*Journal of Research and Innovation for Sustainable Society (JRISS)*
**Volume 8, Issue 1, 2026**
***ISSN: 2668-0416***
***Thoth Publishing House***

**DOI: 10.33727/JRISS.2026.1.10:85-109**

# Governing critical infrastructure resilience in the European Union: the evolution of the legal framework

**Cătălin Peptan[1],**
[1]„Constantin Brâncuși" University of Târgu-Jiu, ORCID: 0000-0002-3424-2812

E-mail: catalinpeptantm@gmail.com

**Abstract:** The study examines the reconfiguration of the European Union's regulatory framework on the protection and resilience of critical infrastructures/entities, in the context of physical-digital interdependencies and the amplification of transboundary hybrid risks, assessing the transition from an approach centered on the protection of infrastructures as strategic assets to an integrated model oriented toward resilience and the continuity of essential services. In this regard, the study assesses the extent to which the current normative architecture - structured around Directive (EU) 2022/2557 on the resilience of critical entities (CER), Directive (EU) 2022/2555 on cybersecurity (NIS2), and Regulation (EU) 2024/2847 on the cyber resilience of products with digital elements (CRA) - establishes a coherent and complementary framework. The methodology adopted is legal-analytical, combining doctrinal analysis of hard law norms (directives and regulations) with soft law instruments (strategies, action plans, communications, and recommendations). The study's main contribution lies in conceptualising the CER-NIS2-CRA triad as a three-level normative model: the resilience of entities and essential services, the governance of operational cyber risks, and the security of digital products "by design" throughout their life cycle. The analysis highlights both normative convergence toward systemic risk management and structural tensions that may affect operational coherence and uniform implementation at the EU level.
**Keywords:** *critical infrastructures; protection; resilience; cybersecurity; resilience governance*

## 1. Introduction

### *1.1. The general context of the study*

Within a European space marked by *increasingly complex interdependencies* (economic and commercial; political and institutional; security and defense; energy-related; legal and regulatory; social and demographic; cultural and informational), *critical infrastructures represent the fundamental pillars* of the functioning of modern societies. They include the full range of systems, services, assets, and networks indispensable for maintaining the essential functions of the state, the safety of citizens, public health, economic security, and social order [1-3].

Recent crises - the COVID-19 pandemic; large-scale cyberattacks on energy, financial, and information networks; and the conflict in Ukraine; the climate and environmental crisis - have demonstrated how vulnerable the European Union (EU) can be to hybrid threats, particularly when these target interconnected critical infrastructures [4-7]. Thus, the protection and resilience of critical infrastructures has become a *priority domain* within European security policies [8, 9], being closely correlated with the digital agenda, defence policy, civil protection, and societal resilience.

In this context, the *EU has gradually developed a regulatory framework* aimed at harmonizing Member States' efforts to strengthen the protection and resilience of critical infrastructures, contributing to: ensuring the functioning of the internal market and supply chains; increasing the resilience of economic

and social systems; enhancing the capacity for a common response to cross-border threats; and fostering the development of a shared security culture among Member States.

*1.2. Working hypothesis, objectives, and contribution of the study*

This study examines the reconfiguration of the EU regulatory framework on the protection and resilience of critical infrastructures/entities, in the context of physical-digital interdependencies and the intensification of cross-border hybrid risks. The purpose of the analysis is not the cumulative listing of the relevant legal instruments, but rather the assessment of the *coherence* and *functionality* of the regulatory framework as a whole, including its capacity to ensure better integration between the physical and cyber dimensions of risks and to support the continuity of essential services in crisis situations with cascading effects.

Within this framework, the research advances the following ***working hypothesis***:

**Hypothesis (H):** *The EU's current regulatory architecture, built around Directive (EU) 2022/2557 on the resilience of critical entities (CER) [10], Directive (EU) 2022/2555 on cybersecurity (NIS2) [11], and Regulation (EU) 2024/2847 on the cyber resilience of products with digital elements (CRA) [12], outlines an integrated model for the governance of resilience across the entire "entity-system-product" chain, oriented toward the management of systemic risks and the continuity of essential services; however, its practical effectiveness is liable to be diminished by structural frictions, in particular procedural overlaps, imperfect institutional coordination, and capacity asymmetries among Member States.*

The hypothesis is deliberately formulated along a dual axis: the *existence of normative and teleological* convergence towards resilience and the management of risks with cross-sectoral impact; and the persistence of *systemic constraints* likely to generate operational dysfunctions and heterogeneous implementation practices, with an impact on the resilience of the EU space.

To support this hypothesis, the study pursues ***three main objectives***, as follows:

**O1 -** *Normative reconstruction and paradigm shift:* highlighting the transition from the protection of infrastructures as strategic assets - reflected in the Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP) [13] and Directive 2008/114/EC [14] - to a post-2022 framework oriented toward the resilience of entities and the continuity of essential services (CER/NIS2), as well as the extension of "by design" security to the realm of digital products (CRA).

**O2** - *Systemic analysis of the CER-NIS2-CRA architecture:* identifying the internal logic of the integrated model (resilience, risk management, operational continuity), the governance mechanisms (obligations, reporting, supervision), and the areas of functional complementarity among the instruments, with a delineation of their respective normative intervention layers.

**O3** - *Critical assessment of coherence and structural limits:* examining the tensions generated by physical-digital integration and multilevel governance (EU-Member States-operators/manufacturers), with a focus on the risks of procedural overlap and "double reporting," the coordination of competent authorities, the harmonization-subsidiarity relationship, and the effects of capacity asymmetries on practical convergence among UE Member States.

The ***theoretical and analytical contribution*** of the study consists in proposing a systemic analysis of the CER-NIS2-CRA triad, conceptualized as a three-level regulatory model: the *entity level* (CER - resilience of critical entities and continuity of essential services); the *operational system level* (NIS2 - governance of cyber risks at organizational and network level); and the *product/technology level* (CRA - upstream "by design" security of digital products throughout their life cycle).

This approach enables an examination of responsibilities, complementarities, and potential implementation shortcomings, thereby offering an explanatory framework for understanding the EU's shift toward resilience governance.

Finally, the study adopts necessary ***delimitations*** to ensure coherence: the analysis focuses on *EU normative instruments* relevant to critical infrastructures and cybersecurity, without engaging in an in-depth examination of parallel legal regimes (for example, EU criminal law frameworks addressing cybercrime and attacks against infrastructures) or the classified dimension of cooperation with intelligence

agencies, except insofar as these influence the governance and resilience logics of the framework under examination.

*1.3. Research methodology*

The present study adopts a ***qualitative legal-analytical methodology***, grounded in the doctrinal analysis of EU law and in the integrated examination of relevant public policies in the field of the protection and resilience of critical infrastructures. The methodological approach is oriented toward substantiating the working hypothesis through an understanding of the *normative logic* and *governance mechanisms* embedded in the European resilience architecture, rather than toward an empirical evaluation of implementation at the national level.

*1.3.1. Type of legal analysis*

The research primarily employs: *legal doctrinal analysis,* applied to EU *hard law* instruments (directives and regulations), with the aim of identifying the object, scope of application, obligations, coordination mechanisms, and normative limits of each act; *systemic and functional analysis*, which enables the examination of relationships of complementarity, overlap, or tension among different normative instruments, in particular between the CER Directive, the NIS2 Directive, and the CRA Regulation; *public policy analysis,* applied to *soft law* instruments (strategies, communications, action plans), in order to understand their role as mechanisms of guidance, convergence, and normative anticipation. This methodological combination reflects the hybrid nature of the field under analysis, situated at the intersection of EU internal market law, EU internal security, risk governance, and resilience policies.

*1.3.2. Integrated approach and the CER-NIS2-CRA analytical framework*

To ensure analytical coherence, the study employs an integrated conceptual framework that treats the European normative architecture as a three-level model, corresponding to different layers of risk and normative intervention: *the entity and essential service level,* analyzed through the lens of the CER Directive, which regulates the organizational and physical resilience of critical entities and the continuity of vital services; *the operational system and network level,* analyzed through the NIS2 Directive, which establishes reinforced requirements for cyber risk governance, incident management, and managerial accountability; *the product and technology level,* analyzed through the CRA Regulation, which introduces mandatory "by design" and "by default" cybersecurity requirements for products with digital elements.

This framework enables an assessment of how EU law seeks to cover the entire risk chain - from technological components and products, to operational systems, and ultimately to the functioning of essential services - and to reduce systemic vulnerabilities generated by physical-digital interdependencies.

*1.3.3. Criteria for analysis and evaluation*

The evaluation of the regulatory framework is conducted on the basis of explicit *analytical criteria,* applied transversally to the instruments under review*: normative coherence*, understood as the compatibility of objectives, definitions, and institutional mechanisms; *functional complementarity,* namely the capacity of the instruments to cover different layers of risk without generating excessive redundancies; the *degree of harmonization*, analyzed in relation to the transition from minimum harmonization (the NIS Directive) to reinforced harmonization (the NIS2 Directive and the CRA Regulation); *compliance with the principle of subsidiarity*, particularly in areas sensitive to the sovereignty of EU Member States; *practical implementability,* assessed in light of the complexity of obligations, the risk of administrative overlap, and the need for coordination among multiple competent authorities; and the *capacity to reduce systemic risks*, including cascading effects and vulnerabilities in supply chains.

These criteria primarily allow for a descriptive analysis, while at the same time enabling a critical assessment aimed at identifying the structural limits of the European normative architecture.

*1.3.4. Sources and materials used*

The research is based on: *primary sources,* consisting of EU Treaties, directives, regulations, communications, and official strategies of the European institutions; *secondary sources,* including specialized literature in the fields of EU law, cybersecurity, and risk governance, as well as relevant reports in the field; and *evaluation and impact assessment documents* prepared by the European Commission, used to contextualize normative objectives and rationales.

