ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Protection of the EU's Critical Infrastructures: Results and Challenges

Robert Mikac | Faculty of Political Science, University of Zagreb, Croatia,
ORCID: 0000-0003-4568-6299

Abstract

At the end of 2022 and the beginning of 2023, the EU adopted several new legislative acts aimed at improving the resilience and protection of network and information systems and critical entities across the Union. The objective of this research is to list these acts, show their mutual connections and focus specifically on analysing the potential weaknesses of two legislative acts, namely: the NIS2 Directive and the CER Directive. The NIS2 Directive is a significant piece of legislation that aims to improve the cybersecurity of the European Union, while the CER Directive is a crucial piece of legislation that aims to improve the physical security of critical entities in the Union. These two documents are applied in parallel and contain many mutual references, which means that weaknesses in one document may have significant consequences for the implementation of the other. Using standard desktop analysis of primary and secondary sources, this paper reviews results and challenges in the protection of the EU's critical infrastructures by primarily focusing on these two documents. The research identifies and explains certain weaknesses, concluding with suggestions for possible solutions.

Keywords
critical infrastructures, EU legislative framework, NIS2 Directive, CER Directive, results and challenges

Received: 30.08.2023

Accepted: 22.12.2023

Published: 31.12.2023

Cite this article as:
R. Mikac "Protection of the EU's Critical Infrastructures: Results and Challenges," ACIG, vol. 2, no. 1, 2023, DOI: 10.60097/ACIG/162868.

Corresponding author:
Robert Mikac, Faculty of Political Science, University of Zagreb, Croatia; ORCID: 0000-0003-4568-6299; E-MAIL: robert.mikac@fpzg.hr

1. Introduction

"Our daily lives depend on a wide variety of services – such as energy, transport, and finance, as well as health. These rely on both physical and digital infrastructure" [1, p. 2]. Physical infrastructure enables us to work, travel and benefit from essential public services such as hospitals, transport and energy supplies. In contrast, digital infrastructure facilitates a multitude of new, extremely exciting and unpredictably dynamic jobs and processes, virtual realities and artificial intelligence, freedom of speech and possibilities of action. On one hand, all this progress makes the world a pleasant place to live, while, on the other, it raises many questions, many of which contain a security component. What happens in cyberspace has numerous implications for the physical world since "cyber" has become part of the physical reality all around us. Therefore, efficient functioning of physical and digital infrastructure has become one of the key areas of security for individuals, many economies, states, companies of all profiles and large multinational organisations such as the European Union.

The protection of critical physical and digital infrastructure is one of the key areas of national security for many countries around the world and one of the key security priorities of the European Union. The *2020 EU Security Union Strategy* emphasises four strategic priorities for the Security Union, namely: "(i) a future proof security environment, (ii) tackling evolving threats, (iii) protecting Europeans from terrorism and organised crime, (iv) a strong European security ecosystem" [1, p. 6]. The first strategic priority discusses achievements and challenges related to critical physical and digital infrastructure and states "if these infrastructures are not sufficiently protected and resilient, attacks can cause huge disruption – whether physical or digital – both in individual Member States and potentially across the entire EU" [1, p. 6]. Due to the discussion that follows, it is important to point out that the Strategy asserts that "the EU's existing framework for protection and resilience of critical infrastructures has not kept pace with evolving risks" [1, p. 6] with respect to which two directives are considered under the existing framework: *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,* and *Directive (EU) 2016/1148 of 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.*

The security risks are very diverse. Many authors believe that the digital revolution is transforming every aspect of our lives, both

creating enormous opportunities but also increasing exposure to threats [1; 6; 7; 8; 9; 14; 17]. Ulrik Franke et al. state that "with poor cyber security, society is vulnerable, both to accidents and to attacks" [3, p. 116]. Alok Mishra and associates believe that "cyber threats have risen as a result of the growing trend of digitalisation and excessive reliance on the digital world" [4, p. 1]. Sam Maesschalck and associates argue that Industrial Control Systems were not designed with internet connectivity in mind, and often lack basic security features, making them vulnerable to cyberattacks [5]. In addition to the possibility of technical failures, Stefan Varga and associates recognise people as the main sources of security risks to critical infrastructures.

> "People can either (i) take inadvertent unintentional actions, without having a malicious or harmful intent, e.g., by doing mistakes, errors and omissions, (ii) fail to take action in a given situation, where actions otherwise would have prevented an undesired outcome, or (iii) act deliberately with the intent to do harm, e.g., by acts of fraud, sabotage, theft and vandalism" [10, p. 2].

Johan David Michels and Ian Walden identified the risks to critical infrastructure from under-investment in cybersecurity measures and insufficient information sharing [11]. Although critical physical and digital infrastructure areas have become extremely connected over the last 10 years, the focus of policy makers, academics and practitioners has mostly been directed towards the latter area, as well as cyberspace. This is understandable because, as Tomasz Aleksandrowicz says, "cyberspace is now the basis for the functioning of a state's critical infrastructure" [12], both digital and physical.

Although these two areas are inextricably linked, to the best of our knowledge, in the academic world the primary focus is on considering the effectiveness of cyber protection of critical infrastructures and comparing different legal instruments related to it. Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert discuss the new EU cybersecurity framework, a new Regulation on ENISA (the EU Cybersecurity Act), and the relationship between the NIS1 Directive and the EU's General Data Protection Regulation (GDPR) [13]. The interplay between the NIS1 Directive and the GDPR in a cybersecurity threat landscape is a topic dealt with by Mark D. Cole and Sandra Schmitz-Berndt [14]. Further on the same topic, Sandra Schmitz-Berndt and Stefan Schiffner analyse reporting obligations, as well as certain limitations and differences, with respect to the NIS1 Directive and GDPR [15]. Sandra Schmitz-Berndt then discusses mandatory cybersecurity

incident reporting under the NIS2 Directive [16], and the reporting threshold for a cybersecurity incident under the NIS1 Directive and NIS2 Directive [17]. Comparison of the NIS1 Directive and NIS2 Directive was carried out through several different studies [18; 19; 20]. Finally, it is worth highlighting the comparison of the NIS2 Directive Proposal with the development of Italian and German cybersecurity laws [21]. None of these studies included a comparison of legal instruments related to the protection of critical physical infrastructures.

