishes maximum levels for administrative fines that should be provided in national laws for non-compliance with the obligations introduced by the Regulation[116]. In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU is delegated to the European Commission for, inter alia, updating the lists of critical products and specifying the definitions of these products, as well as specifying the minimum content of a EU declaration of conformity[117].

3.4. In Brief: The Interplay Between the NIS 2.0 Proposal and the CRA

The NIS 2.0 Proposal and the CRA Proposal both seek to regulate cybersecurity on a horizontal level with the CRA complementing the NIS 2.0 Directive in many aspects. Taking the example of supply chain security, the CRA recognises that cybersecurity of the entire supply chain can only be ensured if all its components are secure. Under the NIS 2.0 Directive, Member States have to address supply chain security in their national cybersecurity strategies, and ensure that supply chain security forms part of the mandatory security measures employed by EEs and IEs. Further, the Directive introduces a EU coordinated risk assessment of critical supply chains. However, due to the limited scope of application of the Directive, this leaves out a wide range of products with digital elements. In fact, most of the hardware and software products on the market are currently not covered by any EU legislation tackling their cybersecurity [45]. Accordingly, the CRA seeks to close the existing regulatory gaps: As regards the

[106] Recitals 19 and 35, Art. 11(1) and (2) CRA Proposal.

[107] Recital 35, Art. 11(4) CRA Proposal.
[108] Art. 10(6) CRA Proposal.
[109] Art. 10 CRA Proposal.
[110] Art. 13(6) CRA Proposal.
[111] See Art. 14 CRA Proposal.

[112] Here: Regulation (EU) No 2019/1020 of the European Parliament and of the Council of 20.06.2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.06.2019, p. 1. See also [47].

[113] Arts. 41 et seq. CRA Proposal.
[114] Art. 43 CRA Proposal.
[115] Recital 59, Arts. 45 and 46 CRA Proposal.
[116] Art. 53 CRA Proposal.
[117] Arts. 50 et seq. CRA Proposal.

security of services provided by EEs and IEs the CRA will have a direct impact by facilitating the compliance with supply chain requirements in that the Regulation ensures that the products that EEs and IEs use for the provision of their services are developed in a secure manner, and provided with security updates[118].

Correlation between the two legislative proposals will certainly arise in the field of vulnerability disclosure, incident reporting and information sharing. As outlined above, the CRA introduces reporting obligations similar to those for IEs and EEs under the NIS 2.0 Proposal. Once ENISA is made aware of an actively exploited vulnerability, it is requested to forward the notification to the relevant CSIRTs or, respectively, to the SPOCs designated under the NIS Directive as well as informing the relevant market surveillance authority[119]. Thereby ENISA ensures that the national CSIRTs and the SPOCs are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of EEs and Ies[120].

Where the information notified is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level, ENISA shall also submit the information to the EU-CYCLONe established by the NIS 2.0 Directive[121]. By this, the CRA supports the EU-CYCLONe in fulfilling its tasks under Article 14 NIS 2.0 Proposal. ENISA also prepares a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements for the NIS Cooperation Group[122], And thereby again contributes to the information gathering of a NIS cooperation forum. The CRA also encourages manufacturers of products with digital elements to consider disclosing fixed vulnerabilities to the European vulnerability database established under the NIS 2.0 Directive[123] – enriching the information sharing platform from which any natural and legal person may benefit.

4. Conclusion/Outlook

While the EU's approach to cybersecurity has long being implemented in a piecemeal fashion, this approach has recently changed. Although the legislative landscape is still characterised by fragmentation and coexistence of national and European cybersecurity laws, the COVID-19 pandemic and further circumstances have triggered a change in how cybersecurity is addressed. Obviously this has been the result of the increased interconnectedness and interdependencies when it comes to technology.

Although already the NIS Directive introduced a horizontal approach to cybersecurity regulation, this did not prevent fragmentation across the EU. However, the systemic and structural changes introduced by the NIS 2.0 Directive amount to a fundamental shift of approach towards covering a wider segment of the economies across the EU. At the same time, the Proposal seeks to streamline the obligations imposed on the entities covered and to ensure a higher level of harmonisation responding to the fragmentation that the original NIS Directive resulted in.

