Int. Cybersecur. Law Rev. (2022) 3:35–49
https://doi.org/10.1365/s43439-022-00048-9

Analysis of the cybersecurity ecosystem in the European Union

Zsolt Bederna · Zoltan Rajnai

Received: 12 January 2022 / Accepted: 17 February 2022 / Published online: 24 March 2022

Abstract The information society is a complex network of interconnected public and private entities and human beings. Many of them choose a certain level of technological development from the generally available solutions to support internal processes attaining objectives that support operations, creating technological dependence via internal or external services of the information and communication technologies (ICTs). Due to the technological development and technological dependence caused by ICTs, a society-wide political need has arisen for tackling security requirements for cyberspace in several sectors to satisfy the individuals' needs that directly or indirectly define the requirements for such services, resulting in a complex ecosystem with several participants. Although the European Union has formulated some crucial rules via regulations and directives with which it increasingly defined cybersecurity stakeholders from time to time, there are several missing affected parties. This paper aims to review the relevant technological, societal, and economic factors of the information society creating the necessity to strictly handle cybersecurity requirements and analyse decisive stakeholders via a theoretical framework. Furthermore, it also identifies the current legislative framework issues to identify pain points.

Keywords Cybersecurity legislation · Cybersecurity stakeholders · Essential services · NIS Directive · Information society

Zsolt Bederna (✉) · Zoltan Rajnai
Doctoral School for Safety and Security Sciences, Obuda University, Budapest, Hungary
E-Mail: bederna.zsolt@stud.uni-obuda.hu; bederna.zsolt@bederna.hu

1 Introduction

Technology is one of the most decisive factors of the information society, as the information and communication technology (ICT) services infiltrate society's everyday activities, including the economy. So, natural persons and legal entities must continually struggle to keep up with technological improvements to speed up operations and bridge physical distances. However, due to technological advancement, society has a growing dependence on ICTs and their safe use; therefore, the legislature process must regulate security commitments.

In 2007, during the cyberattack campaign against Estonia, the European Union (EU) recognised the importance of cybersecurity, and it emphasised taking the necessary steps to elevate the level of cyber-defence capabilities, resulting in several changes in legislation framework.

However, as the hypothesis of this work, the legislative approach is still not comprehensive enough to ensure the security of the European Digital Single Market (DSM) of the EU today, which results in unregulated areas of the essential services' and digital services' cybersecurity. This deficit creates a gap in the (cyber) resilience of the information society.

The paper first reviews the relevant technological, social, and economic factors of the information society and discusses legislation framework changes affecting cybersecurity capabilities. It then parses decisive stakeholders affecting the cybersecurity level in the EU, introducing a theoretical framework, and lastly, the paper identifies pain points of the current and proposed cybersecurity approaches. The paper closes with the conclusion.

2 Review of fundamental interrelations of the information society

The post-industrial changes have affected several aspects of everyday life. The term information society originated in the 1960s and is a concept that responds to the expansion and ubiquity of information, but still, today, it has ambiguous meanings. Researchers tried to explain the term via emphasising several aspects over the last half-century. As a result of the previous definitional approaches, Webster [50] highlighted five characteristics of the information society as technological, cultural, spatial, occupational, and economic perspectives.

The most common definitions of the information society highlight the technological aspects that cause an increase in the importance of ICT, signalling an information society's emergence. According to the technological approach, people live in an information society because ICTs have become widespread and increasingly important in everyday life.

Indeed, as Kurzweil [32, p. 381] formulated the generalisation of Moore's Law in his essay "The Law of Accelerating Results", "an analysis of the history of technology shows that technological change is exponential, contrary to the commonsense 'intuitive linear' view". This advancement realised cyberspace's vision due to the improvement of ICT devices and services. However, like many other terms, cyberspace also has diverse definitions. According to The European Union Agency for

Cybersecurity (ENISA) [12, p. 7], "cyberspace is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information". However, Kuehl created a more comprehensive definition [31, p. 28]: according to him, cyberspace is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies".

Technology development has also caused, for example, the convergence of industrial controls and even entertainment systems with ICT bringing more endpoints into cyberspace, requiring a differentiation between Information Technology (IT) and Operational Technology (OT) [45]. IT is widely applied where ICT supports business processes or processes data, such as finances. At the same time, OT services are the basis for technological processes, such as manufacturing or streaming, from which even smart cities gain advantages [33].

The required intermediate step was the increase of the Internet connection's penetration. Among EU households, penetration was 68% in 2010 and 92% as an estimate in 2021 [26]. In the same period, the number of companies with Internet connections increased from 95% to 98%. Furthermore, by the end of 2018, 22 billion devices (e.g., PC, notebook, smartphone, Internet of Things) will be connected to the Internet worldwide, according to an analysis conducted by Help Net Security [28]. Thus, it is tempting to approach the information society only from the perspective of technology regarding its simplicity. However, the rapid development and convergence of technology and globalisation cause functional, behavioural, and cultural changes; and the information society can be considered a new way of life, for example, individuals in an overall region benefit ICTs [47] and smart cities [14] in their everyday lives, organisations do automation [38], and the overall nation may have a higher productivity rate [4].

