Centrum für Europäische Politik
FREIBURG | BERLIN

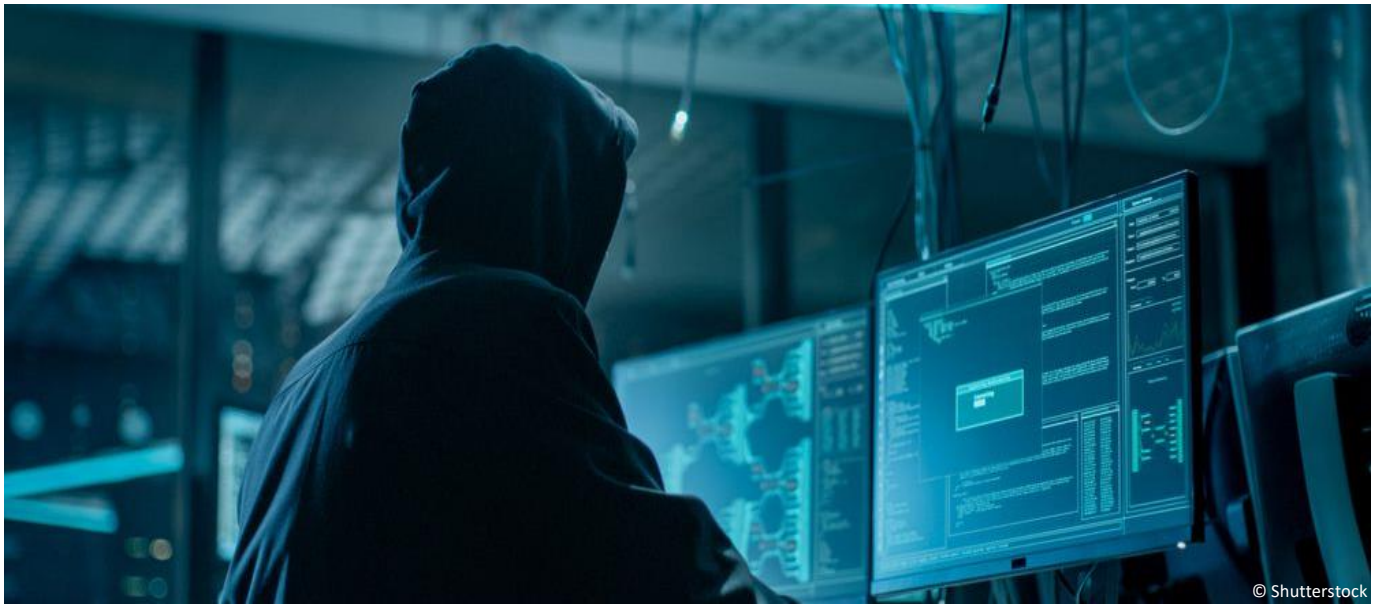
cepAdhoc

No. 9 | 2021 18 October 2022

NIS 2 Directive: New EU Rules on Cybersecurity

Cyber risks and attacks are an increasing threat to European security

Philipp Eckhardt



The ongoing digital transformation and escalating geopolitical threats significantly increase the risk of cyber incidents. Cybersecurity has become one of the most important pillars of sovereign security. On 13 May 2022, the European Parliament and the Council agreed on new cybersecurity legislation. In future, around 160,000 companies and public bodies will be subject to uniform EU requirements regarding the management of cyber risks and the reporting of cybersecurity incidents and threats. This cepAdhoc reveals what is in store for companies and public bodies and evaluates the new regulations.

- The more clearly defined scope of the NIS 2 Directive creates greater legal certainty and prevents distortions of competition. The question remains, however, whether the supervisory authorities are not, in practice, overburdened with the supervision of approximately 160,000 institutions. Greater prioritisation would therefore have been appropriate.
- Paying more attention to risks in supply chains, which are often cross-border in nature, is right and increases the level of cybersecurity in the EU. However, responsibility should not rest solely on the shoulders of the institutions. Cybersecurity is, on the one hand, a public good and, on the other, a sovereign interest.
- Reporting obligations are appropriate as institutions affected by cyber incidents often have little incentive to report them voluntarily, partly due to the resulting reputational damage. The reports often have a major external benefit as they help others to identify and close security gaps.
- Strengthening the risk management of private and public sector companies and entities, and imposing stricter reporting requirements on them, can only be one component of the necessary regulation. It is therefore right that, with the recently released proposal for a "Cyber Resilience Act", the Commission will add another key element to the cyber resilience of Europe's interconnected economies.