The NIS 2.0 Proposal not only details an incident reporting procedure and strengthens the security requirements for the entities encompassed, it also entails measures aimed at improving policy building approaches at Member States level. New frameworks for supplier relationship risk management and coordinated vulnerability disclosure are introduced. While the NIS Directive aims at ensuring the continuity of services to guarantee the proper functioning of the Union's economy and society, the building of cybersecurity capabilities across the EU and the mitigation of growing threats to NIS used by critical entities, it does not specifically address the cybersecurity of products. The cybersecurity of products is moreover an indirect consequence in terms of security of the supply chain. Similarly, the current EU regulatory framework on products, the NLF, does not address specifically the challenges linked to the cybersecurity of digital products. This existing regulatory gap will now be filled with the CRA.

[118] Cf. Recital 11 CRA Proposal.
[119] Art. 11(2) CRA Proposal.
[120] Cf. Recitals 19 and 34 CRA Proposal.
[121] Art. 11(3) CRA Proposal.
[122] Art. 10(6) CRA Proposal.
[123] Recital 34 CRA Proposal.

Similar to the original NIS Directive in terms of services provided by OESs and DSPs, the CRA is the first EU-wide legislation that introduces common cybersecurity rules for manufacturers and developers of products with digital elements. Also similar to the NIS Directive in terms of the cybersecurity level of certain critical services, the CRA responds to a perceived low level of cybersecurity of products with digital elements throughout the product lifecycle. In that regard, it addresses the not only the product lifetime but also the whole supply chain from manufacturers to importers and distributors.

The outlined proposals are exemplary for an overall tendency to align legislation and reduce complexity between different, often sectoral regulatory approaches to cybersecurity. The common denominator for both proposals is that they address the underlying technology on a risk-based approach.

The described interplay between the initiatives shows an effort for a coherent approach to cybersecurity at EU level that closes regulatory security gaps in the digital value chain and eliminates conflicting or overlapping regulations [48]. At this point, it is worth highlighting again that compliance with cybersecurity requirements under the CRA does not stop once a product is placed on the market. While the EU legislation on products usually relies on the concept of 'placing a product on the market'[124], the CRA explicitly implements a product lifecycle approach since technological products may evolve over time: they may become insecure, or may be applied in a new context. As regards the latter, it must be noted that technological advancement nowadays relates more to new technological application than progress in the basic underlying technology.

The Commission is optimistic about the CRA's potential to become an international point of reference beyond EU's internal market [49]. Clearly with its obligation upon manufactures and importers in terms of conformity with the cybersecurity requirements and the presumption of compliance when applying European certification schemes or standards, the CRA has the potential to push forward EU standards internationally and influence global markets. Also, the NIS Directive with its supply chain security elements and obligations imposed upon entities that offer essential or important services in the EU has extraterritorial reach. Legislation in the field of digital economy naturally influences global markets when drafted by an important market for data-driven businesses [50]. This externalisation of EU law has been referred to as the 'Brussels Effect' [50]. With the EU's market power in the digital economy, the data protection regime under the GDPR has proven a strong example of said effect due to both technical and economic non-divisibility of the products and services across global users. Whether the CRA, or the NIS Directive will shape international standards in the same way as the GDPR remains to be seen [51, 52].

Ultimately, the legislative initiatives of the CRA and NIS 2.0 Directive have proven that although there is no explicit mandate for the EU to regulate cybersecurity, the existing legal basis allows for far-reaching horizontal legislation detached from sectoral security objectives. By following a risk-based approach, the instruments provide a regime that adapts the level of regulation to the risk level while at the same time providing a uniform approach to regulate the underlying technology. This approach is also reflected in the EECC and DORA Proposal (addressed in section 2) which also seek to harmonise a previously existing fragmented regulatory landscape.

Funding

The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/ EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/works.

[124] This does not apply for medical products under Regulation (EU) 2017/745 of the European Parliament and of the Council of 05.04.2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Devices Regulation).

REFERENCES

[1] K. Okereafor, *Cybersecurity in the COVID-19 pandemic*. Boca Raton: CRC Press, 2021.

[2] Europol. (2021). *European Union serious and organised crime threat assessment 2021*. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf. [Accessed: Oct. 24, 2022].

[3] BBC. (2021, May 20). *Cyber-attack on Irish Health Service 'catastrophic'*. [Online]. Available: https://www.bbc.com/news/world-europe-57184977. [Accessed: Oct. 24 2022].

[4] BSI. (2021). *Die Lage der IT-Sicherheit in Deutschland 2021*. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf%20?__blob=publicationFile&v=4. [Accessed: Oct. 24, 2022].