Furthermore, according to the spatial structure approach, people live in an information society due to the use of information technologies and globalisation, so physical space is becoming less and less important. People are surrounded by networks that provide a new framework for social processes, such as production and distribution. On the other hand, according to the cultural approach, the information society results from a global, increasingly advancing digital media culture, which becomes the primary source of meaning and defines the framework for their lives.

While the spatial perspective highlights the geographical stress based on sociology and economics, the cultural perspective stresses the growth of symbols and signs, including the services available on the Internet. For example, social network sites have shortened the distance and caused several changes in cultural aspects. Unsurprisingly, they are one of the most widely used services today. The private use of social networks in the EU grew from 36% to an estimated 65% between 2011 and 2021 according to Eurostat [26]. However, there are many more ICT services that become ever more fundamental for society. For example, the EU articulates the importance of eGovernment, eHealth, and eEducation services in connection with information society [16]. Thus, unsurprisingly, regarding the various eGovernment activities of individuals in the EU, Eurostat reported an increase in such activities from 40% to an estimated 53% between 2010 and 2021.

Therefore, the new postmodern world of the information society has caused new needs based on a mixed reality of the physical and virtual worlds. "These new needs surface with the increasing ability for people to connect, society and the culture" [7, p. 9], resulting in the complement of Maslow's pyramid with the individual, singular, and global needs. The individual needs allow humans to use ICTs to access and administer information; the singular needs are the dynamics between the subjects, understood as the identity formation of the human grouping to which it belongs; and the global needs include knowledge transfer and digital inclusion.

It is precisely the extremely rapid technological development that is one of the most important key features, affecting the everyday life of the citizens and the operation of the organisations. According to Kovacs [30], "the digitization of society and the economy means how the social and economic functions of the given country are integrated and how they are built on digital technology". Regarding the purpose and importance of the digital services that the citizens recognise as end-users, there are digital services that can help satisfy needs belonging to one of the layers of Maslow's pyramid [34, 35], explaining human behaviour and motivations. Admittedly, as per [8], several companies, including start-ups, create software services to cater to different needs by, e.g., accessing easier food and housing, providing home (i.e., physical) security and cybersecurity, meeting people and finding love, or creating possibilities for a vibrant social life.

However, today, the EU follows a simple approach and describes the information society as a "significant degree of activity focuses on the creation, distribution, use and reuse of information, which activities take place by ICT" [24]. This simple definition is related to its economic and occupational aspects, voicing that people live in an information society because the information sector and information-type work dominate the economy. Moreover, the economic aspect emphasises the involvement of information businesses and trades, which has expanded over time in contributing to the Gross National Product. This kind of focus shift has also affected occupations. The occupational approach describes the information society based on Bell's post-industrial theory [46], in which the majority of jobs are mostly informational related.

In connection with these two aspects, the DSM is necessarily one of the most fundamental concepts of the EU. As Micossi [36, p. 32] wrote in his research article, "over the past thirty years, the SEM [Single European Market] has made impressive progress, growing to cover the main economic activities, from manufactured goods to all categories of services, network utilities and public services, public procurement and the recognition of professional qualifications, as well as the market for codified technology, that for long lagged behind".

Recognising the economic importance of cyberspace, the EU accepted the equal importance of the DSM and even made it a foundation for the economy. Thus, "Information and Communications Technology (ICT) is no longer a specific sector but the foundation of all modern innovative economic systems" [18]. For example, Eurostat [26] points to the increased usage of Internet banking and online shopping. Furthermore, several industrial production changes are also based on the convergence of IT and OT represented by the concept of Industry 4.0, which refers to the efficient production and operating processes, also demonstrating economic and occupational shifting [48].

3 Evolution of the legislative framework from a security perspective

In 2013, the first strategy was accepted in the EU [17] with the motto of "An Open, Safe and Secure Cyberspace". It pronounced five strategic priorities: (1) achieving cyber resilience; (2) drastically reducing cybercrime; (3) developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (4) developing the industrial and technological resources for cybersecurity; and (5) establish a coherent international cyberspace policy. The strategy aimed to repel cybercriminal activities by cooperation with the newly established European Cybercrime Centre (EC3), and it encouraged cooperation between the public and private sectors to enhance CSDP capabilities.

