BRIEFING

Implementation Appraisal

European Parliament

Directive on security of network and information systems (NIS Directive)

EU cybersecurity policy

This briefing is one in a series of 'implementation appraisals', produced by the European Parliamentary Research Service (EPRS), on the operation of existing EU legislation in practice. Each briefing focuses on a specific EU law that is likely to be amended or reviewed, as envisaged in the European Commission's annual work programme. 'Implementation appraisals' aim to provide a succinct overview of publicly available material on the implementation, application and effectiveness to date of an EU law, drawing on input from EU institutions and bodies, as well as external organisations. They are provided by the EPRS Ex-Post Evaluation Unit, to assist parliamentary committees in their consideration of new European Commission proposals, once tabled.

SUMMARY

The EU cybersecurity strategy 2020-2025 underlines that 'security is not only the basis for personal safety, it also protects fundamental rights and provides the foundation for confidence and dynamism in our economy, our society and our democracy'.

The NIS Directive (Directive on security of network and information systems across the Union, Directive (EU) 2016/1148) entered into force in August 2016 as the first horizontal EU cybersecurity legal act. It forms part of the EU cybersecurity policy and in particular the EU's cybersecurity strategies.

In 2020, the European Commission announced the revision of the NIS Directive with the aim to increase cybersecurity. Between July and October 2020, the Commission ran a public consultation designed to contribute to the revision of the NIS Directive. The proposal is expected in the fourth quarter of 2020.

Definitions of cybercrime, cyber-thread and cybersecurity

Cybercrime, or computer crime, is defined by *Encyclopaedia Britannica* as 'the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy'. Cybersecurity, or computer security, is defined as 'the protection of computer systems and information from harm, theft, and unauthorized use'. There are four major types of cyber-threat:

- theft of data, such as that of military secrets from government computers;
- vandalism, including the destruction of data by a computer virus;
- fraud, such as employees at a bank channelling funds into their own accounts; and
- invasion of privacy, such as the illegal accessing of protected personal financial or medical data from a large database.

Author: Anna Zygierewicz

Ex-Post Evaluation Unit

PE 654.198 – November 2020

EN

EU citizens' concerns about cybersecurity by Eurobarometer

- Three quarters (76 %) of respondents to the Eurobarometer survey on Europeans' attitudes towards cybersecurity who used the internet, believed that the risk of becoming a victim of cybercrime was increasing. Their main concerns were the misuse of their personal data (46 %) and the security of online payments (41 %).
- Cybersecurity concerns had led more than nine in ten (93 %) respondents, who used internet, to change their behaviour in some way, more specifically: 42 % did not open emails from unknown persons; 42 % had installed antivirus programmes or applications; 37 % had changed an email account password; 32 % only visited websites they knew and trusted, or only used their own computer; 30 % had changed an online banking password; and 25 % had changed an online social network password.
- More than four in ten (46 %) respondents to the Eurobarometer survey on Attitudes towards the impact of digitalisation on daily lives said 'they would like take a more active role in controlling the use of their personal information (e.g. on their energy consumption, online shopping habits, health)'.

Source: Europeans' attitudes towards cyber security, Special Eurobarometer 499, January 2020 and Attitudes towards the impact of digitalisation on daily lives, Special Eurobarometer 503, December 2019.

According to the 2013 EU cybercrime strategy, cybercrime 'commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target'. Cybercrime comprises:

- traditional offences (e.g. fraud, forgery and identity theft),
- content-related offences (e.g. online distribution of child pornography or incitement to racial hatred), and
- offences unique to computers and information systems (e.g. attacks against information systems, denial of service, and malware).

According to the strategy, 'cyber-security commonly refers 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. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein'.

The European Court of Auditors in its briefing paper Challenges to effective EU cybersecurity policy, states that: 'cybersecurity involves preventing, detecting, responding to and recovering from cyber incidents. Incidents may be intended or not and range, for example, from accidental disclosures of information, to attacks on businesses and critical infrastructure, to the theft of personal data, and even interference in democratic processes. These can all have wide-ranging harmful effects on individuals, organisations and communities'. Under Regulation (EU) 881/2019, a cyber-threat is 'any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons'. It also defines cybersecurity, as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'.