Jurisprudential analysis is used to a limited extent, as the field of the protection and resilience of critical infrastructures is predominantly characterized by *ex ante* regulation and administrative compliance mechanisms, with a limited number of relevant disputes at the level of the Court of Justice of the EU.

*1.3.5. Methodological limitations*

The study does *not pursue an exhaustive comparative analysis* of the European normative framework concerning the protection and resilience of critical infrastructures, *nor does it include empirical case studies*. These limitations are deliberately assumed, as the objective of the research is to assess the normative coherence of the European framework in this field, as a prerequisite for the functioning of resilience mechanisms.

*1.4. Review of the relevant literature*

The body of scholarly literature relevant to the analysis of the EU regulatory framework on the protection and resilience of critical infrastructures highlights a significant conceptual and normative evolution, from approaches centered on protecting infrastructures as isolated strategic assets toward integrated models of systemic resilience governance, adapted to physical-digital interdependencies and cross-border risks.

An *initial doctrinal corpus* examines the EU's transition from early critical infrastructure protection policies, crystallized around the EPCIP [13] and Directive 2008/114/EC [14], toward a resilience-oriented paradigm. In this regard, specialized studies emphasize the conceptual shift from the protection of critical assets to the management of vulnerabilities and cascading effects within interdependent socio-technical systems, which has required a reconceptualization of the object of regulation at the European level [15-17].

From a critical-institutional perspective, reports produced by the Centre for European Policy Studies (CEPS) highlighted, as early as the post-2008 period, the difficulties of harmonization in the field of critical infrastructure protection, the central role of Member States and private operators, and the risks generated by limited exchanges of sensitive information [18, 19]. These analyses foreshadow many of the solutions later adopted in the CER Directive, particularly the orientation toward risk assessments, the continuity of essential services, and organizational responsibility.

Complementarily, the *governance and resilience literature*, including periodic analytical reports and assessments produced by the Organisation for Economic Co-operation and Development (OECD), describes resilience as a systemic capacity that combines prevention, shock absorption, adaptation, and recovery, going beyond the logic of sequential protection [20].

A *second major strand of the literature* addresses the resilience of critical infrastructures as a multi-level governance issue, in the context of shared competences and the constraints imposed by EU Member States' sovereignty in the field of security. Classical analyses of cross-border crisis management in the EU show that the effectiveness of the European response depends less on formal centralization and more on the capacity for coordination, institutional learning, and procedural convergence [21-23].

More recent studies on critical infrastructure governance emphasize that interdependencies are not exclusively technical but also institutional: fragmented competences, the multiplication of supervisory authorities, and administrative asymmetries can themselves become sources of systemic vulnerability [24, 25]. These studies provide an important explanatory framework for the divergences identified between the CER and NIS2 Directives with regard to the delineation of responsibilities and the coordination of competent authorities.

*With regard to cybersecurity*, the literature highlights the shift from a model of minimum harmonisation, characteristic of the NIS Directive [26], to a more prescriptive model of cyber risk governance, specifically associated with the NIS2 Directive [11]. The analyses highlight the importance of extending the scope of application to additional sectors, introducing the accountability of management bodies, and addressing supply chains as vectors of systemic risk [27-29].

An important role in the applied literature is played by the documents and guidelines developed by the European Union Agency for Cybersecurity (ENISA), which translate the legal requirements of the NIS2 Directive into operational practices and maturity indicators. They thus provide clear benchmarks for assessing the implementation of the Directive and the administrative capacities of EU Member States, as well as for identifying and/or highlighting the persistence of asymmetries [30, 31].

An *emerging body of literature* analyses the CRA Regulation [12] as an extension of the logic of product safety and conformity law into the field of cybersecurity. The authors emphasize the innovative nature of the horizontal, risk-based approach, as well as the upstream shift of responsibility toward manufacturers and suppliers of digital technologies, imposing *secure-by-design* obligations throughout the entire lifecycle of products [32, 33].

At the analytical level, the relationship between the CRA Regulation and the instruments governing cybersecurity (in particular the NIS2 Directive) was examined, supporting the idea of reconfiguring the governance of digital platforms through the institutionalization of cybersecurity "by design" as a normative and organizational practice [34].

Complementing the academic literature, the European Commission's *impact assessment documents* and *staff working documents* constitute essential sources for understanding the normative rationales underlying the adoption of the CER and NIS2 Directives and the CRA Regulation. These documents explicate the shortcomings of the previous framework, public policy objectives, and regulatory options considered, providing a useful interpretative background for legal doctrinal analysis [35-37].

## 2. The European regulatory framework in the field of the protection and resilience of critical infrastructures

### *2.1. General considerations*

This chapter serves as a *normative* and *conceptual foundation*, providing a detailed and structured systematization of the main legal and strategic instruments relevant to the protection and resilience of critical infrastructures. The descriptive approach is methodologically justified, as the field under analysis is characterized by high normative density, rapid evolution, and fragmented literature, and the clarification of the legal framework constitutes a necessary precondition for the subsequent integrated analysis.

The *descriptive character* does not represent a limitation of the study, *but rather a deliberate methodological choice*, intended to support the original analysis developed in Chapter 3. This approach is explicitly formulated and consistently maintained, thereby contributing to the transparency of the research process.

### *2.2. Defining the concepts of critical infrastructure (CI) / European critical infrastructure (ECI)*

According to Article 2(a) of Directive 2008/114/EC, *"critical infrastructure" (CI)* is defined as *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"* [14]. This definition highlights a systemic and functional approach to critical infrastructures, emphasizing their essential role in vital societal functions and the well-being of the population, as well as the fact that the impact of their disruption or destruction is assessed in relation to the consequences for the State's capacity to maintain its fundamental functions.

The same directive introduces into EU legislation the concept of *"European critical infrastructure" (ECI)* as an extension of the notion of national critical infrastructure. According to Article 2(b), a European critical infrastructure is *"a critical infrastructure located in Member States the disruption or*

*destruction of which would have a significant impact on at least two Member States"* [14]. The definition captures the cross-border and interdependent dimension of European critical infrastructure, highlighting that its relevance derives not only from its location, but above all from its significant impact on multiple Member States.

Conceptual approaches to the issue of critical infrastructures have evolved significantly over the past decade, in line with the increasing complexity of interconnections and cyber vulnerabilities, leading to a deeper understanding of their protection from the perspective of European systemic resilience.

*2.3. Context for the emergence of European policies on critical infrastructures*

The *first European initiatives* on the protection of critical infrastructures emerged in the early 2000s, against the backdrop of *an intensification of terrorist attacks and the globalization* of energy and transport infrastructures. In 2006, the European Commission adopted the Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP) [13]; in 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 [14] was adopted, initially focused on the energy and transport sectors; and in 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 (NIS Directive) [26] was adopted.

Subsequently, *technological developments and the intensification of cyber threats* prompted a revision of this approach. In 2020-2022, the European Commission promoted a new regulatory architecture, articulated around 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 (CER Directive) [10], and 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) [11], which are intended to harmonize the protection of physical and digital critical entities. In parallel, the EU Cybersecurity Strategy for the Digital Decade [JOIN(2020) 18 final] [38] and Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act - CRA) [12], further consolidate the integration between infrastructure resilience and cybersecurity.

*2.4. Legal and strategic instruments in the field of critical infrastructures*

*2.4.1. Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP)* [13]

Adopted on 12 December 2006, the EPCIP constitutes, according to Section 1, a *strategic public policy* document through which the Commission proposes the creation of a coherent EU-level framework aimed at strengthening the protection of critical infrastructures against a wide spectrum of threats, including terrorist, accidental, and natural threats.

In accordance with Section 2, the *overall objective* of the EPCIP is to *ensure the continuity of society's vital functions* by strengthening prevention, preparedness, and response capacities to major disruptions of critical infrastructures, particularly in situations where their effects go beyond national borders. In this regard, the Communication responds to the requests formulated by the European Council concerning the development of an integrated European strategy in the field of critical infrastructure protection.

According to Section 3, *European critical infrastructures are defined* as assets of major importance to the EU which, in the event of disruption or destruction, generate cross-border effects on one or more Member States as a result of the interdependencies among interconnected infrastructures. The Communication highlights the interdependent and cross-sectoral nature of these infrastructures, as well as the *need for a coordinated approach at EU level* in the case of infrastructures with significant cross-border impact.

Section 4 presents a *coherent set of institutional, operational, and cooperative measures* intended to facilitate the development and implementation of the EPCIP. These include a dynamic action plan structured across three levels - strategic, European, and national - the establishment of a secure warning and information-sharing network, the use of expert groups as mechanisms for public-private dialogue and the provision of sectoral expertise, the establishment of strict principles governing the exchange of sensitive information, as well as the continuous identification and analysis of geographic and sectoral interdependencies, all of which are aimed at strengthening the protection of critical infrastructures at the EU level.

According to the provisions set out in Section 5, *primary responsibility for the protection of national critical infrastructures* rests with the EU Member States and their owners or operators, while the European Commission has a supporting and guidance role, upon request.

In this context, the Communication promotes the establishment of national critical infrastructure protection programmes, based on harmonized national criteria that assess the geographical impact of disruptions and the severity of public, economic, environmental, political, psychological, and health effects, as well as on dialogue with operators, the identification of sectoral and geographical interdependencies, and the development of contingency plans, with the aim of ensuring a comparable level of protection across the EU and avoiding fragmentation of the internal market through divergent national frameworks.