Returning again to the *2020 EU Security Union Strategy*, which emphasises that "the EU's existing framework for protection and resilience of critical infrastructures has not kept pace with evolving risks", it is further stated that "the legislative framework needs to address this increased interconnectedness and interdependency, with robust critical infrastructure protection and resilience measures, both cyber and physical" [1, p. 6].

> "At the same time, Member States have exercised their margin of discretion by implementing existing legislation in different ways. The resulting fragmentation can undermine the internal market and make cross-border coordination more difficult – most obviously in border regions. Operators providing essential services in different Member States have to comply with different reporting regimes" [1, p. 6].

Therefore, it was particularly emphasised that the European Commission is looking for new legal frameworks for both physical and digital infrastructures [1, pp. 6–7]. After several years of work, at the end of 2022, three legislative acts were published in the same Official Journal of the European Union, namely, two directives and one regulation: (i) *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)* [22] (hereinafter: NIS2 Directive); (ii) *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of criticzal entities and repealing Council Directive 2008/114/EC* [23] (hereinafter: CER Directive); and (iii) *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011* [24] (hereinafter: DORA).

The aim of this paper is analysing two complementary documents – the NIS2 Directive and CER Directive – because the first document is

focused on improving the cybersecurity of network and information systems across the European Union, and the second on strengthening the resilience and protection of critical entities across the Union.[1] The rationale for such a study design is twofold. First, in normative terms, the NIS2 Directive represents the central document for cybersecurity in the EU in connection with strengthening the resilience and protection of network and information systems, and the CER Directive in the area of strengthening the resilience and protection of critical entities. Second, on an operational and implementation level, network and information systems and critical entities represent one of the key bloodstreams of the Union, Member States, numerous organisations, all economies and a growing number of citizens. That is why it is essential to analyse the strengths and weaknesses of these two documents, which is the narrower purpose of this research. It is clear that both directives have resulted in numerous changes and improvements in the existing normative framework and will lead to better vertical and horizontal operational solutions. However, there is always room for additional work on the quality of legislative acts, which brings us to the question posed by this research: What are the weaknesses of these two directives?

With respect to structure, the *Introduction* is followed by a second section called *From Council Directive 2008/114/EC to the CER Directive*, which will analyse the two above-mentioned directives. The next section, *From the NIS1 Directive to the NIS2 Directive*, will provide an analysis of the two directives in question, followed by a section titled *Discussion*, which will connect the research results from the perspective of the research question and discuss the findings and their implications within the broader context of protecting critical EU infrastructures. *Conclusion* will summarise the analysis and all segments of the research, and provide final comments as well as the significance of the findings.

2. From Council Directive 2008/114/EC to the CER Directive

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [25] (hereinafter: Council Directive 2008/114/EC) was the first step in a multi-step process to identify and designate critical European infrastructures and assess the need to improve their protection. As such, this Directive was focused on the energy and transport sectors [25: recital 5]. This Directive set out a procedure for the identification and designation

1 An analysis of DORA is beyond the scope of this research, so here we only outline its key features and links to the NIS2 Directive. The objective of DORA is to strengthen information security and cybersecurity in the financial sector to maintain operational resilience in case of serious operative disruptions. It refers to entities that operate in the financial sector and third parties that provide services related to information and communication technologies. The NIS2 Directive will also apply to financial institutions (key sector – banking), whereas DORA is lex specialis. The NIS2 Directive aims to secure the resilience of essential and important entities in terms of cybersecurity, and DORA is intended to strengthen the security of financial entities.

of critical European infrastructure and a common approach to assessing the need to improve the protection of such infrastructure to contribute to the protection of people [25: article 1]. It was pointed out that there are a certain number of critical infrastructures at the level of the Union (at the time of the publication of the Directive, the term "Community" was used), the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such infrastructure should be identified and designated through a common procedure [25: recital 7]. It was additionally emphasised that this Directive complements existing sectoral measures at the level of the Community and Member States [25: recital 10], and that the primary and ultimate responsibility for protecting critical European infrastructures rests with the Member States and the owners/operators of such infrastructures [26: recital 6].

The Directive was relatively short, with only a few articles. The first article sets out the purpose of the Directive, and the second provides definitions. The third article defines the criteria for identifying critical infrastructures, while the fourth article sets out the methods for designating critical infrastructures. The fifth article describes the purpose of the Operator security plan and who is responsible for creating said plan, while the sixth describes the function of Security Liaison Officers. The seventh article refers to reporting of generic data by Member States to the Commission on a summary basis on the types of risks, threats and vulnerabilities encountered in the energy and transport sectors in which critical European infrastructure has been designated. The eighth article states that the European Commission shall support, through the relevant Member State authority, the owners/operators of designated critical European infrastructures by providing access to available best practices and methodologies, as well as training and the exchange of information on new technical developments related to critical infrastructure protection. The ninth article describes the requirements for the protection of sensitive information relating to critical infrastructure protection. The tenth article requires Member States to designate contact points for the protection of critical infrastructure [25].

