# GOVERNING CRITICAL INFRASTRUCTURE RESILIENCE IN THE EUROPEAN UNION: THE EVOLUTION AND LIMITS OF THE INSTITUTIONAL FRAMEWORK

**PEPTAN CĂTĂLIN**
*LECTURER, PHD, "CONSTANTIN BRÂNCUŞI" UNIVERSITY OF TÂRGU-JIU, ROMANIA*
*ORCID: 0000-0002-3424-2812*
*e-mail: catalinpeptantm@gmail.com*

***Abstract***

*The study examines the transformation of the European Union's (EU) governance framework in the field of critical infrastructure resilience, in the context of the proliferation of hybrid risks characterized by physical-digital interdependencies. Starting from the premise that contemporary threats can no longer be conceptualized as distinct phenomena, the study explores how the new normative instruments - particularly Directives (EU) 2022/2557 (CER) and (EU) 2022/2555 (NIS2) - respond to a risk landscape characterized by systemic interdependencies and cascading effects.*

*Methodologically, the study combines an institutional and legal analysis of the European architecture for the protection and resilience of critical infrastructures with a functional assessment based on hypothetical hybrid crisis scenarios. This approach enables the identification of persistent operational gaps between sectoral responsibilities, levels of governance, and coordination mechanisms. The study's main contribution lies in proposing an integrated analytical framework for assessing the EU's capacity to manage interconnected physical-digital risks, while highlighting the limitations of the current fragmented governance model.*

*The study argues that, despite recent normative advances, the resilience of critical infrastructures remains constrained by a deficit in operational coordination and by insufficient integration between cybersecurity policies, civil protection, and crisis management. In conclusion, the study underscores the need to strengthen forms of hybrid governance capable of overcoming traditional sectoral divisions and enabling a systemic approach to complex risks at the European level.*

***Keywords:*** *critical infrastructures; protection; resilience; multilevel governance.*

***JEL Clasification****: H12; H54; H56*

## 1. Introduction

### 1.1. General premises

The EU's institutional framework for the protection and resilience of critical infrastructures is the result of an evolutionary process of intersectoral integration between security policies, civil protection, digitalization, and risk management, driven by the transboundary and systemic nature of contemporary threats. Although Member States retain primary competences in the field of national security, in accordance with the TEU [1, Art. 4(2)], the EU has progressively developed a multilevel governance architecture aimed at ensuring coherence, coordination, and complementarity of national actions in situations of risk or crisis with cross-border impact.

This architecture is grounded in the principle of subsidiarity, combined with mechanisms of European solidarity in crisis management, and involves a set of institutional actors and cooperation mechanisms. At the political and normative level, central roles are played by the European Commission, the Council of the European Union, and the European Parliament, while at the technical and operational level specialized agencies and structures are involved, such as the European Union Agency for Cybersecurity (ENISA) [2], the Computer Emergency Response Team for the EU institutions (CERT-EU) [3], and the Emergency Response Coordination Centre (ERCC) [4].

Complementarily, the European institutional architecture includes platforms and formal mechanisms of cooperation established through sector-specific legal instruments, such as the Cooperation Group and the CSIRT Network under the regime set by the NIS [5] / NIS2 [6] Directives, as

well as the coordination mechanisms provided by the CER Directive on the resilience of critical entities [7], which facilitate information sharing, strategic coordination, and public-private dialogue. Overall, this framework reflects the transition from a fragmented, predominantly national approach to an integrated model of European governance of critical infrastructure resilience, tailored to the interdependent nature of physical and digital risks.

### 1.2. Research hypothesis, objectives, and contribution of the study

***Research hypothesis.***

The research is structured around the following ***hypothesis (H)*** - *The EU's institutional architecture in the field of critical infrastructure protection and resilience is characterized by a structural gap between normative initiatives and operational coordination capacity*, a gap driven by the predominantly non-coercive nature of EU instruments and by the distribution of competences between the European level and that of the Member States.

Although the EU has developed, particularly since 2022, a coherent normative framework - materialized mainly through the CER and NIS2 Directives - these developments have not eliminated the structural constraints related to institutional interoperability, decision-making synchronization, and the management of cascading effects in situations of hybrid and cross-border crisis.

The central hypothesis of the study argues that the effectiveness of European resilience governance does not depend decisively on the expansion of coercive competences at the EU level, but rather on the ability of existing mechanisms to function as instruments of institutional orchestration, based on cooperation, procedural interoperability, information sharing, and institutional learning.

***Research objectives.***

***General research objective (G.O.)*** - *To analyse and evaluate the EU's institutional architecture in the field of critical infrastructure protection and resilience, from the perspective of its capacity to manage complex, hybrid, and cross-border risks within a multilevel governance framework shaped by legal and political constraints related to Member State sovereignty.*

In order to achieve this general objective, the study pursues the following ***specific objectives***:

**O1.** *Mapping the EU-level institutional framework* relevant to the protection and resilience of critical infrastructures, with a focus on the roles and competences of the main European institutional actors and on the mechanisms established by the CER and NIS2 Directives.

**O2.** *Analysing the functional logic of the EU's institutional architecture* by identifying the levels of governance (normative-strategic, political-institutional coordination, and technical-operational) and the relationships between them.

**O3.** *Assessing the degree of integration of the physical and digital dimensions of resilience* within EU policies and mechanisms, particularly in the context of hybrid risks and sectoral interdependencies.

**O4.** *Identifying the structural limitations of the EU's non-coercive governance model*, with an emphasis on institutional interoperability, information sharing, decision-making temporality, and the management of cascading effects.

**O5.** *Functionally testing the institutional architecture* through the application of a qualitative evaluation matrix to relevant crisis scenarios, designed to highlight the actual capacity for coordination under conditions of operational pressure.

**O6.** *Formulating analytical conclusions* regarding the operating conditions and long-term sustainability of EU resilience governance, with relevance for both academic research and public policymaking.

***Contribution of the study.***

The contribution of the study is *theoretical, analytical, and methodological*, situated at the intersection of European studies, public policy analysis, and risk governance.

From a *theoretical perspective*, the research contributes to the conceptualization of critical infrastructure protection as an *issue of resilience governance*, rather than exclusively as a field of

sectoral security or technical risk management. The study integrates concepts such as multilevel governance, governance by orchestration, systemic risks, and hybrid crises, offering an analytical framework applicable to other areas of EU policy as well.

From an *analytical perspective*, the study proposes a *qualitative evaluation matrix* of the EU's institutional architecture, which enables a functional assessment of coordination capacity beyond the formal description of competences. Applying this matrix to crisis scenarios contributes to the identification of recurring patterns of institutional vulnerability and of the conditions under which non-coercive cooperation can become effective.

From a *methodological perspective,* the study demonstrates the usefulness of scenario-based analysis as an instrument of institutional assessment in a field characterized by limited access to operational data for security-related reasons.

### 1.3. Research methodology

The research is based on a *qualitative, interdisciplinary, and multi-method analysis*, specific to a field - the protection and resilience of critical infrastructures - characterized by institutional diversity, sectoral interdependencies, and limitations in access to operational empirical data.

***The research design*** is structured around an *institutional and functional analysis* of the EU framework for critical infrastructure protection. The study combines legal-institutional analysis with functional evaluation tools, aiming to move beyond a purely descriptive level and to examine how institutional mechanisms may operate effectively in crisis situations.

***The methods and instruments used*** are articulated as follows:

*Documentary and legal analysis*, employed to examine EU Treaties, relevant legislation (in particular the CER and NIS2 Directives), European strategic documents, reports of EU agencies, specialized academic literature, and soft law instruments. This method allows for the identification of the normative framework, institutional competences, and formal cooperation mechanisms.

*Comparative institutional analysis*, applied to identify the roles, functions, and relationships among actors involved at different levels of governance, as well as to highlight asymmetries between the normative and operational levels.

*Construction of a "qualitative evaluation matrix"*, which operationalizes the analysis of the institutional architecture through a set of functional criteria and indicators (clarity of roles, interoperability, information sharing, decision-making temporality, physical-digital integration, management of cascading effects, and institutional learning).

*Scenario analysis,* used as the main instrument for the functional testing of the institutional architecture. The scenarios are designed to reflect plausible hybrid crises, characterized by sectoral interdependencies and the overlap of physical and digital dimensions, enabling the assessment of institutional flows and friction points under conditions of operational pressure.

***Methodological justification*.** The choice of these methods is justified by the *impossibility to access sensitive operational data* related to incidents in the field of critical infrastructures. In this context, scenario analysis and qualitative evaluation provide an appropriate methodological framework for examining potential institutional capacities and the structural limits of EU governance.

***Methodological delimitations*.** The study focuses on *governance at the EU level*, without developing in-depth national case studies, and does not seek to quantitatively measure institutional performance. The results should be interpreted as analytical assessments of the capacities and structural constraints of the institutional architecture, rather than as operational evaluations of performance in real incidents.

### 1.4. Review of the specialized literature

The specialized literature on the protection of critical infrastructures and their resilience at the EU level is extensive, interdisciplinary, and continuously evolving, reflecting the complexity of the field and the diversity of contemporary threats. It brings together contributions from security studies, public policy analysis, European studies, risk governance, and, more recently, from literature dedicated to systemic resilience and hybrid crises. Despite this thematic diversity, the literature remains fragmented, often structured along sectoral lines (energy, transport, cybersecurity) or around the traditional distinction between physical and digital security.

***Security - and risk management-centered approaches.*** The earliest relevant contributions in the field of critical infrastructures were characterized by a *classical security logic*, focused on physical protection, the prevention of sabotage, and the reduction of vulnerabilities to deliberate threats. The literature at this stage addresses critical infrastructures as strategic assets, whose protection constitutes a responsibility of the state, explicitly assumed within national security policies. The studies focus on identifying critical sectors, assessing risks, and developing protection measures proportional to the level of threat [8-11].

Subsequently, with the increase in the frequency of natural and technological disasters, the literature addressed issues specific to risk *management and civil protection*, placing emphasis on the continuity of essential functions and on post-crisis recovery capacity [12-14]. This transition marked an initial conceptual evolution; however, approaches largely remained sectoral and were treated from the perspective of national-level responsibility, with limited attention paid to the European dimension of institutional coordination.

***Literature on resilience and systemic risks.*** A second important body of literature is represented by studies dedicated to resilience, a concept that has experienced accelerated development over the past two decades. Within this framework, critical infrastructures are analyzed as components of complex socio-technical systems, characterized by interdependencies, non-linearity, and the potential emergence of cascading effects. The literature on systemic risks emphasizes that local disruptions can generate disproportionate consequences, exceeding the management capacity of individual actors [15-18].

Although these contributions provide a solid conceptual framework for understanding the vulnerabilities of critical infrastructures, they often focus on the technical and functional dimensions of resilience, *paying relatively limited attention to the institutional and governance mechanisms* through which resilience is built and maintained. Consequently, resilience-focused literature explains well why infrastructures are vulnerable, but less so how political and institutional responses are coordinated at the supranational level.

***Contributions from European studies and multilevel governance.*** The literature in this field offers a third set of relevant perspectives through the analysis of *multilevel governance* and the distribution of competences between the EU and the Member States. Numerous authors highlight the legal and political constraints that limit the EU's ability to act coercively in sensitive domains such as national security and the protection of essential infrastructures. In this context, the EU is conceptualized as an actor with a coordinating, standard-setting, and facilitating role, rather than as an operational authority [19-23].

Studies dedicated to European cybersecurity and civil protection policies highlight the emergence of *forms of governance based on networks, cooperation, and soft law*, which allow for the integration of national capacities without a formal transfer of sovereignty. However, some analyses tend to focus either on a single normative instrument (for example, the NIS/NIS2 Directive) or on a single institutional dimension, without providing an integrated assessment of the European architecture as a whole [24-26].

