ANNALS OF THE "CONSTANTIN BRÂNCUȘI" UNIVERSITY OF TÂRGU JIU
LETTER AND SOCIAL SCIENCE SERIES

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

2/2025 ***https://alss.utgjiu.ro***

CONSIDERATIONS REGARDING THE REGULATORY FRAMEWORK IN ROMANIA ON THE ISSUE OF CRITICAL INFRASTRUCTURE PROTECTION

Cătălin PEPTAN

„Constantin Brâncuși" University of Târgu Jiu, Romania

Abstract: *The paper analyzes the institutional architecture and regulatory framework of Romania in the field of critical infrastructure protection, aiming to assess the level of coherence, efficiency, and adaptability to the new European requirements regarding the resilience of essential infrastructures. Using a qualitative methodology based on documentary and comparative analysis, the study investigates the functional relationships among the main responsible authorities - the Ministry of Internal Affairs (MAI), the National Coordination Center for Critical Infrastructure Protection (CNCPIC), the National Cyber Security Directorate (DNSC), and the interinstitutional support structures - in the context of transposing Directive (EU) 2022/2557 (CER) and aligning with Directive (EU) 2022/2555 (NIS2). The results highlight a moderate institutional coherence, with overlapping competencies and difficulties in coordinating responses to incidents with hybrid components. Although the legislative framework has been significantly strengthened recently through Law No. 294/2024 and Government Emergency Ordinance no. 155/2024 (approved by Law No. 124/2025), the operationalization process is still ongoing, requiring performance indicators and integrated monitoring mechanisms. The paper emphasizes the need for an adaptive governance model based on interinstitutional cooperation, public-private partnerships, and digital tools such as the NIS2@RO platform, as a main vector for strengthening infrastructural resilience. The conclusions underline the importance of convergence between physical and cyber security, the clarity of institutional roles, and the integration of a unified system for risk reporting and assessment as prerequisites for sustainable critical infrastructure protection in Romania.*

Keywords: *critical infrastructures, protection, resilience, institutional framework, Romania*

Contact details of the author(s): catalinpeptantm@gmail.com

1. INTRODUCTION

1.1. General Context of the Topic

In a global context characterized by increasingly pronounced economic, technological, and geopolitical interdependencies, critical infrastructures constitute the foundation of modern states' functioning. They represent the ensemble of systems, facilities, services, and networks indispensable for maintaining the vital functions of society, national security, public health, social order, and economic stability.

In Romania, the protection of critical infrastructures has become a strategic priority amid European integration, accelerated digitalization, and the multiplication of hybrid threats - ranging from cyberattacks targeting energy and financial infrastructures to disruptions caused by health crises, natural disasters, or regional conflicts. The COVID-19 pandemic, the war in Ukraine, the economic contraction within the European area, and major cyber incidents in recent years have highlighted the vulnerability of national critical infrastructures, as well as the importance of strengthening systemic resilience (Mărcău *et al.*, 2025; Zmădu, 2021; Nemoianu, 2025).

In this context, Romania, as a member state of the European Union (EU), has gradually developed its own institutional and regulatory framework for protecting critical infrastructures, aligned with European requirements and best practices. Thus, the protection of critical infrastructures is no longer perceived merely as an administrative obligation but as a strategic process integrated into the broader framework of national security, civil protection, and defense policies.

1.2. The Importance of Critical Infrastructure Protection in the Current National Context

The role of critical infrastructures in ensuring state security is essential. Any malfunction in energy, communications, transport networks, or financial systems can generate chain effects on the economy and public services. Moreover, the increasing dependence on digital technologies amplifies the risks associated with cyberattacks, making critical infrastructure protection a domain of integrated security.

In Romania, the importance of critical infrastructure protection is reflected in: strengthening response capacities to incidents and crises; enhancing institutional and operational resilience; protecting citizens and the national economy against major disruptions; aligning with European standards on the resilience of critical entities; and developing a security culture at both societal and institutional levels.

Therefore, the protection of critical infrastructures is a dynamic process that requires the continuous adaptation of the regulatory framework and institutional structures to new and emerging risks.

1.3. The Context of the Emergence of National Policies in the Field

Romania began developing its national framework for critical infrastructure protection in the 2000s, in parallel with European initiatives in the field - *Directive 2008/114/EC* (Directive 2008/114/EC, 2008). The first significant step was the adoption, in 2010, of *Government Emergency Ordinance No. 98 of November 3, 2010, on the identification, designation, and protection of critical infrastructures* (Government of Romania, 2010) - as subsequently amended - followed in 2011 by the adoption of *Government Decision No. 718 of July 13, 2011, approving the National Strategy for the Protection of Critical Infrastructures* (Government of Romania, 2011a), which established the

principles and general directions of action, the procedures for identifying and designating national and European critical infrastructures, as well as the responsibilities of the institutions involved.