The 10 most common cyber-threats, according to the ENISA Threat Landscape Report 2018, are: 1) malware; 2) web-based attacks; 3) web-application attacks; 4) phishing; 5) denial of service; 6) spam; 7) botnets; 8) data breaches; 9) insider threat; and 10) physical manipulation, damage, theft or loss.

Cost of cybercrimes and cybersecurity

Cyber-attacks are one of the fastest growing crimes worldwide, and the fastest growing crime in the United States (US). Cyber-attacks are also growing in size, cost and sophistication. By 2021 cybercrime damage will cost US$6 trillion[1] annually, up from US$3 trillion in 2015, according to the 2019 Official annual cybercrime report prepared by the Herjavec Group. The report also stresses that 'cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind'.

The average cost of the cybercrime is also growing, according to the Ninth Annual Cost of Cybercrime Study, prepared by Accenture Security, from US$11.7 million in 2017 to US$13 million in 2018. In 2018,

the average annual cost of cyber-attacks (by country), according to the above-mentioned report, totalled US$27.4 million in the US (US$21.2 million in 2017), US$13.6 million in Japan (US$10.5 million in 2017), $13.1 million in Germany (US$11.2 million in 2017), US$11.5 million in the United Kingdom (US$8.7 million in 2017) and US$9.7 million in France (US$7.9 million in 2017).

The average annual cost of cybercrime in the most affected industries in 2018, according to the above-mentioned report, totalled: US$18.38 million in banking (US$16.6 million in 2017), US$17.8 million in utilities (US$15.1 million in 2017), US$16 million in the software industry (US$14.5 million in 2017), US$15.8 m on automotive industry (US$10.7 million in 2017), and US$15.8 million in insurance (US$12.9 million in 2017).

Given the growing number of cyber-attacks and the growing costs of those attacks, spending on information security is also increasing worldwide. Global spending on cybersecurity will exceed US$1 trillion cumulatively for the five-year period from 2017 to 2021, according to Cybersecurity Ventures. The global security market is worth around US$150 billion now and is expected to rise to US$208 billion in 2023 and US$400 billion in 2026 according to various estimates.

Introduction to EU cybersecurity policy

In March 2009, the Commission published a communication Critical Information Infrastructure Protection 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (COM(2009) 149) that focused on prevention and awareness, and defined a plan of immediate action to strengthen the security and resilience of critical information infrastructure (CII) and to raise trust in the information society. The communication also cited the 2008 estimates of the World Economic Forum, according to which there was a 10 to 20 % probability of a major CII breakdown in the following 10 years, with a potential global economic cost of approximately US$250 billion.

In February 2013, the EU proposed a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1) outlining the EU's vision for the domain, clarifying roles and responsibilities and setting out the actions required 'based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world'. The publication of the strategy was followed by the publication of a Commission proposal for a directive on network and information security (NIS) – the NIS Directive – the first EU-level legislation on cybersecurity.

First EU sanctions against cyber-attacks

On 20 July 2020, the Council of the EU decided to impose restrictive measures against six individuals (two from China and four from Russia) and three entities (one from China, one from North Korea and one from Russia) responsible for an attempted cyber-attack against the Organisation for the Prohibition of Chemical Weapons (OPCW), and cyber-attacks publicly known as 'WannaCry', 'NotPetya', and 'Operation Cloud Hopper'. The sanctions imposed included a travel ban and an asset freeze. In addition, EU persons and entities were forbidden from making funds available to those listed in the sanctions.

This was the first time that the sanctions, part of the EU's cyber diplomacy toolbox 'to prevent, deter and respond to malicious cyber activities directed against the EU or its Member States', had been used. The legal framework for them was adopted in May 2019 and has recently been renewed.