***Literature on hybrid crises and physical–digital integration.*** An emerging strand of the literature is *dedicated to hybrid threats*, highlighting the blurring of boundaries between traditional conflicts, cyberattacks, infrastructural sabotage, and information manipulation. These studies highlight that critical infrastructures constitute preferred targets of hybrid strategies, precisely because of their central role in the functioning of modern societies [27-30]. Although the combined nature of physical and digital vectors is explicitly acknowledged, the analytical integration of these dimensions remains limited. Approaches are often parallel: cybersecurity is predominantly treated from a technical and normative perspective, while the protection of physical infrastructures is analyzed through the lens of functional resilience and civil protection. Institutional mechanisms capable of ensuring convergence and systematic coordination between these domains are rarely addressed in a coherent manner.

***Identified gaps and positioning of the study.*** The analysis of the specialized literature reveals three major gaps. First, there is *analytical fragmentation* among sectoral approaches, which limits the ability to capture interdependencies and cascading effects among critical infrastructures. Second, the literature pays insufficient attention to the *concrete functioning of the European institutional architecture*, focusing either on normative analysis or on the technical dimension of resilience. Third, *physical-digital integration* is treated more as a declarative objective than as a problem of institutional design and operational coordination.

The present study positions itself at the intersection of these research directions, proposing an integrated analysis of the European institutional architecture for the protection of critical infrastructures from the perspective of resilience governance. By employing the concepts of *multilevel governance* and *governance by orchestration*, by constructing an *qualitative evaluation matrix*, and by *functionally testing* existing mechanisms through hybrid crisis scenarios, the research contributes to overcoming the fragmentation of the literature and to a more nuanced understanding of the potential and limitations of the European model.

## 2. Institutions involved in the protection and resilience of critical infrastructures

### 2.1. The European Commission

The European Commission plays a central role, within the limits of the competences conferred by the Treaties, in defining, coordinating, and monitoring EU policies on the protection and resilience of critical infrastructures, acting as a legislative initiator, political coordinator, and supervisor of implementation at the level of the Member States. Its activity is structured through several sectoral or transversal Directorates-General, with support or coordination functions, each having specific responsibilities.

Within the category of ***sectoral Directorates-General*** are included:

***Directorate-General for Migration and Home Affairs*** (DG HOME) [31] - is responsible for the development and coordination of EU policies in the field of internal security, including cybersecurity, the protection of critical infrastructures, and cooperation among Member States for the management of cross-border risks.

***Directorate-General for Communications, Networks, Content and Technology*** (DG CONNECT) [32] - develops and implements digital policies aimed at preparing Europe for the digital age, areas such as digital infrastructure, cybersecurity, regulation of digital markets, and the promotion of cutting-edge technologies, thereby contributing to increased digital resilience and to strengthening the EU's Digital Single Market.

***Directorate-General for Energy*** (DG ENERGY) [33] - develops and coordinates EU policies in the energy sector, including security of energy supply, the integration of energy markets, and the transition to clean and efficient energy sources, thereby contributing to the resilience of the European energy system within the framework of EU energy and climate policies.

***Directorate-General for Mobility and Transport*** (DG MOVE) [34] - is responsible for the development and implementation of EU policies in the field of mobility and transport, aiming to

build a safe, efficient, sustainable, and interconnected European transport system. Through its mandates, it contributes to the sectoral resilience of critical transport infrastructures within the framework of European mobility and infrastructure policies.

***Directorate-General for European Civil Protection and Humanitarian Aid Operations*** (DG ECHO) [35] - is responsible for coordinating the EU response to emergencies and crises by managing civil protection and humanitarian aid policies and mechanisms, mobilized both within the EU and internationally, with a view to preventing, mitigating, and managing the consequences of disasters and major crises.

***Directorate-General for Health and Food Safety*** (DG SANTE) [36] - plays a direct sectoral role in the protection and resilience of critical infrastructures in the fields of health and food safety, through the development and coordination of EU policies on public health, the prevention and management of cross-border health threats, and the assurance of the continuity of essential food supply chains.

***Directorate-General for Environment*** (DG ENV) [37] - develops and coordinates EU environmental policies, having a direct sectoral role in strengthening the resilience of critical infrastructures, in particular drinking water and wastewater infrastructures, by integrating the prevention and management of environmental risks into the European regulatory framework.

***Directorate-General for Internal Market, Industry, SMEs*** (DG GROW) [38] - is responsible for policies related to the internal market, industry, and supply chains, having an indirect sectoral role in the protection and resilience of critical infrastructures by strengthening industrial capacities, product safety, and the resilience of supply chains for essential goods and technologies.

***Directorate-General for Climate Action*** (DG CLIMA) [39] - develops and coordinates EU policies in the field of climate action, having a transversal role in strengthening the resilience of critical infrastructures by integrating climate risk assessment and management into relevant sectoral policies, particularly for infrastructures exposed to the effects of climate change.

Within the category of ***Directorates-General with a transversal, support, or coordination role*** are included:

***Directorate-General for Research and Innovation*** (DG RTD) [40] - plays a transversal support role in the protection and resilience of critical infrastructures by supporting research and innovation in the fields of security, risk management, and the development of advanced technologies relevant for adapting critical infrastructures to emerging threats.

***Directorate-General for Defence Industry and Space*** (DG DEFIS) [41] - fulfills a strategic sectoral role in the protection and resilience of critical infrastructures in the space domain by managing EU policies on space and the defence industry and by strengthening strategic autonomy and the continuity of essential satellite services, which are explicitly recognized as critical sectors.

In addition, the European Commission monitors the transposition and implementation of the CER and NIS2 Directives at the level of EU Member States, assesses national resilience reports, and ensures coherence between sectoral policies and horizontal policies related to security and the continuity of essential services.

## 2.2. The European Parliament

The European Parliament plays an essential role in the EU's institutional architecture in the field of protection and resilience of critical infrastructures, primarily through its legislative, democratic oversight, and political guidance functions, as follows:

***Legislative function.*** Pursuant to the Treaty on European Union (TEU) [1, Art. 14(1)], the European Parliament acts as a co-legislator, alongside the Council of the European Union, within the ordinary legislative procedure provided for by the Treaty on the Functioning of the European Union (TFEU) [42, Art. 289], participating in the adoption of legal acts relevant to the protection and resilience of critical infrastructures. Within this framework falls the Parliament's contribution to the adoption of the CER Directive [7] and the NIS2 Directive [6], as well as of other related in-

struments in the field of cybersecurity and digital resilience. Through the amendments it proposes and the positions it adopts, the European Parliament influences the substance of the norms, seeking to clarify the obligations of EU Member States, ensure the proportionality of security measures, and integrate requirements concerning the protection of fundamental rights.

***Democratic scrutiny and oversight of EU policies.*** Pursuant to the provisions of the TEU [1, Article 14(1)] and the TFEU [42, Article 230], the European Parliament exercises democratic control over the manner in which the European Commission designs and implements policies on the protection and resilience of critical infrastructures. This role is carried out through hearings, parliamentary questions, evaluation reports, and plenary debates on the application of European legislation, as well as through monitoring the transposition and implementation of the CER and NIS2 Directives at the level of the Member States. In this context, the Parliament contributes to maintaining a balance between security objectives, the continuity of essential services, and respect for the rule of law.

***Functions of specialized parliamentary committees.*** The activity of the European Parliament in the field of critical infrastructures is structured mainly through specialized parliamentary committees, which ensure thematic expertise and continuity of political oversight. A central role is played by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) [43], which is competent in matters of internal security, the protection of fundamental rights, justice, and home affairs, and which oversees resilience policies from the perspective of their impact on civil liberties and democratic governance, as enshrined in the TEU [1, Articles 2 and 6]. Complementarily, the Committee on Industry, Research and Energy (ITRE) [44] contributes to addressing the sectoral dimensions of critical infrastructures, in particular in the fields of energy, transport, digital infrastructure, and the internal market, playing a relevant role in aligning security objectives with those of competitiveness and the energy transition. Last but not least, the Subcommittee on Security and Defence (SEDE) [45] addresses the strategic and defence dimension of critical infrastructures.

***Political guidance and strategic orientation function.*** In addition to its legislative role, the European Parliament shapes EU policies in the field of the protection and resilience of critical infrastructures through resolutions, reports, and political positions. These instruments, adopted pursuant to its representative function as provided for by the TEU [1, Art. 10(2)], promote an integrated approach to resilience that encompasses physical, digital, societal, and environmental dimensions, as well as the need for cooperation at the European and international levels.

***Function of integrating the fundamental rights dimension.*** An important contribution of the European Parliament consists in integrating the fundamental rights dimension into policies concerning critical infrastructures. Through its legislative and oversight activities, the Parliament seeks to ensure that security and resilience measures are compatible with the protection of privacy, personal data, civil liberties, and the principles of the rule of law.

At the same time, the European Parliament supports the ***development of a European financial framework dedicated to investments in resilience***, using budgetary instruments and multiannual programming to integrate security and risk-adaptation objectives into the EU's recovery and innovation policies. In this regard, through the exercise of its budgetary and political oversight powers, pursuant to the provisions of the TEU [1, Art. 14(1)] and the TFEU [42, Art. 314], the Parliament has supported the allocation of resources, through the Recovery and Resilience Facility (RRF) [46], for the modernization of essential infrastructures, the strengthening of the resilience of energy, digital, and health systems, and the reduction of structural vulnerabilities highlighted by recent crises. Complementarily, the Parliament supports the implementation of the Horizon Europe programme [47] as a strategic instrument for financing research and innovation in the fields of security, risk management, and the development of advanced technologies aimed at enhancing the resilience of critical infrastructures, thereby contributing to the implementation of an integrated approach that links public investment, technological innovation, and the EU's resilience objectives.

## 2.3. The Council of the European Union

The Council of the EU plays a central role in the field of the protection and resilience of critical infrastructures, primarily through its legislative functions and its role in coordinating the policies of the Member States, as follows:

***Legislative function.*** The co-legislative function of the Council of the EU is exercised jointly with the European Parliament, pursuant to the provisions of the TEU [1, Art. 16] and the TFEU [42, Art. 289]. Through its participation in the ordinary legislative procedure, it contributes directly to the adoption of the binding regulatory framework applicable to the Member States in the field of the protection and resilience of critical infrastructures. Particularly relevant is its contribution to the adoption of the CER Directive and the NIS2 Directive, which constitute the main pillars of the European security and resilience architecture.

Within the legislative process, the Council of the EU represents the interests of the Member States and acts as the principal forum for negotiation, in which differences in administrative capacity, levels of risk, strategic priorities, and normative approaches are reconciled. It also plays an essential role in balancing protection and resilience objectives with national competences in the field of national security, as enshrined in the TEU [1, Art. 4(2)].

The negotiations conducted within the Council of the EU have had a significant influence on the delineation of the scope of the adopted legal acts, on the degree of harmonization imposed on the Member States, and on the design of the coordination mechanisms established by the CER and NIS2 Directives. In this respect, the Council has contributed to the establishment of a predominantly non-coercive approach, based on risk assessments, cooperation, information exchange, and primary national responsibility, avoiding the direct transfer of operational competences to the EU level. This option reflects a structural compromise between the need for strengthened European action and respect for the prerogatives of the EU Member States.

***Policy coordination function of EU Member States.*** On the basis of the TEU [1, Article 16(1)], the Council of the EU exercises policy coordination functions among the Member States, including in crisis situations. This role is implemented through the adoption of conclusions and other soft law instruments, in accordance with the TFEU [42, Article 292], which express common positions and guide the action of EU institutions. In contexts of crises with cross-border impact - such as major disruptions of energy infrastructures, large-scale cyberattacks, or emergency situations with cascading effects - the Council of the EU facilitates the alignment of national responses and the strengthening of European solidarity, without substituting the operational competences of the Member States.