Romania strengthened the link between physical and digital critical infrastructures through the implementation of *Law No. 362/2018* (Parliament of Romania, 2019), which transposed the *NIS Directive (EU) 2016/1148* (European Union, 2016) on the security of network and information systems. Further progress was made with *Law No. 294/2024* (Parliament of Romania, 2024a) and *Government Emergency Ordinance no. 155/2024* (Government of Romania, 2024), approved by *Law No. 124/2025* (Parliament of Romania, 2025a), which transpose into national law the provisions of *Directive (EU) 2022/2557 (CER)* (European Union, 2022) on the resilience of critical entities. This marks the transition to an integrated approach that connects cybersecurity with the protection of critical infrastructures.

Moreover, the *National Defense Strategy of Romania for the period 2020–2024* (Parliament of Romania, 2020) identifies critical infrastructures as essential elements of national security. The document emphasizes the importance of protecting and strengthening their resilience against hybrid, cyber, and systemic risks in order to ensure the continuity of the state's vital functions and societal stability.

A central role in the national architecture is played by the National Coordination Center for Critical Infrastructure Protection (CNCPIC) (National Center for Critical Infrastructure Protection, n.d.), under the authority of the Ministry of Internal Affairs (MAI), which ensures coordination, monitoring, and analysis in this field. Additionally, other institutions - such as the Department for Emergency Situations (DSU), the Romanian Intelligence Service (SRI), the National Cyber Security Directorate (DNSC), and line ministries - contribute to the protection of infrastructures within their respective sectors.

1.4. Purpose, Hypotheses, and Objectives of the Study

Research Purpose:

The study aims to analyze the coherence, efficiency, and level of integration of Romania's institutional framework for critical infrastructure protection in the context of transformations generated by the new European directives on the resilience of critical entities (*CER*) and cybersecurity (*NIS2*). The research seeks to provide a comprehensive assessment of how the responsible institutions - at national, sectoral, and operational levels - cooperate in the prevention, protection, and response to incidents that may affect the functioning of essential services.

The main contribution of the study lies in integrating two complementary perspectives: the normative-institutional analysis (governance, competences, mechanisms) and the assessment of resilience capacity (organizational, operational, and cyber). Through this approach, the research offers a conceptual model applicable to the analysis of critical infrastructure resilience at both national and European levels.

Research Hypotheses

Hypothesis 1. The current institutional framework for the protection of critical infrastructures exhibits a good level of coherence, yet it is characterized by overlapping competences and by cooperation among actors that remains in need of improvement.

Hypothesis 2. The national transposition of the European directives (*CER* and *NIS2*) has not yet been fully operationalized at the level of institutional practices and reporting processes.

Hypothesis 3. The maturity of public–private cooperation and information sharing regarding risks and incidents is uneven across sectors, being more advanced in those with a strong cyber component.

Hypothesis 4. The level of institutional and operational resilience is positively correlated with the clarity of responsibilities, the frequency of interinstitutional exercises, and the analytical capacity of institutions.

Hypothesis 5. The integration of the cyber dimension into critical infrastructure management leads to a significant increase in prevention and response capacity to major incidents.

Research Objectives

General Objective*:*

To evaluate Romania's institutional and regulatory framework for critical infrastructure protection in relation to European requirements for resilience and cybersecurity.

Specific Objectives*:*

O1. To analyze the governance structure and the distribution of competences among the main institutions involved.

O2. To assess the degree of alignment between national legislation and the *CER* and *NIS2* directives.

O3. To examine interinstitutional and public–private cooperation mechanisms.

O4. To identify the main vulnerabilities and directions for strengthening institutional resilience.

O5. Assessing the need for an integrated governance model for critical infrastructure protection.

1.5. Research Methodology

The research has a qualitative, analytical, and documentary character, being based on an integrated analysis of the normative, institutional, and strategic framework regarding the protection of critical infrastructures in Romania. The methodological approach aims to highlight the coherence of the national governance system, the degree of alignment with European requirements concerning resilience and cybersecurity, as well as the main institutional dysfunctions that affect the implementation of public policies in the field.

The research process was carried out in several interdependent stages, in which the analytical methods were applied complementarily. In the *first stage*, a documentary analysis was conducted, focusing on the identification and examination of relevant national and European legislation (*Government Emergency Ordinance No. 98/2010, Law No. 362/2018, Law No. 294/2024, Government Decision no. 35/2019, Government Decision No. 733/2022, Government Emergency Ordinance no. 155/2024, Law No. 124/2025*, and the *CER* and *NIS2 Directives*). This analysis allowed for the delineation of the conceptual and institutional framework for critical infrastructure protection and for understanding its evolution in the European context

In the *second stage*, an institutional analysis was applied, focusing on identifying the main actors - such as CNCPIC, DNSC, DSU, sectoral authorities, and essential service operators - and examining their roles, competences, and coordination relationships. The analysis sought to highlight the functioning of the institutional architecture, the degree of integration of the cyber dimension, and the existence of interinstitutional cooperation mechanisms.