On 22 October 2020, the Council of the EU decided to impose another restrictive measures. This time, on two individuals and one body (all from Russia) that were responsible for or took part in the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April and May 2015.

Source: EU imposes the first ever sanctions against cyber-attacks, Council of the EU, press release of 20 July 2020 and Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack, Council of the EU, press release of 22 October 2020, with relevant Council of the EU documents.

In September 2017, the cybersecurity package was presented, including, inter alia, proposals for a cybersecurity act and for a regulation on a European Cybersecurity Competence Network and Centre. The cybersecurity package was followed by the communication Making the Most of the Directive on Security of Network and Information Systems, published to assist Member States with guidance and best practice examples as well as to ensure harmonised transposition of the new rules.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 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) was published in the Official Journal (OJ L 151) on 7 June 2019 and entered into force 20 days later.

The Cybersecurity Act:

- strengthens ENISA by granting the agency a permanent mandate, reinforcing its financial and human resources and generally enhancing its role in helping the EU to achieve joint, high-level cybersecurity;
- establishes the first EU-wide cybersecurity certification framework, to ensure a common approach to cybersecurity certification in the EU's internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. internet of things) and services.[2]

In May 2020, a communication Europe's moment: Repair and Prepare for the Next Generation (COM(2020) 456) was adopted by the Commission, announcing the new cybersecurity strategy, which 'will look at how to boost EU-level cooperation, knowledge and capacity. It will also help Europe strengthen its industrial capabilities and partnerships, and encourage the emergence of SMEs in the field'. It was also announced, that the strategy would be accompanied by 'the review of the Directive on security of network and information systems and a proposal for additional measures on Critical Infrastructure Protection'.

On 24 July 2020, the Commission published its EU Security Union Strategy 2020-2025 (COM(2020) 605), which succeeded the European Agenda on Security (2015-2020). The strategy underlined that 'Cyber-attacks and cybercrime continue to rise. Security threats are also becoming more complex: they feed on the ability to work cross-border and on inter-connectivity; they exploit the blurring of the boundaries between the physical and digital world; they exploit vulnerable groups, social and economic divergences'. The Commission announced that by the end of 2020, it planned to 'complete the review of the NIS Directive, propose ideas need for a Joint Cyber Unit (to further coordinate cybersecurity operational capabilities across the EU) and to adopt a new Cybersecurity Strategy'.

The May 2020 proposed Recovery Plan for Europe envisages additional investment in cybersecurity, including from the Horizon 2020 programme and the upcoming Digital Europe programme.

Introduction to the NIS Directive

The NIS Directive entered into force in August 2016. Based on Article 114 of the Treaty on the Functioning of the European Union, the directive's objective is to achieve a high common level of security of network and information systems within the EU so as to improve the functioning of the internal market (Article 1.1). The directive provided the first horizontal EU law on cybersecurity and covers several key economic sectors (see Annex II) and digital service providers (DSPs) (see Annex III).

The NIS Directive was designed to improve: a) Member States' cybersecurity capabilities; b) the cooperation between Member States; and c) Member States' supervision of critical sectors. On the latter, the Commission's communication (COM(2017) 476 final/2) specifies that the third objective of the directive is to promote 'a culture of risk management and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSPs)'. To achieve these three objectives, the directive provides for a number of measures (see Table 1 and ENISA visual tool).