A central instrument of critical infrastructure protection, as highlighted in Section 6, is *contingency planning,* whose role is to reduce the impact of systemic disruptions through a coordinated approach involving infrastructure operators, competent national authorities, and cross-border cooperation within the EPCIP framework.

Finally, Section 7 underscores the *importance of the external dimension* of critical infrastructure protection, given that threats and interdependencies extend beyond EU borders, thereby necessitating enhanced international cooperation, the exchange of best practices, and the harmonization of standards. These efforts are supported, according to Section 8, by European *financial instruments* dedicated to the prevention, preparedness, and management of the consequences of security risks, intended to support the effective implementation of the EPCIP.

*2.4.2. 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* [14]

Adopted on 8 December 2008, Directive 2008/114/EC constitutes the *first common legislative framework* at EU level *dedicated to the identification and designation of European critical infrastructures* (ECIs), as well as to the assessment of the need to improve their protection, with a view to reducing vulnerabilities and limiting the consequences of significant disruptions or destruction, as provided for in Article 1.

In Article 2, paragraphs (a) and (b), the Directive defines the concepts of *critical infrastructure* and *European critical infrastructure*, as presented in Chapter 2.2.

In accordance with Articles 3 and 4, the directive establishes the *procedure for the identification* (Annex III) and *designation* of European critical infrastructures, which involves the application of sectoral and cross-sectoral criteria, including the assessment of the potential impact of the disruption of the infrastructure concerned. The cross-sectoral criteria relate in particular to impacts on casualties, economic effects, and effects on the public, while sectoral criteria are set out in the annexes corresponding to each sector.

The Directive has a limited sectoral scope of application, initially being confined to two sectors considered a priority, namely energy and transport, as listed in Annex I, which details the relevant subsectors within each field.

A central element of the directive is the establishment of the obligation for operators of *designated European critical infrastructures* to draw up operator security plans, as provided for in Article 5. These plans must identify critical assets, relevant risks, and existing or planned security measures for the protection of the infrastructure concerned.

Furthermore, under Article 6, Member States are required to designate, for each identified European critical infrastructure, a security liaison *officer responsible for facilitating cooperation and communication* between critical infrastructure operators and the competent national authorities.

The directive also provides, in Article 7, for the obligation of Member States to *carry out threat and risk* assessments and to support critical infrastructure operators in *improving levels of protection*, in accordance with national competences and the principle of subsidiarity.

Although Directive 2008/114/EC represented an *innovative normative step* at the time of its adoption, it was subsequently subject to criticism in the academic literature and in institutional evaluations, particularly due to its narrow sectoral scope, limited to energy and transport, as well as the low level of harmonisation and uniform implementation across EU Member States. These structural limitations highlighted the need for a more comprehensive and integrated approach.

In this context, Directive 2008/114/EC constituted the *conceptual and normative foundation* for subsequent developments in European policy on critical infrastructures, which led to the adoption of a broader framework focused on the resilience of critical entities, materialized through Directive (EU) 2022/2557 (the CER Directive).

*2.4.3. 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 (NIS Directive)* [26]

Adopted on 6 July 2016, the NIS Directive establishes, pursuant to Article 1, *the first EU-level legal framework aimed at ensuring a high common level of security of network and information systems*, with the aim of ensuring optimal conditions for the functioning of the internal market and strengthening trust in the digital environment.

In accordance with Articles 4 and 5, the directive applies to the following categories of entities: *operators of essential services,* identified by the Member States on the basis of the criteria set out in Article 5(2) and Annex II; and *digital service providers*, as defined in Article 4(6) and listed in Annex III.

The sectors relevant for the identification of operators of essential services include, according to Annex II, areas such as energy, transport, banking, financial market infrastructures, health, the supply and distribution of drinking water, as well as digital infrastructure, insofar as the disruption of the respective services would have a significant impact on society or the economy.

Pursuant to Article 7, the NIS Directive obliges EU Member States to adopt *national strategies for the security of network and information systems*, within which strategic objectives, public policy measures, governance structures, and relevant national-level cooperation mechanisms are to be established.

The directive establishes distinct obligations regarding risk management and incident notification, differentiated according to the category of entity. Thus, pursuant to Article 14, *operators of essential services* are required to adopt appropriate *technical and organizational measures* for the effective management of risks and threats to the security of the network and information systems used in the provision of their services, and to *notify*, without undue delay, incidents having a significant impact. *Digital service providers* are subject to *similar but* more limited obligations under Article 16, reflecting the differentiated and more flexible approach adopted by the directive with respect to this category of entities.

With regard to the institutional framework, the NIS Directive establishes cooperation mechanisms at EU level, including the *Cooperation Group* - established under Article 11, with a strategic role in supporting and facilitating cooperation among the Member States - and the *CSIRT Network* (Computer Security Incident Response Teams) - provided for in Article 12, aimed at promoting operational cooperation, information exchange, and the coordination of responses to cybersecurity incidents. In this context, ENISA plays a role of technical support and expertise, particularly with regard to facilitating cooperation, the exchange of best practices, and the development of Member States' capacities.

The NIS Directive enshrines a *minimum harmonisation* approach, allowing EU Member States significant discretion in the identification of operators of essential services, the determination of security

requirements, and the application of supervision and enforcement regimes, which in practice has led to a high level of regulatory fragmentation across the EU.

Accordingly, the NIS Directive represents the *cornerstone of European cybersecurity policy*, providing the first coherent legal framework in this field, while also serving as the starting point for the subsequent strengthening of regulation through the adoption of the NIS2 Directive.

*2.4.4. 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 (the CER Directive)* [10]

Adopted on 14 December 2022, the CER Directive repeals Directive 2008/114/EC pursuant to Article 27 and *establishes a new European regulatory framework focused on strengthening the resilience of critical entities*, moving beyond the previous approach predominantly centered on the physical protection of critical infrastructures, as reflected in Article 1.

The CER Directive applies to entities operating in eleven critical sectors, as listed in the Annex to the Directive: energy; transport; banking; financial market infrastructures; health; drinking water; wastewater; digital infrastructure; public administration; space; and the production, processing, and distribution of food.

In accordance with Article 4, the CER Directive provides that each EU Member State shall *adopt and regularly update a national strategic framework* setting out objectives, measures, governance mechanisms, and intersectoral and cross-border cooperation arrangements, with a view to ensuring a high and sustainable level of resilience of critical entities, and shall communicate it to the European Commission.

The directive imposes on Member States the obligation to *carry out national risk assessments*, pursuant to Article 5, in order to identify threats relevant to the provision of essential services, including natural hazards, man-made risks, accidents, acts of sabotage, terrorism, and other hybrid threats. These assessments form the basis for the *identification of critical entities*, in accordance with Article 6, as well as for the *establishment of appropriate resilience measures*. In this context, Article 7 specifies that a *significant disruptive effect* is determined by the scale and duration of the impact of an incident on users, dependent sectors, public safety, the economy, and the continuity of essential services, including at cross-border level.

At the same time, the CER Directive establishes a reinforced *governance and coordination framework*, providing in Article 9 for the obligation of EU Member States to designate competent authorities responsible for the implementation of the Directive, as well as, in accordance with Article 11, the establishment of mechanisms to facilitate cooperation and information exchange at EU level.

The Directive establishes, in Article 17, a special regime for *critical entities of particular European significance*, defined as entities that provide essential services to at least six EU Member States, whose designation is carried out through a procedure of notification, consultation, and confirmation at the level of the European Commission. For these entities, the Commission may, in accordance with Article 18, organise *advisory missions* aimed at assessing compliance with resilience obligations, issuing opinions and recommendations, and strengthening cooperation, information exchange, and mutual learning among EU Member States, while respecting national competences in the relevant fields.

Furthermore, the Directive establishes, through Article 19, the *Critical Entities Resilience Group* as a mechanism for coordination and information exchange between the Member States and the Commission, and enshrines, through Article 20, the role of the Commission in supporting competent authorities and critical entities through guidance, best practices, assessments, advisory missions, training, and the analysis of cross-border and intersectoral risks. At the same time, particular attention is also given to issues of *supervision and enforcement*, as reflected in the provisions of Articles 21 and 22.

Through this regulatory architecture, the CER Directive marks a *paradigm shift* from the concept of *"protection"* of critical infrastructures to that of *"resilience"* of critical entities, understood, pursuant to Article 2, as the set of capacities for prevention, resistance, absorption, adaptation, and recovery following incidents with significant impact, reflecting the need for continuous adaptation to a security environment characterized by complex, interconnected, and systemic threats.

*2.4.5. 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)* [11] Adopted on 14 December 2022, the NIS2 Directive repeals the NIS Directive pursuant to Article 44 and establishes a *strengthened legal framework for achieving a high common level of cybersecurity of network* and information systems across the Union, as provided for in Article 1.

The Directive applies to the entities defined in Article 3 and listed in Annex I (*sectors of high criticality*) and Annex II (*other sectors of critical importance*). The areas covered include: energy; transport; banking; financial market infrastructures; health; drinking water and wastewater; digital infrastructure; public administration; space; the production and distribution of food; postal and courier services; waste management; the chemical industry; the manufacture of critical products; digital service providers; as well as research organizations.

It is relevant to note that this legislative act regulates the *national governance framework in the field of cybersecurity* through the provisions of Articles 7-13, which are based on the national cybersecurity strategy (Article 7). The strategy defines strategic objectives, public policies, sectoral priorities, governance and cooperation mechanisms, as well as measures for prevention, preparedness, response, and recovery in relation to cybersecurity incidents. This framework is operationalised through the designation of competent authorities and a single point of contact (Article 8), cyber crisis management authorities (Article 9), and CSIRT teams, with clearly defined tasks, adequate resources, and obligations of coordination and information exchange at national, cross-border, and intersectoral levels (Articles 10-13). Accordingly, national governance is conceived as an integrated, multi-level system that combines strategic planning, institutional coordination, vulnerability management, public–private cooperation, and operational capacities for incident and crisis management, with a view to ensuring a high and sustainable level of cybersecurity.