Subsequently, through comparative and correlation analysis, the degree of compliance of national legislation with the requirements of the European directives was assessed, identifying both areas of overlap and implementation gaps. This gap analysis made it possible to formulate conclusions regarding the maturity level of the governance system and the need to update normative instruments.

The results of these three stages were intended to provide a coherent overview of how Romania manages critical infrastructure protection.

The research relies exclusively on official and public sources - normative acts, strategic documents, institutional reports, and specialized studies - while adhering to the principles of scientific rigor, transparency, and academic ethics. The limitations of the study stem from the absence of empirical data and the inaccessibility of classified information; however, these are compensated through source triangulation and a comparative approach to European and national legislation.

2. CONCEPTUAL AND REGULATORY FRAMEWORK

2.1. Definition of Critical Infrastructure

According to *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), critical infrastructure is defined as "*an element, a system, or a part thereof, located on the national territory, which is essential for maintaining the vital functions of society, health, safety, security, and the economic and social well-being of the population, and whose disruption or destruction would have a significant impact on the state*". This definition reflects a systemic and integrated approach, highlighting: the essential character of infrastructure for the functioning of society; the interdependence of sectors (economic, energy, information, health, transport, etc.); and the potentially major impact of dysfunctions on national security.

Furthermore, the aforementioned legal act defines European critical infrastructure as "a *national critical infrastructure whose disruption or destruction would have a significant impact on at least two EU Member States*". This definition emphasizes a transnational and interdependent approach, underlining: the shared and interconnected nature of critical infrastructures at the EU level; and the need for supranational cooperation and coordination in matters of protection and resilience, given the potentially far-reaching effects of incidents on the security, economy, and societal functioning of multiple states.

In its current understanding, critical infrastructure may be physical (networks, equipment, facilities, logistical resources) or cyber (information systems, databases, digital infrastructures), and their protection must be conceived within a unified framework, with a focus on integrated resilience.

2.2. The General Regulatory Framework on National Critical Infrastructures

Romania's system for the protection and resilience of critical infrastructures is based on a coherent set of legal regulations, structured around *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), which establishes the principles, sectors, and institutional responsibilities in the field. Article 2, paragraph (1) of *Government Emergency Ordinance No. 98/2010* defines the scope of the regulation, indicating the sectors and subsectors of national critical infrastructures (see Table 1). This measure represents the operational foundation of the national critical infrastructure protection system and aims to cover the entire spectrum of infrastructures that can be considered critical. By clearly defining areas of action and institutional responsibilities, it ensures: comprehensive coverage of infrastructures that require protection; effective institutional accountability; and an organizational framework that enables continuous coordination, monitoring, and assessment of risks and vulnerabilities.

Note: *Government Emergency Ordinance No. 98 of November 3, 2010*, has undergone successive improvements through *Law No. 225/2018* (Parliament of Romania, 2018), *Government Emergency Ordinance No. 61/2019* (Government of Romania, 2019a), *Law No. 344/2023* (Parliament of Romania, 2023a), and *Law No. 294/2024* (Parliament of Romania, 2024a).

No.	Sector	Main Subsectors	Responsible Public Authority
1	Energy	Production, transmission, and distribution of electricity; extraction, transport, and distribution of natural gas; oil and petroleum products	Ministry of Energy
2	Transport	Air, rail, road, naval, and subway transport; logistics infrastructures; traffic control	Ministry of Transport and Infrastructure
3	Water and Environment	Water supply, sewerage, protection of water resources, dams, hydrotechnical installations, environmental monitoring	Ministry of Environment, Waters and Forests
4	Public Health	Strategic hospitals, emergency networks, pharmaceutical and medicine distribution infrastructures	Ministry of Health
5	Information and Communications	Telecommunications networks, internet, digital services, data centers, emergency radiocommunications	Ministry of Economy, Digitalization, Entrepreneurship, and Tourism
6	Financial and Banking	Banks, stock exchanges, payment systems, insurance, treasury, electronic financial infrastructure	Ministry of Finance / National Bank of Romania (NBR)
7	Food Supply and Agriculture	Production, storage, and distribution of food; vital agri-food chains	Ministry of Agriculture and Rural Development
8	Public Administration and Public Order	Public administration system, emergency services, police, gendarmerie, civil protection	Ministry of Internal Affairs (MAI)
9	Defense and National Security	Strategic military infrastructures, defense logistics, special communications	Ministry of National Defense (MoND) / Special Telecommunications Service (STS)
10	Justice and Foreign Affairs	Courts, prosecutor's offices, penitentiary system, diplomatic infrastructures	Ministry of Justice / Ministry of Foreign Affairs
11	Research and Education	Strategic research infrastructures, universities of national importance, scientific databases	Ministry of Education and Research
12	Emergency Services and Civil Protection	Inspectorates for Emergency Situations (ISU), SMURD, emergency communications, intervention logistics	Department for Emergency Situations (DSU) – coordinated by the Ministry of Internal Affairs (MAI)