As the threat landscape has evolved over time, with the emergence of new threats and the increasing interconnectedness of physical and cyber domains, questions have arisen regarding the continued relevance of the current Directive and the need for an update. The European Commission has prepared a comprehensive evaluation study on the scope of the Directive.[2] According to the 2019 *Evaluation*

2 —— This report has been prepared by EY and RAND Europe for the European Commission's Directorate-General for Migration and Home Affairs (DG HOME). The author of this text has been interviewed several times by companies that are preparing a report on the achievements of the current Directive, its weaknesses, its implementation in national legislation, public-private partnerships in the protection of critical infrastructure, and ideas for creating a new Directive.

study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection 10 years after entering into force, "the Directive appears today to have partial to limited relevance, notably in view of recent technological, economic, social, policy/political and environmental developments and current challenges" [26, p. 1]. The Member States adopted a variety of approaches in transposing the Directive in their national legislation [27, p. 14]. Member States have different starting points and approaches towards the identification of potential critical European infrastructure [27, p. 17], while the process of designating critical European infrastructure tends to be less formalised [27, p. 19]. Regarding the Operator security plan, "each Member State adopted this provision using their own interpretations of what needed to be done; this has led to the adoption of different criteria for use in assessing risks for each Member State" [27, p. 21]. The next challenge was the criteria for determining the Security Liaison Officer. Member States applied the requirements that the Security Liaison Office should satisfy very differently (in terms of role, key responsibilities, clearance, etc.) [27, pp. 21–22]. The same was true of very similar claims for national contact points for the protection of critical infrastructure [27, p. 23]. Regarding the reporting of Member States to the Commission, the procedure was established; however, it lacked sufficiently high-quality use of information collected by the Commission, which "has not systematically provided feedback on these reports, nor has it worked to synthesise the situational pictures at the MS level in order to create a pan-EU assessment of critical infrastructure vulnerability" [27, p. 22]. The final assessment is how the Directive "appears to be broadly consistent with relevant sectoral legislation. However, its coherence is limited by the existence of several overlaps with other pieces of legislation and policy documents." Additionally, "the Directive has been partially effective in achieving its stated objectives." Also, the evaluation found that the Directive generated some EU added value [26, pp. 2–6]. For all these reasons, it was necessary to adopt a new and updated directive.

The CER Directive was adopted to eliminate weaknesses observed during the evaluation of Directive 2008/114/EC, which was carried out in 2019 and found that,

> "due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical

entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted to enhance the resilience of critical entities" [23, recital 2].

The CER Directive has repeatedly upgraded the scope and reinforced the resilience and protection of critical infrastructures through various measures and activities.

It is necessary to highlight the key differences between Council Directive 2008/114/EC and the CER Directive:

- **Scope and Coverage:** Council Directive 2008/114/EC focuses exclusively on the energy and transport sectors, while the CER Directive expands the scope to include all critical entities that provide essential services in 11 sectors [23, annex 1].
- **Risk Assessment Approach:** Council Directive 2008/114/EC emphasises a top-down, risk-based approach to critical infrastructure protection, while the CER Directive encourages a more holistic, multi-dimensional approach that considers both physical and cyber threats [23, article 5 and 12].
- **Security Plan Requirements:** The security plan requirements in Council Directive 2008/114/EC were limited to the energy and transport sectors, while the CER Directive mandates the development of security plans for all critical entities, regardless of sector [23, article 13].
- **Incident Response and Recovery Mechanisms:** Council Directive 2008/114/EC provides limited guidance on incident response and recovery, while the CER Directive emphasises the need for robust incident response and recovery plans to ensure continuity of critical services [23, article 15].
- **Information Sharing and Cooperation:** Council Directive 2008/114/EC encourages information sharing between Member States and the Commission, while the CER Directive strengthens this requirement by establishing a centralised information-sharing platform (a Critical Entities Resilience Group is hereby established) and promoting the exchange of best practices and lessons learned [23, article 19].
- **Review and Update Mechanism:** Council Directive 2008/114/EC does not explicitly provide for a regular review and update

> process, while the CER Directive mandates the establishment of a review mechanism to ensure that the Directive remains relevant and effective considering changing threat landscapes and technological advancements [23, article 20].

Overall, the CER Directive represents a significant update to Council Directive 2008/114/EC, reflecting the evolving nature of critical infrastructure threats and the growing importance of a holistic approach to critical infrastructure protection. The CER Directive is a crucial piece of legislation that aims to improve the physical security of critical entities in the European Union, where critical entities represent providers of essential services, and play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. As in the example of the NIS2 Directive, the CER Directive aims at better regulation and alignment of differences between the entities involved in the provision of essential services, which are increasingly subject to diverging security requirements imposed under national law. Therefore, the new Directive seeks to lay down harmonised minimum rules to ensure the provision of essential services in the internal market, to enhance the resilience of critical entities and to improve cross-border cooperation between competent authorities. This Act also recognises other challenges relevant to the regulation of this area and considerable effort has gone into their resolution and normative improvements.

3. From the NIS1 Directive to the NIS2 Directive

Directive (EU) 2016/1148 of 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 [28] (hereinafter: NIS1 Directive) was the first horizontal legal instrument undertaken at an EU level for the protection of network and information systems across the Union [3; 11; 12; 13; 14; 16; 17; 18; 20; 29]. The Directive aimed to achieve the following:

> "(a) [to lay] down obligations for all Member States to adopt a national strategy on the security of network and information systems; (b) [to create] a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; (c) [to create] a computer security incident response teams network ('CSIRTs network') in order to contribute to the development

> of trust and confidence between Member States and to promote swift and effective operational cooperation; (d) [to establish] security and notification requirements for operators of essential services and for digital service providers; (e) [to lay] down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems" [28, article 1].