Table of Contents

List of Tables

1 Context

According to the Federal Criminal Police Office (BKA), the number of cybercrime offences increased in 2021 by 12% compared to the previous year and, according to figures from the Bitkom Association, losses resulting from cybercrime more than doubled compared to 2019, reaching a peak of €223.5 billion.[1,2] Furthermore, against the backdrop of the Russian invasion of Ukraine, fears are growing that there will be even more cyberattacks, especially on critical infrastructures such as energy suppliers, waterworks and hospitals.[3,4]

At EU level, the Network and Information Security Directive ["NIS 1 Directive", (EU) 2016/1148] has been in force since 2016. In particular, it obliges Member States to establish national cybersecurity strategies and establishes various bodies to strengthen cooperation between Member States in the field of cybersecurity. It also stipulates that Member States must establish binding cybersecurity risk management rules and cybersecurity incident reporting requirements.

In mid-December 2020, the EU Commission submitted a proposal to revise the Directive [COM(2020) 823], as it identified some shortcomings in the existing legal framework. In particular, it criticised the fact that the scope of the Directive was "too limited" and thus a large number of companies as well as government bodies fell outside the EU-wide minimum cybersecurity requirements. In addition, the scope was "not sufficiently clear" giving Member States too much leeway in determining who had to comply with the Directive. The Commission was also critical of the fact that Member States had too much freedom in implementing cybersecurity risk management requirements, and it said that the cyber incident reporting requirements were too imprecise. Lastly, the Commission criticised the ineffectiveness of the Directive's supervisory and enforcement provisions.[5]

On 13 May 2022, negotiators from the European Parliament (EP) and the Council agreed on a revision of the NIS 1 Directive.[6] The compromise, which still has to be formally approved by the EP and the Council, is a tough one. In future, approximately 160,000 companies and public institutions in the EU will be subject to uniform EU minimum requirements to ensure a high level of cybersecurity.[7,8] This cep**Adhoc** reveals what is in store for the affected companies and public bodies and provides a brief assessment of the changes that have been made. In this context, we focus on the amendments to the

1 Bundeskriminalamt (BKA), Cybercrime, Bundeslagebild 2021.

2 Bitkom Research 2021, Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, Press release, 5 August 2021.

3 For example, the Council recently pointed out that "malicious behaviour in cyberspace [...] from both State and non-State actors [...] has intensified [...] and [...] with the return of power politics, some countries are increasingly attempting to challenge the rules-based international order in cyberspace". It warns that "large-scale cyber-attacks [...] causing systemic effects have become more common, might undermine our economic security and affect our democratic institutions and processes". [Council of the European Union, Council Conclusions on the development of the European Union's cyber posture, 23 May 2022].

4 As part of the negotiations to establish a special fund for the German Armed Forces, the German government also decided on measures to strengthen cybersecurity, which will be financed through the federal budget.

5 EU Commission, COM(2020) 823, Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, p. 5.

6 Council of the EU, Strengthening EU-wide cybersecurity and resilience - provisional agreement by the Council and the European Parliament, Press release, 13 May 2022.

7 Industry, Research and Energy Committee (ITRE), Cybersecurity: deal with Council to strengthen EU-wide resilience, Press release, 13.05.2022.

8 Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2 Directive).

NIS 2 Directive regarding its scope, the management of cyber risks, the revised reporting requirements as well as the provisions on supervision, enforcement and sanctions.

2 NIS 2 Directive: Tougher EU rules to strengthen cybersecurity

2.1 Amendments to the scope

The agreement presented by the EP and the Council significantly extends the scope of the Directive. In future, under the NIS 2 Directive, many more companies from specific sectors and, for the first time, institutions from the public sector, will have to comply with uniform cybersecurity requirements throughout the EU.