The activity of the Council of the EU in the field of critical infrastructures is structured through its various configurations, depending on the sector concerned (for example, Home Affairs, Energy, Transport, Telecommunications), as provided for in the TEU [1, Article 16(6)], as well as through preparatory work carried out at the level of specialized working parties and the Committee of Permanent Representatives, expressly provided for in the TEU [1, Article 16(7)] and detailed in the TFEU [42, Article 240]. These structures enable the integration of the sectoral dimensions of critical infrastructure resilience and ensure the coherence of Member States' positions in relation to initiatives of the European Commission, while also facilitating the alignment of security policies with those concerning energy, transport, digitalisation, and civil protection.

Although the institution does not hold direct operational competences in the protection of critical infrastructures, its role is essential in providing political legitimacy to European action and in maintaining a functional framework of intergovernmental cooperation. Through its capacity to integrate and harmonize the interests of the Member States and to mediate between the national and supranational levels, it contributes to the stability and sustainability of the European resilience architecture.

## 2.4. The Council of Europe

The Council of Europe plays an indirect but significant role in the field of critical infrastructures by promoting the governance of major risks, societal resilience, and international cooperation in the prevention and management of disasters. Relevant activities in this regard include the following:

***The EUR-OPA Agreement on Major Hazards.*** It represents the Council of Europe's principal instrument in the field of critical infrastructures, aiming to strengthen cooperation among participating states in the areas of prevention, preparedness, and response to natural and technological disasters [48]. As a pan-European mechanism of intergovernmental cooperation (complementary to, yet distinct from, the EU architecture), its activity is structured around a network of specialized centres and thematic programmes. These focus on risk assessment, vulnerability reduction, and the protection of infrastructures exposed to major risks, and emphasize the importance of integrating critical infrastructures into national policies on disaster risk reduction and the strengthening of societal resilience [49].

***Development of national legal and institutional frameworks.*** The Council of Europe supports EU Member States in the development of the legal and institutional framework for the management of major risks, including those that may affect critical infrastructures, through legal expertise, thematic assessments, and policy recommendations. In this regard, the declarations and resolutions adopted encourage states to adopt integrated prevention policies, to strengthen the resilience of essential infrastructures, and to ensure coherence between civil protection, spatial planning, and societal security policies [50].

***Promotion of international cooperation and the development of a risk culture.*** An important pillar of the Council of Europe's contribution is the promotion of international cooperation and the development of a risk culture, through training programmes, the exchange of best practices, and public awareness initiatives. Documents developed within the framework of EUR-OPA, such as "Resolution 2011-1 on ethical principles relating to disaster risk reduction and their contribution to strengthening population resilience to disasters", highlight the responsibility of states to integrate prevention, the protection of persons, solidarity, public information, and respect for human rights into policies aimed at strengthening societal resilience to disasters [51].

***Improving risk governance and protection policies.*** The Council of Europe contributes to improving risk governance through analytical reports, ministerial conclusions, and recommendations adopted within the framework of the EUR-OPA Agreement [48], which promote interinstitutional coordination, the integration of risk assessments into decision-making processes, and the development of coherent preventive policies. These soft law instruments complement the EU's normative framework and support states in adapting national policies to current risks.

In conclusion, through its instruments of intergovernmental cooperation, soft law mechanisms, and the expertise developed within the EUR-OPA Agreement, the Council of Europe meaningfully complements the EU's normative framework, contributing to the consolidation of a coherent, preventive, and resilience-oriented approach to the management of major risks that may affect critical infrastructures. Nevertheless, the role of the Council of Europe in the field of critical infrastructures remains constrained by the non-binding nature of its instruments and by its dependence on the willingness of the UE Member States to transpose the recommendations put forward.

## 3. Sectoral structures and cooperation platforms for critical infrastructures

### 3.1 The European Union Agency for Cybersecurity (ENISA)

The EU has progressively developed a normative and institutional architecture aimed at strengthening cyber resilience, at the centre of which lies ENISA, a governance instrument designed to ensure the convergence of national policies and to facilitate a common approach to cyber risks affecting critical infrastructures [2].

Initially conceived as an agency with limited competences, ENISA operated within an institutional framework based on heterogeneous national regulations and voluntary cooperation - an approach that reflected the perception of cybersecurity as an integral part of national security. The intensification of cyberattacks against critical infrastructures and their predominantly cross-border nature have highlighted the limitations of this institutional framework [52].

The adoption of the Cybersecurity Act Regulation in 2019 marked a decisive stage in the maturation of European cybersecurity policy, through the expansion of ENISA's competences and the recognition of the complex nature of cyber threats [53, Arts. 3-7]. From the perspective of critical infrastructure protection, this change enables the development of instruments capable of responding effectively to systemic risks manifesting across the European space. Accordingly, the establishment of the European cybersecurity certification framework for ICT products, services, and processes [53, Arts. 46-65] has significant implications for critical infrastructures, as their security depends directly on the reliability of the technologies used. Through common certification standards, internal market fragmentation is reduced, trust in technological solutions is strengthened, and vulnerabilities associated with supply chains are mitigated [54].

Beyond the normative dimension, ENISA's contribution to the protection of critical infrastructures lies in its strategic knowledge of cyber threats. The periodic reports produced by the agency provide a systematic analysis of attack typologies, involved actors, and emerging trends [55]. In this way, ENISA represents a key element of European cyber governance, supplying expertise and risk analyses that underpin decision-making processes at the EU level.

ENISA's significant role in this field is also shaped by its involvement in cooperation, coordination, and the management of cyber incidents and crises. The European Commission Recommendation (EU) 2017/1584 [56] emphasizes the need for information exchange between CSIRT teams and national authorities in order to respond effectively to cross-border cyber incidents. In this context, ENISA's involvement - as a facilitator of information sharing and interinstitutional cooperation - contributes to strengthening coordinated incident response capacity at the European level.

Nevertheless, the analysis of ENISA's role highlights the structural limitations of European governance in the field of cybersecurity. The predominantly non-coercive nature of the agency's competences and the importance of national regulatory frameworks may generate uneven levels of protection of critical infrastructures across EU Member States.

### 3.2 The Computer Emergency Response Team for the EU Institutions (CERT-EU)

CERT-EU is the structure responsible for the prevention, detection, and management of cybersecurity incidents affecting EU institutions, agencies, and bodies. Although the *Cybersecurity Act* does not explicitly define the role of CERT-EU, it operates as a specialised operational capability, complementary to ENISA, within an institutional environment characterised by the distribution of cybersecurity competences among multiple entities, each endowed with distinct mandates and responsibilities [3]. In this regard, CERT-EU represents an interface element of European cyber governance, facilitating the connection between the EU institutional level and the broader cybersecurity ecosystem of the Member States, namely the network of national CSIRTs [57].

From a functional perspective, CERT-EU plays a central role in the monitoring of cyber threats, incident analysis, and the provision of early warnings to relevant EU institutions. Through its threat intelligence and information-sharing activities, CERT-EU contributes to enhancing the

capacity of European institutions to anticipate and manage cyberattacks with potential systemic impact [58]. This role is particularly significant in the context of threats aimed at the long-term compromise of European informational and digital infrastructures. At the same time, by contributing to the cybersecurity of EU institutions, CERT-EU indirectly supports decision-making processes, institutional continuity, and public trust in the EU's ability to manage complex risks in an environment marked by hybrid threats and geopolitical competition [57, 58].

Notably, by virtue of their nature and scope, CERT-EU's activities highlight the structural constraints affecting cybersecurity at the EU level, stemming from the absence of direct coercive competences and the Union's reliance on the voluntary cooperation of Member State institutions [59]. Furthermore, the complexity of the European institutional environment may hinder coordination processes and the rapid implementation of security measures in situations of cyber crisis.

Despite these limitations, the progressive consolidation of CERT-EU's role reflects the growing recognition that the cybersecurity of European institutions constitutes an essential component of EU resilience [60].

### 3.3 The European Emergency Response Coordination Centre (ERCC)

ERCC represents the operational core of the EU Civil Protection Mechanism, with the role of coordinating the European response to major emergencies, including natural disasters, technological crises, and events with significant impact on the functioning of critical infrastructures and essential services within European societies [4]. In the current context, marked by strong interdependencies between physical and digital infrastructures, the role of the ERCC has gained increased relevance in crisis management [61].

From an institutional perspective, the ERCC operates as a shared operational capacity within a framework characterised by distributed competences, in which primary responsibility for emergency management remains at the level of the Member States, while the role of the European Union is one of coordination and support. This configuration reflects the application of the principle of subsidiarity, while also highlighting the structural limits of European intervention in the field of civil protection [62].

At the operational level, the ERCC contributes to the anticipation of potential negative effects on critical infrastructures and to supporting decisions regarding resource mobilisation (early warning function) through the continuous monitoring of risks and emergency situations with potential systemic impact, as well as through the collection, analysis, and dissemination of relevant information to the competent European institutions [63]. In addition, the ERCC coordinates mobilisation at EU level within the framework of the Union Civil Protection Mechanism (UCPM), by managing the capacities made available by the Member States and by activating the common rescEU reserves [4]. Rapid mobilisation capacity represents an essential instrument for limiting negative effects on critical infrastructures during major emergencies and for restoring the essential functions of society.

Although the activity of ERCC is primarily focused on risks of a physical and natural nature, recent developments have highlighted an increasingly pronounced convergence between the field of civil protection and the cybersecurity dimension [61]. Accordingly, in situations of complex crises, where natural disasters may be accompanied by digital disruptions or cyberattacks, cooperation between the ERCC, ENISA, and CERT-EU becomes essential for ensuring an integrated and coherent response at EU level.

Nevertheless, the role of the ERCC is shaped by certain structural limitations, such as the absence of direct coercive competences and its dependence on the willingness of EU Member States to provide response capacities for major emergencies. These constraints highlight the persistent tension between the need for enhanced European coordination and the preservation of national sovereignty in the field of emergency management [64, 65].

Despite these constraints, the progressive strengthening of the ERCC's role underscores the recognition of effective emergency management as a core component of EU resilience [66] and

confirms its positioning as an operational pillar of the European crisis management architecture, within a resilience governance model grounded in solidarity, cooperation, and interoperability.

### 3.4 Coordination centres for critical infrastructures

The EU has developed sectoral resilience mechanisms that complement the roles performed by ENISA, CERT-EU, and ERCC, thereby shaping a European approach to the protection of critical infrastructures based on sectoral governance, voluntary cooperation, and standardisation processes, as follows:

The ***European Energy Information Sharing and Analysis Centre (EE-ISAC)*** [67] is a European cooperation platform dedicated to information sharing (among energy operators, public authorities, and other relevant stakeholders) and risk analysis in the energy sector, with a particular focus on cyber and hybrid threats. The role of EE-ISAC is especially relevant in a context marked by high interdependencies between national energy infrastructures and by their increased vulnerability to cyberattacks, sabotage, and deliberate disruptions, as, through the strengthening of voluntary cooperation and trust, it contributes to raising risk awareness and to enhancing the capacity of the European energy sector to prevent, detect, and manage incidents with potential systemic impact.

The ***European Union Agency for Railways (ERA)*** [68] is the EU agency responsible for promoting the safety, interoperability, and efficiency of the European railway system, in a context in which the growing reliance of modern railway systems on digital technologies, automated control systems, and cross-border interconnection amplifies vulnerabilities to cyber threats. ERA contributes to strengthening the resilience of the railway sector through the development of common standards, technical recommendations, and assessment frameworks, thereby supporting EU Member States and operators in managing risks that may affect railway transport safety at the European level.

The ***European Union Aviation Safety Agency (EASA)*** [69] is the EU's central authority in the field of civil aviation safety, playing an essential role in the regulation, oversight, and harmonisation of aeronautical safety standards. In the current context, characterised by the accelerated digitalisation of aviation and the increasing diversification and complexity of threats, EASA has progressively integrated cybersecurity and critical aviation infrastructure resilience dimensions into its mandate. Through the development of regulations, guidelines, and risk assessments, EASA contributes to the anticipation and management of threats that may affect flight safety, airport operations, and air traffic management systems, thereby strengthening the resilience of the European aviation sector.

