BRIEFING

EU Legislation in Progress

European Parliament

The NIS2 Directive

A high common level of cybersecurity in the EU

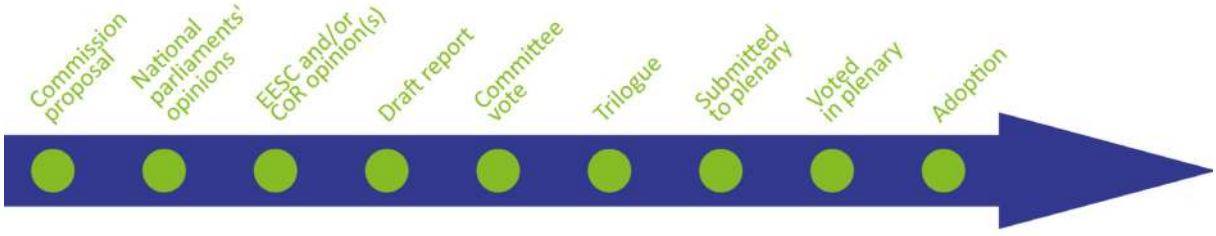
OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Proposal for a directive on measures for a high common level of cybersecurity across the Union		
Committee responsible:	Industry, Research and Energy (ITRE)	COM(2020) 823 16.12.2021
Rapporteur:	Bart Groothuis (Renew, the Netherlands)	2020/0359(COD)
Shadow rapporteurs:	Eva Maydell (EPP, Bulgaria) Eva Kaili (S&D, Greece) Rasmus Andresen (Greens/EFA, Germany) Thierry Mariani (ID, France) Evžen Tošenovský (ECR, Czechia) Marisa Matias (The Left, Portugal)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Procedure completed.	Directive (EU) 2022/2555 OJ L 333, 27.12.2022, pp 80-152.	



EPRS | European Parliamentary Research Service

Author: Mar Negreiro
Members' Research Service
PE 689.333 – February 2023

EN

Introduction

Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. In 2017, Cybersecurity Ventures forecast that global ransomware damage costs would reach US$20 billion by 2021, 57 times more than the amount in 2015. It also predicted that companies would be suffering a ransomware attack every 11 seconds by 2021, up from every 40 seconds in 2016. As a result, businesses have to invest more money to make cyberspace safer for themselves and their customers. Not only companies but also citizens and entire countries have been affected; the first known cyber-attack on a country was mounted on Estonia in April 2007, affecting the online services of banks, media outlets and government bodies for weeks. Since then, many other countries have suffered cyber-attacks, including on critical infrastructure, such as on electric power systems, hospitals or water plants. According to a Eurobarometer survey, about three quarters (76 %) of respondents believe that they are facing an increasing risk of falling victim to cybercrime. In 2019, about 64 % of the US population experienced a data breach and 88 % of organisations worldwide experienced 'spear-phishing' attempts.

Given the growing number and cost of cyber-attacks, spending on information security is also increasing worldwide. The global security market is currently worth around US$150 billion, a figure that many predict will rise to US$208 billion in 2023 and US$400 billion in 2026.

Critical sectors, such as transport, energy, health and finance, have become increasingly dependent on digital technologies to run their core business. While growing digital connectivity brings enormous opportunities, it also exposes economies and societies to cyber-threats. The number, complexity and scale of cybersecurity incidents are growing, as is their economic and social impact.

The coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation of societies around the world. Yet, it has also exacerbated existing problems, such as the digital divide, and contributed to a global rise in cybersecurity incidents. During this unprecedented situation, there has been an increase in malicious cyber-activity across Member States, as revealed by a recent Europol report. Cybersecurity issues are becoming a day-to-day struggle for the EU.

According to monitoring reports from the EU Agency for Network Information Security (ENISA), cybercrime is becoming increasingly monetised, particularly in the case of major cyber-attacks that use ransomware. Likewise, increased e-commerce and cashless payments bring heightened risks of cybercrime attacks and cybersecurity breaches. With payments becoming increasingly cashless, online theft – of money and also of personal data – has been on the rise. An ENISA Threat Landscape 2021 report demonstrates that cyber-attacks are becoming more sophisticated, targeted, widespread and undetected, and concludes that societies face a long road ahead before they can ensure a more secure digital environment. According to Verizon, 86 % of breaches committed in 2019 were financially motivated and 10 % by espionage. About 45 % of breaches featured hacking, 17 % involved malware and 22 % involved phishing. This trend is expected to increase further, in parallel with technological developments such as the proliferation of devices linked to the Internet of Things (IoT). In an increasingly connected world, where 22.3 billion IoT devices are expected to be in use by 2024, the growing challenges in the cybersecurity landscape have led the EU to reflect on how to enhance the protection of its citizens and companies against cyber-threats and attacks.