Table 1. Sectors and Subsectors of National Critical Infrastructures

Although *Government Decision No. 1198/2012 on the designation of national critical infrastructures* (Government of Romania, 2012) - with subsequent amendments in 2015 (Government of Romania, 2015), 2018 (Government of Romania, 2018), 2020 (Government of Romania, 2020), 2021 (Government of Romania, 2021), and 2022 (Government of Romania, 2022a; 2022b) - does not actually publish the lists of critical objectives (as they are classified), the annex includes a table outlining the allocation of institutional responsibilities. This allows, by logical analogy, the identification of the domains/sectors of national critical infrastructures. Each sector is

managed by a competent authority at the national level (usually a ministry or government agency), responsible for identifying the critical infrastructures within its domain and coordinating protection measures.

Government Decision No. 1154/2011 on the approval of the critical thresholds corresponding to the cross-sectoral criteria underlying the identification of potential national critical infrastructures, as well as on the approval of the Methodology for applying these thresholds and establishing the level of criticality (Government of Romania, 2011b), represents a key normative act in strengthening the national framework for critical infrastructure protection. Adopted pursuant to Article 9 (5) of *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), this decision details the operational modalities of the process for identifying, evaluating, and classifying national critical infrastructures. Its main purpose is to establish the critical thresholds corresponding to the cross-sectoral criteria used to determine the level of importance of infrastructures, regardless of the economic or administrative sector in which they operate. At the same time, the decision approves the Methodology for applying these thresholds, which defines the stages and analytical tools used to determine the level of criticality for each evaluated objective. In this way, the document creates a common and coherent framework for responsible public authorities, ensuring uniformity in the evaluation process at the national level.

The decision establishes a phased and rational process of analysis, starting from the assessment of the potential impact of dysfunctions on the population, economy, environment, and public order. Depending on the results obtained, infrastructures are classified according to levels of criticality, which determine the corresponding protection and monitoring measures.

Through this normative act, Romania made a decisive step in implementing the national framework for critical infrastructure protection, ensuring a correlation between national criteria and the European standards set out in *Directive 2008/114/EC* (Directive 2008/114/EC, 2008). At the same time, the decision strengthens the role of the competent institutions - particularly the CNCPIC - in coordinating the process of evaluating and designating infrastructures essential to the functioning of the state.

On the other hand, *Government Decision No. 733/2022* (Government of Romania, 2022c) approves the methodological norms for identifying strategic national objectives in the design phase, establishing the procedural framework for evaluating and selecting investment projects of strategic importance to the state. The act aims at the early identification of projects that may later become national critical infrastructures through a phased process involving: impact assessment, designation as a strategic objective, and subsequent classification as a critical infrastructure. The selection is based on cross-sectoral criteria such as strategic importance, feasibility, sustainability, security, and contribution to national cohesion.

Although Romanian legislation does not explicitly define the concept of "cyber critical infrastructure"- which can logically be understood as deriving from the combination of the concepts of "national critical infrastructures" and "essential network and information systems"- *Law no. 362/2018 on ensuring a high common level of security for network and information systems* (Parliament of Romania, 2019), which transposes *Directive (EU) 2016/1148 (the NIS Directive)* (European Union, 2016), marks the institutionalization of digital infrastructure protection. The act introduces the concept of "operator of essential services", designating entities that provide services critical to the proper functioning of the economy and society - such as those in the fields of energy, transport, health, drinking water supply, digital infrastructure, and financial services. These entities are required to implement appropriate technical and organizational measures to manage risks to the networks and information systems they use.

At present, Romania is in the process of transposing *Directive (EU) 2022/2555 (NIS 2)* (European Union, 2022), which extends security obligations to new categories of essential and important entities, alongside the adoption of an institutionalized framework (the national civil cybersecurity framework) through *Government Emergency Ordinance No. 155/2024* (Government of Romania, 2024), approved *by Law No. 124/2025* (Parliament of Romania, 2025a), with subsequent norms and practical instruments. This is the case of NIS2@RO, designed as a national electronic platform developed by the DNSC for the implementation and monitoring of *Directive (EU) 2022/2555 (NIS2)* in Romania, facilitating the registration of regulated entities, incident reporting, and the secure exchange of information between operators and competent authorities (National Cyber Security Directorate, n.d.).