Furthermore, the NIS2 Directive regulates the *governance framework at EU and international level,* established by Articles 14-19. This framework is based on a multi-level architecture of strategic, operational, and crisis-management cooperation, designed to ensure coherence, trust, and secure information exchange between Member States and EU institutions. At the strategic level, the *Cooperation Group* coordinates policy guidance, the exchange of best practices, risk assessments, and peer reviews, ensuring consistent implementation of the Directive and its interface with EU initiatives and the framework established by the CER Directive (Article 14). At the operational level, the *CSIRT network* facilitates rapid technical cooperation on incidents, vulnerabilities, and coordinated response (Article 15), while EU-CyCLONe manages the political and operational coordination of large-scale cybersecurity incidents and crises (Article 16). The international dimension is reflected in the possibility of concluding agreements between the EU, third countries, and international organisations (Article 17), as well as through reporting, evaluation, and mutual learning mechanisms that contribute to strengthening cybersecurity capacity and resilience across the EU (Articles 18–19).

In accordance with Article 21, the NIS2 Directive establishes the *obligation for the entities concerned to adopt technical, operational, and organizational measures for the effective management of cybersecurity risks*, including, inter alia: policies for risk analysis of information system security, incident and crisis management, supply chain security, security testing and auditing, as well as the use of cryptography and authentication mechanisms.

The Directive significantly strengthens the *responsibility of the management bodies* of entities, providing in Article 20 for their obligation to approve cybersecurity risk management measures, to oversee their implementation, as well as for the possibility of incurring liability in the event of non-compliance with the established obligations.

With regard to incident management, the NIS2 Directive introduces a detailed *regime for the reporting of significant incidents*, laid down in Article 23, which requires the prompt notification of the competent national authorities or CSIRTs through the submission of early warnings, incident notifications, and a final report.

Through its provisions, the NIS2 Directive, in complementarity with the CER Directive, *contributes to the establishment of a coherent and integrated framework for cybersecurity and resilience* at EU level, reflecting the increasingly deep interdependencies between digital and physical infrastructures and the need for a harmonized approach to systemic risks.

*2.4.6. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act - DORA)* [39]

The DORA Regulation establishes a *uniform and directly applicable legal framework* at EU level, with the objective of *strengthening the capacity of financial entities* to prevent, withstand, respond to, and recover from information and communication technology (ICT)-related incidents, as provided for in Article 1. Although the regulation does not directly concern the protection of critical infrastructures in the classical sense of EU law, it regulates a sector classified as critical under both the CER Directive and the NIS2 Directive, having a structural impact on the continuity of essential services and on the stability of the European market.

The scope of application of the regulation is defined broadly, *covering a wide range of financial entities,* including credit institutions, payment institutions, investment firms, financial market infrastructure entities, insurance and reinsurance undertakings, as well as other relevant participants in the financial system, as defined in Article 2. In addition, the regulation introduces a distinct regime governing the relationship between financial entities and third-party ICT service providers, recognizing their critical role in the operational functioning of the financial sector.

The normative structure of the DORA Regulation is built around *five main pillars* that shape a coherent model for the governance of digital operational resilience. The *first pillar* aims to establish a strengthened ICT risk management framework (Chapter II) by setting out obligations relating to internal policies, the responsibilities of management bodies, prevention and detection measures, business continuity plans, and vulnerability management mechanisms. The *second pillar* focuses on establishing a harmonised regime for the management, classification, and reporting of ICT-related incidents (Chapter III), in order to ensure a comparable level of visibility across the EU and to facilitate a coordinated response by competent authorities. The *third pillar* integrates requirements for the periodic testing of digital operational resilience (Chapter IV), going beyond traditional approaches to formal compliance and, in certain cases, introducing the obligation to conduct advanced threat-led penetration testing based on realistic threat scenarios. The *fourth pillar* regulates the management of risks related to third-party ICT service providers (Chapter V) by imposing detailed requirements on contracting, monitoring, exit strategies, and the assessment of concentration risks. Finally, the *fifth pillar* aims to regulate the voluntary exchange of information on threats and vulnerabilities (Chapter VI), with a view to collectively strengthening defensive capabilities and the anticipation of emerging risks.

An innovative element of the Regulation is *the establishment of an EU-level oversight framework for third-party ICT service providers considered critical for the financial sector*, a mechanism that reflects the recognition of the cross-border and systemic nature of digital risks (Chapter V, Section II). This dimension of centralised supervision complements the predominantly national approach found in other EU regulatory instruments and contributes to reducing fragmentation of the internal market in the area of digital resilience.

From the perspective of its relationship with other regulatory instruments, the DORA Regulation operates as a *sector-specific lex specialis* in relation to the NIS2 Directive - for financial entities falling within its scope - in order to avoid overlapping obligations and double reporting in the field of cybersecurity. At the same time, the Regulation stands in a *relationship of functional complementarity* with the CER Directive, insofar as the digital operational resilience of the financial sector constitutes an essential condition for the continuity of critical financial services and for preventing cascading effects on other vital infrastructures and sectors.

By establishing a harmonised framework applicable to strengthening the resilience capacity of financial entities, the Regulation contributes to the *development of the European normative architecture for*

*the protection of critical infrastructures and entities*, in line with the EU's vision of combining horizontal instruments with specialised sectoral regimes.

The DORA Regulation is complemented by Directive (EU) 2022/2556 [40], which aims to ensure the alignment of existing financial sector legislation with the requirements of digital operational resilience, by *affirming the lex specialis character* of DORA for financial entities and clarifying its relationship with the NIS2 Directive, including the avoidance of overlapping obligations and double reporting. In this way, Directive 2022/2556 contributes to the coherent and uniform application of the DORA regime and to strengthening the systemic resilience of the European financial sector.

*2.5. Other related legislative instruments*

Subsequent to the regulatory framework referred to in Chapter 2.4, a series of other normative and strategic instruments further complement the European architecture for cyber resilience and cybersecurity, as follows:

*2.5.1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* [41]. Regulation (EU) 2019/881 establishes, pursuant to Article 1, the EU legal framework on cybersecurity, with the objective of *strengthening ENISA and establishing the European cybersecurity certification framework* for ICT products, services, and processes, in order to ensure a high level of cybersecurity and the proper functioning of the internal market.

In accordance with Articles 3-7 and the relevant provisions concerning ENISA, the Regulation grants it a permanent mandate, defining its main tasks in *supporting Member States and EU institutions* in the prevention, detection, and management of cyber incidents, facilitating cooperation at EU level, developing capacities, and supporting the consistent application of EU law in the field of cybersecurity.

Through the provisions of Articles 13–28, the *Regulation defines the managerial structure* (the Management Board, the Executive Board, the Executive Director, the Advisory Group, and the Network of National Liaison Officers), *their responsibilities*, and the *manner in which ENISA operates at an operational level* to support EU actions in the field of cybersecurity.

A central element of the Regulation is the establishment, under Article 46, of a *European cybersecurity certification framework* applicable to ICT products, ICT services, and ICT processes. Pursuant to Articles 47-49, a uniform mechanism at EU level is established whereby, on the basis of a rolling work programme, the European Commission, with the support of ENISA, develops, adopts, and reviews, through implementing acts, European cybersecurity certification schemes applicable to ICT products, services, and processes, with a view to ensuring a harmonised level of cybersecurity within the internal market.

The *institutional mechanisms of certification and the roles of the actors involved* are regulated in Articles 50-54, which establish the competences of conformity assessment bodies and of national cybersecurity certification authorities. According to Article 56, certification is, in principle, voluntary, without prejudice to the possibility for other acts of EU law or of the Member States to provide for mandatory certification for certain categories of products or services.

The Regulation provides, in Articles 58-60, *mechanisms for cooperation and coordination* between national authorities, the Commission, and ENISA, in order to ensure the consistent application of certification schemes, information exchange, and monitoring of the effectiveness of the European certification framework.

Through Article 62, the Regulation establishes the *European Cybersecurity Certification Group* (ECCG) - a body composed of representatives of the relevant national authorities, chaired by the European Commission and assisted by ENISA - which is tasked with ensuring coordination, advisory support, and cooperation at EU level for the development, implementation, review, and international alignment of European cybersecurity certification schemes.

By establishing a permanent mandate for ENISA and a harmonized framework for cybersecurity certification, Regulation (EU) 2019/881 represents an *essential normative pillar* of the EU's legal architecture in the field of cybersecurity, playing a complementary role to the CER and NIS2 Directives and the CRA Regulation.

*2.5.2. Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [JOIN(2020) 18 final]* [38]

The Joint Communication JOIN(2020) 18 final, entitled *The EU Cybersecurity Strategy for the Digital Decade*, constitutes a strategic EU public policy document setting out the political guidelines and strategic objectives in the field of cybersecurity, in the context of accelerated digital transformation and the growing cyber threats with systemic impact.

The Strategy starts from the premise, set out in the introductory section, that *cybersecurity constitutes an essential condition* for the functioning of the internal market, the protection of critical infrastructures, resilience, and the EU's strategic autonomy. The document emphasizes the cross-sectoral and cross-border nature of cyber risks and the need for an integrated approach at EU level.