Table 1 – Objectives and measures of the NIS Directive

Objective	Measures and tools
Improved cybersecurity capabilities at national level	➢ Member States adopt national strategies on the security of network and information systems. ➢ Member States designate one or more national competent authorities to monitor the application of the NIS Directive at national level. ➢ Member States designate one or more computer security incident response teams (CSIRTs), whose role is described in Article 12 of the NIS Directive.
Increased EU-level cooperation	➢ Member States designate a single point of contact with a liaison function to ensure cross–border cooperation with the relevant authorities in other Member States and with the cooperation mechanisms created by the NIS Directive. ➢ The NIS Cooperation Group supports and facilitates strategic cooperation and the exchange of information among Member States, also aiming to develop trust and confidence. The functioning of the group is based on Commission Implementing Decision (EU) 2017/179 of 1 February 2017. The group is composed of representatives of Member States, the Commission and ENISA (the European Union Agency for Network and Information Security). The Commission also acts as secretariat. ➢ A network of the national CSIRTs contributes to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation. The CSIRTs network is composed of representatives of the Member States' CSIRTs and CERT–EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). ENISA provides the secretariat for the network. The Commission participates as an observer.
Established risk management and incident reporting obligations for operators of essential services and digital service providers	Member States identify operators of essential services (private businesses or public entities with an important role for the society and the economy). Operators are identified in the following seven sectors: ➢ energy: electricity, oil and gas; ➢ transport: air, rail, water and road; ➢ banking: credit institutions; ➢ financial market infrastructures: trading venues, central counterparties; ➢ health sector: health care settings including hospitals and private clinics; ➢ drinking water supply and distribution; ➢ digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries. The operators of essential services (OES) take appropriate security measures and notifies the relevant national authority of serious incidents. The DSPs take appropriate technical and organisational measures to manage the risks posed to the security of NIS, which they use in the context of offering services referred to in Annex III within the EU.

Source: EPRS, based on the NIS Directive and information from the Commission.

The NIS Directive consists of 27 articles grouped in seven chapters, accompanied by three annexes:[3]

- Chapter I 'General provisions', Articles 1 to 6, sets out the scope (Article 1) and main definitions (Article 4), identifies operators of essential services (Article 5) and defines 'significant disruptive effect' (Article 6).
- Chapter II 'National frameworks on the security of network and information systems', Articles 7 to 10, describes the national frameworks that need to be adopted by each Member State on the security of network and information systems.
- Chapter III 'Cooperation', Articles 11 to 13, sets out cooperation mechanisms, including the establishment of the Cooperation Group (Article 11) and of a network of national computer security incident response teams (CSIRTs) (Article 12).

- Chapter IV 'Security of the network and information systems of operators of essential services' Articles 14 to 15, establishes security requirements and incident notification for operators of essential services.
- Chapter V 'Security of the network and information systems of digital service providers', Articles 16 to 18, defines the security requirements for digital service providers.
- Chapter VI 'Standardisation and voluntary notification', Articles 19 to 20, defines standards and the process of voluntary notification.
- Chapter VII 'Final provisions', Articles 21 to 27, lists the NIS Directive's final provisions, including on the review (Article 23) and transposition (Article 25).
- Annex I lists the 'Requirements and tasks of Computer Security Incident Response Teams (CSIRTs)'.
- Annex II 'Types of entities for the purposes of point (4) of Article 4', refers to OESs, and establishes them in seven sectors: 1) energy; 2) transport; 3) banking; 4) financial market; 5) health sector; 6) drinking water supply and distribution; and 7) digital infrastructure.
- Annex III: 'Types of digital services for the purposes of point (5) of Article 4, refers to digital services and defines: 1) online marketplaces; 2) online search engines; and 3) cloud computing service.

Implementation of the NIS Directive

The NIS Directive entered into force in August 2016. Members States had until 9 May 2018 to transpose the directive into national laws. All Member States have fulfilled the obligation. They have also prepared their national cybersecurity strategies and identified operators of essential services. The NIS Cooperation Group has been established and is operational (see below). For more details see Table 2.

NIS Cooperation Group activities

The NIS Cooperation Group has met 16 times to date. The first meeting was held in February 2017 and the most recent in September 2020. This last meeting was partially dedicated to the revision of the NIS Directive. The NIS Cooperation Group has also prepared several documents presenting the guidelines and implementation of the NIS Directive and the EU cybersecurity policy:

- Reference document on security measures for operators of essential services
- Reference document on incident notification for operators of essential services (circumstances of notification)
- Compendium on cyber security of election technology
- Cybersecurity incident taxonomy
- Guidelines on notification of operators of essential services incidents (formats and procedures)
- Guidelines on notification of digital service providers incidents (formats and procedures)
- Reference document on the identification of operators of essential services (modalities of the consultation process in cases with cross-border impact)
- Guidelines for the Member States on voluntary information exchange on cross-border dependencies
- Risk assessment of 5G networks
- Sectorial implementation of the NIS Directive in the energy sector
- Cybersecurity of 5G networks: EU toolbox of risk mitigating measures
- Report on Member States' progress in implementing the EU Toolbox on 5G cybersecurity

CSIRTs' network activities

The CSIRTs network was established on the basis of Article 12 of the NIS Directive, and gathers EU Member States' appointed CSIRTs and CERT-EU (CSIRTs network members). The number of members by Member State ranges from 54 in Spain to 1 in Bulgaria (see also ENISA map).

The CSIRTs network has met 11 times, with the objective 'to continue developing operational-cooperation capability in the EU'. The CSIRTs network meetings take place in different Member States,

e.g. the ninth meeting was organised in Helsinki, Finland and the 10th in Stockholm, Sweden. The 11th meeting, in June 2020, was supposed to take place in Zagreb, Croatia, but was held online.

Table 2 – Calendar of the implementation of the NIS directive

Deadline	Period after entry into force of the NIS Directive	Milestone (articles of the NIS Directive)	Achieved (Yes/No/ Expected)
August 2016	-	NIS Directive enters into force (Article 26)	Yes
February 2017	6 months	Cooperation Group to begin work (Article 11)	Yes (agendas of 16 meetings)
August 2017	12 months	Commission to adopt implementing act on security and notification requirements for digital service providers (DSPs) (Article 16)	Yes (Commission Implementing Regulation (EU) 2018/151)
May 2018	21 months	Member States to transpose NIS Directive into national law by 9 May 2018 and to apply the measures from 10 May 2018 (Article 25)	Yes (detailed information)
November 2018	27 months	Member States to identify 'operators of essential services' (OESs) (Article 24)	Yes (detailed information)
May 2019	33 months (1 year after transposition)	Commission to present report assessing the consistency of Member States' identification of operators of essential services (Article 23)	Yes (OES report)
May 2021	57 months (3 years after transposition)	Commission to review the functioning of the directive, with a particular focus on strategic and operational cooperation, and the scope in relation to OESs and DSPs (Article 23)	Expected

Source: EPRS, based on the NIS Directive, and the Commission's table and information.

European Commission report on operators of essential services

Article 23 of the NIS Directive obliges the Commission to conduct a periodical review of the functioning of the directive and to report to Parliament and Council. The first report should be submitted by 9 May 2021. While preparing reports, the Commission is obliged to take into account the reports of the NIS Cooperation Group and the CSIRTs network on experience gained at a strategic and operational level, as well as to assess the lists contained in Annexes II and III, and consistency in the identification of operators of essential services (OESs) and services in the sectors referred to in Annex II.

On 28 October 2019, as part of the NIS Directive revision, the Commission published a report assessing the consistency of Member States' approaches in the identification of operators of essential services ('OES report'; COM(2019) 546).[4] Member States are obliged by the NIS Directive to define essential services and identify OESs. An OES 'must demonstrate a particularly high level of resilience against cyber-incidents'.

The OES report assessed, between November 2018 and September 2019, information that Members States were obliged to provide. At the date of starting the assessment the Commission had full data on OESs from 23 Member States and partial data from 5 Member States.

OES identification in Member States was as follows:

- The average number of 'identified OESs' in Member States was 633, but the number varied from zero in Austria, Belgium and Slovenia to 10 897 in Finland (due to a large number of operators identified in the health sector) and 1 250 in Portugal. In general, there is a correlation between the size of the country and the number of identified OESs.
- The number of 'services under Annex II' of the NIS Directive by Member State was quite equal. With 35 on average per Member State, the numbers varied from 12 in Hungary and in the Netherlands, and 15 in Germany, to 87 in Poland, 77 in Romania and 70 in France. The number of services identified also varied by sector and subsector, e.g. ranging from 1 to 21 in banking sector.
- 'Additional services' (other than those covered in Annex II) were identified in 11 Member States, e.g. information infrastructures, financial services (not enlisted in Annex II), governmental services, heat, and wastewater.