Through the aforementioned normative acts, Romania strengthens a proactive and unified mechanism for the planning of strategic investments, ensuring the alignment of infrastructural development with national security and resilience objectives.

2.3. Interdependence of Critical Infrastructures

A central element of the concept of critical infrastructure protection is the interdependence among sectors, which reflects the complexity and high degree of connectivity of systems essential to the functioning of modern society (Seppänen, Luokkala, Zhang, Torkki, & Virrantaus, 2018).

In a globalized and digitalized economy, critical infrastructures do not operate in isolation but form a network of functional, technical, and informational dependencies, in which the disruption of one element can generate cascading effects on others. For instance, a simple interruption in electricity supply can cause major dysfunctions in electronic communication networks, transport systems, medical infrastructures, or financial services (Panteli & Mancarella, 2015). Likewise, a failure in IT&C infrastructure may affect the data flows necessary for operating defense, public safety, or emergency management systems (Roshanaei, 2021). These examples illustrate the systemic and interconnected nature of critical infrastructures, where the resilience of one sector directly depends on the robustness of the others.

In Romania, the legislative and strategic framework - established through *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010) and *Government Decision No. 718/2011, which approves the National Strategy for the Protection of Critical Infrastructures* (Government of Romania, 2011a) - explicitly emphasizes the importance of addressing interdependencies. These normative acts promote an integrated vision of security, based on interinstitutional cooperation and the cumulative assessment of risks that may simultaneously affect multiple sectors.

Infrastructure interdependencies manifest on several levels: *Physical*, through material connections between networks (for example, the dependence of transport systems on energy supply or fuel); *Cyber,* through digital interfaces that link data and control infrastructures; *Functional*, through dependencies on support services (logistics, communications, security); and *Geographical*, through the spatial proximity of certain assets and their shared exposure to natural or technological risks.

The recognition of these interdependencies has led to a paradigm shift in critical infrastructure management. Currently, modern protection strategies are based on a systemic and multisectoral approach that integrates risk analysis, continuity planning, and interinstitutional cooperation (Organisation for Economic Co-operation and Development [OECD], 2019). Accordingly, current policies aim to: conduct an integrated analysis of risks and vulnerabilities, by assessing cross-sectoral effects and the potential for disruption propagation (European Union, 2022, Art. 12 para. (2));

establish coordinated continuity and response plans, enabling rapid and efficient reactions in the event of a major incident (European Union, 2022, Art. 12 para. (2); Art. 13 para. (1); International Organization for Standardization, 2019); and promote extensive cooperation between public institutions, the private sector, and local authorities, since critical infrastructures are often operated by diverse public and private entities whose collaboration is essential for collective resilience (Organisation for Economic Co-operation and Development, 2019).

In this context, it should be noted that, from a complementary perspective, public–private cooperation in the field of critical infrastructures in Romania is unevenly developed, with mature sectors such as energy, finance, and telecommunications benefiting from robust collaboration and security mechanisms, while sectors in early stages of development exhibit institutional gaps, coordination deficiencies, and low levels of integration of private actors into risk-management processes (Dănilă, 2012; Năstase, C. et al., 2022; Mitrescu, 2025).

In Romanian legislation, the systemic and multisectoral approach to critical infrastructures is summarized in Table 2:

Principle	**Normative Act**	**Article / Chapter**	**Essence of the Provision**
Systemic, cross-sectoral approach	GEO No. 98/2010	Art. 6 para. (1); Art. 9 para. (3)	Analysis of cross-sectoral effects and interdependencies among infrastructures
Risk and Continuity Analysis	GD No. 1154/2011	Art. 1-2; Annex no. 2	Integration of risk analysis and vulnerability assessment
Public-Private Cooperation	GD No. 718/2011; GD No. 155/2024	Chapters 3, 5, and 6; Article 2(1) (b), (c); Article 3(1)(c); Article 11(1) and (9); Article 12 (2); Article 15(1); Article 21	Interinstitutional partnership and collaboration with private operators
Digital Component / NIS Cooperation	Law No. 362/2018	Art. 25, 32, 33	Coordination between the DNSC and operators of essential services
Integrated Approach and National Resilience	National Defense Strategy of Romania 2020-2024	Chapters 1, 3, and 5	Promotes an integrated vision of national resilience encompassing economic, energy, cyber, and social dimensions; supports public–private partnerships for the protection of critical infrastructures.
NOTE: GEO - Government Emergency Ordinance No. 98/2010; GD - Government Decision			

Table 2. Systemic and Multisectoral Approach to Critical Infrastructures

Through this approach, the protection of critical infrastructures becomes a collective effort based on information sharing, system interoperability, and the development of common capabilities for prevention, response, and recovery. In the current context - marked by complex threats ranging from cyberattacks and energy disruptions to natural disasters and geopolitical risks - the interdependence of infrastructures represents not only a vulnerability but also an opportunity to strengthen national resilience through strategic coordination.