Existing situation

The first step towards the creation and development of an EU cybersecurity ecosystem was the adoption of a cybersecurity strategy in 2013. The strategy identified the achievement of cyber-resilience and the development of industrial and technological resources for cybersecurity as its key objectives. The Directive on Security of Network and Information Systems across the EU (the NIS Directive), which had to be transposed by Member States by 9 May 2018, represents the first piece of EU-wide legislation on cybersecurity. It provided for legal measures to boost the overall level of cybersecurity in the EU, with a focus on protecting critical infrastructure. Among other things, it

established the NIS Cooperation Group, and the network of Computer Security Incident Response Teams (CSIRTs), to ensure both the exchange of information on cybersecurity and cooperation on specific cybersecurity incidents.

In view of the impending deadlines for its transposition into national legislation (by 9 May 2018) and the identification of operators of essential services (by 9 November 2018), the Commission adopted on 13 September 2017 a communication aimed at supporting Member States in their efforts to implement the directive swiftly and coherently across the EU. It introduced an NIS toolkit providing information to Member States on the best practices related to implementing the directive as well as clarifications on some of its provisions.

By 2020, all Member States had communicated to the Commission that they had fully transposed the directive into their national legislation.

Other legislative initiatives linked to cybersecurity date back to 2017, when the Commission submitted a package of cybersecurity measures to further improve the resilience and incident-response capacities of public and private entities, competent authorities and the EU as a whole in the field of cybersecurity and critical infrastructure protection. It also asked for a permanent and enhanced role for the EU cybersecurity agency and the creation of the first EU cybersecurity certification framework, which resulted in the Cybersecurity Act.

Since then, a new EU cybersecurity strategy for 2020-2025 has been adopted, proposing among many things the review of the NIS Directive, the adoption of a new critical entities resilience (CER) directive, a network of security operations centres (SOCs) and new measures to strengthen the EU cyber-diplomacy toolbox. It is in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people.

The threat landscape has changed considerably since the NIS Directive was adopted in 2016, and the scope of the directive needs updating and expanding to meet current risks and future challenges, one such challenge being to ensure that 5G technology is secure. In addition, its transposition and implementation has brought to light inherent flaws in certain provisions or approaches, such as the unclear delimitation of the scope of the directive. Furthermore, since the onset of the coronavirus crisis, the EU economy has grown more dependent on network and information systems than ever before, and sectors and services are increasingly interconnected.

The pandemic has more than confirmed the importance of preparing the EU for the digital decade as well as the need to continually improve cyber-resilience, particularly for those who operate essential services such as healthcare and energy.

Funding for EU cybersecurity initiatives has increased in the 2021-2027 programming period through a mix of instruments such as the Digital Europe Programme, Horizon Europe, the European Defence Fund, and the EU Recovery and Resilience Facility. The EU objective is to reach up to €4.5 billion of combined investment. Notably to go to SMEs under the recently established Cybersecurity Competence Centre and Network of Coordination Centres.

In terms of existing case law, the Court of Justice of the EU in its judgment in Case C-58/08 *Vodafone and others* has shown the need for establishing clear common rules on the scope of application of the NIS Directive and on harmonising the rules on cybersecurity risk management and incident reporting. Current disparities in this area at the legislative, supervisory, national and EU level are obstacles to the internal market, because entities that engage in cross-border activities face different, and possibly overlapping, regulatory requirements and/or their application, to the detriment of the exercise of their freedoms of establishment and of provision of services.

Parliament's starting position

In a resolution of 12 March 2019, the European Parliament called '… on the Commission to assess the need to further enlarge the scope of the NIS Directive to other critical sectors and services that are not covered by sector-specific legislation'.

In a resolution of 3 October 2017 on the fight against cybercrime, in the light of the increasing number of connected appliances, Parliament called for attention to be drawn to the safety of all devices and for action to promote the security-by-design approach. It urged Member States to speed up the setting-up of computer emergency response teams to which businesses and consumers can report malicious emails and websites, as envisaged by the NIS Directive.

In its resolution of 16 January 2016, Towards a Digital Single Market Act, Parliament called for the Commission to put in place a strong cybersecurity agency. More specifically, it called for efforts to be made to improve resilience against cyber-attacks, with an increased role for ENISA.

Council and European Council starting position

In its conclusions of 2 December 2020 on the security of connected devices, the Council encouraged the Commission to assess the complementary sector-specific regulations that should define what level of cybersecurity should be met by the connected device to ensure that specific security and privacy requirements are put in place for devices with higher security risks.