The Directive on security of network and information systems (NIS Directive) [11] poses another critical milestone as it brought cybersecurity closer to the critical infrastructure protection defined in [9]. Due to the multi-shareholder and multilevel approach of the EU, the NIS Directive prescribed obligations: (1) on the Union-level to create a Cooperation Group to support and facilitate strategic cooperation and information exchange among the Member States and to create the computer security incident response teams network (CSIRTs network) promoting operational cooperation; (2) for Member States to adopt a national strategy and to designate the national competent authorities and at least one competent CSIRT for the essential services; and (3) for operators of essential services (OESs) and for digital service providers (DSPs) to comply with the established security-related requirements.

However, one year before the NIS Directive, the Payments Services Directive 2 (PSD2) [10] promoted the development of digital financial services, supporting the entry of new service providers into financial markets. PSD2 enables external third parties to access the banks' current account management system and its data on behalf of bank customers. Because of this, it prescribes cybersecurity-related objectives for companies that it covers. Furthermore, due to the economic value of online services, the trust services also play a significant role in the Digital Single European Market (SEM) and online government services [44] as they provide electronic identification, authentication, and trust services (eIDAS).

Meanwhile, the EU realised the underregulated nature of processing personal data. Due to the technological changes, the quality and quantity of personal data processing changed, amplifying abuses' effects. As a result of multi-round consultations, the General Data Protection Regulation (GDPR) [42] was announced. The GDPR looks at security, including cybersecurity and defence capabilities, from the viewpoint of privacy and incorporates several tasks and obligations in a very high-level form. However, this high-level specification relates to the overall legislation as none of the previously mentioned laws prescribes comprehensive controls, just a limited control set.

For further enhancements of the overall cybersecurity capabilities, ENISA [12] categorised the related terms as a basis for further discussion to be conducive to the EU's cybersecurity strategy, "to ensure a comprehensive approach to addressing the cyber challenges of tomorrow". The authors drew on Maslow's pyramid of needs approach to hierarchically categorising cyberspace needs (Fig. 1), including essen-

Fig. 1 Layers of cybersecurity protection (source: [12, p. 4])

tial security protection, critical asset protection, DSM protection, global stability protection, and democracy and human rights protection.

The European Commission had considered ENISA's proposals and had taken some necessary steps with the Cybersecurity Act [43], which granted a permanent mandate to ENISA with more resources and new tasks to set up and maintain the European cybersecurity certification framework and a vital role as the secretariat in the CSIRTs network. Moreover, at the end of 2020, the EU published its new cybersecurity strategy [21] to further enhance its cybersecurity capabilities for the "Digital Decade", for which the European Commission [20] created the proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive).

The EU's new cybersecurity strategy tends to reinforce the resilience of the infrastructure and critical services by building a European Cyber Shield, a network of security operations centres across the EU, a secure communication infrastructure including the broadband mobile networks, and promoting the secure Internet of Things. It also aims to deal with extreme scenarios affecting the integrity and availability of the global DNS root system by applying European DNS resolver services. The strategy is about reinforcing the presence on the technology supply chain and making up for the deficiencies of cybersecurity skills by enhancing cyber awareness. Furthermore, it aims to strengthen cyber diplomacy and cyber defence and promotes standardisation.

4 A theoretical mapping of cybersecurity stakeholders

4.1 National and supra-national levels

Recognising the cyber resilience issues caused by the high dependence on ICTs, Member States and the EU have identified several stakeholders, such as agencies, councils, as well as non-profit and for-profit organisations, to ensure cybersecurity and resilience at the operational level.

Since its establishment in 2004, legislators have increasingly given ENISA a prominent role. Thus, in addition to promoting technical guidance and standardisation at the EU level, ENISA cooperates with competent EU institutions and authorities, bodies, offices, and agencies of the Union, the Member States, or third countries [43]. In 2018, the EU institutions and bodies agreed on the Arrangement on the organisation and operation of a computer emergency response team for the Union's institutions, bodies, and agencies (CERT-EU) [3]. The CERT-EU's overall task is to contribute to the security of the ICT infrastructure of all EU institutions, bodies, and agencies (as protected organisations). It also coordinates the exchange of information on cybersecurity and responds to cybersecurity incidents for protected organisations. A further important actor in tracking cybercrimes is the EC3, set up in 2013 "to strengthen the law enforcement response to cybercrime in the EU and thus help protect European citizens, businesses, and governments from online crime" [25].

Each Member State's responsibility is to designate (at least) one competent authority and (at least) one CSIRT for essential services and digital services. The competent authorities also play a consultative role, and the designated CSIRTs aim to help manage risks and security incidents. An additional obligation for the Member States is to designate a single point of contact for cross-border cooperation between Member State authorities and relevant authorities in the other Member States or the cooperation group of CSIRTs network. The competent authorities and the single point of contact shall notify and cooperate with the relevant national law enforcement authorities and national data protection authorities.