The purpose of the NIS1 Directive was to enhance the security of network and information systems (NIS) across the European Union. The Directive sets out minimum cybersecurity requirements for operators of essential services (OES), digital service providers (DSP), and Member States. The Directive's key objectives were to: (a) reduce the risk of cyberattacks on NIS; (b) improve the incident response capabilities of OES and DSP; (c) strengthen cooperation and information exchange between Member States and the European Commission; (d) foster cross-border cooperation in investigating and prosecuting cyber-crime. The Directive's main requirements for OES and DSP were: (a) identifying and classifying NIS; (b) implementing appropriate security measures to protect NIS; (c) reporting security incidents promptly to the relevant authorities; (d) conducting regular security assessments; (e) developing and implementing incident response plans; (f) providing regular updates on their cybersecurity measures. The Directive also requires Member States to: (a) establish national NIS authorities to oversee the implementation of the Directive; (b) develop and implement national NIS strategies; (c) foster public-private cooperation on cybersecurity; (d) support OES and DSP in implementing the Directive's requirements; (e) investigate and prosecute cyber-crime effectively. The Directive additionally established a framework for mutual assistance between Member States in the event of a major cybersecurity incident. Finally, the Directive required the European Commission to: (a) monitor the implementation of the Directive and provide guidance to Member States; (b) support the development of cybersecurity standards and best practices; (c) promote international cooperation on cybersecurity [28]. The NIS1 Directive was a significant step towards improving the security of NIS in the Union. It is expected to contribute to the resilience of the Union's critical infrastructure and the protection of its citizens.

The obligations under the NIS1 Directive can be broadly divided into two categories: safeguarding obligations, which require organisations to put in place "appropriate and proportionate" security measures, and information obligations, which require the sharing

or disclosure of information [11, p. 16]. While the NIS1 Directive increased the OES, DSP, and Member States' cybersecurity capabilities, its implementation proved difficult. Member States adopted different approaches, resulting in fragmentation at different levels across the internal market [2, 5]. "Different actors understand cybersecurity differently under different circumstances" [29, p. 2]. Basically, "NIS is work-in-progress" [30, p. 1328], where due to a change in numerous circumstances many countries and organisations acknowledge the need to develop more efficient protection solutions in cyber space and an increase in information security [31].

> "The Directive contributed to improving cybersecurity capabilities at a national level, increased cooperation between Member States, and improved the cyber resilience of public and private entities within the sectors encompassed. However, these improvements seem to be no longer sufficient in light of an expanded threat landscape" [17, p. 1].

"The NIS Directive could be considered a late response to an already exacerbated and well-known problem" [13, p. 11].

Due to the perceived challenges in implementation, the European Commission conducted a comprehensive evaluation study on the scope of the NIS1 Directive. According to the *2020 Commission Staff Working Document Impact Assessment Report Accompanying the document 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*, in spite of the achievements,

> "the NIS Directive also proved its limitations, falling short of ensuring a fully engaging, coherent and pro-active setting that could guarantee an effective take of shared responsibilities and trust among all relevant authorities and businesses… The NIS Directive revealed inherent weaknesses and gaps that make it incapable of addressing contemporaneous and emerging cybersecurity challenges. These concern, among others, a lack of clarity on the NIS scope, insufficient consideration of the increasing interconnectivity and interdependencies within EU economies and societies, the lack of alignment between security requirements and reporting obligations, a lack of effective incentives for information sharing or operational cooperation among relevant authorities and difference in treatment of comparable businesses across Member States and sectors" [32, p. 11].

The NIS1 Directive did not cover all the sectors that provide key services to the economy and society, was deemed to have granted too wide discretionary powers to Member States to mandate the kinds of cybersecurity and incident reporting requirements for OES, and was not perceived to include effective supervision and enforcement [18, p. 225]. NIS1 "transposition proved to be quite divergent across Member States. This has resulted in an uneven playing field, and insufficient preparedness of those entities in the face of new and evolving cybersecurity challenges" [19, p. 3]. For all of these reasons, it was necessary to adopt a new and updated directive.

The NIS2 Directive was adopted to eliminate weaknesses observed during the evaluation study:

> "the existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level" [22, recital 5].

NIS1 and NIS2 directives

> "[lay] down measures 'to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market'. The main difference is that the NIS1 framework focused on the 'security of network and information systems', whereas the NIS2 Directive focuses on the broader notion of 'cybersecurity' as defined in the Cybersecurity Act. This means that the goal is not just to protect network and information systems, but also 'the users of such systems, and other persons affected by cyber threats'. Given the risks cyberattacks pose to users of ICT systems, this is a welcome scope expansion" [19, p. 5].

The main differences between the NIS1 Directive and NIS2 Directive include:

- **Scope:** Although it primarily excludes small and micro-enterprises, NIS2 encompasses a considerably larger scope than NIS1,

incorporating many new categories of entities – particularly government bodies – and places greater emphasis on digital infrastructure and ICT services. Additionally, NIS2 considerably reduces the discretion of Member States, which should lead to a much more uniform application of its scope across the European Union [19, p. 5; 22, article 1 and 7].

- **Member State obligations:** NIS2 more explicitly elaborates the requirements for Member States' national cybersecurity strategies, thus aiming to achieve a more common level of quality [19, p. 5; 22, article 7].

- **Incident management and response:** NIS2 adds a more efficient obligation for ensuring national large-scale incident management and response [19, p. 5; 22, article 14–17; 16; 17].

- **Reporting obligation:** The reporting obligation has been tightened, given that under NIS1 only very little effective reporting occurred [19, p. 5; 22, article 14 and 16; 16; 17].

- **International coordination:** NIS2 focuses more on enforcing effective coordination between Member States, something that did not happen often under the NIS1 framework [19, p. 5; 22, article 11].

- **Information sharing:** Information sharing is more strongly encouraged [19, p. 5; 22, article 11].

- **Supervision and enforcement:** Supervision and enforcement have been tightened [19, p. 5; 22, article 17].

