Council of the
European Union

Brussels, 5 May 2021
(OR. en)

8416/21

Interinstitutional Files:
2020/0359 (COD)
2020/0365 (COD)

PROCIV 44
JAI 478
COSI 77
ENFOPOL 161
CT 58
COTER 54
ENER 156
TRANS 262
TELECOM 180
ATO 31
ECOFIN 408
ENV 275
SAN 266
CHIMIE 54
RECH 189
DENLEG 33
RELEX 380
HYBRID 25
CYBER 122
ESPACE 44
DATAPROTECT 115
MI 307
CSC 176
CSCI 70

COVER NOTE

From:	European Economic and Social Committee
date of receipt:	3 May 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. prev. doc.:	14150/20 + ADD1 14262/20 + ADD1
Subject:	Opinion of the European Economic and Social Committee on - 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 - 2020/0359 (COD)] and - Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities [COM(2020) 829 final - 2020/0365 (COD)]

Delegations will find attached the above-mentioned opinion.

Encl.: TEN/730

TEN/730
Cybersecurity and resilience of critical entities

OPINION

European Economic and Social Committee

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 and Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities

[COM(2020) 823 final - 2020/0359 (COD) - COM(2020) 829 final - 2020/0365 (COD)]

Rapporteur: **Maurizio MENSI**

Referral	European Parliament, 21/01/2021 – 11/02/2021 Council, 26/01/2021 – 19/02/2021
Legal basis	Article 114 of the Treaty on the Functioning of the European Union
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	14/04/2021
Adopted at plenary	27/04/2021
Plenary session No	560
Outcome of vote for/against/abstentions)	243/0/5

1. **Conclusions and recommendations**

1.1 The EESC welcomes the Commission's efforts to make public and private entities more resilient to threats from cyber and physical attacks and incidents. The Committee also agrees that there is a need to strengthen industry and innovation capacity in an inclusive manner, through a strategy based on four pillars: data protection, fundamental rights, security and cybersecurity.

1.2 The EESC notes, however, that, given the relevance and sensitivity of the objectives pursued by the two proposals, a regulation would have been preferable to a directive. Moreover, it is not clear why the Commission did not even consider this option.

1.3 The EESC notes that some of the provisions in the two proposals overlap as they are closely linked and complementary: one proposal focuses primarily on aspects of cybersecurity and the other on physical security. The Committee therefore calls for the possibility of combining the two proposals to form a single text to be considered in the interests of simplification and streamlining.

1.4 The EESC welcomes the proposed removal of the distinction between operators of essential services and digital services providers found in the original NIS Directive. However, with regard to the directive's scope of application, the Committee points out that specific, clearer guidelines are needed to identify those bound by it. In particular, the criteria for distinguishing between "essential" and "important" and the respective requirements to be met should be more precisely defined, so as to ensure that differing approaches at national level do not result in barriers to trade or free movement of goods and services, which could jeopardise businesses and undermine trade.

1.5 Given the complexity of the system outlined in the two proposals, the EESC considers it important that the Commission clarify the exact scope of the two sets of rules, especially where different competing provisions aim to regulate the same matters or subjects.

1.6 The EESC points out that ensuring the clarity of all regulatory provisions is a non-negotiable aim, along with reducing red tape and fragmentation by simplifying procedures, security requirements and incident reporting obligations. Moreover, to this end and for the benefit of members of the public and businesses, it may be worthwhile merging the two proposals to form one single text, thus avoiding a sometimes complicated interpretation and implementation process.

1.7 The EESC recognises the key role, as highlighted in the proposal, of the management bodies of "essential" and "important" entities, whose members are required to follow specific training courses on a regular basis to gain sufficient knowledge and skills to apprehend and manage the various cyber risks and assess their impact. In this regard, the EESC considers that the proposal should specify the minimum content of the knowledge and skills in question, so as to provide guidance at European level on which training competencies are considered sufficient and to prevent the content of the various training courses differing between countries.