2.1.1 Essential entities

As currently, the Directive applies to a range of entities that are classified as "essential"[9], as they are of critical importance to the functioning of a society. These include electricity suppliers, railway companies and banks. In future, however, the list of "essential" entities will be extended considerably. Thus, in future, entities in the areas of hydrogen production, storage and transmission, manufacturers of pharmaceutical products, waste water disposal companies and also certain public administration bodies will fall under this category (see Table 1).[10]

Table 1: Public and private essential entities

The entities marked in red and bold are new additions under the NIS 2 Directive.		
Sector	**Subsector**	**Type of entity**
Energy	Electricity	• Electricity suppliers • Distribution system operators • Transmission system operators • **Electricity producers** • **Nominated electricity market operators (NEMO)** • **Electricity market participants (aggregation, demand response or energy storage services)** • **Recharging infrastructure operators**
	District heating and cooling	**District heating or cooling to promote the use of energy from renewable sources**
	Oil	• Operators of oil transmission pipelines • Operators of oil production, refining and treatment facilities • Operators of oil storage and transmission facilities • **Central oil stockholding entities**
	Gas	• Gas supply undertakings • Gas distribution system operators • Gas transmission system operators • Gas storage system operators • LNG system operators • Natural gas undertakings • Operators of natural gas refining and treatment facilities
	Hydrogen	**Operators of hydrogen production, storage and transmission**
Transport	Air	• Air carriers used for commercial purposes • Airport managing bodies • Airports • Operators of traffic management and traffic control systems
	Rail	• Infrastructure managers

9 Until now, these have been referred to as "operators of essential services".
10 Art. 2 in conjunction with Annex I, NIS 2 Directive.

		• Railway undertakings
	Water	• Inland, sea and coastal passenger and freight water transport companies • Managing bodies of ports • Operators of vessel traffic services
	Road	• Road authorities responsible for traffic management and control except those for whom this is only a non-essential part of their activity • Operators of intelligent transport systems
Banking and financial market infrastructures		• Banks • Operators of trading venues • Central counterparties (CCPs)
Health		• Healthcare providers • EU reference laboratories on serious cross-border threats to health • **Entities carrying out research and development activities of medicinal products** • **Manufacturers of pharmaceutical products** • **Manufacturers of medical devices considered as critical during a public health emergency**
Drinking water		Suppliers and distributors of drinking water except those for whom this is only a non-essential part of their activity
Waste water		Undertakings collecting, disposing or treating waste water except those for whom this is only a non-essential part of their activity
Digital infrastructure		• Internet Exchange Point providers • DNS service providers, except operators of root name servers • TLD name registries • Cloud computing service providers • **Data centre service providers** • **Content delivery network providers** • **Trust service providers** • **Providers of public electronic communications networks and services** • **Managed service providers (MSPs) and managed security service providers (MSSPs)**
Public administration		• **Public administration entities of central governments, except the judiciary, parliaments and central banks** • **Public administration entities at regional level**[11]
Space		**Operators of ground-based infrastructure that support the provision of space-based services**

[1] They are currently referred to in the NIS 1 Directive as "Digital service providers".
[2] They are currently covered by the Regulation on electronic identification and trust services for electronic transactions in the internal market [(EU) No 910/2014].
[3] They are currently covered by the Directive on the European Electronic Communications Code [(EU) 2018/1972].

2.1.2 Important entities

The NIS 1 Directive covered a second category of companies, referred to as "digital service providers". This category will now be abolished under the NIS 2 Directive and replaced by a category referred to as "important entities". Although this category also covers providers of digital services, e.g. providers of online marketplaces and search engines, in future it will also include manufacturers of medical devices, manufacturers of machinery, providers of postal and courier services and car manufacturers, among others (see Table 2).[12]

[11] Public administration entities in the fields of defence, national security, public safety and law enforcement are also excluded.
[12] Art. 2 in conjunction with Annex I, NIS 2 Directive.

Table 2: Public and private important entities

The entities marked in red and bold are new additions under the NIS 2 Directive.		
Sector	**Subsector**	**Type of entity**
Processing / manufacture of goods	**Medical devices and in vitro diagnostic medical devices**	• **Manufacturers of medical devices** • **Manufacturers of in vitro diagnostic medical devices**
	Data processing equipment, electronic and optical products	**Manufacturers of data processing equipment, electronic and optical products**
	Electrical equipment	**Manufacturers of electrical equipment**
	Machinery	**Manufacturers of machinery**
	Vehicles and vehicle parts	**Manufacturers of vehicles and vehicle parts**
	Other vehicle manufacture	**Shipbuilding, manufacture of boats, rail vehicles, aircraft and spacecraft**
Waste management		**Waste management undertakings (principal activity)**
Postal and courier services		**Providers of postal and courier services**
Food		**Food production, processing and distribution in wholesale or industrial production and processing**
Chemicals		**Manufacture and production of substances and mixtures and manufacturers of articles from the substances and mixtures**
Research		**Research institutions whose research serves commercial purposes, except educational institutions**[13]
Digital service providers		• Providers of online marketplaces • Providers of online search engines • **Providers of social networking services platforms**