The NIS2 Directive is a significant piece of legislation that aims to improve the cybersecurity of the European Union. This Act aims to remove wide divergences among Member States (cybersecurity requirements imposed on entities providing services or carrying out activities differed significantly in economic terms among Member States with respect to the type of requirement, their level of detail and the method of supervision; requirements imposed by one Member State differed from, or were even in conflict with, those imposed by another Member State; potentially inadequate design or implementation of cybersecurity requirements in one Member State could have repercussions for the cybersecurity of other Member States, etc.), in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, laying down mechanisms for effective cooperation among the responsible

authorities in each Member State, updating the list of sectors and activities subject to cybersecurity obligations and providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations. The Directive contains stricter provisions on the obligations of Member States, essential and important entities, and EU institutions, and emphasises the need for more efficient cooperation. It also sets out the baseline for cybersecurity risk-management measures, and reporting obligations across the sectors that fall within its scope.

4. Discussion

The CER Directive provides a framework for physical and cyber resilience and protection of providers of critical services. The objective of the CER Directive is to remove flaws and strengthen the resilience of critical entities. Critical entities are those that provide basic services which are essential for maintaining important social functions, economic activities, public health and safety, and the environment. The NIS2 Directive extends the scope of implementation to new sectors and stakeholders, strengthens supervision through sanctions and brings about better and more efficient cooperation between Member States. Instead of operators of essential services and digital service providers (from the NIS1 Directive), the NIS2 Directive introduces the categories of essential and important entities. Both directives boost the upgraded foundations of physical and digital security, ensuring a resilient economy and society within each Member State and the European Union as a whole.

Both directives contain many mutual references, describe how Member States should apply them in coordination and cooperation (between the bodies responsible for their implementation) and explain how to avoid an administrative burden beyond that which is necessary to achieve the objectives of both directives. Among others, they envisage interlinkages between cybersecurity and physical security, a coherent approach between these two directives. It is especially important to single out the provision stipulating that entities identified as critical entities under the CER Directive should be considered to be essential entities under the NIS2 Directive [22, article 2, point 3]. Furthermore, it states that each Member State should ensure that its national cybersecurity strategy provides for a policy framework for enhanced coordination between competent authorities within that Member State under both directives in the context of information sharing about risks, cyber threats, and incidents, as well as concerning non-cyber risks, threats and incidents,

and the exercise of supervisory tasks [22, article 7; 23, article 4]. The competent authorities under both directives should cooperate and exchange information in relation to cybersecurity risks, cyber threats and cyber incidents, and non-cyber risks, threats and incidents affecting critical entities, as well as in relation to relevant measures taken by competent authorities [22, article 8; 23, article 9]. All of this strongly implies joint implementation of provisions from both directives and development of common characteristics in strengthening resilience and protection, but also brings common risks that can manifest in multiple normative areas.

The development of cyberspace and information and communication technologies is extremely fast and difficult to regulate, particularly when it needs to be implemented at an EU level and aligned with the vision of EU institutions, the possibilities of Member States, the needs of various markets and economies, and the expectations of manufacturers of different information and communication technologies. These issues give rise to questions related to the transposition and implementation of the above-mentioned documents. That is why it is necessary to continuously study this topic, analyse the current situation and focus on elements that need better or more comprehensive regulation. This is especially important because many actors within and outside the Union (such as the countries that are currently engaged in pre-accession negotiations on full EU membership) have a very different understanding of how best to apply the provisions of the directives, including whether it is even possible to implement a significant part of both directives' provisions.[3]

The NIS2 Directive has some potential weaknesses that could limit its effectiveness. First, the language of the Directive is quite complex and contains a lot of technical detail. This could make it difficult primarily for state institutions, but also for other stakeholders to understand and implement all the necessary requirements in a timely fashion. For example, the Directive entered into force on 16 January 2023, and Member States were given a 21-month deadline for its transposition, until 17 October 2024, by which time they should adopt and publish measures necessary for harmonisation with the Directive. Transposition entails the transfer of rights and obligations from the Directive into national legislation, which involves the adoption of mandatory provisions of national law, or revocation or amendment of existing regulations. The role of the European Commission is decisive in the elaboration of a certain number of measures. Thus, for example, with regard to sector-specific EU legal acts which require essential or important entities to adopt cybersecurity risk-management measures or notify significant incidents,

3 —— The author of this text has been the national contact point for the protection of critical infrastructure and participated in numerous joint EU meetings. Additionally, he was a member of various national working groups for drafting laws and strategies, leading several of them, including the working group for drafting the Law on Critical Infrastructures. Moreover, as an expert, he was engaged by the UN, EU and DCAF to draft laws and by-laws, and implement workshops in the field of critical physical and digital infrastructure protection in the following countries: Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia, Albania and Kosovo. Throughout these experiences, he identified numerous open questions, which he partially addresses in this analysis.

and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the Commission shall provide guidelines clarifying the application of those measures and requirements by 17 July 2023 [22, article 4]. However, as this research was concluding (at the end of December 2023), this document is still not publicly available (published).

The next example refers to a rather flexible approach to the adoption of a certain number of implementing acts, based on the provision that "the Commission may" adopt them. These are: a) implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group [22, article 14]; b) implementing acts laying down the technical and methodological requirements, as well as sectoral requirements, as necessary, of the measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services [22, article 21]; c) implementing acts further specifying the type of information, format and procedure of a notification, which will ensure that essential and important entities notify about any incident that has a significant impact on the provision of their services [22, article 23]; d) a European cybersecurity certification scheme regarding the use of certain certified ICT products, ICT services and ICT processes [22, article 24].

Additionally, the next example also involves implementing acts to be adopted by the Commission. These are: a) implementing acts laying down the technical and methodological requirements of cybersecurity risk-management measures with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, online search engines and social networking services platforms, and trust service providers [22, article 21]; b) implementing acts regarding reporting obligations (specifying the cases in which an incident shall be considered to be significant) of DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms [22, article 23]. The Commission is required to adopt these acts by 17 October 2024, which is the also deadline for Member States to adopt and publish national measures for harmonisation with the Directive.

The coincidence of these two deadlines should have been avoided, because some countries will wait for the Commission's implementing acts and will not respect the set deadline.