Furthermore, the NIS Directive gives a distinct role to OESs operating in: (1) Energy, (2) Transport, (3) Banking services, (4) Financial market infrastructures, (5) Healthcare, (6) Drinking water supply and distribution, or (7) Digital infrastructure sectors. Also, the NIS Directive distinguishes DSPs operating in the context of offering: (1) the Online Marketplace service, (2) the Online Search Engine service, or (3) the Cloud Computing Service. PSD2 defines obligations for credit institutions, electronic money institutions, post office giro institutions, payment institutions, the European Central Bank, and national central banks. For all entities, the trust service providers play an essential role, according to eIDAS, as they provide electronic identification, authentication, and trust services. Although the GDPR expands cybersecurity obligations in a certain way as it prescribes duties to implement security controls, it is only for protection of personal data, regardless of the organisations' size.

Fig. 2 aims to conceptualise relationships of a small set of different types of stakeholders in national and supra-national grouping, highlighting Member State

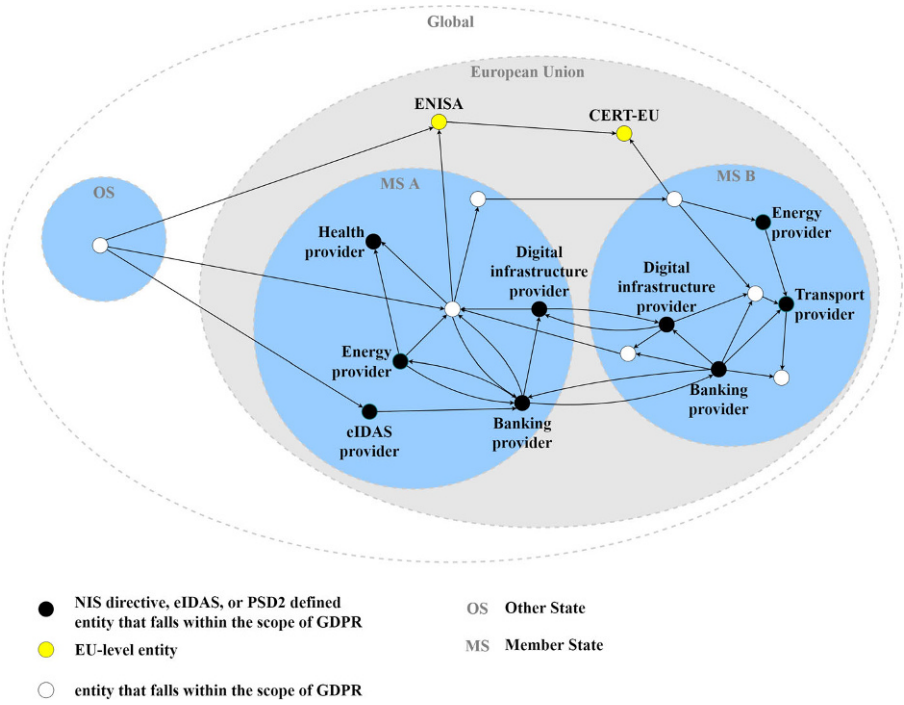

Fig. 2 Conceptualising a subset of stakeholders with hypothetical dependencies (source: own edit)

"A" and "B", as an example, demonstrating various organisational dependencies. Although not illustrated in the figure, there are several citizens as consumers of different products and services at the end of the dependence chains.

From a cybersecurity perspective, there are three types of entities differentiated as: (1) NIS directive, eIDAS, or PSD2 defined entities falling within the scope of GDPR, (2) EU-level entities defined in different legislations (which must of course also comply with the GDPR), and (3) entities falling only within the scope of GDPR regardless of where their headquarters are. Furthermore, an organisation in a Member State purchases products and uses services from other organisations that may belong to the same or another Member State or other states. Of course, EU-level entities, such as ENISA, may use various goods originating outside the EU. All these goods can comprise different business-like services, even security or any other ICT products, tools, and services, that are available globally.

4.2 Organisational level

At the same time, society is made up of individuals with non-profit and for-profit organisations, which are the basic building blocks in terms of the regional and the higher level of the multi-layered cyber resilience approach. However, for most organisations, organisational business services depend on the ICT infrastructure and services via business processes and data. According to Gao et al. [27, p. 307], "the

analytical results unveil the network characteristics that can enhance or diminish resilience, offering ways to prevent the collapse of systems, and guiding the design of technological systems resilient to both internal failures and environmental changes". But the security of ICT services is not only a technological problem. According to the ISACA's Business Model for Information Security (BMIS) [49], security comprises people, processes, and technology.

Concerning the complexity that characterises today's economic relationships, several organisations use external resources [41], creating some dependence on those suppliers. Thus, resilience is a valid characteristic not only for internal ICT infrastructure and processes but also for external ones. Supply chain resilience (SCRes) "is the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them by maintaining continuity of operations at the desired level of connectedness and control over structure and function" [40].