In its conclusions of 2 October 2020, the Council called for accelerating the deployment of very high capacity and secure network infrastructures (including fibre and 5G) all over the EU, and for enhancing the EU's ability to protect itself. It furthermore called on the EU and the Member States to make full use of the 5G cybersecurity toolbox adopted on 29 January 2020.

In its conclusions of 9 June 2020, the Council welcomed '…the Commission's plans to ensure consistent rules for market operators and facilitate secure, robust and appropriate information-sharing on threats as well as incidents, including through a review of the Directive on security of network and information systems (NIS Directive), to pursue options for improved cyber-resilience and more effective responses to cyber-attacks, particularly on essential economic and societal activities, whilst respecting Member States' competences, including the responsibility for their national security'.

Preparation of the proposal

To underpin the proposal and collect evidence, the Commission ran an open public consultation (OPC), launched stakeholder interviews, country visits, workshops and surveys, carried out a study on NIS investment and an impact assessment, and drew up a roadmap.

The main results of some of the finalised input activities are briefly described below.

Open public consultation

The OPC contributed to the evaluation and impact assessment of the NIS Directive. It included questions targeting citizens, stakeholders and cybersecurity experts. The OPC was carried out over a 12-week period, starting on 7 July 2020 and closing on 2 October 2020. A total of 206 replies were collected online, 182 of which were from respondents located in the EU-27. The hottest topic was the lack of a harmonised approach, resulting in significant inconsistencies in the way Member States draw up lists of operators of essential services (OESs) and digital service providers (DSPs). Consequently, companies of the same type might face different requirements depending on the Member State in which they operate. Likewise, a company might be identified as an OES in one Member State and a DSP in another Member State,[1] or as a service provider, thus being excluded from the scope of the NIS Directive in yet another Member State. The responses relating to the identification of OESs suggest that Member States' approaches are often highly heterogeneous. To that end, it was suggested to establish a common set of criteria to ensure a harmonised process of OES identification.

The OPC concluded that some identification practices used by Member States can have a negative impact on the level playing field in the internal market, and potentially render entities more vulnerable to cross-border cyber-threats.

An overwhelming majority of the OPC respondents agreed that common EU rules are needed to address cyber-threats, given that cyber-risks can propagate across borders at high speed.

The overall results revealed that OPC respondents on average show significantly more support for the inclusion of public administrations and data centres within the scope of the NIS Directive.

Figure 1: The number of OESs identified differs significantly across the EU

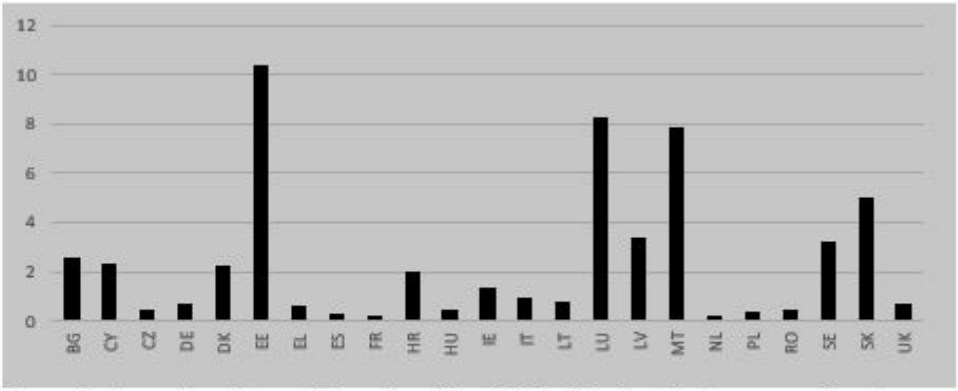


Figure 1: Operators of essential services identified by Member States across all sectors per 100 000 inhabitants[1]

Source: European Commission, 2020.

ENISA study on investments

A December 2020 ENISA NIS investments report presents the findings of a survey of 251 organisations of OESs and DSPs from France, Germany, Italy, Spain and Poland, examining their approaches to cybersecurity spending. The survey showed that 82 % of OESs and DSPs find that the NIS Directive has had a positive effect. However, gaps in investment still exist. When comparing organisations from the EU to their US counterparts, data shows that EU organisations allocate on average 41 % less to cybersecurity than their US counterparts.