1.8 The EESC agrees that ENISA plays a key role in the overall European institutional and operational cybersecurity system. It considers, in this regard, that, in addition to the two-yearly report on the state of cybersecurity in the Union, this body should publish regular, up-to-date information on cybersecurity incidents and sector-specific warnings online. This would be another useful way of providing information to enable operators affected by NIS 2 to better protect their businesses.

1.9 The EESC agrees with the proposal to entrust ENISA with the task of setting up a European Vulnerability Register. It considers that communication of vulnerabilities and the most significant incidents must be made compulsory instead of voluntary, thus ensuring that it is also a useful tool for contracting authorities involved in the various European-level procurement procedures, including those for 5G technologies and products.

2. General comments

2.1 On 16 December 2020, the new EU cybersecurity strategy was presented alongside two legislative proposals: the revision of Directive (EU) 2016/1148[1] on the security of network and information systems (the "NIS 2 Directive") and a new directive on the resilience of critical entities (CER). The strategy, which is a cornerstone of the communication on *Shaping Europe's Digital Future*[2], the recovery plan for Europe and the EU Security Union Strategy, aims to enhance Europe's collective resilience to cyber threats and to guarantee that all individuals and businesses are able to benefit from trustworthy and secure digital services and tools.

2.2 Existing EU measures to protect critical services and infrastructure from cyber and physical risks need to be updated. Cybersecurity-related risks are continuing to evolve as digitalisation and interconnectedness increase. The existing regulatory framework must therefore be revised in line with the EU security strategy, moving beyond the dichotomy between online and offline and an approach based on strict compartmentalisation.

2.3 The two proposals for directives cover a wide range of sectors and address current and future online and offline risks linked to cyber and criminal attacks, natural disasters and other incidents. They also draw on the lessons learned during the current pandemic, which has shown that the increasing dependence of society and the economy on digital solutions leaves them vulnerable and exposed to growing and rapidly changing cyber threats, especially with regard to groups at risk of social exclusion such as people with disabilities. This has led the EU to propose measures to ensure that cyberspace remains a global and open space, based on sound security guarantees, digital sovereignty and leadership. It aims to develop the operational capacity to prevent, deter and respond to potential threats through greater cooperation, with due respect for each Member State's prerogatives in the area of national security.

[1] OJ L 194, 19.7.2016, p. 1.

[2] COM(2020) 67 final.

3. The proposal to revise the Directive on the security of network and information systems

3.1 The NIS Directive (Directive (EU) 2016/1148) was the EU's first cross-cutting regulatory tool in the area of cybersecurity. It aimed to make the EU's network and information systems more resilient to cyber risks. Despite achieving good results, the NIS Directive nevertheless has some limitations. The digital transformation of society, which has picked up the pace due to the COVID-19 crisis, has expanded the threat landscape, highlighting our increasingly interdependent societies' vulnerability to significant, unexpected risks. New challenges have emerged, which call for appropriate and innovative responses. The findings of the broad stakeholder consultation have brought to light the insufficient level of cybersecurity in European businesses, the inconsistent application of the rules in various sectors at national level and the lack of understanding of the main threats and challenges.

3.2 The NIS 2 proposal is closely linked to two other initiatives: the proposed Digital Operational Resilience Act (DORA), applicable to the digital finance sector, and the proposal for a directive on the resilience of critical entities (CER), which extends the scope of application of Directive 2008/114[3] on energy and transport to other sectors, focusing for example on the health sector and on bodies active in research and development of medicines. The CER Directive, which has the same sectoral scope as the NIS 2 Directive with regard to essential entities (Annex I of the NIS 2 Directive), shifts its focus from the protection of physical assets to the resilience of the entities managing them. It also moves from identifying European critical infrastructure with a cross-border dimension to identifying critical infrastructure at national level. The NIS 2 proposal is also in line with and complements other existing regulatory texts such as the European Electronic Communications Code, the General Data Protection Regulation (GDPR) and the eIDAS Regulation on electronic identification and trust services.

3.3 In keeping with the Regulatory Fitness and Performance Programme (REFIT), the NIS 2 proposal aims to reduce red tape for the competent authorities and compliance costs for public and private stakeholders, and to modernise the regulatory framework. In addition, it enhances security requirements on companies, addresses the issue of supply chain security, streamlines reporting obligations, introduces more stringent supervision measures for national authorities and seeks to harmonise penalties in the Member States.