Assessing the state of play, the Commission admitted that 'the NIS Directive had made a considerable contribution to improving cybersecurity capabilities within the Member States and the level of protection of network and information systems throughout the Union'. Nevertheless, a number of issues relating to implementation of the Directive were identified by the Commission, which also provided recommendations for improvement. To highlight some of them:

- Member States have developed different methodologies to identify OESs, to define essential services and set thresholds, which may have 'a negative impact on the consistent application of the NIS provisions across the Union with possible consequences for the well-functioning of the internal market and the effective handling of cyber-dependencies';
- Member States interpret essential services under the NIS Directive differently, and apply differing levels of detail to sets of data, making it difficult to compare the lists of essential services in the whole EU;
- the scope of the NIS Directive risks being fragmented, with some operators being exposed to additional regulation (as they have been identified by Member State) while others providing similar services remaining excluded (as they have not been identified). In order to address these inconsistencies, further work based on the experience of Member States could lead to a better aligned list of essential services;
- The role of the NIS Cooperation Group should be strengthened in order to promote a common understanding on how to implement the directive in a more consistent manner.
- The Cooperation Group should review its reference document on the modalities of the cross-border consultation process in cases to enhance Member States to use of the cross-border consultation procedure when it comes to identifying operators that are providing essential services in more than one Member State.

Public-private partnership

On 5 July 2016, the Commission launched a public-private partnership on cybersecurity. The EU planned to invest €450 million in this partnership, under its research and innovation programme Horizon 2020; the cybersecurity market players, represented by the European Cyber Security Organisation (ECSO), planned to invest three times more. It was expected, that the partnership would trigger €1.8 billion in investment by 2020. In addition to the EU and business, the partnership also gathers national, regional and local public administrations, research centres and academia. The aim of the partnership is 'to foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions for various sectors, such as energy, health, transport and finance'.

European Parliament position / MEPs' questions

During the current term (2019-2024), there have been no parliamentary resolutions on this subject. However, on 12 March 2019, during the last term (2014-2019), Parliament adopted a resolution on

security threats connected with the rising Chinese technological presence in the EU and possible action at EU level to reduce them (2019/2575(RSP)).

Selected written questions by MEPs

Written question by Magdalena Adamowicz (EPP, Poland), 26 May 2020

Given the favourable situation for cyber-attacks during the pandemic, and examples of cyber-attacks presented in the Europol 2020 report, e.g. on the IT of the University Hospital Brno (Czech Republic), which forced the Czech Government to introduced a state of emergency, the Member asked: a) if the Commission had been carrying out enhanced monitoring of cyber-attacks on sensitive infrastructure during the crisis, b) if the Commission had tools to counter such attacks, and c) if the Commission was planning to intensify joint efforts with Member States to minimise the risk of such incidents.

Answer given by Mr Breton on behalf of the Commission, 24 September 2020

Thierry Breton stated that there was close cooperation between the Commission and the Member States, ENISA and other EU bodies involved in cybersecurity to ensure information sharing and a high level protection of OESs and particularly of healthcare providers during the coronavirus crisis. The CSIRTs network was on alert on a 24/7 basis. A newly set up Covid-19 task force composed of the Commission and EU bodies was preparing weekly reports from March until May 2020 to support national authorities and EU institutions. There were obligations concerning the cybersecurity of OESs, and digital service providers offering cloud services to healthcare providers imposed the NIS Directive on Member States. The NIS Cooperation Group, had recently set up a new work stream dedicated to cybersecurity in the health sector with the support of the eHealth Network, the European Cybersecurity Health Group, ENISA and the Commission.