Impact assessment

The Commission conducted an impact assessment (IA) for the current proposal, comprising three different documents. The IA explored four different policy options for the NIS review, including the baseline option: 0) maintaining the status quo; 1) non-legislative measures to align the transposition; 2) limited changes to the NIS Directive for further harmonisation; and 3) systemic and structural changes to the NIS Directive. Option 1 was discarded at an early stage, as it does not depart considerably from the status quo. The analysis led to the conclusion that option 3 – systemic and structural changes to the NIS framework – is the preferred one. Option 3 would envisage a more fundamental shift of approach towards covering a wider segment of the economies across the EU, yet with a more focused supervision targeting proportionally big and key companies, while clearly determining the scope of application. It would also streamline and further harmonise companies' security-related obligations, create a more effective setting for operational aspects, establish a clear basis for shared responsibilities and accountability of the entities concerned, and incentivise information sharing.

The IA was submitted to the Regulatory Scrutiny Board (RSB) on 23 October 2020 and received its feedback in the form of a positive opinion with comments on 20 November 2020. The RSB insisted that the IA should clearly distinguish between 'essential' and 'important' sectors, clarify the criteria for establishing these categories, and consider whether alternative approaches are possible. It asked the Commission to expand on whether the definition of sectoral coverage risks shifting the danger of exposure to other sectors and to analyse how the choice of sectors could be made future proof.

The RSB also observed that the IA should reinforce the problem analysis to better focus on the problems the directive aims to solve. Furthermore, the IA should include a more complete set of options on reporting, supervision and crisis response. It should include ways to interact with the linked European Critical Infrastructure Directive, which is also under revision. Finally, the IA should strengthen the analysis of compliance costs, especially for medium-sized enterprises.

The initial appraisal drawn up by EPRS provides a detailed analysis of the IA. According to it, the NIS2 proposal appears to follow the general considerations of the IA. The preferred option identified in the IA is at the core of the proposal. The monitoring provisions however do not appear to have been laid out in the proposal with the same level of detail as in the IA.

NIS evaluation

Article 23 of the NIS Directive requires the Commission to review the functioning of the NIS Directive periodically. As part of its key policy objective to make 'Europe fit for the digital age' as well as in line with the objectives of the security union, the Commission announced in its work programme 2020 that it would conduct the review by the end of 2020.

On 25 June 2020, the Commission published a combined evaluation roadmap/inception impact assessment on the revision of the NIS Directive, according to which it planned to 'evaluate the functioning of the NIS Directive based on the level of security of network and information systems in the Member States'. The Commission underlined that in addition to the requirement under Article 23 of the NIS Directive, the revision was 'further justified by the sudden increase in the dependence on information technology during the Covid-19 crisis'. The Commission stated that 'depending on the results from the evaluation of the functioning of the NIS Directive, an open public consultation and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union'.

The Commission evaluation analysed the NIS directive for its relevance, EU added value, coherence, effectiveness and efficiency. Its main findings were that the scope of the NIS Directive is too limited in terms of the sectors covered, mainly due to: i) increased digitalisation in recent years and a higher degree of interconnectedness; and ii) the scope of the NIS Directive no longer reflecting all digitalised sectors providing key services to the economy and society as a whole.

Furthermore, the evaluation concluded that the NIS Directive does not provide sufficient clarity as regards the scope criteria for OESs or the national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in some Member States and are therefore not required to put in place security measures and report incidents. For example, certain major hospitals in a Member State do not fall within the scope of the NIS Directive and hence are not required to implement the resulting security measures, while in another Member State almost every single healthcare provider is covered by the NIS security requirements.

The NIS Directive afforded Member States broad discretion when laying down security and incident reporting requirements for OESs. The evaluation shows that in some instances Member States have implemented these requirements in significantly different ways, creating an additional burden for companies operating in more than one Member State.

The supervision and enforcement regime of the NIS Directive is ineffective. The financial and human resources set aside by Member States for fulfilling their tasks (such as OES identification or supervision), and consequently the different levels of proficiency in dealing with cybersecurity risks, vary greatly. This further exacerbates the differences in cyber-resilience among Member States.

Member States do not share information systematically with one another, with negative consequences in particular for the effectiveness of the cybersecurity measures and the level of joint situational awareness at EU level. This is also the case for information-sharing among private entities and for the engagement between the EU level cooperation structures and private entities.

The changes the proposal would bring

The Commission presented on 16 December 2020 a proposal for a directive on measures for a high common level of cybersecurity across the Union (NIS 2), which would repeal and replace the existing NIS Directive (NIS1). The proposed directive aims to tackle the limitations of the current NIS1 regime. The legal basis for both NIS1 and the proposed NIS2 is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules.