### 3.5 The Cooperation Group and the CSIRT Network under the NIS/NIS2 framework

The adoption of the NIS Directive and, subsequently, the NIS2 Directive has established a European model of cybersecurity governance grounded in cooperation, information sharing, and coordination among EU Member States, with the Cooperation Group and the CSIRT Network serving as its central pillars - complementary mechanisms for the management of cyber risks.

The ***Cooperation Group***, initially established under the NIS Directive [5, Art. 11] and further strengthened by the NIS2 Directive [6, Art. 14], represents the primary cooperation mechanism between EU Member States, the European Commission, and ENISA. The Group supports the convergence of national cybersecurity policies by facilitating the exchange of best practices, fostering a shared understanding of cyber risks and threats, and coordinating strategic orientations at EU level, including with regard to the uniform implementation of the NIS2 Directive. In this respect, the Group functions as a strategic governance mechanism, lacking direct coercive powers but playing an essential role in reducing fragmentation and in promoting a coherent approach to cybersecurity across critical sectors.

The ***CSIRT Network***, as provided for under the NIS Directive [5, Art. 12] and the NIS2 Directive [6, Art. 15], constitutes the operational pillar of European cooperation in the field of cyber-

security, complementing the strategic dimension represented by the Cooperation Group. The role of the Network is to support the prevention, detection, and management of cyber incidents with cross-border impact, particularly in essential and important sectors, as defined by the NIS2 Directive. Through early warning mechanisms, information sharing, and technical coordination, the CSIRT Network contributes to strengthening the EU's collective capacity to respond rapidly and effectively to complex cyber threats.

The ***Cooperation Group*** and the ***CSIRT Network*** highlight a functional division at EU level between the strategic-political and the technical-operational levels, a complementarity that allows cybersecurity to be addressed both as a public policy issue and as an operational challenge, without encroaching upon national security competences. The functioning of both mechanisms is based on voluntary cooperation and information sharing, a feature that underscores both the structural limits of European cybersecurity governance and the advantages of a flexible model that contributes to reducing systemic vulnerabilities and strengthening digital resilience at EU level.

### 3.6 Coordination mechanisms provided for by Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)

The adoption of the CER Directive reflects a paradigm shift in the EU's approach to critical infrastructures, marking a transition from a sectoral and reactive model to an integrated framework oriented towards resilience and the management of complex risks, in which coordination mechanisms ensure a coherent and convergent approach among Member States in the face of transboundary and hybrid threats [7], as follows:

The CER Directive establishes accountability *mechanisms requiring EU Member States to put in place resilience frameworks for critical entities* [7, Arts. 5 and 6], based on periodic national assessments of significant risks (natural, technological, cyber, deliberate, etc.) that may affect the provision of essential services. These processes form the basis for the subsequent identification of critical entities, the definition of resilience measures, and coordination between national and European levels.

Furthermore, the Directive introduces *coordination and information-sharing mechanisms between EU Member States and the European Commission* [7, Arts. 5, 7 and 9], establishing obligations related to notification, cooperation, and structured dialogue aimed at ensuring a coherent EU-level approach to the resilience of critical entities and promoting the convergence of national approaches. These obligations strengthen the EU's capacity to develop an overall picture of systemic vulnerabilities and to support the coordination of responses in crisis situations.

In addition, the CER Directive introduces *coordination mechanisms for critical entities of European significance* [7, Art. 7], providing that, where such entities deliver essential services in multiple EU Member States, specific cooperation procedures are established between the affected states and the European Commission.

The Directive also regulates *intersectoral and interinstitutional coordination* [7, Art. 4, complemented by Arts. 5, 9 and 11], through mechanisms designed to operate complementarily with those established under the NIS2 Directive, thereby avoiding overlaps and ensuring an integrated approach to physical and digital resilience.

Finally, the CER Directive provides for the *exchange of best practices and mutual support among EU Member States* [7, Art. 11, complemented by Art. 7], through dedicated European platforms and mechanisms aimed at conducting joint exercises, peer reviews, and strategic guidance at EU level.

Although the coordination mechanisms introduced by the CER Directive strengthen the EU's role in the protection and resilience of critical infrastructures, they remain deliberately non-coercive, in line with the principle of subsidiarity and with Member States' competences in the field of national security.

## 4. Integrated analysis of the EU's institutional architecture in the field of critical infrastructure protection and resilience

### 4.1. Introductory considerations on the need for an integrated analysis

The complexity of contemporary risks - characterised by sectoral interdependencies, transboundary dimensions, and the overlap of physical, digital, and hybrid threats - requires an integrated approach to the protection and resilience of critical infrastructures at EU level, one that highlights the distribution of competences, functional relationships among institutions, coordination mechanisms, and the overall logic of governance, as reflected in the recent literature on the transition from critical infrastructure protection to resilience [19, 21].

Accordingly, the European institutional architecture in this field should be analysed as a multilevel governance system, in which authority is distributed between the national and EU levels, and where capacity for action is exercised predominantly through mechanisms of cooperation, standardisation, and coordination, rather than through hierarchical command or direct operational control. This configuration reflects both the legal constraints imposed by the European Treaties, in particular the Treaty on European Union (TEU) [1, Art. 4(2)], and the political choices of EU Member States.

The present analysis goes beyond the descriptive level of institutional mapping and seeks to identify the levels of governance, the types of authority exercised, and the structural limits of the European resilience model. Accordingly, the institutional architecture is examined not as a mere aggregation of normative competences, but as a set of interdependent functional relationships, whose effectiveness depends on the capacity for cooperation and coordination among the actors involved.

In this context, it should be emphasised that the earlier analyses developed in Chapters 2 and 3 have a predominantly descriptive and institutional-mapping function, a choice that was deliberately assumed, as the aim was to systematise the European institutional framework in this field. This stage provides the necessary foundation for the integrated analysis and functional assessment of the institutional architecture developed in Chapters 4 and 5, which constitute the original analytical contribution of the study.

Table 1 summarises the main functional levels of the EU's institutional architecture in the field of critical infrastructure protection and resilience, the actors involved, the types of authority exercised, and the structural limitations of each level. This synthesis offers the reference framework for the detailed analysis developed in the subsequent subsections and enables the formulation of a critical diagnosis of the EU's capacity to ensure effective operational coordination in the face of systemic risks.

| Functional level | Actors / structures | Type of authority | Main functions | Instruments used | Structural limits |
|---|---|---|---|---|---|
| Normative and strategic | European Commission; Council of the EU; European Parliament | Normative, political | Legislative initiative; strategic guidance; democratic legitimacy | Directives (CER, NIS2); regulations; Council conclusions | Lack of operational competences; intergovernmental compromises |
| Political-institutional coordination | NIS2 Cooperation Group; CER mechanisms; interinstitutional platforms | Coordination, facilitation | Policy alignment; information exchange; crisis coordination | Formal networks; cooperation procedures; risk assessments | Dependence on voluntary cooperation; uneven implementation |
| Technical–operational | ENISA; CERT-EU; ERCC; CSIRT networks | Technical, indirect operational | Risk analysis; early warning; incident support | Reports; exercises; response mechanisms | No coercive authority; limited resources |
| Sectoral | EE-ISAC; ERA; EASA; other agen- | Sectoral | Standardisation; sector-specific | Guidelines; standards; sec- | Sectoral fragmentation; limited cross- |

| | | | | | |
|---|---|---|---|---|---|
| | cies | | resilience | toral assess-ments | sectoral coordina-tion |

**Table 1. Institutional and functional structure of the EU framework for the protection and resilience of critical infrastructures**

It can be observed that the European institutional architecture for the protection and resilience of critical infrastructures is built upon a *multilevel governance* model, lacking a clear operational hierarchy, in which authority is functionally fragmented across levels endowed with asymmetric capacities and instruments, a configuration consistent with the conclusions of recent scholarly studies [19, 20, 21]. In this context, questions arise regarding the EU's ability to translate this architecture into an effective capacity for coordinated action in situations of systemic crisis.

The comparative analysis of functional levels reveals a structural gap between the *normative and strategic level*, characterised by a high density of regulation and political legitimacy, and the *coordination and technical-operational levels*, which concentrate the critical functions for incident management but operate almost exclusively on the basis of voluntary cooperation and indirect authority. This gap generates an inherent risk of a *governance operational deficit* - similar to the risks of incoherence identified in critical analyses of recent European cybersecurity and resilience policies [20, 59] - whereby EU legislative initiatives are not supported by institutional mechanisms capable of ensuring decision synchronisation, resource prioritisation, and response coherence.

In particular, Table 1 highlights a structural vulnerability of the European model: the functions that are decisive for the management of hybrid risks - namely rapid information sharing, inter-institutional coordination, and operational support - are located at levels lacking coercive competences and procedural enforcement capacity. In the absence of clear mechanisms of interoperability and *institutional orchestration*, the effectiveness of this model depends on extra-legal factors, such as a culture of cooperation, mutual trust, and the administrative capacity of EU Member States.

Furthermore, Table 1 underscores the delineation of the *sectoral level* as a distinct tier - justified from the perspective of specialisation and technical expertise - which accentuates the risk of functional fragmentation and indicates that the current institutional architecture is better suited to managing individual sectoral risks than to addressing cascading effects and systemic disruptions, in line with recent studies in the field [70-72].

The synthesis presented should not be understood as a mere institutional map, but rather as a *diagnosis of the structural limitations of EU resilience governance*. It indicates that the primary challenge lies in the difficulty of transforming a densely regulated architecture into a system capable of rapid, coherent, and effective coordination. The detailed analysis of each level, developed in the following sections, seeks to assess the extent to which this model can overcome these structural constraints or whether they represent an inherent cost of European governance, a conclusion consistent with recent critical assessments of the structural limits of European resilience governance [19, 20, 59].

### 4.2. Functional logic of the EU's institutional architecture

From an analytical perspective, the European institutional architecture for the protection and resilience of critical infrastructures can be structured into three interdependent functional levels: the *normative and strategic level*, the *political-institutional coordination level*, and the *technical-operational level*. It should be noted that the sectoral level does not constitute an autonomous level of governance; rather, although distinct in terms of its degree of specialisation, it functionally intersects the other levels, acting as a tier for the implementation, standardisation, and adaptation of resilience requirements to the specificities of each sector (see Chapter 4.1). This structuring makes it possible to highlight how competences and responsibilities are distributed and interconnected in practice.

At the ***normative and strategic level***, the EU's political institutions - the European Commission, the Council of the European Union, and the European Parliament - define the legal framework

and public policy orientations related to critical infrastructure resilience. This level is characterised by the adoption of binding legal acts, such as the CER Directive and the NIS2 Directive, as well as by the use of soft law instruments intended to ensure flexibility and adaptability to the diversity of national contexts. The role of this level is to establish common objectives, minimum requirements, and guiding principles, without substituting the operational competences of EU Member States.

At the ***political-institutional coordination level***, the European architecture relies on mechanisms that facilitate cooperation between Member States and EU institutions, particularly in situations of crisis or systemic risk. These mechanisms include cooperation platforms, institutionalised networks, and coordination procedures, which enable the centralisation and correlation of information, the alignment of political positions, and the coordination of national responses in line with the European framework in the field. In this way, decision-making coherence is ensured and unharmonised interventions are prevented.

At the ***technical-operational level***, specialised EU agencies and structures - ENISA, CERT-EU, and ERCC - provide expertise, operational support, and coordination capacities in the management of incidents and crises affecting critical infrastructures. Although they do not possess direct coercive competences over EU Member States or critical infrastructure operators, they play an essential role in strengthening the EU's collective capacity to prevent, detect, and respond to events with systemic impact.