Moreover, it should be noted that the authors of the NIS2 Directive avoided defining the term "crisis" and/or "cyber crisis" and did not lay down the escalation procedure in the event of a cyber crisis. The Member States are responsible for and committed to cooperation within their national framework, and at the EU level via the CSIRTs network, the Cooperation Group, and the European cyber crisis liaison organisation network (EU-CyCLONe), whereby the Commission has its representative in the Cooperation Group, and an observer in the CSIRTs network and the EU-CyCLONe [22, article 13–17]. This arrangement – without a clear explanation of the term "crisis" and/or "cyber crisis" and failing to lay down the escalation procedure in the event of a cyber crisis – represents a serious challenge for implementation of the Directive and efficient management of cyber crises both at the level of Member States and the EU.

Finally, the NIS2 Directive does not specifically consider the growing threat of quantum computing and artificial intelligence. Quantum computers could pose a significant challenge to current cybersecurity measures, and the Directive does not provide any guidance on how to mitigate this threat. Artificial intelligence is mentioned only in the introductory explanations for the adoption of the Directive as a potential means for strengthening the capability and protection of networks and information systems, without specifying any risks that artificial intelligence could create, such as its uncontrolled autonomy.

Unlike the NIS1 Directive and NIS2 Directive, which both focus on the protection of network and information systems within cyberspace, the CER Directive deviated in two ways from Council Directive 2008/114/EC. First, the scope of application is different – whereas Council Directive 2008/114/EC concentrated on the area of security, the CER Directive focuses on the internal market. Second, Council Directive 2008/114/EC addressed critical infrastructure and the CER Directive honed in on critical entities that provide critical services requiring critical infrastructure. Since this document was prepared simultaneously with the NIS2 Directive, both documents share many similarities, which can be positive, but may also lead to some challenges in implementation.

The CER Directive also introduces numerous improvements. While Council Directive 2008/114/EC devoted attention to the procedures for determining critical European infrastructure in the energy and

transport sectors, where disruptions in operation or destruction would have considerable cross-border effects on at least two Member States, and focused exclusively on the protection of such infrastructure, the CER Directive emphasises improved risk assessment, definition and coherence of the roles and duties of critical entities as providers of services which are crucial for the functioning of the internal market of the Union in 11 sectors. Critical entities, with the help of the state, should strengthen their capacity to prevent, protect against, respond to, remain resilient to, mitigate, absorb and recover from incidents that can disrupt the provision of critical services. It should be noted that the number of sectors and subsectors in the CER Directive is significantly higher compared to Council Directive 2008/114/EC (such an approach is also used in the NIS2 Directive compared to the NIS1 Directive), where categories of entities are defined too broadly, which will lead to great challenges and even problems for Member States in the identification and designation of critical entities.

The CER Directive uses the phrase "the Commission may" much less often when laying down the obligations of the Commission for the adoption of implementing acts. It is used only twice, for issues that do not affect transposition and implementation into national legislation (in the first case, the possibility of inviting experts from the European Parliament to attend meetings of the Critical Entities Resilience Group **[23, article 19]**, and in the second, to adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group **[23]**). However, as in the case of the NIS2 Directive, the CER Directive entered into force on 16 January 2023, and the Member States were given a 21-month deadline for transposition, until 17 October 2024, by which time they must adopt and publish measures necessary for harmonisation with the Directive. The Commission is required to adopt several implementing acts that will enable efficient transposition and implementation into national legislation. The problem is that the final deadline for adoption has only been set for one of them (Risk assessment by Member States), namely, five years after 16 January 2023, whereas several provisions envisage flexibility regarding voluntary adoption and do not set a deadline. These are: a) in cooperation with Member States, to prepare a voluntary common reporting template for reporting on risk assessment of a Member State **[23, article 5]**; b) in cooperation with Member States, to develop recommendations and non-binding guidelines for support to Member States in identifying critical entities **[23, article 6]**; c) upon consultation with the Critical Entities Resilience Group, to adopt non-binding guidelines to facilitate the application of criteria for

determining the significance of negative impact [23, article 7]; d) in cooperation with the Critical Entities Resilience Group, to prepare a joint template for reporting on cross-border cooperation between states; e) upon consultation with the Critical Entities Resilience Group, to adopt non-binding guidelines which further define the technical, security and organisational measures that can be taken as measures for the resilience of critical entities [23, article 13].

Furthermore, as with the NIS2 Directive, the challenges include no mention of "crisis" and lack a detailed elaboration of crisis management escalation procedures. This has been left completely in the hands of Member States, which should develop resilience measures for critical entities to ensure the implementation of risk and crisis management procedures, and protocols and alert routines, but are required to inform the Commission in the event of an incident that has or might have a significant impact on the continuity of the provision of critical services for six or more Member States.

The last challenge refers to the lack of procedural measures related to critical entities built and/or largely managed by EU institutions, whose critical services are used by all Member States. These are critical entities of considerable strategic importance and include: Eurocontrol, a pan-European, civil-military organisation dedicated to supporting European aviation; the Galileo global navigation satellite system; and MeteoAlarm, a European alerting system for extreme weather, etc.

5. Conclusion

With the new package of legislative acts adopted at the end of 2022 and the beginning of 2023, EU institutions attempted to standardise existing practices and challenges in cyberspace, cybersecurity and physical security of network and information systems and critical entities on which business operations in numerous markets depend, as well as the security of states, organisations and individuals. The specific focus of this paper includes two new legislative acts (the NIS2 Directive and the CER Directive), which represent a significant normative improvement and will surely contribute to more efficient measures to strengthen resilience and protection, better cooperation and communication between numerous stakeholders, and less exposure and damage as a result of incidents and irregularities in the functioning of various parts of the system. However, as no perfect regulation exists, the NIS2 Directive and CER Directive have certain weaknesses. This paper addressed the research question posed and demonstrated that these two new

legislative acts have certain flaws that will create challenges for transposition and implementation. Some can be resolved quickly by preparing implementing acts, while the issue of crisis management is more time-consuming and potentially involves a revision of the two documents, or preparation of a supporting document to fill in the existing gaps. In this regard, this research represents a small contribution to the discussion on the protection of the EU's critical infrastructures.