The proposed expansion of the scope covered by NIS2, which would effectively oblige more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Overall, the NIS2 proposal sets itself three general objectives:

- Increase the level of cyber-resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures.[2] For instance, the proposal extends significantly the scope of the current directive by adding new sectors such as telecoms, social media platforms and the public administration (see this factsheet). It establishes that all medium-sized and large entities active in the sectors covered by the NIS2 framework would hence have to comply with the security rules put forward in the proposal, and removes the possibility for Member States to tailor the requirements in certain cases[3] (which had led to much fragmentation with NIS1 implementation, see impact assessment). It removes the distinction made between OESs and digital DSPs, which currently fall into three categories: online marketplaces, search engines and cloud service providers. Finally, it addresses, for the first time, cybersecurity of the ICT supply chain (of special importance in the case of the IoT).
- Reduce inconsistencies in resilience across the internal market in the sectors already covered by the directive, by further aligning i) the de facto scope; ii) the security and incident reporting requirements; iii) the provisions governing national supervision and enforcement; and iv) the capabilities of the Member States' relevant competent authorities. The proposal includes a list of seven key elements that all companies must address or implement as part of the measures they take, including incident response, supply chain security, encryption and vulnerability disclosure. In addition, the proposal envisages a two-stage approach to incident reporting. Affected companies have 24 hours from when they first become aware of an incident to submit an initial report, followed by a final report no later than one month later. Regarding enforcement, it establishes a minimum list of administrative sanctions whenever entities breach the rules regarding cybersecurity risk management or their reporting obligations laid down in the NIS Directive. These sanctions include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures into line with NIS requirements, and administrative fines (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher).
- Improve the level of joint situational awareness and the collective capability to prepare and respond, by i) taking measures to increase the level of trust between competent authorities; ii) by sharing more information; and iii) setting rules and procedures in the event of a large-scale incident or crisis. The proposed new rules improve the way the EU prevents, handles and responds to large-scale cybersecurity incidents and crises by introducing clear responsibilities, appropriate planning and more EU cooperation. The revised directive would establish an EU crisis management

framework, requiring Member States to adopt a plan and designate national competent authorities responsible for participating in the response to cybersecurity incidents and crises at the EU level. The proposed directive would establish an EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe) to support the coordinated management of EU-wide cybersecurity incidents, as well as to ensure the regular exchange of information. The proposed directive would also strengthen the role of the NIS Cooperation Group in making decisions and increasing cooperation between Member States. Member States would still be required to adopt a national cybersecurity strategy and to designate one or more national competent authorities to supervise compliance with the directive; and to designate CSIRTs to handle incident notifications and single points of contact (SPOC) to act as a liaison point with other Member States.

In order to ensure consistency and coherence with related EU legislation, the NIS Directive review in particular takes into account the following three Commission initiatives:

- the review of the Resilience of Critical Entities (CER) Directive, which was proposed alongside the NIS2 proposal, with the objective of improving the resilience of critical entities against physical threats in a large number of sectors. The proposal expands both the scope and depth of the current 2008 directive, including the coverage of 10 sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space;
- the initiative on a digital operational resilience act for the financial sector (DORA);
- the initiative on a network code on cybersecurity with sector-specific rules for cross-border electricity flows (see snapshot analysis from the SPEAR project).

As regards the financial sector, the DORA proposal would provide legal clarity on whether and how digital operational provisions apply, especially to cross-border financial entities, and it would eliminate the need for Member States to individually improve rules, standards and expectations regarding operational resilience and cybersecurity as a response to the current limited coverage of EU rules and the general nature of the NIS1 Directive. At the same time, it is important to maintain a strong relationship for the exchange of information between the financial sector and the other sectors covered by NIS2. To that end, under the DORA proposal, all financial supervisors, the European supervisory authorities (ESAs) for the financial sector and the financial sector-related national competent authorities would be able to participate in the discussions of the NIS Cooperation Group, and to exchange information and cooperate with the single points of contact and with the national CSIRTs under NIS2. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies, and national CSIRTs may cover the financial sector in their activities.

Furthermore, the Commission has aligned the scope in the NIS2 proposal with the proposal for a review of the CER Directive.

As regards ENISA, it would see increased responsibilities within its existing mandate, which involves overseeing the implementation of the NIS. ENISA would be tasked to prepare a report every two years on the state of cybersecurity in the EU and to maintain a European vulnerability registry providing access to information on the vulnerabilities of ICT products and services disclosed on a voluntary basis by essential and important entities and their ICT suppliers. At the same time, ENISA would be required to create and maintain a registry, in which certain types of entities including domain name system service providers, top level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, as well as online marketplaces, online search engines and social networking platforms would notify where they are established in the EU. This is to ensure that such entities do not face a multitude of different legal requirements, given that they provide services across borders to a particularly high extent.