Written question by Lukas Mandl (EPP, Austria), 19 May 2020

In view of the increased number of cyber-attacks (from criminals and state actors) against individuals and public institutions, including by distributing various malware packages, during the pandemic, and cyber-attack examples presented in the Europol 2020 report, e.g. on the University Hospital Brno, the MEP asked about measures that had been taken by the Commission and the four EU organisations dealing with cybersecurity (ENISA, EDA, Europol and CERT-EU) to increase resilience and cybersecurity during the pandemic and beyond, and how the Commission aimed to ensure coherent and effective cooperation between these four organisations while their mandates partly overlapped. The Member also asked about Commission proposals on how to increase the EU's cyber defence capability in the military field, and to what extent the envisaged European Defence Fund might contribute to this end.

Answer by Mr Breton on behalf of the Commission, 22 September 2020

Mr Breton stated that there was close cooperation between the Commission and Member States, ENISA and other EU bodies involved in cybersecurity. A new task force was ensuring that all EU bodies acted in a coherent manner, and prepared weekly situation reports to support national authorities and EU institutions from March to May 2020. The CSIRTs network had been in alert mode to share information on a 24/7 basis. Other activities had also been organised, e.g. ENISA and Europol campaigns on how to be secure in cyberspace, and CERT-EU's technical guidance. The Cooperation Group had a new work stream on cybersecurity in the health sector. In the review of the NIS Directive, the Commission would take into account the lessons learnt from the pandemic. In relation to cyber defence, the European Defence Fund (EDF) and its pre-cursor programmes had supported Member States in building cyber capacity and resilience, by funding collaborative defence R&D projects. The Commission had recently begun to engage with Member States on the EDF priorities for 2021 to 2027.

Written question by María Soraya Rodríguez Ramos (Renew, Spain) and Susana Solís Pérez (Renew, Spain), 1 April 2020

As cybercriminals had taken advantage of the pandemic to attack the databases of European hospitals, e.g. in the Czech Republic and in Spain, where 'phishing' techniques were used to steal crucial data from

the hospitals' IT systems, followed by a threat to release them only on payment of a ransom, the Members asked how the Commission and ENISA were cooperating to monitor and protect critical infrastructure such as hospitals, what emergency protocols were being implemented to support local authorities and hospitals and whether the Commission considered that the level of awareness of cyber-attacks as well as funding and resources dedicated to the protection of the European health system against them were adequate.

Answer by Mr Breton on behalf of the European Commission, 23 July 2020

Mr Breton stated that there was close cooperation between Member States and the EU bodies involved in cybersecurity and regarding the role the CSIRTs network played during the coronavirus crisis. The Commission mentioned obligations deriving from the NIS Directive and new work stream of the NIS Cooperation Group dedicated to cybersecurity in the health sector. The Commission was ensuring that providing funding for OESs remained a priority. Already in 2019, a call had been organised under the Connecting Europe Facility (CEF), providing support to OESs in the health sector and driving forward the creation of sectorial information sharing and analysis centres (ISACs) at EU level The Commission was also working on the establishment of an EU Health ISAC.

Written question by Tomislav Sokol (EPP, Croatia), 4 June 2020

In view of the cyber-attack on an airline's IT system during the coronavirus crisis, endangering the personal data of thousands of travellers, including many EU citizens (such as the credit card data of more than 2 000 passengers), the MEP asked how the Commission intended to protect European consumers more effectively from sophisticated cyber-attacks, thereby increasing the level of cybersecurity in the EU, what practical legal mechanisms the Commission intended to propose within its current legislative mandate in order to enhance consumer protection and if the Commission was working to make the EU a global leader in the area of cybersecurity.

Answer by Mr Breton on behalf of the European Commission, 26 October 2020

Mr Breton informed about initiatives taken by the Commission that addressed cybersecurity and were aim to improve the protection of citizens in all aspects of their lives online and offline, including e.g. improving the cybersecurity of medical devices, rules on the protection of vehicles against cyber-attacks, and ensuring that consumers are provided with security updates when purchasing digital content and digital services. The Commission also decided to accelerate the review of cybersecurity horizontal rules defined in the NIS Directive to Q4/2020. Mr Breton also informed that the ENISA and European Cybercrime Centre (at Europol) offer advice on how citizens can protect themselves against cybersecurity risks.