From a structural perspective, the Strategy is conceptualised around *three main strategic pillars*, as follows. The *first pillar* focuses on strengthening resilience, technological sovereignty, and European leadership in the field of cybersecurity, through the development of a reinforced regulatory framework, investments in secure technologies "by design" and "by default", support for European industrial capacities, and the strengthening of digital supply chain security. The *second pillar* aims to develop operational capabilities for the prevention, detection, deterrence, and response to cyber incidents by enhancing cooperation among EU Member States and strengthening information-sharing and situational awareness mechanisms. The *third pillar* seeks to promote an open, stable, and rules-based global cyber order, by intensifying international cooperation, strengthening partnerships with third countries and international organisations, and promoting responsible state behaviour in cyberspace.

In line with the legislative, operational, and financial instruments operating at EU level, the *Strategy recommends* adapting and expanding the existing regulatory framework, mobilising European funds for cybersecurity, and integrating cybersecurity objectives into the EU's external and development policies. Although it does not establish direct legal obligations, the *document has decisive strategic value*, shaping the directions for the development of EU law in the field of cybersecurity and providing the conceptual framework for the transition from a fragmented approach to an integrated, preventive, and resilience-oriented approach to digital security.

From a systemic perspective, the document serves as an *integrative strategic framework*, underpinning and guiding subsequent normative developments, including the revision of the NIS Directive as reflected in the adoption of the NIS2 Directive, the adoption of the CRA Regulation, and the strengthening of the European architecture on the resilience of critical entities.

*2.5.3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Fit for 55": delivering the EU's 2030 climate target on the way to climate neutrality [COM/2021/550 final]* [42]

The *"Fit for 55"* legislative package represents a coherent set of legislative proposals presented by the European Commission starting in 2021, aimed at achieving, by 2030, a reduction of at least 55% in net greenhouse gas emissions compared to 1990 levels, in accordance with European climate legislation.

From a normative perspective, the aforementioned package constitutes the *central instrument for the legislative operationalization of the EU's climate objectives*, covering key sectors such as: the emissions trading system; energy and energy efficiency; transport; land use, land-use change and forestry; the carbon border adjustment mechanism; and social policies accompanying the transition.

The package seeks to align the *existing legal framework* with the new climate objectives through the revision and supplementation of sectoral legislative acts, introducing an integrated approach that combines market-based mechanisms, regulatory standards, and social solidarity instruments. A defining

element is the integration of the social dimension of the energy transition, through mechanisms designed to mitigate the impact on vulnerable households and on economic competitiveness.

From a systemic perspective, the legislative package marks the *transition from programmatic climate objectives to concrete legal obligations*, having a structural impact on the architecture of EU law in the fields of energy, environment, transport, and industrial policy. Its normative-operational function gives it the role of strengthening energy resilience and integrating the social dimension into the EU's energy transition.

*2.5.4. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (CRA Regulation)* [12]

The CRA Regulation establishes, pursuant to Article 1, a uniform and directly applicable legal framework at EU level, with the objective of *ensuring a high level of cybersecurity for products with digital elements* throughout their entire life cycle and the proper functioning of the internal market.

In accordance with Articles 2 and 3, the Regulation applies to products with digital elements, defined as *software or hardware products* and *standalone software solutions* placed on the EU market, subject to the exclusions expressly provided for by specific sectoral legislation. The Regulation adopts a risk-based approach, classifying products according to their level of criticality (Articles 6-8), namely products subject to general requirements, important products (Classes I and II, listed in Annex III), and critical products (listed in Annex IV). Based on this classification, the conformity assessment procedures set out in Articles 27-30 are determined. The CRA Regulation lays down, in Annex I, a set of *essential cybersecurity requirements* applicable throughout the life cycle of products with digital elements, including obligations related to secure-by-design development, vulnerability management, protection against unauthorized access, ensuring integrity, confidentiality, and availability, as well as secure update mechanisms. Pursuant to Article 13, the Regulation establishes clear *obligations for economic operators*, in particular for manufacturers, with regard to their responsibilities to ensure the conformity of products with the requirements of the Regulation, the implementation of coordinated vulnerability management processes, the documentation of risks, and cooperation with the competent authorities in the context of market surveillance.

The Regulation also introduces *obligations to report* actively exploited vulnerabilities and significant security incidents, as provided for in Articles 14 and 15, with the aim of strengthening a coordinated response at EU level and reducing systemic risks generated by non-compliant or vulnerable products.

The procedures for *assessing the conformity* of products with digital elements with cybersecurity requirements, including the applicable procedures, technical documentation, the EU declaration of conformity and CE marking, as well as the role of notified bodies where applicable (Articles 27-51). The aim is to ensure that only compliant products are placed on the EU market, with clear responsibilities for economic operators throughout the entire product life cycle.

*Market surveillance and enforcement*, regulated in Articles 52-60, confer powers on national and EU authorities and establish procedures for monitoring, verifying, and enforcing the compliance of products with digital elements with the requirements of the Regulation, including through risk-based controls, access to information and documentation, corrective measures, and mechanisms for cooperation and coordination to address non-compliant products. By establishing mandatory cybersecurity requirements applicable to products with digital elements, the *CRA Regulation marks a significant normative development in EU law*, instituting a framework oriented towards prevention and the assumption of responsibility in this field, complementary to the framework established by the NIS2 and CER Directives, thereby contributing to the strengthening of digital resilience.

*2.5.5. Action Plan for Affordable Energy: Unlocking the true value of our Energy Union to secure affordable, efficient and clean energy for all Europeans* [43]

The document adopted by the European Commission sets out a *strategic action plan* aimed at ensuring affordable, secure, efficient, and clean energy in the EU, starting from the finding that persistently high

energy costs continue to affect economic competitiveness and social cohesion. The plan harnesses the EU's potential through an integrated approach structured around *four complementary pillars*, as follows:

The *first pillar - Reducing energy costs* - seeks to lower energy costs for household and industrial consumers, reduce the cost of electricity supply, regulate gas markets to ensure fair energy prices, and promote energy efficiency.

The *second pillar - Building a genuine Energy Union* - aims to accelerate the integration of energy markets at EU level through the modernisation and expansion of cross-border electricity networks, the promotion of digitalisation and interconnectivity of energy systems, and enhanced coordination of national regulations and policies.

*Pillar Three - Attracting investment and ensuring the achievement of objectives* - aims to accelerate the integration of energy markets at the EU level by implementing efficient investment programs for the modernization of cross-border electricity networks, financed both through European funds and from the national budgets of EU Member States.

Finally, the *fourth pillar - Preparing for potential energy crises* - seeks to strengthen the resilience of the energy system by anticipating and managing disruptions caused by external factors, including cyberattacks and market volatility, by reducing climatic and geopolitical risks, and by ensuring security of energy supply.

The plan does not create direct legal obligations for EU Member States but has *strategic and guiding value*, serving as a *framework document* for the coherent adaptation and implementation of European energy legislation and for aligning energy policies with the EU's social and competitiveness objectives. In this way, the plan *contributes to strengthening energy resilience*, decarbonising the economies of the Member States, and integrating the social dimension into the EU's energy transition.

## 3. The European normative architecture for the protection and resilience of critical infrastructures: an integrated analysis

### *3.1. The evolution of the European normative architecture of critical infrastructure resilience*

The analysis of the European normative framework on the protection and resilience of critical infrastructures cannot be carried out solely through a point-by-point examination of the relevant legal instruments in this field. Although the CER and NIS2 Directives, as well as the CRA Regulation, have distinct objectives, scopes of application, and mechanisms, they do not operate individually and in parallel, but rather act upon the same systems, which are characterised by physical and digital interdependencies.

In this context, the EU's normative architecture must be understood not as a mere aggregation of legal acts, but as *a multi-layered legal system* designed to address different levels of risk manifesting at EU level. This systemic approach is essential for assessing the coherence of the post-2022 regulatory framework, from the perspective of how its components interact, complement each other, or overlap in managing risks with cascading effects on essential services.

The current EU normative architecture reflects a *significant conceptual shift*, namely the transition from regulating the protection of critical infrastructures - as isolated objects - towards the governance of resilience - as an emergent property of interconnected socio-technical systems. Within this logic, risk is no longer located exclusively at the level of an identified infrastructure, but is distributed along a functional chain that includes technological components, operational systems, organisational structures, and services provided to the population and the economy [2, 15, 16].

Consequently, the assessment of the European normative architecture requires an *analysis of the interaction between different levels of legal intervention*: *the level of the entity and the essential service,* regulated by the CER Directive; the *level of operational systems and networks*, regulated by the NIS2 Directive; and the *level of products and technology*, regulated by the CRA Regulation. These levels are not autonomous, but mutually influence one another, and the effectiveness of each depends on the coherence of the overall framework.

From this perspective, the present chapter does not seek to provide a descriptive analysis of each instrument individually - an approach undertaken in Chapter 2 - but rather an *integrated analysis of the normative architecture*, aimed at identifying convergences, areas of tension, and the structural

limitations of the European model of governance for the resilience of critical infrastructures. This approach enables a cumulative assessment of the consistency of legal norms, from the perspective of their effects, within an environment characterized by hybrid risks, cross-border interdependencies, and institutional asymmetries among EU Member States.

*3.2. From protection to resilience as a normative paradigm*

This subsection highlights the shift in the *legal paradigm underpinning* the EU architecture in the field of the protection and resilience of critical infrastructures, whereas the previous subsection analyzed the *normative architecture* from a systemic perspective.

A defining dimension of the current European normative architecture is the *transition* from an approach centred on the *protection of critical infrastructures* to one oriented towards their *resilience* and that of the essential services underpinning the functioning of modern societies. This paradigm shift reflects an adaptation of the EU regulatory framework to the dynamic, interdependent, and systemic nature of contemporary risks, which can no longer be effectively managed through mechanisms aimed at protecting isolated assets.