To address key supply chain risks and to assist entities in managing cybersecurity risks related to the ICT supply chain, the NIS Cooperation Group, together with the Commission and ENISA, would be tasked to carry out a coordinated risk assessment per sector of critical ICT services, systems, or products including relevant threats and vulnerabilities. The supply chain risk assessments would consider both technical factors (hardware- or software-related) and, where relevant, non-technical factors (such as suppliers being subject to interference by a non-EU country or state-backed players). This approach largely builds on the previous work of the Commission and the NIS Cooperation Group on the security of 5G networks. The Commission published on 29 January 2020 the 5G risk management toolbox, which listed measures to mitigate the security threats associated with 5G networks. Among others, the EU 5G risk assessment identified security risks related to 5G networks and the 5G supply chain at the EU level. To ensure that entities comply with their obligations addressing ICT supply chain security, the new directive would enable Member States to require essential and important entities to certify specific ICT products, services and processes under the EU Cybersecurity Act. In this context, the draft directive would empower the Commission to lay down which categories of essential entities (due to their criticality) would be required to obtain certification.

The European Electronic Communications Code (EECC) regulates since December 2020 the security of telecoms providers when they are providing electronic communications services in the EU. However, telecoms providers are covered by the current NIS framework if they provide non-telecoms services that fall within the scope of the directive, i.e. cloud computing services. The proposed directive would therefore repeal the corresponding EECC security provisions and entirely regulate the security of telecoms providers, also in cases where they are providing ECS-related services. The same would apply to the security provisions for trust service providers currently found in the eIDAS Regulation.

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on the proposal during its plenary session of 27-28 April 2021.

The EESC notes that some of the provisions in both the NIS2 and CER proposals overlap, as they are closely linked and complementary. The EESC therefore calls for the possibility of combining the two proposals to form one single text. Furthermore, given the relevance and sensitivity of the objectives pursued by the two proposals, it finds that a regulation would have been preferable to a directive.

In addition, the EESC points out that clearer guidelines are needed for distinguishing between 'essential' and 'important' entities, and that the respective requirements to be met should be more precisely defined.

Finally, the EESC agrees that ENISA plays a key role in the overall European institutional and operational cybersecurity system. Thus, in addition to the proposed two-yearly report on the state of cybersecurity in the Union, it should also publish regular, up-to-date information on cybersecurity incidents and sector-specific warnings online.

The European Committee of the Regions (CoR) has not prepared an opinion on the proposal.

National parliaments

The subsidiarity deadline for the submission of reasoned opinions was 17 March 2021. No national parliament submitted any reasoned opinion.

Stakeholder views[4]

From 25 June 2020 to 13 August 2020, all interested stakeholders could provide feedback on the inception impact assessment and roadmap on a dedicated Commission webpage. A total of 42 responses were received from stakeholders, the private sector, research organisations and

citizens from the EU and internationally. Stakeholders broadly pointed to the current fragmentation in the implementation of NIS at the national level, particularly regarding OESs and DSPs. They furthermore emphasised the need to improve EU-level coordination of cyber-attack responses and with other related EU legislation.

The GSMA mobile association strongly recommends that the Commission address the shortcomings and persisting inefficiencies in the NIS Directive by: including software and hardware providers in the scope of the NIS, to ensure robust end-to-end security; reducing red tape and fragmentation, by streamlining processes, security requirements and incident notifications obligations; and improving harmonisation and consistency for providers of Electronic Communications Services, by closely aligning the NIS Directive with other legal instruments (the Cybersecurity Act, the EECC and the European Critical Infrastructure (ECI) Directive).

Eurosmart, the association representing the European digital security industry, believes that 'DSPs should use physical infrastructure exclusively located in Europe. The NIS Directive should leverage the European certification schemes created in the framework of the Cybersecurity Act (CSA) to demonstrate the ability of OES and DSP to meet a high level of protection. Following a risk-based approach, certification of highly critical products must be done at a level 'High' pursuant to the CSA. Security certificate at level 'High' ensures continuous monitoring and maintenance of the certification scheme by a community of recognised experts from the industry. It is the only way to ensure "the state of the art" of security for critical infrastructures'.

The Software Alliance (BSA) states that the general spirit of the existing provisions should be kept, but with a better level of harmonisation and implementation, in particular with regard to service definitions, thresholds, reporting modalities, and the categories of (sub-)sectors recognised as OESs and DSPs across the EU. With regard to the call to expand the scope of the NIS to software products, the BSA also underlines that the sector is already covered by force of the inclusion of cloud services in Annex III, notably through the 'software as a service' principle. For the very limited cases where software would not be delivered or serviced through the cloud (i.e. when embedded), the incident-reporting obligations would be irrelevant, as the manufacturer would not have the visibility of the incident affecting that specific piece of software.