European Court of Auditors

In March 2019, the European Court of Auditors (ECA) published a briefing paper on the Challenges to effective EU cybersecurity policy, to 'provide overview of the EU's complex cybersecurity policy landscape and identify the main challenges to effective policy delivery'. Based on the analysis, the ECA identified four groups of challenges: 1) the policy framework; 2) funding and spending; 3) building cyber-resilience; and 4) responding effectively to cyber incidents.

In relation to the NIS Directive, the ECA paper pointed out, not least, that 'while the NIS Directive's objective was to achieve a high level of security across the EU, it focused explicitly on achieving minimum, not maximum, harmonisation. Gaps will continue to emerge as the cyber-landscape evolves'. The paper also stressed issues with 'the balance of responsibilities between users and providers of digital products, and certain aspects left unaddressed by the NIS Directive'.

European Economic and Social Committee

In March 2018, the European Economic and Social Committee published a report Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber-risks.

The report pointed to the cyber-insurance market, which, according to the report was still quite small (the market was projected to reach US$7.5 billion in annual sales by 2020 – tripling the 2015 amount – and over US$20 billion by 2025), but its growth should be positively influenced by the implementation of the NIS Directive and the EU's General Data Protection Regulation (GDPR). The report also noted that the adoption of the NIS Directive and the GDPR were 'of particular relevance with regards to harmonisation of cybersecurity and data protection across the EU'.

Revision of the NIS Directive

The Commission announced NIS Directive revision in its 2020 work programme, with a deadline by the end of 2020, and confirmed this in the adjusted 2020 work programme. The revision falls under the Commission's priority to make 'A Europe fit for the digital age', and is aimed at increasing cybersecurity.

Combined evaluation roadmap/inception impact assessment

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 despite the obligations of 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 crises'.

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'.

In order to ensure consistency and coherence with related Union legislation, the NIS Directive review will take into account the following Commission initiatives in particular: a) the review of the European programme for critical infrastructure protection; b) the initiative on a digital operational resilience act in the financial sector (DORA), and c) the initiative on a network code on cybersecurity with sector-specific rules for cross-border electricity flows.

Public consultation

On 7 July 2020, the Commission launched public consultations on the NIS Directive, with a deadline of 2 October 2020, to contribute to the review the functioning of the directive. No consultation results are available yet. The feedback received (42 responses) can be found on the Commission website.

Citizens' inquiries

During the current parliamentary term (2019-2024), there have been no citizens' inquiries with respect to the NIS Directive specifically.

Two relevant inquiries were submitted in France at the beginning of 2018 however: 1) on 10 January, an inquiry concerned an information request on EU legislation on computer crime; and 2) on 19 February, an inquiry concerned an information request on the report of the European Committee on Crime Problems published by the Council of Europe.

FURTHER READING

Challenges to effective EU cybersecurity policy, Briefing paper, European Court of Auditors, March 2019.

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

Grajewski M., Cybersecurity, Briefing, What Think Tanks are Thinking, EPRS, European Parliament, October 2018.

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

Latici T., EU cyber sanctions: Moving beyond words, EPRS, European Parliament, September 2020.

Latici T., Understanding the EU's approach to cyber diplomacy and cyber defence, EPRS, European Parliament, May 2020.

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.

Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity, European Commission, updated on 28 October 2019.

Your rights matter: Security concerns and experiences, EU Agency for Fundamental Rights, 2020.

ENDNOTES

[1] 1 trillion equals 1 million million.

[2] The first candidate scheme for certification is ongoing. ENISA has already set up an ad hoc working group to support the preparation of a candidate EU cybersecurity certification scheme.

[3] D. Markopouloua, V. Papakonstantinoua and P. de Herta, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation', *Computer Law and Security Review*, Vol. 35(6), November 2019.

[4] Report from the Commission to the European Parliament and 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/EU on security of network and information systems (COM(2019) 546).

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)