Directive 2008/114/EC [14] represented an *initial normative effort to regulate the protection of critical infrastructures at European level*, but it operated within a limited conceptual framework. As shown in Chapter 2.4.2, the Directive was centred on the identification and designation of European critical infrastructures in a narrow range of sectors (*transport and energy*) and on the adoption of security measures primarily oriented towards the physical protection of clearly defined assets. This approach was based on a linear risk model, in which threats were exogenous in nature and could be managed through ad hoc protective measures, without fully integrating sectoral interdependencies and cascading effects.

Subsequent technological developments and the expansion of digitalization have meant that major disruptions to critical infrastructures are no longer caused exclusively by direct attacks on physical assets (exogenous causes), but are increasingly driven by operational or digital malfunctions, supply chain disruptions, or combinations of hybrid factors [6, 7, 29], thereby highlighting the *limitations of the previous model* and the *need to reconfigure* the object of regulation.

The CER Directive [10], as shown in Chapter 2.4.4, marks this reconfiguration by *conceptualising resilience as a central legal object*. Accordingly, resilience is defined as a set of capacities - prevention, resistance, absorption, adaptation, and recovery - that enable critical infrastructures to cope with incidents having a significant impact on the provision of essential services. Under this Directive, the normative focus shifts from the protection of critical infrastructures to ensuring the continuous functioning of vital services, regardless of the nature of the threats that may affect them.

Accordingly, the normative approach becomes *functional and dynamic*, as risk is no longer assessed exclusively in relation to a material asset, but rather in relation to a system's capacity to maintain its critical functions under conditions of stress. Complementarily, resilience entails the integration of the physical, digital, organisational, and human dimensions of risk, thereby transcending rigid sectoral boundaries. At the same time, the extension of the scope of the CER Directive to eleven critical sectors reflects a *transversal vision* and the recognition of the *systemic nature* of critical infrastructures.

The paradigm shift brought about by the CER Directive does not amount to a substitution of the protection logic, but rather to its extension into a *multilevel model* in which resilience is understood in terms of the capacities that enable critical infrastructures to withstand incidents with a significant impact on the provision of essential services [15, 21, 35]. In this context, the shifts generated by the CER Directive have led to the *adoption of complementary legal regimes* designed to address operational and technological risks "upstream." This explains the role of the NIS2 Directive and the Cyber Resilience Act (CRA) Regulation within the European normative architecture and provides the foundation for the three-level model that will be analyzed in the following section. Accordingly, *resilience becomes a legal object* that cannot be achieved through a single instrument, but rather through the alignment of the functional level (the CER Directive) with the operational level (the NIS2 Directive) and the technological level (the CRA Regulation).

*3.3. The three-level model (entity-system-product) of CER-NIS2-CRA complementarity*

The current EU normative architecture in the field of critical infrastructure protection and resilience is characterized by a progressive and functional integration of the physical, organizational, and digital dimensions of risk, materialized in a coherent *three-level normative model: the level of the entity and the essential service, the level of the operational system and networks, and the level of the product and technology.* This structure reflects the recognition of the interdependencies between physical and digital infrastructures and the need for a normative intervention that covers the entire chain of systemic risk.

The *first level* is shaped by the CER Directive [10], which regulates the *issue of the resilience of critical entities* acting as providers of essential services. As shown in Chapter 2.4.4, the Directive operates within a predominantly physical and organisational register, establishing obligations relating to national risk assessments, the identification of critical entities, the adoption of resilience measures, the development of business continuity plans, periodic testing, and reporting and cooperation mechanisms. In this way, a legal framework has been created for *addressing resilience at the level of a socio-technological ecosystem*.

The *second level* is shaped by the NIS2 Directive [11], which provides a *strengthened legal framework for achieving a high common level of cybersecurity* of networks and information systems across the EU. As shown in Chapter 2.4.5, the NIS2 Directive is not strictly limited to the protection of digital infrastructures, but rather establishes an advanced framework for the governance of cybersecurity risks that may compromise the provision of vital services. The detailed obligations concerning risk management, supply chain security, business continuity, incident management, security testing and auditing, as well as the accountability of management bodies, *reflect a shift toward a consolidated approach to the cybersecurity* of network and information systems. In this regard, the NIS2 Directive represents a *transversal instrument for stabilizing* the level of cybersecurity across EU Member States.

In particular, in the *financial sector*, this logic is complemented by the sector-specific *lex specialis* regime established by the DORA Regulation [39]. This instrument does not add a "fourth level" to the model, but rather complements the operational requirements through detailed provisions on risk management, advanced testing, harmonised incident reporting, and the control of risks stemming from ICT third-party service providers. In this way, the *DORA Regulation limits the risk of overlap with the NIS2 Directive* in the financial domain and strengthens the resilience of this systemically important sector with high levels of cross-border interdependence.

The *third level* is introduced by the CRA Regulation [12], which focuses on the security of products and technologies used in critical infrastructures and essential services. As shown in Chapter 2.5.4, the CRA Regulation establishes mandatory security requirements "by design" and "by default" for products with digital elements, applicable throughout their entire life cycle, from design and development to vulnerability management. Through this approach, the Regulation intervenes "upstream", reducing structural risks generated by insecure or vulnerable products that may compromise operational systems and, ultimately, the continuity of essential services.

Overall, the complementarity between the CER Directive, the NIS2 Directive, and the CRA Regulation establishes an *integrated normative framework*, in which the CER Directive addresses resilience at the level of the entity and the essential service, the NIS2 Directive governs cybersecurity risks at the operational level, and the CRA Regulation reduces technological vulnerabilities at the product level. Although the scholarly literature and the institutional documents analysed do not explicitly formulate a unitary normative model structured on three levels, they converge in supporting the premises that underpin an integrated interpretation of the normative architecture [28, 33-35].

The integration of special sectoral regimes, such as the DORA Regulation, demonstrates the capacity of the European architecture to adapt this general model to the specificities of sectors with high systemic importance. At the same time, this normative complexity generates *challenges of legal and institutional interoperability*, including the risk of double reporting and the need for coordination among competent national authorities, making the effectiveness of the model essentially dependent on the conceptualisation of an integrated national governance of resilience.

Table 1 presents a CER-NIS2-CRA synopsis, offering a rapid and structured comparison of the three instruments by highlighting their regulatory object, scope of application, types of obligations, reporting mechanisms, and supervisory regimes, in order to facilitate an understanding of complementarity and areas of intersection within the European normative architecture of resilience.

**Table 1.** CER–NIS2–CRA Synopsis

| Criterion | CER Directive | NIS2 Directive | CRA Regulation |
|---|---|---|---|
| Type of act | Directive (national transposition) | Directive (national transposition) | Regulation (direct applicablity) |
| Object / purpose | Resilience of critical entities and continuity of essential services (physical + organizational focus, including hybrid risks) | Cybersecurity of networks and information systems (governance, measures, incident reporting) | Cybersecurity of products with digital elements "by design/by default" throughout the entire life cycle |
| Regulated unit | Critical entity + essential service | Entity (essential / important) + IT/OT systems and networks | Product (hardware/software/solution) + economic operators across the market supply chain |
| Scope (logic) | Systemic risk and cascading effects on societal functions | Operational cyber risk (organizational + supply chain + continuity) | "Upstream" technological risk: structural product vulnerabilities |
| Sectors / coverage | 11 critical sectors (energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, food) | "Essential" and "important" entities in high-importance sectors + other critical sectors (lists in annexes; broader coverage than CER) | Horizontal: products with digital elements placed on the EU market, with exclusions/derogations where sectoral regimes apply |
| Identification mechanism | Member States: national risk assessment → designation of "critical entities" | Largely based on size/sector + criteria; classification into "essential" vs. "important" | Does not "identify entities": sets compliance conditions for products + economic roles |
| Key obligations | Risk assessments; resilience measures; business continuity plans; management of incidents with significant impact; exercises/testing; cooperation and information sharing | Minimum risk management measures (policies, incident handling, continuity, supply chain security, testing/audit, cryptography, etc.); management body accountability; incident reporting requirements | Essential security requirements; vulnerability management; technical documentation; secure updates; obligations for manufacturers/importers/distributors; conformity assessment and marking (where applicable) |
| Reporting | Notifications/information to authorities in the event of significant incidents (within the logic of essential service resilience) | Detailed incident reporting regime (early warning + notification + final report; prescriptive deadlines) | Reporting of vulnerabilities /relevant product incidents (focus on actively exploited vulnerabilities and their management) |
| Supervision / authorities | National competent authorities + EU cooperation mechanisms | National authorities, CSIRTs, Cooperation Group; differentiated supervision (stricter for essential entities) | Market surveillance authorities + conformity control mechanisms (product-compliance logic) |
| Sanctions / enforcement | Established under national law (transposition) | Established under national law (transposition), with an orientation toward robust regimes | Direct applicability through market surveillance + sanctions set in national law for infringements (within the logic of the Regulation) |
| Relationship with the others | Complementary to NIS2: covers end-to-end resilience of services; does not replace cybersecurity requirements | Complementary to CER and operationally intersects many sectors; *lex specialis* applies in certain domains (e.g. financial) | Complementary to NIS2/CER: reduces "upstream" risk (insecure products) that feeds operational incidents and disruptions |

The comparative analysis highlights *three major areas of convergence*: a shared orientation toward risk management and the continuity of essential services, moving beyond the logic of point-based protection; complementarity across different layers of risk - the CER Directive at the level of the entity and the service, the NIS2 Directive at the operational and network level, and the CRA Regulation

"upstream," at the product level; and the strengthening of governance through obligations of assessment, reporting, and supervision, with an emphasis on prevention and accountability.