A lot of effort has been invested in the preparation and adoption of both directives, which should be applauded, and they will greatly improve the resilience and protection of network and information systems and critical entities throughout the EU, both individually and collectively with other acts. However, some fear that both directives, particularly the NIS2 Directive, will cause considerable problems in implementation, especially in countries with weak cybersecurity enforcement regimes.

These challenges will likely be exacerbated by the fact that neither directive provides clear guidance on how to implement all of its requirements. Too much flexibility in the adoption of implementing acts by the Commission, which are essential to the transposition and implementation of both directives into national legislations, should have been avoided at all costs. Additional effort was needed to develop said acts and give Member States all the necessary tools for their transposition and implementation. One possibility would have been providing detailed examples and case studies for implementation of all the provisions in the directives.

Both directives list too many sectors, subsectors and categories on the basis of which it is possible to identify and designate essential and important entities (according to the NIS2 Directive), and critical entities (according to the CER Directive). This feels like a too broad approach, where too much room has been left for different interpretations. It is highly probable that too many operators of various facilities, networks and/or systems will be declared essential and important entities, and critical entities, which will lead to challenges in implementation compared to the NIS1 Directive and Council Directive 2008/114/EC. I will provide two examples, one from Europe and the other from the US, which illustrate the problem of identification and designation of critical physical infrastructures (or according to the new conceptualisation – critical entities providing critical services via critical infrastructure). The first example involves the number of identified and designated national critical infrastructures. The available data are very interesting. Here are some of the countries that submitted their

data on critical infrastructures for the purposes of evaluating Council Directive 2008/114/EC: Austria, approx. 400; Czech Republic, approx. 1,900; Estonia, 14; France, 1,438; Hungary, 270; Germany, approx. 1,700; Poland, approx. 550; Portugal, 162; Slovenia, 63 [33]. The research was conducted in 2018 and 2019 and the study was published by the Commission in 2020. Although each country has a certain number of sectors in which it is possible to identity and designate critical infrastructures, the final numbers clearly illustrate a very different understanding of what is critical within each country. The second example involves the number of sectors in which critical infrastructures have been identified and designated in the US, a global leader in regulation of this area. Though the process initially identified a smaller number of sectors, they increased over time to include several thousand facilities, networks and systems designated as critical infrastructures within 16 sectors. Pragmatic Americans realised this was too much and decided to retain all 16 sectors, selecting four that were deemed "more important" than the others and calling them "sectors with lifeline functions": communications, energy, transport and water [34, p. 175]. These two examples show the challenges that arise when it is possible to identify and designate too many elements in too many sectors as critical infrastructure, which consequently leads to problems in implementation, cooperation, coordination and management.

The biggest oversight was the failure to elaborate the issue of crisis and crisis management in both directives. This was left to the Member States and the Union will secure a platform for their cooperation, which is not a satisfactory solution. This is risky for three reasons. First, we all know that the Union is extremely dependent on external energy sources supplied from remote locations, where the majority of transport oil and gas pipelines and shipping routes pass through areas of insecurity and conflict. Second, the initial reaction to the COVID-19 pandemic and the ensuing crisis demonstrated a belated response and the unpreparedness of EU institutions to deal with crisis management. Instead of the European Union managing the crisis on European soil, it was reduced to offering support to Member States. Third, the war in Ukraine has revealed significant discrepancies in points of view and common policies between the EU and Member States, not to mention between the Member States themselves. That is why it is important for the Union to exert stronger leadership in crisis management. The current situation, in which the Union hopes that its Member States will solve crises of a supranational character, with a representative of the Commission as an observer, is not a good solution and a dangerous one because Member States are not capable of this. Instead, the EU should become an active "crisis manager" by addressing all these key issues. There are many obstacles to achieving

this, but with these new legislative acts, an opportunity was lost to adopt a stronger position at the centre of events and resolve potential crisis situations. In addition, the parts of the directives linked to crisis management refer to the exchange of information from operators to competent state institutions and then to the European Commission, with no mention of what the reverse process would look like.

References

[1] The European Commission. (Jul. 24, 2020). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM(2020) 605 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605. [Accessed: Nov. 12, 2023].

[2] P. Contreras, "The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges," in *Proceedings of the International Conference on Cybersecurity*, Situational Awareness and Social Media. Springer Proceedings in Complexity, C. Onwubiko, C. et al. Singapore: Springer, 2023, pp. 327–341, doi: 10.1007/978-981-19-6414-5_18.

[3] U. Franke, J. Turell, I. Johannson, "The Cost of Incidents in Essential Services – Data from Swedish NIS Reporting," in *Critical Information Infrastructures Security. CRITIS 2021. Lecture Notes in Computer Science*, vol. 13139, D. Percia David, A. Mermoud, T. Maillart, Eds. Cham: Springer, 2021, pp. 116–129, doi: 10.1007/978-3-030-93200-8_7.

[4] A. Mishra, Y. I. Alzoubi, M. J. Anwar, A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers & Security*, vol. 120, 2022, pp. 1–23, doi: 10.1016/j.cose.2022.102820.

[5] S. Maesschalck, V. Giotsas, B. Green, N. Race, "Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security," *Computers & Security*, vol. 114, pp. 1–25, 2022, doi: 10.1016/j.cose.2021.102598.

[6] M. Mirtsch, K. Blind, C. Koch, G. Dudek, "Information security management in ICT and non-ICT sector companies: A preventive innovation perspective," *Computers & Security*, vol. 109, pp. 1–23, 2021, doi: 10.1016/j.cose.2021.102383.