2.1.3 Exemptions for small entities

In principle, the NIS 2 Directive will only apply to essential and important entities that exceed the thresholds for medium-sized entities. For example, it is stipulated that the entities must have at least 50 employees, an annual turnover of at least 10 million euros or an annual balance sheet total of at least 10 million euros.[14]

2.1.4 Entities that are always covered regardless of their size

Some essential or important public and private entities are also covered by the Directive regardless of their size (no thresholds). This applies, inter alia, to[15]

- operators of public electronic communications networks and services,
- entities that are the sole provider of a service in a Member State that is essential for the maintenance of critical societal or economic activities and
- providers of services whose disruption could pose a significant risk to public safety, public security or public health, or to cross-border system stability.

In principle, the public administration entities of central governments are also covered, regardless of their size. This also applies to public administration entities at regional level, if the failure of the services they provide would have a significant impact on societal or economic activities. Member

[13] However, Member States may decide to apply the Directive to educational institutions, in particular if they carry out critical research activities (Art. 2(2b)).
[14] Art. 2, NIS 2 Directive.
[15] Art. 2, NIS 2 Directive.

States may also decide that public administrations at local level are also covered by the NIS 2 Directive (Member State option).[16]

2.1.5 Exempt entities

The Directive does not cover "public administrations" in the areas of defence, national security, public safety or law enforcement, nor does it cover parliaments or central banks.[17] Also exempt are a large number of development banks - e.g. the Kreditanstalt für Wiederaufbau - provided that a Member State has also chosen to exempt them from the sector-specific cybersecurity requirements of the Regulation on the operational resilience of finance companies [Digital Operational Resilience Act (DORA), see cep**PolicyBrief**].[18,19]

2.1.6 Sector-specific legislation

Where sector-specific EU legislation on cybersecurity exists for entities within the scope of the NIS 2 Directive - such as the Regulation on the operational stability of financial undertakings - these entities do not need to comply with the NIS 2 Directive's requirements on cyber risk management (see section 2.2) and cyber incident and threat reporting (see section 2.3), provided that the sector-specific rules are at least equivalent to the NIS 2 Directive's requirements in this respect.[20]

[16] Ibid.
[17] Ibid.
[18] The DORA Regulation was negotiated in parallel with the NIS 2 Directive and complements the Directive with sector-specific provisions to strengthen the cyber-security of financial companies. A trilogue agreement on this legislation was reached on 11 May. More details here.
[19] Art. 2 (3d), NIS 2 Directive.
[20] Art. 2b, NIS 2 Directive.

2.2 Managing cyber risks

Like the NIS 1 Directive, the NIS 2 Directive also requires that the essential and important entities to which it applies, take measures to adequately manage cybersecurity risks. At the same time, the NIS 2 Directive is now more specific, and clearly limits the discretion of the Member States.

2.2.1 Measures on cybersecurity risk management:

The entities covered by the Directive must take "appropriate and proportionate technical, operational and organisational measures" to manage the risks to the security of the network and information systems (NIS) which they use for their activities or for the provision of their services. In addition, the measures taken must contain or prevent the consequences of cyber incidents for the recipients of their services and for other services.[21] The measures, aimed at protecting not only the security of the NIS but also its physical environment, must include[22]

- risk analysis,
- creation of information system security policies,
- measures for handling cybersecurity incidents, i.e. prevention, detection, analysis and containment measures as well as response and post-incident recovery measures,
- business continuity and crisis management measures (e.g. backup management and disaster recovery),
- measures to ensure supply chain security,
- basic cyber-hygiene practices and cybersecurity training,
- use of multi-factor authentication or continuous authentication solutions, and
- strategies and procedures for the use of cryptography and, where necessary, encryption technology .