3.4 The NIS also helps to boost the exchange of information and cooperation on cyber crisis management at European and national level. The proposal no longer distinguishes between operators of essential services and digital services providers as did the NIS Directive. Its scope of application covers medium or large companies in sectors identified as critical to the economy and to society. These public or private entities are divided into two categories: "essential" and "important", each subject to different supervisory measures. However, Member States do have the option of considering smaller entities that have a high risk profile.

3.5 A new network of EU security operations centres, powered by artificial intelligence (AI), is planned. They will act as a real "cybersecurity shield", able to detect signs of a cyber attack early enough to allow for proactive action, before damage occurs. The significance of AI for

[3] OJ L 345, 23.12.2008, p. 75.

cybersecurity is also highlighted in the US National Security Commission on Artificial Intelligence (NSCAI) report published on 1 March 2021. As a result, Member States and critical infrastructure operators will have direct access to threat information in the form of "Threat Intelligence", as part of a European security network.

3.6 The Commission also addresses the problems of supply chain security and security in relationships with suppliers: the Member States, in cooperation with the European Commission and ENISA, can carry out coordinated risk assessments of critical supply chains, based on the successful approach taken for 5G networks, which was set out in the recommendation of 26 March 2019[4].

3.7 The proposal tightens and harmonises rules on security and reporting obligations for companies and establishes a common approach to risk management, which includes a minimum list of basic security measures to be applied. More specific provisions are included on the incident reporting process, on the content of reports and on deadlines. The proposal outlines a two-stage process: companies have 24 hours to submit an initial summary report, to be followed by a final detailed report within one month.

3.8 Member States are required to appoint national authorities responsible for managing crises, supported by specific plans and a new operational cooperation network: the EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe). The Cooperation Group will have an enhanced role in shaping strategic decisions and a register of vulnerabilities found in the EU will be established and managed by ENISA; information sharing and cooperation between Member States' authorities will be stepped up, including cooperation on cyber crisis management.

3.9 The proposal introduces more stringent supervisory measures for national authorities and stricter enforcement requirements. It also aims to harmonise penalties across all Member States.

3.10 In this connection, the proposal for a directive sets out a number of administrative sanctions for breaches of cybersecurity and reporting obligations. It lays down provisions on the liability of natural persons who hold representational or managerial positions in companies that are covered by the directive. In this sense, the proposal improves the way in which the EU prevents, manages and responds to incidents and large-scale cybersecurity crises, by establishing clear responsibilities, proper planning and greater cooperation at EU level.

3.11 The Member States will be able to jointly monitor the implementation of EU rules and assist one another in the event of cross-border problems. They will be able to establish a more structured dialogue with the private sector, coordinate the disclosure of vulnerabilities found in software and hardware sold on the internal market and coordinate the assessment of security risks and threats linked to new technologies, as happened for 5G.

[4] OJ L 88, 29.3.2019, p. 42.

4. **The proposal for a directive on the resilience of critical entities**

4.1 In 2006, the EU set up the European programme for critical infrastructure protection (EPCIP) and in 2008 it adopted the Directive on European critical infrastructure (ECI), which applies to the energy and transport sectors. Both the EU Security Union Strategy for 2020-2025[5] adopted by the European Commission and the recently adopted counter-terrorism agenda underline the importance of guaranteeing the resilience of critical infrastructure against physical and digital risks. However, both the assessment of the implementation of the ECI Directive carried out in 2019 and the impact assessment of the proposal considered in this opinion have shown that existing European and national measures do not guarantee that operators will be able to cope with the current risks. For this reason, the Council and the Parliament have called on the Commission to review the current approach to protecting critical infrastructure.