[7] D. Polverini, F. Ardente, I. Sanchez, F. Mathieux, P. Tecchio, L. Beslay, "Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process," *Computers & Security*, vol. 76, pp. 295–310, 2018, doi: 10.1016/j.cose.2017.12.001.

[8] C. Banasiński, M. Rojszczak, "Cybersecurity of consumer products against the background of the EU model of cyberspace protection," *Journal of Cybersecurity*, vol. 7, no. 1, pp. 1–15, 2021, doi: 10.1093/cybsec/tyab011.

[9] H. Kavak, J. J. Padilla, D. Vernon-Bido, S. Y. Diallo, R. Gore, S. Shetty, "Simulation for cybersecurity: state of the art and future directions," *Journal of Cybersecurity*, vol. 7, no. 1, pp. 1–13, 2021, doi: 10.1093/cybsec/tyab005.

[10] S. Varga, J. Brynielsson, U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Computers & Security*, vol. 105, pp. 1–18, 2021, doi: 10.1016/j.cose.2021.102239.

[11] J. D. Michels, I. Walden, "How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive," Queen Mary School of Law Legal Studies, Research Paper No. 291/2018, pp. 1–47. [Online]. Available: https://ssrn.com/abstract=3297470. [Accessed: Nov. 18, 2023].

[12] T. Aleksandrowicz, "The Act on the National Cybersecurity System as an Implementation of the NIS Directive," *Internal Security*, vol. 12 no. 1, pp. 179–193, 2020, doi: 10.5604/01.3001.0014.3196.

[13] D. Markopoulou, V. Papakonstantinou, P. de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation," *Computer Law & Security Review,* vol. 35, no. 6, pp. 1–11, 2019, doi: 10.1016/j.clsr.2019.06.007.

[14] M. D. Cole, S. Schmitz-Berndt, "The Interplay between the NIS Directive and the GDPR in a Cybersecurity threat landscape," University of Luxembourg Law Working Paper No. 2019–017, pp. 1–20. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3512093. [Accessed: Dec. 3, 2023].

[15] S. Schmitz-Berndt, S. Schiffner, "Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR," *International Review of Law, Computers & Technology*, vol. 35, no. 2, pp. 101–115, 2021, doi: 10.1080/13600869.2021.1885103.

[16] S. Schmitz-Berndt, „Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Proceedings in Complexity. C. Onwubiko et al. Singapore: Springer, 2023, pp. 343–351, doi: 10.1007/978-981-19-6414-5_19.

[17] S. Schmitz-Berndt, "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS2 Directive," *Journal of Cybersecurity*, vol. 9, no. 1, pp. 1–11, 2023, doi: 10.1093/cybsec/tyad009.

[18] T. Sievers, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations," *International Cybersecurity Law Review*, vol. 2, pp. 223–231, 2021, doi: 10.1365/s43439-021-00033-8.

[19] N. Vandezande, „Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor," SSRN, pp. 1–16, 2023. [Online]. Available: https://ssrn.com/abstract=4383118. [Accessed: Dec. 10, 2023].

[20] A-V. Dragomir, "What's new in the NIS2 Directive Proposal Compared to the Old NIS Directive," *SEA – Practical Application of Science*, vol. 9, no. 27, pp. 155–162, 2021 [Online]. Available: https://seaopenresearch.eu/Journals/articles/SPAS_27_1.pdf. [Accessed: Nov. 30, 2023].

[21] S. Schmitz-Berndt, P. G. Chiara, "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive," *International Cybersecurity Law Review*, no. 3, pp. 289–311, 2022, doi: 10.1365/s43439-022-00058-7.

[22] The European Parliament and the Council of the European Union. (Dec. 14, 2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. [Accessed: Aug. 12, 2023].

[23] The European Parliament and the Council of the European Union. (Dec. 14, 2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&qid=1692286376725. [Accessed: Aug. 12, 2023].

[24] The European Parliament and the Council of the European Union. (Dec. 14, 2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554. [Accessed: Aug. 13, 2023].

[25] The Council of the European Union. (Dec. 8, 2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114. [Accessed: Aug. 14, 2023].

[26] The European Commission, Directorate-General for Migration and Home Affairs. *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Executive summary*, 2019, doi: 10.2837/353895.

[27] The European Commission, Directorate-General for Migration and Home Affairs. *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection – Final report*, 2019, doi: 10.2837/864404.

[28] The European Parliament and the Council of the European Union. (Jul. 6, 2016). Directive (EU) 2016/1148 of 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. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Accessed: Aug. 14, 2023].

[29] V. Papakonstantinou, "Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?" *Computer Law & Security Review*, vol. 44, pp. 1–15, 2022, doi: 10.1016/j.clsr.2022.105653.

[30] O. Michalec, S. Milyaeva, A. Rashid, "Reconfiguring governance: How cyber security regulations are reconfiguring water governance," *Regulation & Governance*, vol. 16, no. 4, pp. 1325–1342, 2022, doi: 10.1111/rego.12423.

[31] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, B. Klepacki, "Information security assessment in public administration," *Computers & Security*, vol. 90, pp. 1–11, 2020, doi: 10.1016/j.cose.2019.101709.

[32] The European Commission. *Commission Staff Working Document Impact Asessment Report Accompanying the document 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, SWD/2020/345 final – part 1/3,* 2020. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:d51e4bbb-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF. [Accessed: Dec. 13, 2023].

[33] The European Commission, Directorate-General for Migration and Home Affairs. *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Annex II*, 2020. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/71835078-b043-11ea-bb7a-01aa75ed71a1/language-en/format-PDF/source-search. [Accessed: Aug. 21, 2023].

[34] R. Mikac, I. Cesarec, R. Larkin, *Critical infrastructure: A platform for the successful development of the security of nations*. Zagreb: Jesenski i Turk (in Croatian), 2018.