The proportionality of the measures should be measured according to the institution’s degree of risk exposure, its size, the probability of cyber incidents and their severity. In addition, social and economic effects should be taken into account.[23]

The Commission may lay down technical, methodological and, where appropriate, sectoral specifications for risk management measures, by means of implementing acts.[24]

2.2.2 Focus on supply chain

One area of focus of the NIS 2 Directive is that of cyber threats within the supply chain. Thus, the essential and important entities are obliged to take measures to strengthen the security of their supply chains. These will focus on the relationship between the entities and their "direct" suppliers and service providers (e.g. cloud service providers). For example, entities are to look at the specific vulnerabilities and cybersecurity practices of each "direct" supplier or service provider and, in particular, closely examine the quality of delivered products. In addition, entities must, as part of their risk management, examine those ICT products and services from their suppliers and service providers

[21] Art. 18 (1), NIS 2 Directive.
[22] Art. 18 (2), NIS 2 Directive.
[23] Art. 18 (1), NIS 2 Directive.
[24] Art. 18 (5), NIS 2 Directive.

which have been identified as especially critical by the EU Commission, in conjunction with the Cooperation Group[25] and ENISA.[26,27]

2.2.3 Cybersecurity certification

In future, if the Commission deems the level of cybersecurity to be insufficient, it will be able to determine by means of delegated acts that certain categories of essential or important entities may only use ICT products or ICT services which have been certified or require certification under European cybersecurity schemes. Member states can also oblige individual essential or important entities to use only certain ICT products or ICT services which they either develop themselves or obtain from third parties, and are certified under European cybersecurity certification systems. This will then also allow the entities to demonstrate compliance with the cyber risk management measures.[28]

2.2.4 Governance

The NIS 2 Directive will significantly increase the responsibility, of the governing bodies of essential and important entities, to manage cyber risks. Thus, in future, it will explicitly be their responsibility to approve the risk management measures and to monitor their implementation. Governing bodies may be held liable for non-compliance with the requirements of the Directive. They will also be obliged to undertake regular training on cybersecurity risks and their impact on the entity, and they should also enable all their employees to attend similar training courses.[29]

2.3 Reporting cyber incidents and threats

Like the NIS 1 Directive, the recast NIS 2 Directive requires the relevant entities to report cybersecurity incidents. Whereas the provisions of the NIS 1 Directive were quite vague and left broad scope for interpretation, the NIS 2 Directive now provides clearer rules as to which incidents should be reported, when, how and to whom.

2.3.1 Which cyber incidents and threats must be reported?

Essential and important entities must report all "significant" cyber incidents. Cyber incidents are considered to be "significant" if they[30]

- cause or may cause severe operational disruption of the entity's service,
- cause severe financial losses to the entity,
- cause or may cause considerable material or non-material losses to other natural or legal persons.

[25] The Cooperation Group is a body composed of representatives of the Member States, the Commission and ENISA. It supports the exchange of information between Member States regarding the application of the Directive.
[26] The European Network and Information Security Agency (ENISA) is an EU cybersecurity agency established in 2004.
[27] Art. 18 (2) and (3), Art. 19, NIS 2 Directive.
[28] Art. 21, NIS 2 Directive.
[29] Art. 17, NIS 2 Directive.
[30] Art. 20 (1) and (3), NIS 2 Directive.

The entities must also, where appropriate, inform the users of their services, who could potentially be affected by a "significant cyber threat",[31] about (remedial) measures with which they can take in response to the threat. If necessary, they will also inform users about the threat itself.[32]

2.3.2 When to report cyber incidents

24-hour reporting deadline: In principle, the notification must be made "without undue delay". However, a report in the sense of an "early warning" must be submitted, in any event, within 24 hours after having become aware of such an incident. This initial notification must state whether the incident is believed to have been caused by an unlawful or malicious act and the extent to which it has cross-border impact.[33]

72-hour reporting deadline: A second report must be submitted within 72 hours of having become aware of the cyber incident. This should update the initial report and contain an initial assessment of the incident, especially regarding its severity and impact and, if possible at this stage, regarding any indicators of compromise.[34]

Intermediate report: A further report must be made at the request of the CSIRT or the competent authority. This takes the form of an intermediate report and contains status updates.[35]

Final report: A final report must also be submitted within one month after the 72-hour reporting deadline, describing the severity and impact of the incident, the type of threat, the cause and the mitigation measures taken.[36]