Furthermore, according to Webster's five definitional perspectives of the information society, technological development causes changes, affecting organisations, in various ways. These changes cause public and private entities to create new services, discarding obsolete practices, offering existing services for customers in new ways, or even the internal ICT services may offer new digital tools for streamlining processes [39]. Therefore, organisations aggregately determine the actual maximum

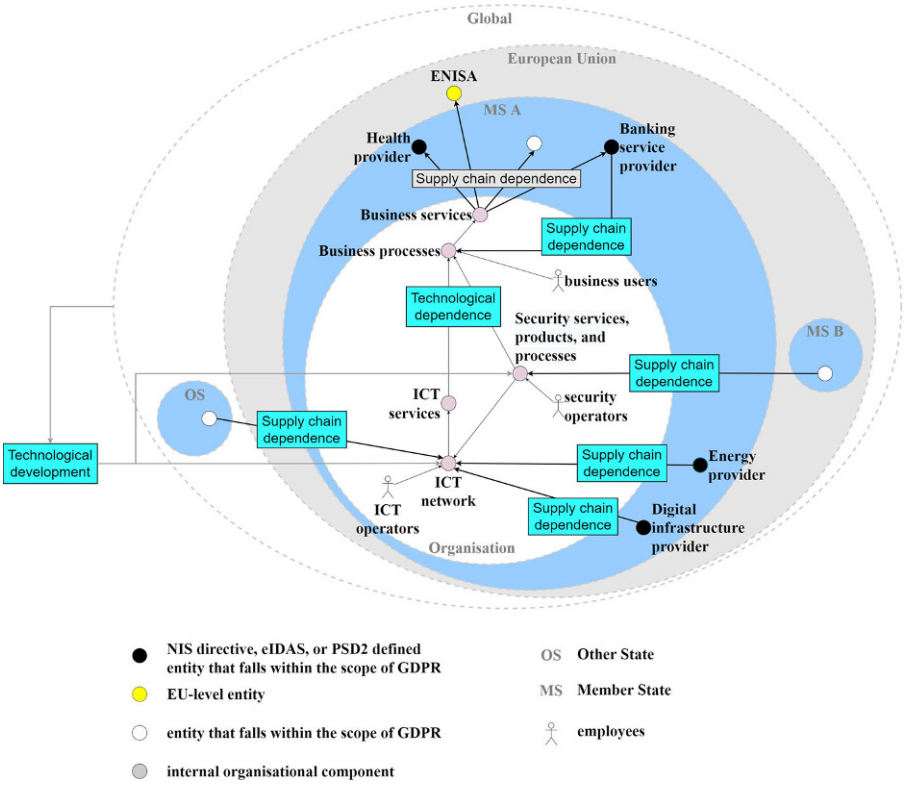

Fig. 3 Conceptualising the ecosystem of an organisation (source: own edit)

technological capabilities, from which an organisation may choose the appropriate level for its operation.

Fig. 3 conceptualises an organisation with its suppliers and customers, displayed in the previously applied multi-layer approach. The examined Organisation originates from Member State A, depicted on Fig. 2, which connects to ENISA, the Energy provider, Digital infrastructure provider, Banking provider, eIDAS provider, and the entities in Other State and in Member State B. In its internal operation, the business services apply and depend on ICT services. Furthermore, external resources may complete or substitute internal resources in business, ICT, or security services, processes, or other resources, causing supply chain dependence. On the other hand, the business services supplied by the ICT services cause supply chain dependence for the Organisation's customers supplying other organisations' objectives and satisfying individuals' needs.

5 Analysing the proposed legislative changes

Rapid technological improvements and increased digitisation have caused growing dependence on ICT services, increased supply chain dependence, intensifying complexities of such services, expanding cyberspace and hence cybersecurity stakeholders. However, these growing complexities in cyberspace demand the appropriate level of organisational cybersecurity and resilience capabilities, which increases the existing difference among organisations.

According to the European Commission [22], the NIS 2 Directive proposal eliminates the distinction between OESs and DSPs and "expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap—meaning that all medium and large companies in selected sectors will be included in the scope. (Thus, in Fig. 2, more organisations would be illustrated by black-filled circles.) At the same time, it leaves some flexibility for the Member States to identify smaller entities with a high-security risk profile". But what about those organisations which are not OES or a DSP but offer an important service for citizens, or are an important (or even dominant) economic entity whose downtime noticeably affects the DSM?