[5] BSI. (2022). *Die Lage der IT-Sicherheit in Deutschland 2022*. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=5. [Accessed: Oct. 24, 2022].

[6] European Parliament. (2021). *Recent cyber-attacks and the EU's Cybersecurity Strategy for the Digital Decade*. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_EN.pdf. [Accessed: Oct. 24, 2022].

[7] Politiets Sikkerhetstjeneste. (2020, Dec. 8). *Datainnbruddet mot Stortinget er ferdig etterforsket*. [Online]. Available: https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/. [Accessed: Oct. 26, 2022].

[8] BBC. (2018, Feb. 28). *Fancy Bear: Germany investigates cyber-attack 'by Russians'*. [Online]. Available: https://www.bbc.com/news/world-middle-east-43232520. [Accessed: Oct. 26, 2022].

[9] L. Cerulus. (2021, Feb. 15). *France identifies Russia-linked hackers in large cyberattack*. [Online]. Available: https://www.politico.eu/article/france-cyber-agency-russia-attack-security-anssi/. [Accessed: Oct. 26, 2022].

[10] European Commission. (2022, Oct. 18). *Critical infrastructure: Commission accelerates work to build up European resilience*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238. [Accessed: Oct. 24, 2022].

[11] J. Plucinska. (2022, Oct. 6). *Nord Stream Gas 'sabotage': Who's being blamed and why?* [Online]. Available: https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/. [Accessed: Oct. 24, 2022].

[12] J. Thurau. (2022, Oct. 25). *Germany's critical infrastructure is poorly protected*. [Online]. Available: https://www.dw.com/en/germanys-critical-infrastructure-is-poorly-protected/a-63505983. [Accessed: Oct. 26, 2022].

[13] C. Vallance. (2022, May 10). *UK blames Russia for satellite Internet hack at start of war*. [Online]. Available: https://www.bbc.com/news/technology-61396331. [Accessed: Oct. 24, 2022].

[14] European Commission. (2022, Oct. 18). Proposal for a Council Recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure, COM(2022) 551 final. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-13713-2022-INIT/en/pdf. [Accessed: Oct. 24, 2022].

[15] European Commission. (2022, June 28). *Security Union: Commission welcomes today's political agreement on new rules to enhance the resilience of critical entities*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4157. [Accessed: Oct. 26, 2022].

[16] European Commission. (2020, Dec. 16). Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020) 829 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829. [Accessed: Oct. 26, 2022].

[17] U. v. d. Leyen. (2021, Sep. 15). *2021 State of the Union Address*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701. [Accessed: Oct. 24, 2022].

[18] European Commission & High Representative of the European Union for Foreign Affairs and Security Policy. (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecruity Strategy of the European Union: An open, safe and secure cyberspace, JOIN(2013) 1 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:0001:FIN. [Accessed: Oct. 24, 2022].

[19] European Commission. (2015, May 6). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single MArket strategy for Europe, COM(2015) 192 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192. [Accessed: Oct. 24, 2022].

[20] European Commission. (2022, May 13). *Commission welcomes political agreement on new rules on cybersecurity of network and information systems*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985. [Accessed: Oct. 26, 2022].

[21] European Commission. (2020, Dec. 16). Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN. [Accessed: Oct. 26, 2022].

[22] European Parliament. (2022, Nov. 10). Consolidated text and legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.html. [Accessed: Oct. 26, 2022].

[23] European Parliament. (2022). Legislative resolution of 10 November 2022 on the proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)). [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0381_EN.pdf. [Accessed: Oct. 26, 2022].

[24] European Commission. (2022, Mar. 22). Proposal for a Regulation of the European Parliament and of the Council laying down measures on a high level of cybersecurity at the institutions, bodies, offices and agencies of the Union, COM(2022) 122 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0122. [Accessed: Oct. 26, 2022].

[25] European Commission. (2022, Mar. 22). Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union, COM(2022) 119 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0119. [Accessed: Oct. 26, 2022].

[26] European Commission. (2022, Sep. 15). Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/2010, COM(2022) 454 final. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/89543. [Accessed: Oct. 11, 2022].

[27] G. G. Fuster, L. Jasmontaite, "Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights," in *The Ethics of Cybersecurity*, M. Christen, B. Gordijn, M. Loi, Eds. Cham: Springer, 2020, pp. 97–115.