Progress report: If a cyber incident is still not resolved within one month, a progress report must be submitted instead of the final report. The final report must then be submitted no later than one month after the incident has been successfully remedied.[37]

2.3.3 Where to report cyber incidents

Cyber incidents must be reported in the first instance to the national Computer Security Incident Response Teams (CSIRTs) or to the competent national authorities as appropriate. If the notification goes to a competent authority, the authority must forward the notification to the CSIRT. Where appropriate, entities must also inform their users of their services.[38] It is stipulated that notification of such cyber incidents should not result in a higher liability risk for the reporting entity.[39]

2.3.4 Reaction of the supervisory authorities

The CSIRT or the competent authority must provide initial feedback without delay and, if possible, within 24 hours, and provide assistance with remedial action if requested by the company. The CSIRT or the competent authority may inform the public about the incident, or require the affected entity to

[31] A "significant cyber threat" is a cyber threat that can be assumed to have the potential to severely impact the NIS of an entity or its users by causing considerable material or immaterial losses [Art. 4 (7a)].
[32] Art. 20 (2), NIS 2 Directive.
[33] Art. 20 (1) and (4), NIS 2 Directive.
[34] Art. 20 (4), NIS 2 Directive.
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Art. 20 (1), NIS 2 Directive.
[39] Art. 20 (1), NIS 2 Directive.

do so, if raising public awareness may prevent an incident, will help to deal with it or is in the public interest.[40]

2.4 Supervision, enforcement and sanctions

The NIS 2 Directive provides that both essential and important facilities will be subject to supervision. Thus, national supervisory authorities will ensure that entities comply with the requirements for risk management and the reporting of cyber incidents. In general, national authorities will be granted a minimum range of supervisory powers, including on-site inspections or regular and targeted security audits of supervised entities, including ad hoc audits in the case of significant cyber incidents.[41]

Supervision of important entities is less stringent than for essential entities. Whilst important entities are only subject to ex-post supervision, activated on the basis of evidence or indications of potential breaches of the Directive, essential entities are subject to full - i.e. ex-ante and ex-post - supervision.[42]

National supervisory authorities are also to be given a range of enforcement powers. For example, they will be allowed to issue warnings to essential and important entities for failure to comply with the Directive. They will also be able to issue binding instructions, for example on steps to prevent or contain cyber incidents, including deadlines for their implementation.[43]

If companies fail to comply with the enforcement measures, the authorities can impose sanctions. Sanctions may be imposed on the entities themselves and on the persons responsible for their management.[44]

2.5 Transposition of the NIS 2 Directive

Now that the Council and the EP have reached agreement in the trilogue, the two legislative bodies must formally approve the compromise that has been found. This is likely to be in the early autumn. Once the Directive enters into force, Member States will then have 21 months to incorporate the necessary legal and administrative provisions into national law.[45] The Directive is therefore unlikely to apply until 2025 at the earliest.

[40] Art. 20 (7), NIS 2 Directive.
[41] Art. 29 (1) and (2) and Art. 30 (1) and (2), NIS 2 Directive.
[42] Recital 70, Art. 29 and Art. 30, NIS 2 Directive.
[43] Art. 29 (4) and Art. 30 (4), NIS 2 Directive.
[44] Art. 29 (5) and (6) and Art. 30 (5) and (6), NIS 2 Directive.
[45] Art. 38, NIS 2 Directive.

3 Assessment

Against the background of increasing cyber threats and incidents, the EP and the Council have now decided to use the NIS 2 Directive to oblige a large number of companies as well as public sector institutions to take increased measures to manage cybersecurity risks and to report significant cyber incidents to supervisory authorities. But are these regulatory requirements really necessary to strengthen European cyber resilience? In principle, it could be argued that companies should already have a vested interest in adequately protecting their network and information systems (NIS) from cyber incidents and threats because, in the event of an attack, failure to do so may result in considerable loss of sales and damage to reputation. Companies must surely therefore be willing to invest in the stability of their systems. This conclusion is often misplaced however because the economic incentives for investing in cybersecurity are generally insufficient. Firstly, companies affected by a cyber incident often do not have to bear the full cost of the lack of security of their network and information systems. Instead, they are frequently able to pass on some of these costs to third parties, such as their customers. Secondly, the efforts of one company to strengthen its cyber resilience often also increase the resilience of other companies. However, companies rarely factor these positive externalities into their decision-making. Uniform requirements for the management of cyber risks are therefore appropriate, particularly in view of the nature of cybersecurity as a public good and the fundamental sovereign interest in stable and resilient economies. The more important a company is for the basic supply or functioning of a society, the more this applies, since its impairment or failure will involve particularly high costs for society. The differentiation in the depth of regulation between essential and important companies is therefore appropriate, irrespective of the many interdependencies and critical dependencies that also exist between essential and important companies.