Thus, understanding and managing the interdependencies among critical infrastructures form the foundation of sustainable national security, capable of ensuring the continuity of the state's vital functions and the protection of society against systemic risks and cascading effects.

3. NATIONAL INSTITUTIONAL FRAMEWORK FOR THE PROTECTION OF CRITICAL INFRASTRUCTURES

3.1. General Premises

The protection of critical infrastructures represents a central pillar of national security, as these infrastructures support the vital functions of the state and society. Romania, as a member state of the EU and NATO, through the legislation adopted in this field, has assumed the obligation to develop a coherent institutional system capable of preventing, managing, and mitigating the effects of threats to critical infrastructures, whether physical, cyber, or hybrid in nature. Thus, the national system has evolved into an integrated network of public authorities and private entities, coordinated centrally by the MAI through the CNCPIC. This architecture enables a unified and coordinated approach, in accordance with the principles of interinstitutional cooperation, shared responsibility, and subsidiarity.

3.2. The Ministry of Internal Affairs (MAI) and the National Center for the Coordination of Critical Infrastructure Protection (CNCPIC)

The MAI is the central institution responsible for ensuring national coordination in the field of critical infrastructure protection. According to *Government Emergency Ordinance No. 98/2010 on the identification, designation, and protection of critical infrastructures* (Government of Romania, 2010), Article 4, as amended by point 4, Article I of *Law No. 225/2018* (Parliament of Romania, 2018), it is specified that: *"the responsibility for organizing and carrying out the activities necessary for the implementation of the legislation specific to the field of critical infrastructure protection (CIP) lies with the Ministry of Internal Affairs, hereinafter referred to as M.A.I., through the National Center for the Coordination of Critical Infrastructure Protection (CNCPIC)."*

Furthermore, *Government Decision No. 718/2011* (Government of Romania, 2011a) approves the National Strategy for the Protection of Critical Infrastructures (Article 1) and establishes the obligation of CNCPIC to elaborate the action plan for the implementation of the strategy (Article 2).

By virtue of its responsibilities, the MAI develops policies, methodological norms, and regulations, supervises the implementation of sectoral measures, and maintains relations with European and international bodies. Consequently, the main duties of the MAI are as follows:

1. *National coordination of activities related to critical infrastructure protection* (Art. 4, para. 1 of *Government Emergency Ordinance No. 98/2010*, as amended by point 4, Art. I of *Law No. 225/2018*; Government of Romania, 2010; Parliament of Romania, 2018) - ensuring interinstitutional coordination between public authorities responsible for various domains/sectors and managing the general framework for cooperation with the European Commission and EU Member States regarding European critical infrastructures.
2. *Development of the normative and methodological framework* (Art. 4, para. 2 of *Government Emergency Ordinance No. 98/2010*, as amended by point 4, Art. I of *Law No. 225/2018*, and Art. 9, para. 5 of *Government Emergency Ordinance No. 98/2010*; Government of Romania, 2010; Parliament of Romania, 2018) - includes the procedures, criteria, and methodologies for identifying and designating national and European critical infrastructures; risk and vulnerability assessment methodologies; as well as technical guidelines and standards for implementing protection measures.

3. *Implementation and monitoring of the National Strategy for the Protection of Critical Infrastructures* (Government of Romania, 2011a, Art. 2), through CNCPIC, which is responsible for: developing the action plan for the implementation of the strategy; monitoring the stage of implementation of the established measures; and periodically assessing the effectiveness of policies in the field.

4. *Designation and support of competent authorities by sector* (*Government Emergency Ordinance No. 98/2010*, Art. 6, paras. 1–3, supplemented by point 7, Art. I of *Law No. 225/2018*; Government of Romania, 2010; Parliament of Romania, 2018) - coordinates the process of designating public authorities responsible for each critical infrastructure sector; provides technical assistance and methodological coordination to these authorities.

5. *Management of information exchange and international cooperation* (*Government Emergency Ordinance No. 98/2010*, Art. 6, para. 1, supplemented by point 7; Art. I of *Law No. 225/2018*; Government of Romania, 2010; Parliament of Romania, 2018) - maintains contact with relevant European structures (for example, the Directorate-General for Home Affairs of the European Commission); coordinates reporting mechanisms to European institutions regarding critical infrastructures; and ensures Romania's participation in cooperation networks and international exercises in the field.