At the same time, the *following situations* of tension emerge: the risk of overlapping obligations and double reporting for highly digitalized critical entities; institutional fragmentation resulting from the multiplicity of competent authorities and supervisory regimes; and asymmetries in administrative capacity across EU Member States. These factors may lead to uneven implementation and to unequal systemic resilience.

At the procedural level, the complementarity of the CER-NIS2-CRA framework often gives rise to *operational tensions*, as the same factual situation may simultaneously trigger distinct legal obligations.

A *first typical scenario* is that of a cyber incident with operational effects within an entity operating in a critical sector (for example, energy or healthcare), where the compromise of an IT/OT system generates both a risk of interruption of an essential service and a significant cybersecurity incident. In such a situation, the logic of the CER Directive directs the response toward ensuring service continuity and notifying the incident to the competent authority responsible for the resilience of critical entities, while the NIS2 Directive activates a prescriptive reporting regime to the national competent authority/CSIRT, with distinct deadlines and formats. In the absence of internal coordination mechanisms (at the entity level) and institutional cooperation (at the national level), there is a risk that the same disruption will be reported in parallel, with partially redundant content, to different authorities, thereby increasing the administrative burden precisely at the moment when response capacity needs to be at its highest.

A *second relevant scenario* concerns the overlap between an operational incident and a product vulnerability. If the incident is facilitated by an exploited vulnerability in a widely used product with digital elements (for example, a software component integrated into control systems or digital infrastructure), a third procedural flow may be triggered: the reporting obligations associated with the CRA Regulation, aimed at notifying actively exploited vulnerabilities and relevant product-related incidents, in parallel with the reporting of the incident by users/operators under the provisions of the NIS2 Directive and with the management of the impact on service continuity under the provisions of the CER Directive. In this framework, a structural tension emerges: the NIS2 and CER Directives are centered on effects at the level of the entity and the service, while the CRA Regulation seeks to control risk "upstream," at the level of the product and economic operators. The lack of procedural articulation between these levels may lead to multiple notifications regarding the same situation, made by different actors (the user entity, the manufacturer, potentially supply chain providers).

A *third scenario*, frequently encountered in practice, arises from the existence of sector-specific *lex specialis* regimes, such as the DORA Regulation, in areas of high systemic importance. In the case of a financial institution subject to the Regulation, an ICT incident may trigger the harmonized reporting and testing regime, while the same entity may, in certain circumstances, also remain subject to the obligations of the NIS2 Directive, and its functioning may be relevant for the continuity of certain essential services within the meaning of the CER Directive.

In light of the foregoing, it can be observed that, despite the EU architecture's aim to *avoid overlaps* through *lex specialis* rules, the plurality of regulatory regimes and competent authorities may give rise, at the national level, to operational fragmentation (reporting to different authorities, partially convergent but procedurally distinct requirements). Consequently, the *issue of double reporting constitutes an inherent risk of multilevel governance*, which must be managed through explicit coordination mechanisms, procedural interoperability, and institutional cooperation.

### *3.4. Functional convergence between hard law and soft law instruments*

A structural element of the European normative architecture in the field of critical infrastructures is the *combination of hard law instruments* (directives and regulations) *with soft law instruments* (strategies, action plans, communications, recommendations). This combination is driven by the fact that primary competences in the field of infrastructure protection lie mainly at the national level - as evidenced by the provisions of the main hard law instruments presented in Chapter 2.4 and Chapter 2.5 - while the

diversity of risks and their administrative governance require a degree of flexibility that these instruments cannot fully provide.

*Soft law instruments*, such as the EU Cybersecurity Strategy for the Digital Decade [38], *function as mechanisms of guidance and integration,* providing a conceptual framework for the alignment of sectoral policies. They enable rapid adaptation to the evolution of threats and can operate as platforms for convergence among EU Member States, without imposing legal constraints. Moreover, these instruments *facilitate external cooperation and interoperability with international partners*, which is particularly important in a context where risks are transboundary and globalised.

However, *reliance on soft law instruments entails certain problematic aspects*, given their non-binding nature, which may lead to uneven implementation, gaps between necessity and capacity for action, or differences in the prioritization of risks. Accordingly, the role of soft law instruments should be understood as complementary - providing support and coordination - rather than as a substitute for binding rules.

Within the current normative architecture, *soft law instruments maximise their utility when they converge with hard law instruments*, contributing to the operationalisation of normative objectives, the reduction of fragmentation in implementation, and the consolidation of coherent governance of critical infrastructure resilience.

*3.5. Coherence, tensions, and structural limits of the normative architecture*

Despite the progress made in recent years, the *European normative architecture in the field of critical infrastructures remains marked by structural tensions*.

The *first tension* lies between the need for harmonization at the European level and national competences in the field of critical infrastructures [3, 15, 35]. This limitation is evident in the context in which the CER Directive retains a deliberately non-centralised and non-coercive nature, based on risk assessments and primary national responsibility.

The *second tension* concerns the *integration of physical and digital dimensions* and the risk of regulatory overlap [15, 28, 32]. Although the CER and NIS2 Directives are designed as complementary instruments, in practice the delineation between physical, organisational, and cyber measures may be difficult, particularly in sectors where infrastructure is highly digitalised (such as energy, transport, health, and digital infrastructure). This situation may generate the risk of formal compliance, whereby entities focus on fulfilling procedural requirements without achieving a genuine strengthening of their resilience.

The *third tension* relates to *asymmetries in capacities and resources* [1, 21, 22]. The current normative architecture presupposes the existence of competent national and European authorities capable of conducting complex risk assessments, supervising critical entities, managing reporting obligations, and coordinating incident responses. Given the significant differences among EU Member States in terms of institutional and administrative capacity, there is a risk of entrenching a "multi-speed resilience", in which levels of protection and response capacity remain uneven, ultimately affecting the systemic resilience of the EU.

Finally, a *structural limitation* is determined by the *systemic nature of contemporary risks* [20, 24, 25]: global supply chains, dependence on third-party providers, interdependencies among infrastructures, and the uncertainty associated with emerging risks (technological and climatic) reduce the capacity for anticipatory regulation of vulnerabilities. Under these conditions, the effectiveness of the normative architecture depends not only on the quality of the legal norms, but also on institutional capacities for learning, adaptation, and cooperation among states, agencies, and the private sector in the management of critical infrastructures.

Overall, the European normative architecture for the protection and resilience of critical infrastructures is characterised both by a *significant increase in coherence* and by the *integration of physical and digital dimensions*. It nevertheless remains conditioned by the structural tension between integration and sovereignty, by the risk of fragmentation resulting from uneven implementation, and by the complexity of contemporary systemic risks.

## 4. Limitations of the study

Although this study pursues a broad and integrated analysis of the EU normative framework on the protection and resilience of critical infrastructures, it is subject to *explicitly acknowledged methodological and analytical limitations*, which stem both from the object of the research and from the constraints necessary to maintain the coherence and depth of the analysis.

A *first limitation* arises from the *predominantly legal-doctrinal and systemic nature of the approach*, which prioritises the analysis of legal norms and governance mechanisms established at EU level, to the detriment of an empirical assessment of their implementation at national level. The study does not include detailed comparative analyses of the transposition of the CER and NIS2 Directives into the domestic law of the Member States, nor does it provide evaluations based on operational data concerning the concrete effectiveness of resilience measures. Consequently, the conclusions primarily address the coherence and normative potential of the European architecture, rather than its practical outcomes.

A *second limitation* is determined by the *relatively early stage of application of the normative framework under analysis.* A significant part of the core instruments (the CER and NIS2 Directives and the CRA Regulation) are either in the process of transposition or in the initial stages of implementation, and for some of them - particularly the CRA Regulation - there is as yet no consolidated implementation experience or relevant case law. This situation limits the possibility of formulating definitive conclusions regarding the actual impact of the normative architecture on the reduction of systemic risks and cascading effects.

*Thirdly*, the study does not address in depth *parallel or related legal regimes*, such as EU criminal law concerning attacks against information systems, NATO regimes for the protection of critical infrastructures, or mechanisms of cooperation with intelligence agencies. Although these areas are relevant to critical infrastructure resilience, their inclusion would have exceeded the proposed analytical framework and diluted the focus on the EU's normative legal architecture.

*Another limitation* relates to the *complexity of the concept of resilience*, which combines legal, technical, organisational, and societal dimensions. The present study addresses the resilience of critical infrastructures predominantly as an object of legal regulation and public governance, without engaging in a detailed examination of their technical dimensions, which may influence the perception of the adopted approach.

*Finally,* the analysis is *constrained by the accelerated dynamics of issues related to critical infrastructures*, characterised by rapid technological developments, the emergence of new threats (including those related to artificial intelligence, automation, and other emerging technologies), and continuous normative adjustments. The conclusions therefore reflect the current normative stage at EU level and may require revision as the regulatory framework is further developed or adjusted.

*These limitations do not diminish the relevance of the study*; rather, they define its scope of validity and may serve as directions for future research, oriented towards analysing the implementation of the normative framework governing the protection and resilience of critical infrastructures at EU level or within the Member States.

## 5. Conclusions

The present study was conducted on the basis of the working hypothesis established and the objectives O1-O3 formulated in the introductory chapter, with the *aim of assessing the coherence and functionality of the EU normative framework governing the protection and resilience of critical infrastructures*. The analysis highlights the transition from a sectoral approach to an integrated model oriented towards resilience, the management of systemic risks, and the continuity of essential services.