[28] European Commission & High Representative of the Union for Foreign Affairs and Security. (2017). Joint Communication to the Parliament and the Council, resilience, deterrence and defence: Building strong cybersecurity for the EU, JOIN(2017) 450. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450. [Accessed: Oct. 26, 2022].

[29] European Commission. (2019, Mar. 29). Commission Recommendation of 26 March 2019, cybersecurity of 5G networks, COM(2019) 2335 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534. [Accessed: Oct. 26, 2022].

[30] A. Bendies. (2017). *A paradigm shift in the EU's common foreign and security policy*. [Online]. Available: https://www.swp-berlin.org/publications/products/research_papers/2017RP11_bdk.pdf. [Accessed: Oct. 26, 2022].

[31] European Commission. (2020, Feb. 19). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM(2020) 67 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067. [Accessed: Oct. 26, 2022].

[32] European Commission. (2021, Aug. 24). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM(2020) 605 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021AE0879. [Accessed: Oct. 26, 2022].

[33] European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020, Dec. 16). Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018&qid=1671800243772. [Accessed: Oct. 26, 2022].

[34] C. Calliess, A. Baumgarten, "Cybersecurity in the EU - the example of the financial sector: A legal perspective," *German Law Journal*, pp. 1149–1179, 2020, doi: 10.1017/glj.2020.67.

[35] European Commission. (2013, Feb. 7). Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 048 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0048. [Accessed: Oct. 26, 2022].

[36] A. Bendiek, E. Pander Maat. (2019, Oct. 2). *The EU's regulatory approach to cybersecurity*. [Online]. Available: https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf. [Accessed: Oct. 26, 2022].

[37] European Commission. (2020, Sep. 24). Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595. [Accessed: Oct. 26, 2022].

[38] European Commission. (2009, Mar. 30). Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009) 149 final. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF. [Accessed: Oct. 26, 2022].

[39] European Commission et al. (2021). Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No 2020-665. Final study report. [Online]. Available: https://www.ceps.eu/wp-content/uploads/2022/07/KK0921034ENN.en_compressed.pdf. [Accessed: Oct. 26, 2022].

[40] European Commission. (2021). Report from the Commission to the European Parliament and to the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148, COM(2019) 546 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546. [Accessed: Oct. 26, 2022].

[41] S. Schmitz-Berndt, A. Machalek. (2022). *EnCaViBS - Summary report on cooperation*. [Online]. Available: https://encavibs.uni.lu/wp-content/uploads/sites/158/2022/08/EnCaViBS-questionnaire-report_cooperation.pdf. [Accessed: Oct. 26, 2022].

[42] S. Schmitz-Berndt, "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive", *Journal of Cybersecurity*, 2023 (forthcoming).

[43] European Commission. (2020, Dec. 16). Commission Staff working document, Impact assessment report, SWD(2020) 345 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345. [Accessed: Oct. 26, 2022].

[44] T. Sievers, "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations," *International Cybersecurity Law Review*, vol. 2, pp. 223–231, 2021.

[45] European Commission. (2022, Sep. 15). *Cyber Resilience Act*. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. [Accessed: Oct. 28, 2022].

[46] European Commission. (2022). "Call for evidence for an impact assessment," *Ref. Ares*, 1955751.

[47] P. G. Chiara, "The Cyber Resilience Act: The EU Commission's Proposal for a horizontal regulation on cybersecurity for products with digital elements," *International Cybersecurity Law Review*, pp. 255–272, 2022.

[48] bitkom. (2022). *Position paper on a Cyber Resilience Act (CRA)*. [Online]. Available: https://www.bitkom.org/sites/main/files/2022-05/20220519_CRA_Bitkom_Positionspapier_eng_final.pdf. [Accessed: Oct. 26, 2022].

[49] European Commission. (2022, Sep. 15). *State of the Union: EU Cyber Resilience Act - questions & answers*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375. [Accessed: Oct. 29, 2022].

[50] A. Bradford, „Digital economy," in *The Brussels Effect: How the European Union rules the world*. New York: Oxford University Press, 2020. pp.131–170.

[51] D. E. Sanger, N. Perlroth. (2021, June 8). *Pipeline attack yields urgent lessons about U.S. cybersecurity*. [Online]. Available: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. [Accessed: Oct. 24, 2022].

[52] P. Contreras. (2022, June 8). *EnCaViBS poster series: NISD in a nutshell – penalties*. [Online]. Available: https://encavibs.uni.lu/2022/06/08/nisd-in-a-nutshell-penalties/. [Accessed: Oct. 26, 2022].