6. *Support in emergency management* (Parliament of Romania, 2004, Art. 24, paras. 1-4; Government of Romania, 2016, Art. 6, para. 1) - through the Department for Emergency Situations (DSU) and the General Inspectorate for Emergency Situations (IGSU), the MAI contributes to: the operational response to incidents affecting critical infrastructures; the restoration of functionality to affected infrastructures; and post-event analysis aimed at improving resilience.

7. *Analysis, evaluation, and technical support through CNCPIC* (*Government Emergency Ordinance No. 98/2010*, Art. 5, paras. 1–2, as amended by point 2, Art. I of *Law No. 18/2011*; Government of Romania, 2010; Parliament of Romania, 2011; Annex No. 2 to Government Decision No. 1154/2011, Government of Romania, 2011b), which carries out: the analysis of risks and vulnerabilities of critical infrastructures; management of databases regarding national and European critical infrastructures; coordination of information exchange between authorities and operators; and advisory support for decision-makers.

It is also worth noting that the MAI, through CNCPIC, is responsible for the national transposition of obligations derived from EU initiatives regarding the resilience of critical and essential digital infrastructures, such as *Directive 2008/114/EC* and *Directive (EU) 2022/2557 – the CER Directive*.

Furthermore, the MAI extends its coordination activities to emerging critical infrastructures, such as IT networks, healthcare systems, logistics chains, and 5G communication infrastructures. In this context, CNCPIC collaborates with authorities such as the DNSC and the Ministry of Energy to ensure an integrated approach to the protection and resilience of critical infrastructures.

Through the entirety of its responsibilities, the MAI - through CNCPIC - acts as the central coordinating authority of the national system for the protection and resilience of critical infrastructures, ensuring the connection between Romania's national security policies and its European commitments.

3.3. Institutions and Complementary Structures

The institutional architecture for the protection of critical infrastructure is multi-level, involving numerous institutions, each with specific responsibilities:

- *Department for Emergency Situations (DSU)* (Art. 1 of Government Emergency Ordinance No. 1/2014; Government of Romania, 2014) - has responsibilities for the coordination and control of civil protection activities at the national level, the development of policies and strategies in the field, the organization of operational interventions, and the training of the population.
- *Romanian Intelligence Service (SRI)* (Romanian Intelligence Service, n.d.; Parliament of Romania, 2023b, Art. 14) - holds competences related to national security, including the protection of strategically important and cyber critical infrastructures, providing the intelligence and counterintelligence component necessary for their defense.
- *National Cyber Security Directorate (DNSC)* (Parliament of Romania, 2021; Parliament of Romania, 2019, Arts. 25–33; Parliament of Romania, 2024b, Art. 2, letter c) - is the national competent authority in the field of network and information systems security, with responsibilities for developing and implementing public policies and the regulatory framework on cybersecurity, monitoring, preventing, and managing cyber incidents, coordinating the national CSIRT network, international cooperation with EU and NATO institutions, as well as operational and advisory support for public and private entities providing essential or vital services.
- *Line ministries* (Government of Romania, 2010, Art. 2, para. (1); Government of Romania, 2012, Art. 2 and Annex 2; Government of Romania, 2019b; Government of Romania, 2011b) – act as competent authorities for specific critical infrastructure sectors: Ministry of Energy - for the energy sector; Ministry of Transport and Infrastructure - for road, rail, air, and naval infrastructure; Ministry of Health - for the medical sector; Ministry of Finance - for the financial and banking system; Ministry of Environment, Waters and Forests - for the water and natural resources sector.
- *Local public authorities* (Parliament of Romania, 2004, Art. 25; Government of Romania, 2016, Art. 4, para. 1) - are responsible for implementing protection measures at the territorial level, in cooperation with the structures of the Ministry of Internal Affairs.

This complex institutional network is essential for an integrated approach to risk management and for addressing interdependencies among different critical infrastructure sectors.

3.4. Public–Private Cooperation

A central element of the national policy for critical infrastructure protection is the public-private partnership. Given that the majority of critical infrastructures are owned or managed by private economic operators (particularly in the energy, transport, and communications sectors), their cooperation with state institutions is vital for crisis prevention and management.

The legal framework - *Government Emergency Ordinance No. 98/2010 on the identification, designation, and protection of critical infrastructures* (Government of Romania, 2010), approved by *Law No. 18/2011* (Parliament of Romania, 2011), and the government decisions establishing the sectoral implementation framework, such as: *Government Decision No. 1154/2011, Government Decision No. 1198/2012, Government Decision No. 557/2016*, and *Government Decision No. 35/2019* —- provides that operators are required to: designate persons responsible for critical infrastructure security; develop their own security plans; participate in information exchange and in exercises organized by the authorities; report major incidents that could affect the functioning of the infrastructure.