Digital Europe, the industry association, believes that the current NIS scope should be maintained. The review should, however, ensure that Member States are more closely aligned in defining OESs and DSPs to avoid fragmentation.

BEUC, the European consumer association, states that the scope of the NIS is not broad enough, especially when it comes to DSPs. As regards OESs, the discrepancies in their selection criteria has created legal fragmentation in the EU.

The European Data Protection Supervisor (EDPS) published an opinion on the cybersecurity strategy and the NIS 2 Directive on 11 March 2021 in which, among other things, he issues specific recommendations to ensure that the proposal correctly and effectively complements existing Union legislation on personal data protection, in particular the GDPR and the ePrivacy Directive. He also asks to clarify the different use of the terms 'cybersecurity' and 'security of network and information systems' across the text: to use the term 'cybersecurity' in general, and the term 'security of network and information systems' only for technical purposes when the context allows it.

The Body of European Regulators for Electronic Communications (BEREC) has published an opinion on 19 May 2021, on the NIS2 proposal recommending that the security of the telecoms sector should continue to be regulated under the EECC. According to BEREC, including the telecoms sector under the scope of NIS2 risks reducing the security level already established through sector-specific regulatory practice since the Framework Directive came into effect in 2009.

Legislative process

In the European Parliament, the Committee on Industry, Research and Energy (ITRE) was assigned the file (rapporteur: Bart Groothuis, Renew, the Netherlands). The Committees on Foreign Affairs (AFET), on Internal Market and Consumer Protection (IMCO), on Transport and Tourism (TRAN) and on Civil Liberties, Justice and Home Affairs (LIBE) all submitted opinions.

On 13 April 2021, the European Commission presented the legislative proposal to Parliament's lead committee, ITRE. MEPs welcomed the proposed review of NIS. The most common concern raised by MEPs was about its compatibility with other proposed or existing EU legislation, including DORA, CER, the Cybersecurity Act, the EECC and the GDPR.

The ITRE draft report was published on 3 May 2021, and the four committee opinions were adopted in July 2021. The ITRE committee adopted its report on 28 October 2021, with 70 votes in favour to 3 against, with 1 abstention. MEPs also voted to open trilogue negotiations with Council, with this mandate confirmed in plenary in November.

The report calls for tighter cybersecurity obligations in terms of risk management, reporting obligations and information-sharing. It aims to lower the administrative burden and to improve cybersecurity incident reporting. In addition, the report states that EU countries would have to meet stricter supervisory and enforcement measures, and harmonise their sanctions regimes.

The report also states that the Commission should ensure that appropriate guidance is given to all micro- and small enterprises falling within the scope of the NIS2 Directive. The report also supports policies promoting the use of open-source cybersecurity tools, which are of particular importance for SMEs as they face significant costs for implementing cybersecurity tools.

Among other things, the rapporteur added the notion of 'active defence'[5] in his draft report. The report as adopted says that Member States should adopt policies on the promotion of active cyber-defence as part of their national cybersecurity strategies.

The report intends to broaden the sectorial scope to also include academic, knowledge and research institutions which had been left outside the scope of NIS2 by the Commission, while many national cybersecurity strategies cover them.

In June 2021, the Council took stock of progress on NIS2. One of its concerns related to the interaction of NIS2 with sectoral legislation, in particular CER and DORA. During the discussions, most Member States stated that it was imperative to view NIS2 as the horizontal framework for cybersecurity in the EU and that it should serve as a baseline standard for minimum harmonisation of all relevant sectoral legislation in this field. Other concerns raised related to the significant expansion of the scope of the revised rules, the size-cap criteria as the sole element to be considered when identifying essential and important entities to be covered, the proposed legal basis (i.e. single market), and national security concerns.

The Council adopted its negotiating position on 3 December 2021. Compared to the initial proposal for NIS2, the Council introduced a number of significant changes. For instance it introduced additional criteria to determine the entities to be covered by NIS2, excluding from its scope entities operating in defence and national security, public security, law enforcement and the judiciary, as well as parliaments and central banks. It aligned the text with other related proposed legislation, such as the CER Directive and DORA. Furthermore, it simplified the incident-reporting obligations, to avoid over-reporting, and extended the period for Member States to transpose NIS2 into national law to two years, instead of 18 months.