However, the scope of the NIS 2 Directive also gives cause for criticism. On the one hand, the revision of the NIS 1 Directive clarifies the scope thereby creating more legal certainty about who is affected by the NIS 2 regulations. This also limits the possibilities for regulatory arbitrage and prevents distortions of competition. On the other hand, however, the scope of the Directive is now too wide because it also includes many companies whose products or services cannot be considered absolutely key to the supply and functioning of a society. These include companies from the manufacturing sector, such as manufacturers of machinery. In addition, there must be some doubt as to whether the supervisory authorities are not, in practice, overburdened with the supervision of approximately 160,000 companies and public bodies, making greater prioritisation more appropriate. Furthermore, the size of an institution is inappropriate as the sole criterion for its inclusion in the scope, as this alone does not necessarily indicate a higher cybersecurity risk. Other criteria should also have played a role here, such as a company's customer numbers.

The fact that essential and important entities now have to include supply chain risks in their risk management, to a greater extent than under the NIS 1 Directive, may increase the level of cybersecurity in the EU. However, responsibility for ensuring cybersecurity should not rest solely on the shoulders of the essential and important entities at the end of the value chain because intensive auditing of every single supplier in the supply chain would not only be time-consuming, but would also involve huge costs. It is therefore appropriate that the focus is now on direct suppliers. Direct requirements for the suppliers of ICT products and services are also crucial, i.e. they should be made jointly responsible. It is therefore to be welcomed that the Commission is planning legislative steps on

this, with the "Cyber Resilience Act", expected on 13 September 2022, and that it wants to create cybersecurity requirements for digital products.

The obligation to report significant cyber incidents to supervisory authorities is appropriate because entities affected by such incidents often have little incentive to do so voluntarily, owing to high reporting costs and the potential reputational damage associated with such reports. However, the reports often have a major external benefit as they help others to identify and close security gaps. The establishment of clear deadlines and procedures for reporting cyber incidents is also a positive development. On the one hand, these deadlines increase legal clarity and, on the other, they reduce the administrative burden for the institutions concerned, as they can now submit the report to a central office. The rapid reporting of cyber incidents is imperative to ensure that damage is contained quickly. The 24-hour reporting deadline is therefore ambitious but ultimately unavoidable. However, the value of this initial report should not be overestimated because it is doubtful whether any very useful information can be provided within such a short period of time. This is especially true for smaller companies who may not have access to large in-house resources for analysing cyber incidents, especially since such short reporting deadlines can also tie up valuable capacity that would be better deployed in dealing with the cyber incident.

In principle, of course, the stricter risk management measures and reporting obligations of the NIS 2 Directive will not be enough to guarantee the resilience of the European business landscape against cyber risks. They are just one component. However, they form a cornerstone of a whole range of regulatory measures, both national and European. In addition to the steps outlined in this cepAdhoc, the NIS 2 Directive also contains, for example, numerous measures to improve cooperation between the Member States, as well as between the relevant authorities, in the event of cyber incidents. In addition, the "European Union Cybersecurity Agency (ENISA)" has been given numerous new tasks, and an EU regulatory framework, for certifying the cybersecurity of information and communication technology, has already been created [Regulation (EU) 2019/881, see cep**PolicyBrief** (on ENISA) and cep**PolicyBrief** (on cybersecurity certification)]. The "Cyber Resilience Act" recently proposed by the Commission is also intended to make a significant contribution to strengthening the security of Europe's networked economies.

Centrum für Europäische Politik
FREIBURG | BERLIN

Author:

Philipp Eckhardt
Policy Analyst, Financial Markets and Information Technology

eckhardt@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Strasse 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN,
the **Centre de Politique Européenne** PARIS and
the **Centro Politiche Europee** ROMA form
the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

The Centres for European Policy Network analyses and assesses the policy of the European Union independently of individual or political interests, in alignment with the policy of integration and according to the principles of a free, market-based system.