4.2 The EU Security Union Strategy adopted by the Commission on 24 July 2020 recognised the growing interconnection and interdependence between physical and digital infrastructure, while highlighting the need for more coherence and consistency between the ECI and NIS directives. To this end, the CER proposal, which has the same objective scope of application as the NIS 2 with regard to essential entities, extends the original scope of application of Directive No 114/2008, applying solely to energy and transport, to the following sectors: banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, and space. It also sets out clear responsibilities and proper planning and provides for increased cooperation. In this regard, a reference framework should be created for all risks and Member States must be supported in their efforts to ensure that critical entities are able to prevent, resist and absorb the consequences of incidents, regardless of whether risks are the result of natural disasters, incidents, terrorism, internal threats or public health emergencies such as the current situation.

4.3 Every Member State will be required to adopt a national strategy to guarantee the resilience of critical entities, to carry out regular risk assessments, and, on the basis of these assessments, to identify critical entities. Critical entities must in turn carry out risk assessments, adopt appropriate technical and organisational measures to boost resilience and report incidents to national authorities. Entities that provide services to or in more than one third of Member States are subject to specific oversight, including specific advisory missions organised by the Commission.

4.4 The CER proposal provides for different forms of support to Member States and critical entities, including the preparation of an EU-level overview of risks and the development of best practices and methodologies, along with training activities and exercises to test the resilience of critical entities. The cross-border cooperation system also includes an ad hoc expert group, the Critical Entities Resilience Group, which will be a forum for strategic cooperation and the exchange of information between Member States.

[5] COM(2020) 605 final.

5. Proposed changes to the legislative proposal concerned

5.1 The EESC welcomes the Commission's efforts to make public and private entities more resilient to threats from cyber and physical attacks. This is particularly significant and relevant in the light of the rapid digital transformation brought about by the COVID-19 outbreak. It also shares the view expressed in the communication on *Shaping Europe's Digital Future* that Europe must reap the benefits of the digital era and should strengthen its industry – especially small and medium-sized enterprises – and innovation capacity in an inclusive manner, through a strategy based on four pillars: data protection, fundamental rights, security and cybersecurity, as essential prerequisites for a society that is based on the power of data.

5.2 However, in light of the findings of the impact assessment and the consultation prior to the NIS 2 proposal, and taking into account the repeatedly emphasised aim of avoiding the fragmentation of national rules (which was also called for in the communication of 4 October 2017 on the implementation of the NIS Directive[6]), it is not clear to the EESC why the Commission did not propose the adoption of a regulation instead of a directive. This option was not even considered.

5.3 The EESC notes that some of the provisions in the two proposals overlap as they are closely linked and complementary: one proposal focuses primarily on aspects of cybersecurity and the other on physical security. It should also be noted that the critical entities referred to in the CER cover the same sectors and are the same as the "essential" entities referred to in NIS 2[7]. In addition, all critical entities covered by the CER are subject to the NIS 2 cybersecurity obligations. Then the two proposals set out a number of bridge clauses to ensure continuity between them, including: provisions for reinforced cooperation between the authorities, sharing information on oversight activities, notifying the NIS 2 authorities about the identification of critical entities pursuant to the CER and regular meetings between their respective cooperation groups to take place at least once a year. The two proposals also share the same legal basis, Article 114 of the TFEU, which aims to complete the internal market by harmonising national rules, as interpreted, inter alia, by the EU Court of Justice in its judgement on Case C- 58/08, *Vodafone and others*. The possibility of combining the two proposals to form a single text should be considered in the interests of simplification and streamlining.

5.4 The EESC welcomes the removal of the distinction between operators of essential services and digital services providers found in the original NIS Directive. However, with regard to its scope of application, the Committee points out that specific, clearer guidelines are needed to identify those bound by the directive. In addition to the references set out in Annex I and II, the NIS 2 Directive refers to several sets of criteria which differ from one another and involve sensitive quantitative and qualitative assessments that could be carried out differently at national level. This may again lead to the fragmentation that this legislative proposal aims to avoid. It is important to ensure that inconsistent approaches at national level do not result in barriers to

[6] COM(2017) 476 final.

[7] Annex 1: OJ L 194, 19.7.2016, p.1.

competition or free movement of goods and services, which could jeopardise businesses and undermine trade.