### 4.3. Integration of the physical and digital dimensions of resilience

The current European institutional architecture for the protection and resilience of critical infrastructures reflects a unitary approach to resilience, understood as an emergent property of interdependent socio-technical systems, in which physical and digital disruptions are perceived as interconnected dimensions of the same risk ecosystem. In the scholarly literature, this evolution is often associated with the development of forms of *hybrid governance* [73-75].

From a normative perspective, this approach is materialised through the complementarity between the CER Directive [7] and the NIS2 Directive [6], instruments that operate within different legal frameworks but converge on the same functional objective, namely ensuring the continuity of essential services in the event of incidents with systemic impact [19, 20, 21]. The CER Directive addresses resilience through a predominantly functional logic, focused on the capacity of critical entities to prevent, absorb, and recover from such incidents, regardless of their nature. By contrast, the NIS2 Directive strengthens the cybersecurity of networks and information systems, highlighting that digital incidents can generate systemic effects comparable to those caused by major physical disruptions.

However, the physical-digital integration achieved through these instruments remains, to a large extent, an integration of objectives and normative logic, rather than one that is fully realised at the institutional and operational levels. From a multilevel governance perspective, the European architecture operates predominantly according to a logic of *multilevel orchestration*, whereby the EU establishes common objectives, procedural frameworks, and cooperation mechanisms, without possessing direct coercive competences over operational implementation. Within this model, the integration of physical and digital dimensions is not imposed hierarchically, but must be achieved through coordination, procedural alignment, and information sharing among authorities with distinct responsibilities.

This limitation becomes apparent both at EU level and at the level of Member States, in the way the mechanisms established under the CER Directive and the NIS2 Directive operate in parallel. Although designed to address the same hybrid risks, they function through separate institutional channels and partially divergent procedural logics, which, in the absence of explicit mechanisms for interoperability and operational integration, may generate asynchronous responses in crisis situations. At national level, this challenge is further amplified by the fragmentation of responsibilities between authorities primarily oriented towards managing physical impacts and service continuity

and those specialised in cybersecurity. In this context, physical-digital integration requires not merely informal cooperation, but the capacity to correlate risk assessments, information flows, and operational decisions within a coherent *hybrid governance* framework.

The integration of the physical and digital dimensions of resilience thus becomes a critical test of the EU's institutional architecture's actual governance capacity, as also highlighted by several recent specialist studies [19, 20, 21]. Although the current normative framework provides the foundations for an integrated approach to hybrid risks, its effectiveness depends on the ability of *multilevel orchestration* mechanisms to transform legal complementarity into effective operational coordination. The persistence of an *institutional orchestration deficit* risks limiting the impact of the post-2022 reforms, turning physical-digital integration into a declared objective that remains insufficiently internalised within the administrative and operational practices of EU Member States.

### 4.4. The non-coercive character and the role of institutional cooperation

A defining structural feature of the European institutional architecture in the field of critical infrastructure protection and resilience is its predominantly non-coercive character. The EU does not possess direct competences to impose operational protection measures, to intervene in the management of critical infrastructures, or to substitute national authorities in incident management. These responsibilities lie with the EU Member States and key operators, reflecting the legal limits imposed by the Treaties - particularly the TEU [1, Art. 4(2)] - as well as the significance of critical infrastructures from the perspective of national security. In this context, European governance in this field is based on an alternative model of exercising authority, commonly referred to as *governance through orchestration*, which is centred on institutional cooperation, procedural coordination, and normative alignment, rather than on hierarchical command or direct coercion.

The non-coercive nature of this model generates a range of *functional advantages*, such as tailoring resilience measures to national and sectoral specificities and avoiding the rigid standardisation of Member State responses in the face of heterogeneous and dynamic risks. Moreover, voluntary cooperation and information-sharing among EU Member States foster the gradual convergence of intervention and response, as well as the development of a shared risk management culture [20, 76, 77].

At the same time, this model also gives rise to problematic aspects, stemming from the EU's limited capacity to ensure the real-time synchronisation and coordination of decisions, the prioritisation of resources, and the coherence of national responses, particularly in the management of hybrid risks, where physical and digital interdependencies require rapid and coordinated action among institutional actors. Consequently, the effectiveness of *governance through cooperation* depends to a large extent on extra-legal factors, such as the level of mutual trust among EU Member States, their willingness to cooperate and share sensitive information, and the administrative capacity of the competent national authorities [20, 76, 77].

Therefore, the non-coercive character of the European institutional architecture should not be interpreted exclusively as a normative limitation, but rather as a structural choice with ambivalent implications. It provides flexibility and respects Member State sovereignty, but it also conditions governance effectiveness on high levels of cooperation, trust, and institutional capacity. Analysing this balance between national autonomy and European coordination is essential for understanding both the potential and the limits of the European resilience model.

### 4.5. Structural limitations and operating conditions of EU resilience governance

The integrated analysis of the EU-level institutional architecture for the protection and resilience of critical infrastructures highlights that the current governance model is characterised by a persistent structural tension between high normative density and a limited operational capacity for coordination in situations of systemic crisis [19, 52, 59]. Although the post-2022 reforms have significantly strengthened the legal framework for resilience, they have not eliminated the gap be-

tween the strategic level of objective-setting and the operational levels responsible for the effective management of risks. This reality is an inherent consequence of a multi-level, non-coercive governance model based on cooperation and national responsibility. The integration of the physical and digital dimensions of resilience, although advanced from a normative perspective through the complementarity between the CER and NIS2 Directives, remains contingent upon the capacity of national and European institutions to coordinate procedural mechanisms characterised by differing temporalities, mandates, and operational logics.

From this perspective, the effectiveness of European resilience governance depends on the simultaneous fulfilment of a set of conditions that cannot be ensured solely through regulation: the existence of functional mechanisms of institutional interoperability; high levels of trust and willingness to share sensitive information; and convergent administrative and technical capacities among EU Member States [19, 25, 59]. In the absence of these conditions, the current architecture risks generating fragmented and asynchronous responses, particularly in the face of hybrid crises with cascading effects.

Accordingly, the principal vulnerability of the European model does not lie in the absence of actors or legal instruments, but in the difficulty of transforming *normative orchestration* into robust *operational coordination.* This finding suggests that future developments in European policy on the protection and resilience of critical infrastructures will need to focus not only on expanding the normative framework, but also on strengthening institutional mechanisms for coordination, interoperability, and operational learning. In this sense, resilience governance appears less as a problem of legal competence and more as one of institutional capacity and cooperative design within a context of multiple interdependencies.

### 4.6. Evaluation matrix of the EU's institutional architecture in the field of critical infrastructure protection and resilience

In order to systematically assess the functioning of the European institutional architecture for the protection and resilience of critical infrastructures - beyond the mere description of actors and existing mechanisms - the specialised literature indicates the need to operationalise the analysis through a coherent set of *evaluation criteria* and *functional indicators*, materialised in various forms of an *evaluation matrix* [78–80].

The matrix proposed in this study does not aim at a quantitative measurement of institutional performance, but rather provides a qualitative framework for comparative assessment, appropriate to the non-coercive and multilevel nature of European governance.

The selected criteria reflect the core functions of resilience - prevention, coordination, response, and adaptation - and are formulated so as to be applicable transversally across the different institutional levels and mechanisms analysed (normative, coordination, and technical-operational):

*Clarity of institutional roles and responsibilities* - refers to the extent to which the institutional architecture coherently defines competences, responsibilities, and functional relationships among the actors involved. Role clarity is essential to avoiding overlaps, responsibility gaps, and decision-making ambiguities in crisis situations.

*Institutional and procedural interoperability* - reflects the capacity of institutional structures and mechanisms to function in a coordinated manner, through compatible procedures, integrated communication channels, and a shared operational language. In the context of hybrid risks, interoperability is a necessary condition for correlating physical and digital responses.

*Capacity for rapid and secure information exchange* - analyses the existence and functionality of early warning mechanisms, the sharing of sensitive information, and the dissemination of risk analysis among national authorities, European agencies, and critical infrastructure operators.

*Temporality and speed of decision-making coordination* - concerns the capacity of the institutional architecture to support decision-making and response coordination within timeframes com-

patible with the dynamics of systemic crises. Differences in temporality between physical and digital channels constitute a critical evaluation factor.

*Integration of the physical and digital dimensions of resilience* - measures the extent to which institutional mechanisms enable a unified approach to risks that simultaneously affect physical infrastructures and digital systems, avoiding their treatment as separate domains of intervention.

*Capacity to manage cascading effects and sectoral interdependencies* - evaluates the extent to which the European architecture enables the identification, anticipation, and management of chain impacts of disruptions across multiple interconnected critical sectors.

*Mechanisms for institutional learning and adaptation* - analyse the existence of institutionalised processes for post-crisis evaluation, joint exercises, exchange of best practices, and adjustment of policies and procedures based on lessons learned.

For each evaluation criterion, qualitative indicators can be identified that allow for an assessment of the degree of functionality of the institutional architecture, as presented in the "evaluation matrix" set out in Table 2.

| Criterion | | Functional indicators |
|---|---|---|
| **Code** | **Description** | |
| C1 | Clarity of institutional roles and responsibilities | Existence of clearly delineated mandates; avoidance of institutional overlaps; mechanisms for the designation of competent authorities |
| C2 | Institutional and procedural interoperability | Common procedures; cooperation protocols; interinstitutional exercises; compatibility of national frameworks |
| C3 | Capacity for rapid and secure information exchange | Secure channels; early warning mechanisms; clear rules on the classification and use of information |
| C4 | Temporality and speed of decision-making coordination | Institutional reaction time; the availability of functional decision-making escalation mechanisms; capacity for real-time coordination |
| C5 | Integration of the physical and digital dimensions of resilience | Coherence between CER and NIS2; coordination between civil protection authorities and cybersecurity authorities |
| C6 | Capacity to manage cascading effects and sectoral interdependencies | Intersectoral risk assessments; cross-sector mechanisms; systemic analysis capacity |
| C7 | Mechanisms for institutional learning and adaptation | Post-event evaluations; updating of procedures; dissemination of lessons learned |

**Table 2. EU institutional architecture evaluation matrix for critical infrastructure protection and resilience**

The proposed matrix constitutes an analytical tool that enables the functional testing of the EU's institutional architecture against its declared resilience objectives. By applying the criteria and indicators to the mechanisms analysed (ENISA, CERT-EU, ERCC, the Cooperation Group, and the CER mechanisms), it becomes possible to identify both areas of institutional convergence and zones of friction or structural vulnerability.

This matrix will be used in the following chapter to assess the EU's capacity to manage hybrid crisis scenarios and to formulate conclusions regarding the conditions under which non-coercive governance can generate effective operational coordination.

## 5. Functional testing of the EU's institutional architecture in hybrid crises

### 5.1. Considerations on the transition from institutional mapping to functional testing

The previous chapter has shown that the European institutional architecture for the protection and resilience of critical infrastructures operates within the paradigm of non-coercive multi-level governance, in which normative coherence and strategic orientation are ensured at the EU level, while implementation capacity and response capabilities remain predominantly anchored at the national and sectoral levels. This configuration means that the assessment of its performance depends to a large extent on the concrete manner in which cooperation mechanisms succeed in generating operational coordination among the actors involved.

The present analysis moves beyond the descriptive level and seeks to conduct a functional testing of the institutional architecture, using the *evaluation matrix* presented in Chapter 4.6. The research logic is pragmatic: since the EU architecture is designed to manage cross-border risks and crises with cascading effects, its performance must be assessed in relation to its capacity to sustain coordination flows, rather than solely in relation to the formal distribution of competences.