The European Commission, LSEC (Leaders in Security), and PwC [23] conducted research focusing on the EU's cybersecurity ecosystem. During data collection, they reached out to companies to measure the cybersecurity industry that: (1) provided exclusively cybersecurity products and services, (2) provided cybersecurity products and services, among other activities, or (3) provided products and services that are part of the cybersecurity value chain. In the operation of technology and related cybersecurity processes, various local and global, small and large Managed Service Providers (MSPs), Managed Security Services Provides (MSSPs), and hardware and software manufacturers have huge further responsibilities.

Furthermore, even though some elements of eGovernment services were elevated on the EU level by the eGovernment Action Plan 2016–2020 [19], it has wholly remained on the level of national legislation, because Member States prevented the integration of eGovernment into the NIS Directive. However, incident records

support the inclusion of eGovernment services [5]. For example, the malware of Operation Pawn Storm (APT28) was inside the IVBB (German Informationsverbund Berlin-Bonn) network from December 2017 and present until the end of February 2018, which may have affected German and EU-wide information [2]. Secondly, in June 2019, a cybersecurity breach affected more than 4 million Bulgarians' personal data and financial records and the EU's EUROFISC anti-fraud network data [37].

But expanding subjects to comply with obligations without prescribing a minimum set of control obligations gives no real security level improvement, so the European Commission [22] proposal prescribes a minimum list of basic security requirements for the subjects of the NIS 2 Directive. The proposal aims to impose a risk management approach to strengthen security requirements and to address both cyber and physical resilience of critical entities and networks, including more specific incident reporting and managing the security of supply chains and supplier relationships. In contrast, the current NIS Directive distinguishes OESs and DSPs and may effectuate different obligations for them. But PSD2 and eIDAS subjects will possibly not be affected by this type of formulation of more precise requirements. Additionally, although the GDPR prescribes cybersecurity obligations to protect personal data in cyberspace, it does not have effective content mandating a concrete wide range of cybersecurity controls.

However, a more significant issue arises from the legislative nature of the NIS Directive, as the prescribing of security requirements without minimum requirements is allotted to Member States with different capabilities. This statement deals with lower-level entities. For example, according to Brodin [6], small- and medium-sized enterprises suffer from a lack of resources or knowledge to effectively plan and implement cybersecurity (and data privacy) capabilities, even though they pose a vital role in DSM. However, larger organisations may also encounter problems in security-related processes, according to a global survey conducted between August 2019 and October 2019 [15].

At the same time, organisations, regardless of their size, must keep up a more complex legislative framework. Hypothetically, if a security incident affects an OES's IT system offering a payment service and the incident has an impact on personal data, there is an obligation to notify and cooperate with possibly different competent authorities under Articles 6, 14, and 16 of the NIS Directive, Articles 33 and 34 of the GDPR, and Article 19 of PSD2. Article 19 of eIDAS prescribes a further obligation for trust services providers.

As a further issue, illustrated in Fig. 2, organisations have become more vulnerable to supply problems since "supply chains become longer (more tiers), larger (more depth), and more complex" [1, p. 1525]. A recent supply chain attack was conducted against SolarWinds [51] that seriously affected its customers via its monitoring tools applied worldwide by several organisations. The most prominent publicly known example is FireEye, a known important supplier of public entities in the United States. However, probable OESs, DSPs, and other cybersecurity entities in the EU suffer from this attack directly from SolarWinds, FireEye, or as a chain effect. Although SolarWinds and other similar entities fall under the scope of the GDPR to protect its customers' personal data, its internal development and application delivery is not properly affected. Therefore, regarding supply chain risks for cybersecurity

stakeholders, there is currently no sufficient set of requirements, and each entity selects and manages its suppliers according to its internal policies, if they have any.

Lastly, cybersecurity standards are still fragmented due to the lack of cross-Member State interoperable solutions and the lack of higher-level mechanisms. The Cybersecurity Act has created a voluntary framework for European Union-wide cybersecurity certification for ICT products, services, and processes [29], as illustrated in Fig. 3. Since, typically, organisations implement cybersecurity capabilities in a risk-based approach, it is an apparent deficiency that there is no standard approach to identifying interdependencies, conducting business impact analyses, and modelling risks. Currently, to promote impact analysis, ENISA [13] has created its Interdependencies tool that "contributes to the NIS Directive (Article 3) objective for a common and converged level of security in network and information systems at EU level, and it does not intend to replace existing standards, frameworks or good practices in use by OESs".

6 Conclusion

Based on the review and analysis of information society and cybersecurity interrelations, the paper identified some crucial pain points of the current cybersecurity legislative framework and correlated them with the EU's new cybersecurity strategy and the draft version of the NIS 2 Directive.

Currently, there are stakeholders missing from the EU-level cybersecurity ecosystem, like eGovernment entities and organisations that are not in the specified categories of OESs and DSPs, even though they offer important services for citizens or represent significant (or even dominant) economic entities, whose downtime noticeably affects the DSM. Solving this issue partially, at least, the NIS 2 Directive will add new sectors based on their criticality for the economy and society. According to the draft, all medium and large companies in selected sectors will be included in the scope; simultaneously, smaller entities with a high-security risk profile may be identified by Member States.