Interinstitutional trilogue negotiations started on 13 January 2022 and a second meeting took place on 17 February. On 13 May, during the third trilogue meeting, the Parliament and Council reached a political agreement. The revised directive sets out minimum rules for a regulatory framework, and lays down cooperation mechanisms among relevant authorities in each Member State. It expands the list of sectors and activities subject to cybersecurity obligations, and improves their

enforcement, providing for remedies and sanctions which would vary between essential services and important entities. Parliament negotiators had insisted on the need for clear and precise rules for companies. The reporting obligations have been simplified and streamlined to give entities more time to report than the initial 24 hours proposed by the Commission. This is in order to avoid over-reporting and creating an excessive burden on the entities covered. The text has been aligned with sector-specific legislation, in particular with the DORA Regulation and the CER Directive, to provide legal clarity and ensure coherence.

The NIS2 directive would introduce a size-cap rule for determining which entities meet the criteria to qualify as operators of essential services and important entities. This means that all medium-sized and large entities operating within the sectors covered by the directive or providing services covered by the directive would fall within its scope. The co-legislators maintain this general rule but with additional provisions to ensure proportionality and clear-cut criticality criteria for determining them. Such entities would fall under the jurisdiction of the Member State in which they are established, not of the Member State in which they provide their services.

The directive would also formally establish the EU-CyCLONe network, which will support the coordination and management of large-scale incidents.

In addition, a voluntary peer-learning mechanism would be established to support learning from good practice.

As demanded by the Council, the directive would not apply to entities carrying out activities in areas such as defence and national security, public security, law enforcement and the judiciary. Parliaments and central banks are also excluded from the scope. However, as demanded by the Parliament it will apply to public administration entities at central and regional level. In addition, Member States may also decide that it applies to entities at local level.

The political agreement was endorsed by the ITRE committee on 13 July 2022, and then adopted by Parliament in plenary on 10 November 2022, with 577 votes in favour, 6 against and 31 abstentions. The text was then adopted by the Council on 28 November 2022 and signed by both co-legislators on 14 December 2022. It was published in the Official Journal on 27 December 2022, and entered into force on 16 January 2023. Member States have 21 months – until 17 October 2024 – to transpose the directive into national law.

EP SUPPORTING ANALYSIS

Zygierewicz A., Directive on security of network and information systems (NIS Directive), Implementation appraisal briefing, EPRS, European Parliament, November 2020.

Kononenko V., Improving the common level of cybersecurity across the EU, Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament, February 2021.

Erbach G. with O'Shea J., Cybersecurity of critical energy infrastructure, Briefing, EPRS, European Parliament, October 2019.

Negreiro M., ENISA and a new cybersecurity act, Briefing, EPRS, European Parliament, July 2019.

Negreiro M. with Belluomini A., The new European cybersecurity competence centre and network, Briefing, EPRS, European Parliament, July 2020.

OTHER SOURCES

High common level of cybersecurity across the Union – NIS 2 Directive, European Parliament Legislative Observatory.

Challenges to effective EU cybersecurity policy, European Court of Auditors (ECA) Briefing Paper, March 2019.

Report assessing the consistency of the approaches in the identification of operators of essential services, European Commission, 2020.

Internet organised crime threat assessment (IOCTA) 2020, Europol, 2020.

ENDNOTES

[1] In addition to the OPC, the Commission gathered evidence through a commissioned study assessing the consistency of the approaches in the identification of operators of essential services. Besides giving an overview of how Member States have identified operators of essential services, the study assesses whether the methodologies used are consistent across the EU.

[2] The Commission proposal covers the following sectors and subsectors: i) 'essential entities': energy (electricity, district heating and cooling, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health; manufacture of pharmaceutical products including vaccines; drinking water; waste water; digital infrastructure (internet exchange points; DNS providers; TLD name registries; cloud computing service providers; data centre service providers; content delivery networks; trust service providers; and public electronic communications networks and electronic communications services); public administration; and space. ii) 'important entities': postal and courier services; waste management; chemicals; food; manufacturing of medical devices, computers and electronics, machinery equipment, motor vehicles; and digital providers (online market places, online search engines, and social networking service platforms).

[3] Under the NIS2 proposal, 'essential' and 'important' entities are deemed to be under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the jurisdiction of each of these Member States. At the same time, certain types of entities would be under the jurisdiction of the Member State in which they have their main establishment in the EU. These entities include, but are not limited to, domain name system service providers, top level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, as well as online marketplaces, online search engines and social networking platforms.

[4] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.

[5] Active cyber defence is the proactive prevention, detection, monitoring, analysis and mitigation of network security breaches, combined with the use of capabilities deployed within and outside the victim network.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Fourth edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.