This approach is consistent with the study's hypothesis regarding the asymmetry between normative regulation and the operational capabilities of European governance. In the terms outlined in Chapters 4.1-4.5, functional testing aims to verify whether the model of *governance through cooperation* can reduce the operational deficit or whether, on the contrary, this deficit represents a persistent structural cost of European governance.

## 5.2. Institutional evaluation through scenario-based analysis

In the absence of a single operational authority responsible for managing critical infrastructure issues at the EU level, and given the often confidential nature of incidents affecting critical infrastructures, direct empirical evaluation of institutional performance is limited. Consequently, the use of *scenario-based analysis* is proposed, a method frequently employed in public policy studies and risk governance research [14, 70, 71, 80].

The proposed method does not seek to substitute legal analysis, but rather to complement it, based on the following clarification: while legal norms establish obligations and procedural mechanisms, scenarios allow for the observation of the temporal and functional compatibility of these mechanisms, as well as for the identification of points of institutional friction in crisis situations.

The scenarios used in the present study are designed to capture interdependencies between sectors, the overlap between physical and digital dimensions, the need for rapid information exchange, and the activation of higher decision-making levels. For each scenario, the *evaluation matrix* (see Chapter 4.6) is applied as an analytical framework, and the results are synthesised in qualitative terms (high/medium/low), with a focus on the mechanisms that facilitate or hinder coordination.

The selection of scenarios is guided by a *set of cumulative criteria*, intended to ensure institutional relevance, analytical transferability, and the explanatory value of the results, as follows:

The *first criterion* concerns the *systemic relevance of the sector under analysis*. Critical energy and logistics infrastructure sectors were selected, as they are characterised by a high degree of interdependence with other economic sectors and by their societal importance. The selected sectors meet this criterion insofar as they are regarded in the specialised literature and in EU documents as "nodal sectors," whose disruption generates cascading trans-sectoral effects.

The *second criterion* relates to *simultaneous exposure to physical and digital risks*. The selected scenarios allow for the examination of situations in which technical malfunctions, cyberattacks, physical failures, and operational constraints manifest as interconnected dimensions of the same crisis process. This characteristic is essential for testing the study's central hypothesis, which posits that the institutional separation between cybersecurity and the protection of physical infrastructures constrains the capacity for an integrated response.

The *third criterion* is *institutional relevance at the EU level*. The scenarios were designed such that their management exceeds the exclusive capacities of EU Member States and entails coordination, support, or intervention mechanisms at the European level. This includes the activation or mobilisation of instruments such as cooperation mechanisms, crisis management structures, civil protection mechanisms, or interinstitutional coordination processes. In this respect, the scenarios are intended to test the functionality of multi-level governance rather than the operational performance of an individual actor.

The *fourth criterion* concerns the *ability of the scenarios to highlight coordination gaps and ambiguities of competence*. Preference was given to scenarios that generate simultaneous pressures on multiple normative frameworks, sectoral policies, and institutional structures, precisely in order

to observe the extent to which the current governance architecture facilitates - or, conversely, fragments - the collective response. The objective is not to assess the technical efficiency of response measures, but to identify institutional bottlenecks and the limits of existing orchestration mechanisms.

Finally, the *fifth criterion* is *analytical transferability*. The scenarios were formulated at a sufficiently high level of abstraction to avoid dependence on specific national contexts or unforeseen events, thereby allowing the proposed analytical framework to be applied to other types of critical infrastructures as well. This methodological choice is consistent with the study's objective of contributing to the development of an analytical instrument for the governance of hybrid risks.

The ***first scenario analysed*** (Scenario A) consists of a *complex cyber campaign targeting operators in the energy sector*, affecting industrial control systems (OT/ICS) and generating progressive disruptions in electricity supply. Given the interdependence between the energy sector and other sectors, the incident produces cascading effects on transport systems (signalling systems, traffic management), communications (base stations, data centres), and potentially on healthcare services (continuity of medical facilities, storage and distribution systems for temperature-sensitive medical products).

The typical institutional flow in such a scenario involves, in parallel, the activation of mechanisms specific to the NIS2 Directive (reporting, CSIRT coordination, operational information exchange) and the CER Directive (continuity of essential services, physical and organisational resilience measures, coordination with the competent authorities for critical entities). Concretely, at the EU level, ENISA supports risk analysis and the exchange of good practices, the CSIRT network facilitates technical cooperation, and, if the incident escalates into a societal crisis, civil protection and coordination mechanisms are activated complementarily through the ERCC.

The application of the evaluation matrix proposed in Chapter 4.6 to this scenario is presented in Table 3.

| **Criterion** | | **Explanation** |
|---|---|---|
| **Code** | **Level of assessment** | |
| C1 | High | The major risk emerges at the point of interference between the digital and physical dimensions, when a cyber incident produces material effects on the functioning of the infrastructure. This highlights a relatively clear allocation of initial responsibilities, while also revealing vulnerabilities in the area of overlapping institutional competences. |
| C2 | Medium | Although procedures and cooperation frameworks exist among the authorities involved, institutional interoperability is affected by procedural differences and by a lack of synchronisation between the structures responsible for cybersecurity and those responsible for the protection of physical infrastructures. |
| C3 | Medium | Information exchange is possible through existing secure channels; however, the speed of transmission and the extent of information sharing are constrained by differing classification regimes and by institutional reluctance to share sensitive data in the early phases of the incident. |
| C4 | Low-Medium | Decision-making coordination is hampered by the lack of clear synchronisation of institutional temporalities and by the delayed activation of higher decision-making levels, which slows the integrated response during the critical phase of the crisis. |
| C5 | Medium | The integration of the physical and digital dimensions is advanced at the normative level, but remains only partially functional at the operational level due to insufficient coordination between civil protection authorities and cybersecurity authorities. |
| C6 | Low | The capacity to anticipate and manage cascading effects is limited, as intersectoral risk assessments are fragmented and cross-sector mechanisms remain insufficiently tested in scenarios with systemic impact. |
| C7 | Medium | Formal post-event evaluation and procedure-updating mechanisms exist; however, the process of disseminating lessons learned and of institutional adaptation is slow and uneven across sectors and levels of governance. |

**Table 3. Evaluation matrix in the case of a cyberattack (Scenario A)**

Scenario A highlights the fact that the effectiveness of the institutional architecture in the field of critical infrastructure protection and resilience depends on the ability to operationalize the integrated implementation of the CER and NIS2 Directives at national level, through interoperability procedures, coordination centers, and joint exercises.

The ***second scenario*** analysed (Scenario B) refers to a *deliberate physical incident affecting a critical logistics node of national and cross-border relevance*, such as a port terminal, a railway hub, or a major distribution centre. The incident generates significant disruptions to transport and supply flows, with an impact on the internal market, the continuity of logistics chains, and the functioning of economic sectors dependent on just-in-time deliveries. The crisis is further amplified by secondary disruptions of logistics management information systems and by a dynamic of information influence, characterised by disinformation and the contestation of the authorities' response.

In this scenario, the institutional flow is initially centred on the activation of national security and civil protection mechanisms. The authorities competent for emergency management, security, and transport continuity assume operational coordination, while the critical infrastructure operator implements measures to mitigate the impact and to progressively restore functionality. In parallel, insofar as IT systems are affected, the mechanisms provided for under the NIS2 Directive are activated, and national CSIRTs are involved in the analysis and management of secondary digital disruptions.

As the effects of the incident propagate beyond the initially affected area, the crisis acquires a systemic dimension. The disruption of the logistics node generates delays in supply chains, affecting other critical infrastructures and interdependent economic sectors, including the energy sector, industrial production, or the distribution of essential goods. In this context, the coordination mechanisms provided for under the CER Directive on the resilience of critical entities are activated, particularly in situations where the logistics node serves multiple Member States or is identified as a critical entity of European significance. Information exchange with the European Commission aims to assess the cross-border impact and to prevent cascading effects.

The application of the evaluation matrix proposed in Chapter 4.6 to this scenario is presented in Table 4.

| **Criterion** | | **Explanation** |
|---|---|---|
| **Code** | **Level of assessment** | |
| C1 | Medium | Institutional responsibilities are relatively clearly defined in the initial phase of the physical incident; however, ambiguities emerge as the effects propagate to digital infrastructures and related sectors, generating overlaps of competence among sectoral authorities. |
| C2 | Low-Medium | Institutional interoperability is constrained by procedural fragmentation between the actors responsible for managing physical incidents and those operating in the field of digital security, with cooperation being more sequential than integrated. |
| C3 | Low | Information exchange is affected by the lack of common physical-digital information flows and by difficulties in correlating technical data originating from different sources, which delays the formation of a comprehensive operational picture. |
| C4 | Medium | Although decision-making coordination mechanisms are activated relatively quickly in the physical domain, the transfer of decision-making to higher levels and the integration of the digital dimension occur with delay, generating asynchronies in the response. |
| C5 | Low | The integration of the physical and digital dimensions of resilience is weakly operationalised, with cooperation between civil protection authorities and cybersecurity authorities being reactive and insufficiently structured in the initial phase of the crisis. |
| C6 | Medium | Cascading effects are identified progressively; however, the capacity for systemic anticipation is limited, as intersectoral assessments are activated late and predominantly in reaction to already manifest disruptions. |
| C7 | Medium | Institutional learning processes are triggered post-crisis; however, procedural adaptation remains fragmented, and the integration of lessons learned into future planning is uneven across sectors. |

**Table 4. Evaluation matrix in the case of a deliberate physical attack (Scenario B)**

Scenario B shows that the European institutional architecture is effective in managing the immediate impact of a deliberate physical incident on logistics infrastructures, but faces significant difficulties in ensuring rapid cross-border coordination and in managing cascading effects amplified by the digital and informational dimensions. As in Scenario A, the effectiveness of the response depends decisively on the capacity of Member States to operationalise the cooperation and interoperability provided for by the European framework.

### 5.3. A synthetic framework for assessing vulnerabilities and operating conditions

The comparative analysis of the two scenarios - *a cyberattack targeting the energy sector (Scenario A) and a deliberate physical incident affecting a critical logistics node of national and cross-border relevance (Scenario B)* - makes it possible to identify recurring patterns in the functioning of the European institutional architecture for the protection and resilience of critical infrastructures. Although the two scenarios differ in terms of their triggering events and initial dynamics, they test the same coordination mechanisms and reveal the *same structural limits of European resilience governance*, as follows:

*The asymmetry between normative clarity and operational ambiguity*. In both scenarios, the EU-level legal framework provides a relatively clear delineation of formal competences and cooperation mechanisms; however, at the moment of crisis escalation, the interfaces between the physical and digital domains become areas of institutional friction. Both in the case of a cyber incident with physical impacts and in that of a physical incident with secondary digital effects, it is not fully clear where the responsibility of each authority begins and ends, which complicates real-time coordination.

*Institutional and procedural interoperability.* The scenarios show that the existence of multiple mechanisms - the CER and NIS2 Directives, CSIRT networks, and civil protection arrangements - does not automatically guarantee their coordinated functioning. Differences in procedures, operational language, and sectoral priorities lead to parallel responses which may be effective at the sectoral level but insufficiently synchronised at the systemic level. This problem becomes particularly evident during escalation phases, when rapid alignment of decisions is required among authorities with different responsibilities.

*The problem of divergent temporalities.* Scenario A highlights the time pressure inherent in the management of cyber incidents, where the response window is extremely short, while Scenario B shows that, although the initial response to physical incidents is rapid, cross-border and intersectoral coordination is more cumbersome, requiring consultation and decision-making synchronisation. In both scenarios, the European architecture encounters difficulties in synchronising these temporalities, which amplifies the risk of unanticipated cascading effects.

*Dependence on voluntary information sharing.* Both scenarios demonstrate that the effectiveness of the European response depends decisively on the willingness of states and private operators to share relevant information on incident management. In the absence of coercive mechanisms, any reluctance or delay in information provision reduces the capacity to anticipate the evolution of the crisis and constrains coordination at the EU level.