As a further improvement, the draft aims to enhance the security of supply chains and supplier relationships as supply chains become lengthier, larger, and more complex, affecting cybersecurity and cyber resilience, which is currently an untreated problem.

The current NIS Directive allows Member States to create their own regulations and requirements without harmonisation. Fortunately, the draft prescribes a minimum list of basic security requirements. However, there is no standard approach to identifying interdependencies and conducting business impact analysis, and there is no standard to model risks, taking into account all BMIS elements. Although ENISA's Interdependencies tool aims to foster impact analysis, it is not a mandatory standard; therefore, in the authors' opinion, both impact analysis and risk modelling currently remain unaddressed. Nevertheless, how such a model can consider technological dependence and supply dependence is a good question.

Lastly, ENISA's expanded tasks and obligations have helped reduce the difference in capabilities and resources, but the complex legislative framework remains.

Acknowledgements This work results from research at the Doctoral School for Safety and Security Sciences at Obuda University; furthermore, it takes some elements of the first author's thesis conducted for the Master of Business Administration at Eötvös Loránd University.

Funding Open access funding provided by Óbuda University.

Conflict of interest Z. Bederna and Z. Rajnai declare that they have no competing interests.

References

1. Alfarsi F, Lemke F, Yang Y (2019) The importance of supply chain resilience: an empirical investigation. Procedia Manuf. https://doi.org/10.1016/j.promfg.2020.01.295
2. Anomali (2019) APT28 timeline of malicious activity. https://forum.anomali.com/t/apt28-timeline-of-malicious-activity/2019. Accessed 26 Sep 2020
3. Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU), Official Journal C 12 1 (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018Q0113(01)
4. Arvina MB, Pradhanb RP, Nairc M (2021) Uncovering interlinks among ICT connectivity and penetration, trade openness, foreign direct investment, and economic growth: the case of the G-20 countries. Telemat Inform. https://doi.org/10.1016/j.tele.2021.101567
5. Bederna Z, Rajnai Z, Szadeczky T (2021) Attacks against energy, water and other critical infrastructure in the EU. 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE). https://doi.org/10.1109/cando-epe51100.2020.9337751
6. Brodin M (2019) A framework for GDPR compliance for small- and medium-sized enterprises. Eur J Secur Res. https://doi.org/10.1007/s41125-019-00042-z
7. Carrasco-Sáez JL, Butter MC, Badilla-Quintana MG (2017) The new pyramid of needs for the digital citizen: a transition towards smart human cities. Sustainability. https://doi.org/10.3390/su9122258
8. CBInsight (2015) Maslow's hierarchy of startups: how tech wants to meet your every need. https://www.cbinsights.com/research/maslows-hierarchy-of-needs-startups/. Accessed 28 Dec 2020
9. Council Directive 2008/114/EC of 8 December 2008on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal L 345 75 (2008). http://data.europa.eu/eli/dir/2008/114/oj
10. Directive (EU) 2015/2366of the European Parliament and of the Council of 25 November 2015on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, Official Journal L 337 35 (2015). http://data.europa.eu/eli/dir/2015/2366/oj
11. Directive (EU) 2016/1148of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal L 194 1 (2016). http://data.europa.eu/eli/dir/2016/1148/oj
12. ENISA (2017) ENISA overview of cybersecurity and related terminology. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Accessed 21 May 2021