With regard to *Objective O1*, which is dedicated to mapping the evolution of the normative framework at the EU level in the field of critical infrastructures, the study has identified a *clear transition from a fragmented and sectoral framework* - crystallised around the EPCIP and Directive 2008/114/EC - *towards an integrated architecture* oriented towards resilience and the management of systemic risks, as reflected in the CER and NIS2 Directives and the CRA Regulation. This evolution reflects not only an expansion of the scope and legal instruments, but also a profound conceptual shift in this area.

As regards *objective O2*, the integrated analysis of the current normative architecture made it possible to identify a coherent internal logic based on the *functional complementarity of the core instruments*. Conceptualizing the CER-NIS2-CRA triad as a three-level normative model - entity/essential service, operational system/network, and product/technology - provides a systemic interpretative framework for European normative intervention. The CER Directive strengthens the organizational and physical resilience of critical entities, the NIS2 Directive establishes an advanced regime of cybersecurity risk governance at the operational level, and the CRA Regulation shifts security responsibility "upstream" to manufacturers, through mandatory "by design" cybersecurity requirements throughout the entire life cycle of digital products. The integration of special sectoral regimes, such as the DORA Regulation, demonstrates the model's capacity to be adapted to sectors of high systemic importance.

In relation to *objective O3*, the critical assessment of the structural limits of the normative architecture highlighted the *persistence of several tensions*. The first concerns the balance between European harmonization and national competences, which explains the retention of a significant degree of flexibility in the CER Directive. The second tension derives from physical-digital integration, which, although necessary to address hybrid risks, generates the risk of overlapping obligations, double reporting, and institutional fragmentation. The third limitation consists of asymmetries in administrative and operational capacity among Member States, which may lead to uneven implementation and, implicitly, to a "multi-speed resilience" at EU level.

With regard to the working *hypothesis formulated* in the introduction, the overall conclusion of the study is that the current EU normative architecture, in principle, establishes a *coherent and complementary framework for the protection and resilience of critical infrastructures/entities*. This coherence stems from the alignment of objectives, the shared orientation toward risk management and the continuity of essential services, and the coverage of different layers of physical and digital risk. However, this coherence is predominantly normative and conceptual in nature, with its practical effectiveness being contingent upon national-level implementation and the institutional capacity of EU Member States.

Overall, the study shows that the EU has made *significant progress in the governance of critical infrastructures*, by moving from a fragmented normative framework to an integrated architecture oriented toward resilience and systemic risk management. Nevertheless, the success of this model does not depend solely on the quality of the adopted rules, but essentially on the ability of EU Member States to transpose and apply the requirements coherently, to design and operationalize integrated national coordination mechanisms, and to ensure effective cooperation among authorities, operators, and producers.

By explicitly relating to the working hypothesis and the stated objectives, the *conclusions confirm the study's theoretical and analytical contribution* by providing a systemic analysis of the CER-NIS2-CRA triad as a normative model of European resilience, thereby creating the premises for future research focused on examining the practical implementation of the normative framework at the level of EU Member States, assessing its impact on the reduction of systemic risks, and adapting the normative framework to emerging threats in the decades to come.

**References**

[1]. Sommerer, N., Schauer, S., Latzenhofer, M., & Schnabl, A. (2025, May). How Critical is Critical? Towards a Decision Framework for Disaster-specific Critical Entities. In *Proceedings of the International ISCRAM Conference*.

[2]. Greiving, S., Terfrüchte, T., Fleischhauer, M., Hartz, A., & Furkert, M. (2025). Services of general interest and critical infrastructures: interdependencies and implications for resilience and territorial cohesion. *European Planning Studies*, *33*(3), 329-351.

[3]. Becker, M. (2025). Transposing EU-Legislation on Critical Infrastructure Protection Legal Implementation Performance in the Baltic Sea Region. *International Journal of Critical Infrastructure Protection*, 100781.

[4]. European Commission. (2025). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on*

*ProtectEU - A European internal security strategy* (COM(2025) 148 final). Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0148

[5]. Council of the European Union. (2024). *Hybrid threats and the EU response*. https://www.consilium.europa.eu/en/policies/hybrid-threats/

[6]. European Commission, Joint Research Centre. (2023). *Strengthening EU resilience to hybrid threats and critical entities*. https://joint-research-centre.ec.europa.eu/projects-and-activities/strengthening-eu-resilience-hybrid-threats-and-critical-entities_en

[7]. Barichella, A. (2022, September). *Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe* (Policy Paper No. 281). Jacques Delors Institute. https://institutdelors.eu/content/uploads/2025/04/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf

[8]. European Union. (2016). *Shared vision, common action: A stronger Europe - A global strategy for the European Union's foreign and security policy*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/3eaae2cf-9ac5-11e6-868c-01aa75ed71a1

[9]. Council of the European Union. (2022). *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security*. Publications Office of the European Union. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

[10]. European Union. (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*. *Official Journal of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

[11]. European Union. (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)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[12]. European Parliament & Council. (2024). *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*, *Official Journal of the European Union*, L 2847. https://eur-lex.europa.eu/eli/reg/2024/2847/2024-11-20/eng

[13]. European Commission. (2006). *Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP)* [COM(2006) 786 final]. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0786

[14] Council of the European Union. (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* (OJ L 345, pp. 75–82). *EUR-Lex*. https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng

[15]. Pursiainen, C., & Kytömaa, E. (2023). *From European critical infrastructure protection to the resilience of European critical entities: What does it mean?* Sustainable and Resilient Infrastructure, 8(5), 1–15. https://doi.org/10.1080/23789689.2022.2128562

[16]. Rød, B., Lange, D., Theocharidou, M., & Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering*, *36*(4), 04020039.

[17]. Theocharidoui, M., Galbuserai, L., & Giannopoulosi, G. (2018). Resilience of critical infrastructure systems: Policy, research projects and tools. *Domains of resilience for complex interconnected systems.*, 147.

[18]. Renda, A., & Haemmerli, B. (2010). Protecting critical infrastructure in the EU: CEPS task force report.

[19]. Carrera, S., & Den Hertog, L. (2016). A European Border and Coast Guard: What's in a name? *CEPS paper in liberty and security in Europe*.
[20]. Organisation for Economic Co-operation and Development. (2014). *Boosting resilience through innovative risk governance*. OECD Reviews of Risk Management Policies. https://doi.org/10.1787/9789264209114-en
[21]. Boin, A., Busuioc, M., & Groenleer, M. (2014). *Building European Union capacity to manage transboundary crises: Network or lead-agency model?* Regulation & Governance, 8(4), 418–436.
[22]. Knodt, M., Fraune, C., & Engel, A. (2022). *Local governance of critical infrastructure resilience: Types of coordination in German cities.* Journal of Contingencies and Crisis Management, 307–316.
[23]. Blondin, D., & Boin, A. (2020). Cooperation in the face of transboundary crisis: A framework for analysis. *Perspectives on Public Management and Governance*, *3*(3), 197-209.
[24]. Gim, C., & Miller, C. A. (2022). Institutional interdependence and infrastructure resilience. *Current Opinion in Environmental Sustainability*, *57*, 101203.
[25]. Sonesson, T. R., Johansson, J., & Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety science*, *142*, 105383.
[26]. European Union. (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 (NIS Directive)*. *Official Journal of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148
[27]. Mentzelou, K., Chountalas, P. T., Kitsios, F. C., Magoutas, A. I., & Dasaklis, T. K. (2025). Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity and Privacy*, *5*(4), 97.
[28]. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890.
[29]. Ruohonen, J. (2024). A Systematic Literature Review on the NIS2 Directive. *arXiv preprint arXiv:2412.08084*.
[30]. European Union Agency for Cybersecurity. (2025, June). *Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of the NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures* (Version 1.0). https://www.enisa.europa.eu/publications/technical-implementation-guidance-on-commission-implementing-regulation-eu-2024-2690
[31]. European Union Agency for Cybersecurity (ENISA). (2025). *NIS Investments 2025*. ENISA. https://www.enisa.europa.eu/publications/nis-investments-2025
[32]. Teichmann, F. (2025). The cyber resilience act as a new paradigm for product security: a compliance roadmap. *International Cybersecurity Law Review*, 1-17.
[33]. Chiara PG. Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? *European Journal of Risk Regulation*. 2025;16(2):469-484.
[34]. Teichmann, F. M. J. (2026). Platform governance under NIS2 and the Cyber Resilience Act: cybersecurity by design as social practice. *Information, Communication & Society*, 1-14.
[35]. European Commission. (2020). *Impact Assessment accompanying the proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities* (SWD(2020) 358 final). Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0358
[36]. European Commission. (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* (SWD/2020/345 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345

[37]. European Commission. (2022). *Commission staff working document: Impact assessment report accompanying the document proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (SWD/2022/282 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0282

[38]. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020). *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade* [JOIN(2020) 18 final]. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018

[39]. European Parliament & Council. (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* (Digital Operational Resilience Act). *Official Journal of the European Union, L 333*, 1–79. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554

[40]. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector* (Text with EEA relevance) (OJ L 333, 27.12.2022, p. 153). *EUR-Lex*. https://eur-lex.europa.eu/eli/dir/2022/2556/oj

[41]. European Parliament & Council of the European Union. (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* (Text with EEA relevance) (OJ L 151, 7.6.2019, pp. 15–69). *EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2019/881/oj

[42]. European Commission. (2021). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'Fit for 55': delivering the EU's 2030 climate target on the way to climate neutrality* (COM(2021) 550 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0550

[43]. Directorate-General for Energy [European Commission]. (2025). *Action Plan for Affordable Energy: Unlocking the true value of our Energy Union to secure affordable, efficient and clean energy for all Europeans*. https://energy.ec.europa.eu/publications/action-plan-affordable-energy-unlocking-true-value-our-energy-union-secure-affordable-efficient-and_en