*Sectoral fragmentation.* Although EU-level sectoral agencies and platforms generate a high level of technical expertise, this is not always accompanied by effective mechanisms for intersectoral analysis. In both the energy and logistics sectors, the management of cascading effects remains dependent on national capacities to address such challenges, with the EU playing a predominantly facilitative role and providing indirect coordination.

Despite these limitations, the comparative analysis also highlights the *operating conditions of the non-coercive architecture*. In both scenarios, where common procedures and well-established institutional relationships exist, coordination of actions is faster and more coherent, contributing substantially to the mitigation of the negative effects generated by incidents. This suggests that the

effectiveness of European resilience governance is not determined exclusively by the formal institutional design, but rather by the degree of effective operationalization of cooperation and interoperability at the national and sectoral levels.

Overall, the *evaluation of the two scenarios confirms the study's hypothesis*: the EU institutional architecture in the field of critical infrastructure protection and resilience is normatively robust, but remains vulnerable in situations requiring rapid coordination, the management of cascading effects, and the integration of the physical and digital dimensions. These vulnerabilities constitute a structural cost of a multi-level governance model based on orchestration and voluntary cooperation, which implies that future consolidation efforts should focus on procedural interoperability and decision-making synchronisation rather than on expanding coercive competences at the EU level.

Accordingly, the *potential of the post-2022 reforms* (the CER and NIS2 Directives) *depends on the capacity to transform normative complementarity into a coherent set of interoperable institutional practices*, particularly at the national level, where the spheres of competence associated with the physical and digital dimensions of resilience intersect. Within the logic of non-coercive governance, directions for institutional consolidation should be oriented towards: procedural standardisation of information exchange between the mechanisms established under the CER and NIS2 Directives; the development of joint hybrid exercises; the strengthening of intersectoral systemic analysis capacities; and the establishment of institutional learning mechanisms aimed at attenuating asymmetries in national capacities.

## 6. Limitations of the research

Any analysis of the European institutional architecture in the field of critical infrastructure protection and resilience is inevitably shaped by a set of *methodological and conceptual limitations*, determined both by the nature of the field under examination and by the research choices adopted. Acknowledging these limitations is important for guiding future research directions in the area of European resilience governance.

A *first limitation* of the research derives from its *predominantly qualitative and conceptual character*. The study is based on an analysis of the normative framework of the institutional architecture and of coordination mechanisms, employing an interpretative methodology in the absence of quantitative data capable of substantiating institutional performance in the management of real incidents through empirical measurement. This limitation is inherent to the field, where detailed information on real incidents is often classified or fragmented.

A *second limitation* relates to the use of *scenario analysis as the main instrument for functional testing*. The selected scenarios are constructed as plausible analytical models, intended to highlight likely institutional flows and points of systemic friction, rather than to reproduce real events. Although this method is appropriate for evaluating governance under conditions of uncertainty and complexity, it inevitably entails a degree of abstraction, with results depending on the way in which the scenarios are constructed.

An *additional limitation* arises from the *emphasis placed on the European level of governance*, to the detriment of a detailed analysis of its transposition at the national level. Although the study highlights the central role of EU Member States in the protection and resilience of critical infrastructures and underscores significant differences in administrative and institutional capacity, it does not address national case studies. This methodological choice limits the ability of the research to capture concrete differences in performance and best practices among EU Member States.

Furthermore, the *research is constrained by the rapid dynamics of the European normative and institutional framework*, given that the field of critical infrastructure protection and resilience is characterized by continuous transformations, adaptation to emerging threats, and accelerated technological developments. The analysis relies primarily on the post-2022 normative and institutional framework, in particular the CER and NIS2 Directives.

Another *important limitation* of the study is determined by *restricted access to sensitive operational information*, as the effective functioning of coordination mechanisms in real crisis situations is largely inaccessible to the public and, implicitly, to academic research, for legitimate security reasons. This constraint reduces the possibility of direct empirical validation of the performance of the institutional architecture under analysis.

Overall, the *identified limitations do not invalidate the conclusions of the study*, but rather delineate the framework within which they should be interpreted. They reflect the inherent constraints of analysing EU governance in the field of critical infrastructure protection and resilience and highlight the need for future research that combines EU-level institutional analysis with national case studies, operational empirical data, and interdisciplinary perspectives.

## 7. Conclusions

The analysis of the European institutional framework in the field of the protection and resilience of critical infrastructures has shown that, over the past two decades, the EU has developed an increasingly dense, complex, and integrated governance architecture, progressively adapted to the cross-border, systemic, and hybrid nature of contemporary risks (confirming the general objective - O.G - and the specific objective O1). This evolution reflects a *significant conceptual shift*: the transition from a fragmented, sectoral, and predominantly national approach to critical infrastructure protection towards a European model of resilience governance, oriented towards the continuity of essential functions and the management of interdependencies among infrastructures, sectors, and levels of governance.

The study has demonstrated that the European institutional architecture is the result of a compromise between the need for a strengthened European-level response and the preservation of the Member States' primary competences in the field of national security, as enshrined in the Treaties (confirming objective O2 concerning the analysis of the functional logic of the institutional architecture). This compromise is embodied in a *non-coercive, multi-level governance model* in which the EU exercises predominantly indirect authority, based on regulation, coordination, standard-setting, and the facilitation of cooperation, without possessing direct operational competences in the management of critical infrastructures or the crises associated with them.

From this perspective, the *analysis confirms the central hypothesis of the research: the structural gap between normative initiatives and operational coordination capacity constitutes an inherent feature of European resilience governance* (in full alignment with objective O4 concerning the identification of the structural limits of the European non-coercive model). The post-2022 reforms, materialized in particular through the CER and NIS2 Directives, have significantly strengthened the legal framework and clarified objectives, requirements, and cooperation mechanisms. Nevertheless, they have not eliminated the structural constraints generated by the distribution of competences, the voluntary nature of cooperation, and the dependence on the uneven institutional capacities of the EU Member States.

The analysis has shown that the *EU institutional architecture operates across multiple distinct functional levels* - normative-strategic, politico-institutional coordination, technical-operational, and sectoral - characterized by asymmetries in terms of the type of authority exercised, the instruments available, and the capacity for real-time action (confirming objectives O1 and O2). While the normative level is marked by a high density of regulation and strong political legitimacy, the levels that concentrate the critical functions for incident and crisis management operate almost exclusively on the basis of voluntary cooperation and indirect authority. This configuration generates an *operational governance deficit*, particularly in situations requiring rapid decision synchronization and the management of cascading effects.

The *progressive integration of the physical and digital dimensions of resilience* constitutes one of the most important achievements of the recent European normative framework (confirming objective O3). The complementarity between the CER and NIS2 Directives reflects an advanced

understanding of hybrid risks and of the complex nature of critical infrastructures. However, the analysis has demonstrated that this integration remains, to a large extent, one of objectives and normative logic, rather than one fully internalized at the institutional and operational levels. The persistence of parallel procedural mechanisms, divergent temporalities, and fragmented responsibilities limits the capacity to produce unified responses in situations of complex crisis.

The *functional testing of the institutional architecture* through scenario analysis confirmed these findings (in fulfillment of objective O5). Both the scenario of a cyberattack against the energy sector with cascading effects and that of a deliberate physical incident affecting a critical logistics node with a secondary digital component revealed the same recurring patterns of vulnerability: difficulties in institutional interoperability, problems of decision-making synchronization, critical dependence on voluntary information sharing, and a limited capacity for the anticipatory management of sectoral interdependencies. In both cases, the effectiveness of European coordination depended less on the existence of the normative framework and more on the degree of effective operationalization of cooperation.

At the same time, the analysis has shown that the *EU's non-coercive architecture has potential for further evolution.* In situations where common procedures exist, institutional relationships are well established, and institutional capacities are convergent, European mechanisms can facilitate coordination, reduce fragmentation, and support the management of crises with transboundary impact. This suggests that the central problem of European resilience governance is not the absence of formal competences, but rather the institutional capacity to transform normative orchestration into effective operational coordination (confirming objective O6).

Consequently, the fundamental conclusion of the study is that the *future evolution of the European framework for the protection and resilience of critical infrastructures does not depend decisively on the expansion of the EU's coercive competences* - an option that is difficult to achieve from both a legal and political perspective - but on the *strengthening of mechanisms* for procedural interoperability, institutional learning, and decision-making synchronization. Resilience governance thus appears less as a matter of formal sovereignty and more as an issue of institutional design of cooperation within a system characterized by multiple interdependencies (confirming the general objective - O.G).

Through the integrated approach proposed, the *evaluation matrix*, and the functional testing of the institutional architecture, the study contributes to a more realistic and nuanced understanding of the potential and limits of the European model for the protection and resilience of critical infrastructures (fulfilling the theoretical, analytical, and methodological contribution outlined in Chapter 1). The study's conclusions indicate that the *EU possesses the necessary prerequisites to function as an orchestrator of resilience*, but that the effectiveness of this role remains conditional on political will, administrative capacity, and the degree of cooperation among the Member States.

## 8.References

[1]. European Union. (2016). *Tratatul privind Uniunea Europeană* (*versiune consolidată*) [*Treaty on European Union* (consolidated version)], *Official Journal of the European Union* C 202, 7 June 2016. https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0020.01/DOC_2&format=PDF

[2]. European Union Agency for Cybersecurity (ENISA). (n.d.). *Home*. ENISA. https://www.enisa.europa.eu/

[3]. CERT-EU. (n.d.). *Cybersecurity Service for the Union institutions, bodies, offices and agencies*. https://cert.europa.eu/

[4]. European Commission. (n.d.). *Emergency Response Coordination Centre (ERCC)*. European Civil Protection and Humanitarian Aid. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en

[5]. 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

[6]. 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

[7]. 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

[8]. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11-25. https://doi.org/10.1109/37.969131

[9]. Luiijf, H. A. M., Burger, H., Klaver, M., & Marieke, H. (2003). *Critical infrastructure protection in the Netherlands: A Quick-scan*. Copenhagen, Denmark: EICAR Denmark.

[10]. Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. *JRC Technical Notes*, *1*(1), 1-53.

[11]. Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. *JRC Science and Policy Report*, 6.

[12]. Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., ... & von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, *19*(4), 733-752. https://doi.org/10.1193/1.1623497

[13]. Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., … Seager, T. P. (2013). Measurable resilience for actionable policy. In I. Linkov & J. Palma-Oliveira (Eds.), Resilience and risk: Methods and application in environment, cyber and social domains (pp. 87–102). Springer.

[14]. Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., & Panda, A. (2022). Resilience stress testing for critical infrastructure. *International Journal of Disaster Risk Reduction*, *82*, 103323.

[15]. Little, R. G. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology*, *9*(1), 109-123.

[16]. Duenas-Osorio, L., & Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. *Structural Safety*, *31*(2), 157-167.

[17]. Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Rngineering & System Safety*, *121*, 43-60.

[18]. Brunner, L. G., Peer, R. A. M., Zorn, C., Paulik, R., & Logan, T. M. (2024). Understanding cascading risks through real-world interdependent urban infrastructure. *Reliability Engineering & System Safety*, *241*, 109653. https://doi.org/10.1016/j.ress.2023.109653

[19]. 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*(sup1), 85-101. https://doi.org/10.1080/23789689.2022.2128562

[20]. Becker, M. (2025). *Transposing EU-legislation on critical infrastructure protection legal implementation performance in the Baltic Sea region*. *International Journal of Critical Infrastructure Protection*, *50*, 100781. https://doi.org/10.1016/j.ijcip.2025.100781

[21]. Alexopoulos, M. J., Niemi, A., Skobiej, B., & Sill Torres, F. (2025). Examination of the Critical Infrastructure Resilience Directive From the Maritime Point of View. *JCMS: Journal of Common Market Studies*, *63*(2), 667-678.