13. ENISA (2021) Interdependencies between OES and DSPs. https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-a-tool-for-the-mapping-of-dependencies-to-international-standards. Accessed 23 May 2021
14. Eremiaab M, Tomab L, Sanduleacc M (2017) The smart city concept in the 21st century. Procedia Eng. https://doi.org/10.1016/j.proeng.2017.02.357
15. Ernst & Young (2020) How does security evolve from bolted on to built-in? https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report-single-pages.pdf. Accessed 26 Sep 2020
16. European Commission (2010) EUROPE 2020 A strategy for smart, sustainable and inclusive growth (COM(2010) 2020). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF. Accessed 27 Dec 2020
17. European Commission (2013) Cybersecurity strategy of the European Union: an open, safe and secure Cyberspace (JOIN/2013/01 final). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001. Accessed 22 Jan 2020
18. European Commission (2015) A digital single market strategy for europe (COM(2015) 192 final). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52015DC0192. Accessed 27 Dec 2020
19. European Commission (2016) EU egovernment action plan 2016–2020—accelerating the digital transformation of government. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0179. Accessed 29 Jan 2020
20. European Commission (2020a) 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN. Accessed 22 May 2021
21. European Commission (2020b) The EU's cybersecurity strategy for the digital decade. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. Accessed 22 May 2021
22. European Commission (2021) Proposal for directive on measures for high common level of cybersecurity across the Union. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union. Accessed 04 Jun 2021
23. European Commission, LSEC, PwC (2019) Cybersecurity industry market analysis. https://doi.org/10.2759/018751
24. European Union Information society. https://eur-lex.europa.eu/summary/glossary/information_society.html. Accessed 9 Dec 2020
25. Europol (2021) European cybercrime centre—EC3. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. Accessed 23 May 2021
26. Eurostat (2021) Digital economy and society. https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database. Accessed 20 Jan 2022
27. Gao J, Barzel B, Barabási AL (2016) Universal resilience patterns in complex networks. Nature. https://doi.org/10.1038/nature16948
28. Help Net Security (2019) Number of connected devices reached 22 billion, where is the revenue? https://www.helpnetsecurity.com/2019/05/23/connected-devices-growth/. Accessed 28 May 2020
29. Kohler C (2020) The EU Cybersecurity act and European standards: an introduction to the role of European standardization. Int Cybersecur Law Rev. https://doi.org/10.1365/s43439-020-00008-1
30. Kovacs L (2017) Comparative study on digital economy and society of Austria and the Visegrad countries. Econ Manag 2:36–47
31. Kuehl DT (2009) From cyberspace to cyberpower: defining the problem. In: Cyberpower and national security. Potomac Books and National Defense Univerity, In, pp 24–42. https://doi.org/10.2307/j.ctt1djmhj1.7
32. Kurzweil R (2004) The law of accelerating returns. In: Alan Turing: life and legacy of a great thinker. https://doi.org/10.1007/978-3-662-05642-4_16
33. Lom M, Pribyl O (2020) Smart city model based on systems theory. Int J Inf Manage. https://doi.org/10.1016/j.ijinfomgt.2020.102092
34. Maslow AH (1943) A theory of human motivation. Psychol Rev 50(4):370–396. https://doi.org/10.1037/h0054346
35. Maslow AH (1970) Motivation and personality, 2nd edn. Harper & Row,
36. Micossi S (2016) 30 years of the single European market. In: Bruges European economic policy briefings
37. Orr J (2019) Incident of the week: 4 million Bulgarian citizens affected by tax agency data breach. CYBER Security Hub, 2019.

38. Parida V, Sjödin D, Reim W (2019) Reviewing literature on digitalization, businessmodel innovation, and sustainable industry:past achievements and future promises. Sustainability. https://doi.org/10.3390/su11020391
39. Parviainen P, Tihinen M, Kääriäinen J, Teppola S (2017) Tackling the digitalization challenge: how to benefit from digitalization in practice. Int J Inf Syst Proj Manag. https://doi.org/10.12821/ijispm050104
40. Ponomarov SY, Holcomb MC (2009) Understanding the concept of supply chain resilience. IJLM. https://doi.org/10.1108/09574090910954873
41. Prawesh S, Chari K, Agrawal M (2021) Industry norms as predictors of IT outsourcing behaviors. Int J Inf Manage. https://doi.org/10.1016/j.ijinfomgt.2020.102242
42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119 1 (2016). http://data.europa.eu/eli/reg/2016/679/oj
43. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act, Official Journal L 151 15 (2019). http://data.europa.eu/eli/reg/2019/881/oj
44. Regulation (EU) No 910/2014of the European Parliament and the Council of 23 July 2014on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal L 257 73 (2014). http://data.europa.eu/eli/reg/2014/910/oj
45. Ryba M (2014) The role of ICT components in the functioning of critical infrastructure. In: Świątkowska J (ed) Critical infrastructure security—the ICT dimension. The Kosciuszko Institute, pp 59–62
46. Scase R, Bell D (1974) The coming of post-industrial society: a venture in social forecasting. Br J Sociol. https://doi.org/10.2307/590163
47. Tranosab E, Ioannidesc YM (2019) ICT and cities revisited. Telemat Inform. https://doi.org/10.1016/j.tele.2020.101439
48. Trotta D, Garengo P (2018) Industry 4.0 key research topics: a bibliometric review. 2018 7th International Conference on Industrial Technology and Management, ICITM 2018. https://doi.org/10.1109/ICITM.2018.8333930
49. von Roessing R (2010) The ISACA business model for information security: an integrative and innovative approach. In: Pohlmann, N., Reimer, H., Schneider, W. (eds) ISSE 2009 securing electronic business processes. Vieweg+Teubner. https://doi.org/10.1007/978-3-8348-9363-5_4
50. Webster F (1994) What information society? Inf Soc. https://doi.org/10.1080/01972243.1994.9960154
51. Wolpoff D (2020) After the fireeye and solarwinds breaches, what's your failsafe? TechCrunch.