5.5 According to the NIS 2 Directive, critical operators in sectors considered as "essential" by the proposal considered in this opinion are also subject to more general resilience-enhancing obligations, with an emphasis on non-cyber risks, as per the CER Directive. However, the latter explicitly states that it does not apply to matters covered by the NIS 2 Directive. In fact, the CER Directive states that as cybersecurity is sufficiently addressed in the NIS 2 Directive, matters covered by it should be excluded from the scope of the CER, without prejudice to the special provisions for entities in the digital infrastructure sector. The CER Directive further notes that entities in the digital infrastructure sector are in essence based on network and information systems and fall within the scope of the NIS 2 Directive, which also addresses the physical security of such systems as part of their cybersecurity risk management and reporting obligations. At the same time, the CER does not rule out the possibility that specific provisions could be applied to them.

5.6 In light of this complex picture, the EESC considers it essential that the Commission clarify the exact scope of application of the two sets of rules, particularly in areas where competing provisions aim to regulate the same matters or subjects.

5.7 Ensuring the clarity of all regulatory provisions, and especially those included in extensive and complex texts such as the proposals considered in this opinion, should be a non-negotiable aim, at every level, along with reducing bureaucracy and fragmentation, simplifying procedures, security requirements and incident reporting obligations. In addition, it is important to ensure that increasing the number of bodies assigned to specific tasks does not make it more difficult to clearly identify their competences, as this would undermine the objectives pursued. For this reason and for the benefit of members of the public and businesses, it may be worthwhile merging the two proposals to form one single text, thus avoiding a sometimes complicated interpretation and implementation process.

5.8 In several cases, the NIS 2 refers to provisions in other legal texts such as Directive 2018/1972 establishing the European Electronic Communications Code, which is governed by the principle of speciality. Some of the provisions in this directive are explicitly repealed (Articles 40 and 41), while others will still apply in accordance with the above-mentioned principle, without any clarification being provided in this regard. The EESC would like to see any doubts dispelled regarding this point in order to avoid problems of interpretation. The EESC also endorses the Commission's aim of harmonising the system of penalties for failure to comply in the area of risk management, with a view to improving information-sharing and cooperation at EU level.

5.9 The EESC recognises the key role, as highlighted in the proposal, played by the management bodies of "essential" and "important" entities in the cybersecurity strategy and risk management, as they have to approve risk management measures, oversee their implementation and be accountable for any non-compliance. In this connection, members of these bodies are required to take specific training courses on a regular basis in order to acquire sufficient knowledge and skills to apprehend and manage the various cyber risks and assess their impact. However, the EESC considers that the proposal should specify the content of such knowledge and skills, so as to provide guidance at European level on which training competencies are considered sufficient to meet the requirements set out in the proposal, in order to prevent the training course content and requirements differing between countries.

5.10 The EESC agrees that ENISA plays a key role in the overall European institutional and operational cybersecurity system. In this regard, it considers that, in addition to the report on the state of cybersecurity in the Union, this body should publish up-to-date information on cybersecurity incidents and sector-specific warnings online. This would be a useful way of providing information to enable stakeholders affected by NIS 2 to better protect their businesses.

5.11 The EESC agrees that access to accurate and timely information on vulnerabilities affecting ICT products and services can help to ensure better cybersecurity risk management. In this regard, publically available sources of information on vulnerabilities are an important tool for competent national authorities, computer security incident response teams (CSIRTs), companies and users. The EESC therefore agrees with the proposal to entrust ENISA with the task of setting up a European Vulnerability Register. Essential and important entities and their suppliers would be able to report information to this register, so as to enable users to adopt the appropriate mitigation measures. The EESC considers, however, that this communication of vulnerabilities and the most serious incidents must be made obligatory instead of voluntary, thus ensuring that it is also a useful tool for contracting authorities involved in the various European-level procurement procedures, including those for 5G technologies and products. The register would then contain information that can be used for evaluating tenders, as it could be used to check both their quality and the reliability of European and non-European contractors in terms of the security of the products and services included in the call for tenders, in accordance with the Recommendation on the Cybersecurity of 5G networks of 26 March 2019. The register should also ensure that the information it contains is made available in a way that avoids any kind of discrimination.

Brussels, 27 April 2021

Christa SCHWENG
The president of the European Economic and Social Committee