[22]. Hooghe, L., & Marks, G. (2001). *Multi-level governance and European integration*. Bloomsbury Publishing PLC.

[23]. Abbott, K. W., Genschel, P., Snidal, D., & Zangl, B. (2021). Orchestration: Global governance through intermediaries. In *The Spectrum of International Institutions* (pp. 140-170). Routledge.

[24]. Ruohonen, J., Rindell, K., & Busetti, S. (2025). From Cyber Security Incident Management to Cyber Security Crisis Management in the European Union. *arXiv preprint arXiv:2504.14220*.

[25]. Ausfelder, A., Eick, A., Hartlapp, M., Mespoulet, R., Saurugger, S., Terpan, F., & Cappellina, B. (2024). EU soft-law: Non-binding but enforceable. *European Law Journal*, *30*(4), 668-684.

[26]. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890.

[27]. Olech, A. (2025). Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses. *Terroryzm. Studia, analizy, prewencja*, (Special), 133-158.

[28]. Pestana, G., & Sofou, S. (2024). Data governance to counter hybrid threats against critical infrastructures. *Smart Cities*, *7*(4), 1857-1877.

[29]. Papadopoulos, L., Demestichas, K., Muñoz-Navarro, E., Hernández-Montesinos, J. J., Paul, S., Museux, N., ... & Levak, J. (2024). Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach. *International Journal of Critical Infrastructure Protection*, *44*, 100657.

[30]. Geri, M. (2024). Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future 'energy-resources-climate'security nexus. *Journal of Strategic Security*, *17*(3), 15-34.

[31]. Directorate-General for Migration and Home Affairs. (2024, 8 February). *About us*. European Commission. https://home-affairs.ec.europa.eu/who-we-are/about-us_en

[32]. Directorate-General for Communications Networks, Content and Technology. (n.d.). *About us*. European Commission. https://commission.europa.eu/about/departments-and-executive-agencies/communications-networks-content-and-technology_en

[33]. Directorate-General for Energy. (n.d.). *About us*. European Commission. https://commission.europa.eu/about/departments-and-executive-agencies/energy_en

[34]. Directorate-General for Mobility and Transport. (n.d.). *About us*. European Commission. https://commission.europa.eu/about/departments-and-executive-agencies/mobility-and-transport_en

[35]. Directorate-General for European Civil Protection and Humanitarian Aid Operations. (n.d.). *About us*. European Commission. https://civil-protection-humanitarian-aid.ec.europa.eu/who/about-echo_en

[36]. European Commission. (n.d.). *Directorate-General for Health and Food Safety (DG SANTE)*. https://commission.europa.eu/about/departments-and-executive-agencies/health-and-food-safety_en

[37]. European Commission. (n.d.). *Directorate-General for Environment (DG ENV)*. https://commission.europa.eu/about/departments-and-executive-agencies/environment_en

[38]. European Commission. (n.d.). *Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW)*. https://commission.europa.eu/about/departments-and-executive-agencies/internal-market-industry-entrepreneurship-and-smes_en

[39]. European Commission. (n.d.). *Directorate-General for Climate Action (DG CLIMA)*. https://commission.europa.eu/about/departments-and-executive-agencies/climate-action_en

[40]. European Commission. (n.d.). *Directorate-General for Research and Innovation (DG RTD)*. https://commission.europa.eu/about/departments-and-executive-agencies/research-and-innovation_en

[41]. European Commission. (n.d.). *Directorate-General for Defence Industry and Space (DG DEFIS)*. https://commission.europa.eu/about/departments-and-executive-agencies/defence-industry-and-space_en

[42]. European Union. (2016). *Tratatul privind funcționarea Uniunii Europeană* (*versiune consolidată*) [*Treaty on the Functioning of the European Union* (consolidated version)], *Official Journal of the European Union* C 202/47, 7 June 2016. https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0020.01/DOC_3&format=PDF

[43]. Committee on Civil Liberties, Justice and Home Affairs. (n.d.). *About | LIBE*. European Parliament. https://www.europarl.europa.eu/committees/en/libe/about

[44]. Committee on Industry, Research and Energy. (n.d.). *About | ITRE*. European Parliament. https://www.europarl.europa.eu/committees/en/itre/about

[45]. Committee on Security and Defence. (n.d.). *About | SEDE*. European Parliament. https://www.europarl.europa.eu/committees/en/sede/about

[46]. European Commission. (n.d.). *Recovery and Resilience Facility*. https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en

[47]. European Commission. (n.d.). *Horizon Europe*. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

[48]. Council of Europe. (n.d.). *European and Mediterranean Major Hazards Agreement (EUR-OPA) - Statute of the Agreement*. https://www.coe.int/en/web/europarisks/eur-opa-in-brief

[49]. Council of Europe. (2021). *EUR-OPA Major Hazards Agreement - Strategic Framework 2021-2030* (as referenced in ministerial documentation). Council of Europe. https://rm.coe.int/ministerial-declaration-14th-ministerial-meeting-of-the-european-and-m/1680a4b97f

[50]. Council of Europe. (n.d.). *EUR-OPA Major Hazards Agreement - Resolutions*. https://www.coe.int/en/web/europarisks/resolutions

[51]. Council of Europe. (2011). *Resolution 2011-1 on ethical principles relating to disaster risk reduction and contributing to people's resilience to disasters* (EUR-OPA Major Hazards Agreement). https://www.coe.int/en/web/europarisks/resolutions#2011—1

[52]. Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254-1272.

[53]. 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 (Cybersecurity Act)* (OJ L 151, 7.6.2019, pp. 15–69). EUR-Lex. https://eur-lex.europa.eu/eli/reg/2019/881/oj

[54]. European Union Agency for Cybersecurity (ENISA). (2021). *ENISA Threat Landscape 2021* (ETL 2021) (Report No. TP-AE-21-293-EN-N). Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/98368007-475a-11ec-91ac-01aa75ed71a1/language-en

[55]. European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity certification framework* (Publications Office of the European Union) [fără număr de raport]. https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework

[56]. European Commission. (2017). *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises* (OJ L 239, 19.9.2017, pp. 36–58). EUR-Lex. https://eur-lex.europa.eu/eli/reco/2017/1584/oj

[57]. European Parliament & Council of the European Union. (2023). *Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union* (OJ L 2841, 18.12.2023). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2841

[58]. CERT-EU. (2025). *Threat Landscape Report 2024: A year in review*. https://cert.europa.eu/publications/threat-intelligence/tlr2024/

[59]. Ruohonen, J. (2024). *The Incoherency Risk in the EU's New Cyber Security Policies*. In R. van de Wetering, R. Helms, B. Roelens, S. Bagheri, Y. K. Dwivedi, I. O. Pappas, & M. Mäntymäki (Eds.), *Disruptive Innovation in a Digitally Connected Healthy World: 23rd IFIP WG 6.11 Conference on e-Business, e-Services and e-Society, I3E 2024* (pp. 284–295). Springer. https://doi.org/10.1007/978-3-031-72234-9_24

[60]. European Parliament. Research Service. (2024). *Cybersecurity actors in the EU*. European Parliament. https://epthinktank.eu/2024/01/10/cybersecurity-actors-in-the-eu/

[61]. European Commission. (2025). *EU Civil Protection Mechanism*. European Civil Protection and Humanitarian Aid Operations. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en

[62]. European Parliament & Council of the European Union. (2013). *Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism* (Text with EEA relevance) (OJ L 347, 20.12.2013, pp. 924–947). EUR-Lex. https://eur-lex.europa.eu/eli/dec/2013/1313/oj/eng

[63]. European Commission. (2023). *EU Civil Protection Mechanism: How the Emergency Response Coordination Centre (ERCC) works*. European Civil Protection and Humanitarian Aid Operations. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en

[64]. Schimmelfennig, F. (2024). *Crisis and polity formation in the European Union*. Journal of European Public Policy, 31(4), 1–20. https://doi.org/10.1080/13501763.2024.2313107

[65]. Ladi, S. (2024). *Reconceptualising the EU–member states relationship in the pursuit of fast policy responses*. Journal of European Public Policy, 31(2), 1–18. https://doi.org/10.1057/s41295-024-00384-6

[66]. Efstathiou, P., Maniou, M., Antonakakis, E., Dimitraki, E., Nikolidaki, S., & Boundali, V. (2025). *Integrated crisis and disaster management in the European Union: From local preparedness to global security challenges*. European Journal of Public Health, 35(Supplement_5), ckaf165.079. https://doi.org/10.1093/eurpub/ckaf165.079.

[67]. European Energy - Information Sharing & Analysis Centre. (n.d.). *Home – EE-ISAC*. https://www.ee-isac.eu/

[68]. European Union Agency for Railways. (n.d.). *European Union Agency for Railways (ERA) – Moving Europe towards a sustainable and safe railway system without frontiers*. https://www.era.europa.eu/

[69]. European Union Aviation Safety Agency. (n.d.). *EASA | Your safety is our mission*. https://www.easa.europa.eu/en

[70]. Gerbec, M., Čaleta, D., Modic, J., Giunta, G., & Durante, N. G. (2025). Cross-CI Assessment of Risks and Cascading Effects in ATLANTIS Project. *Applied Sciences*, *15*(19), 10374. https://doi.org/10.3390/app151910374

[71]. Cha, Y.; White, C. J.; Gonzalez, P. L. M.; et al. (2025). *Assessing the cascading impacts of natural hazards on Critical National Infrastructure (CNI) using Scotland as a case study.* npj Natural Hazards, 2, 108. https://doi.org/10.1038/s44304-025-00161-9

[72]. Barquet, K.; Englund, M.; Inga, K.; et al. (2023). *Conceptualizing multiple hazards and cascading effects on critical infrastructures.* Disasters, e12591. https://doi.org/10.1111/disa.12591

[73]. Teichmann, F.; Sergi, B. S. (2025). *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem.* Computer Law & Security Review, 59, 106209. https://doi.org/10.1016/j.clsr.2025.106209

[74]. Wang, R.; Qiu, H.; Liu, R.; Huo, H.; Cheng, X.; Liu, X. (2025). *A hybrid governance framework for adaptive and sustainable urban energy management.* Sustainable Cities and Society, 130, 106638. https://doi.org/10.1016/j.scs.2025.106638

[75]. Brighi, R., & Adinolfi, G. (2025). *EU Cybersecurity Policies in Cyber-Physical Ecosystems: Challenges and Perspectives.* European Journal of Risk Regulation, 16(2), 466–468. https://doi.org/10.1017/err.2025.10026

[76]. Mikac, R. (2023). Protection of the EU's critical infrastructures: results and challenges. *Applied Cybersecurity & Internet Governance*, *2*(1), 1-25.

[77]. Schmitz-Berndt, S., & Cole, M. D. (2022). Towards an efficient and coherent regulatory framework on cybersecurity in the EU: the proposals for a NIS 2.0 directive and a cyber resilience act. Applied Cybersecurity & Internet Governance, 1(1), 1-17.

[78]. Fuggini, C., Solari, C., De Stefano, R., Bolletta, F., & De Maio, F. V. (2023). Assessing resilience at different scales: from single assets to complex systems. *Environment Systems and Decisions*, *43*(4), 693-707.

[79]. Rathnayaka, B., Robert, D., Adikariwattage, V., Siriwardana, C., Meegahapola, L., Setunge, S., & Amaratunga, D. (2024). A unified framework for evaluating the resilience of critical infrastructure: Delphi survey approach. *International Journal of Disaster Risk Reduction*, *110*, 104598. https://doi.org/10.1016/j.ijdrr.2024.104598

[80]. Kopustinskas, V., Foretic, H., & Asensio Bermejo, I. (Eds.). (2024). *Resilience assessment: Methodological challenges and applications to critical infrastructures* (Proceedings of the 63rd ESReDA Seminar, Joint Research Centre, Ispra, Italy, 25–26 October 2023). Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC139101/JRC139101_01.pdf