In turn, the state - primarily through the CNCPIC within the MAI - ensures methodological support, general coordination, and the protection of sensitive data transmitted within the cooperation framework.

However, the public-private partnership remains a work in progress, facing challenges such as: lack of trust between the public and private sectors; absence of economic incentives for investment in protection; differences in technological and managerial capacity among operators.

To overcome these limitations, the *National Strategy for Critical Infrastructure Protection* (Government of Romania, 2011a) promotes a modern vision of national security, in which public–private cooperation, transparency, and trust form the main pillars of a sustainable protection and resilience system.

Through this framework of ongoing collaboration, Romania aims to develop an integrated security ecosystem, where all public institutions and private operators act in a coordinated manner to achieve common objectives of security and continuity of essential services.

3.5. Critical Assessment and Development Perspectives

Although Romania has a relatively well-defined institutional framework, evaluations conducted in recent years highlight the need for structural adjustments and legislative updates. Among the main development directions are: modernizing the activities of the institutions involved in the *National Strategy for the Protection of Critical Infrastructures* (Government of Romania, 2011a), through the implementation of the digital dimension and the resilience principles established by *Directive (EU) 2022/2557*; creating a unified incident reporting and analysis system, interoperable across sectors; strengthening the CNCPIC's capacities through additional resources and modern analytical tools; continuous professional training for personnel involved in the protection of critical infrastructures; improving public communication and education regarding security culture.

These directions aim to transform the institutional framework from a predominantly reactive system into a proactive and adaptable one, capable of dynamically responding to current security challenges.

The national institutional framework for the protection of critical infrastructures is the result of a gradual construction process, based on coordination among administrative levels, economic sectors, and international partners. Although there are challenges related to resources, communication, and interoperability, the Romanian system is compatible with European standards and provides a solid foundation for strengthening national resilience.

4. NATIONAL MECHANISMS AND INSTRUMENTS FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE

4.1. General Premises

In Romania, the protection of critical infrastructure is carried out through regulations, institutional structures, operational mechanisms, and technical instruments capable of ensuring the prevention, reduction, and management of risks. The central objective of the issue under analysis is the identification, designation, and protection of national critical infrastructures, in close correlation with European critical infrastructures, so as to ensure the continuous operation of vital services and their resilience to natural, technological, human, or cyber threats.

4.2. Identification and Designation of Critical Infrastructures

The identification of critical infrastructures represents a fundamental stage in the process of establishing a national and European system for the protection of elements essential to the functioning of society. According to Article 9 of *Government Emergency Ordinance No. 98/2010*

(Government of Romania, 2010) - with subsequent amendments presented in Chapter 2.2 - approved by *Law No. 18/2011* (Parliament of Romania, 2011), this process aims to delineate those infrastructures whose disruption or destruction would have a significant impact on national security, the economy, public health, or the well-being of the population.

The responsibility for identifying critical infrastructures lies with public authorities designated for specific sectors of activity. These authorities act in cooperation with the owners, operators, or administrators of the infrastructures, who are obliged to actively participate in defining the criteria and critical thresholds. Thus, the identification process is a complex one, based on interinstitutional collaboration and detailed technical and economic assessments.

Identification is carried out through the application of sectoral and cross-sectoral criteria. The sectoral criteria are established by the heads of the responsible public authorities through specific orders for each field (energy, transport, communications, health, food, etc.) and address the particularities of each economic sector. The cross-sectoral criteria, common to all fields, are defined by ordinance and concern three essential dimensions of potential impact: the victims criterion, which assesses the possible number of deaths or serious injuries; the economic effects criterion, which considers material losses, degradation of services or products, and possible environmental consequences; the effects on the population criterion, analyzed from the perspective of disruptions to daily life, loss of essential services, and decline in public confidence. These criteria are not cumulative, as fulfilling any one of them is sufficient to justify the inclusion of an infrastructure in the category of critical infrastructures. The critical thresholds corresponding to these criteria - that is, the levels of impact severity triggering the qualification of an infrastructure as critical - are established by *Government Decision No. 1154/2011* (Government of Romania, 2011b), ensuring a unified and coherent approach at the national level.

The actual identification procedure involves a step-by-step selection process: the existing infrastructures within a sector are inventoried, the defined criteria and thresholds are applied, the cross-sectoral impact is assessed, and finally, a list is drawn up of infrastructures that meet the conditions to be considered potential national or European critical infrastructures. In the case of the latter, the process also includes an analysis of cross-border impact, determining the extent to which the disruption of an infrastructure located on Romanian territory could affect other EU member states.

The identification process is, therefore, a strategic and preventive endeavor, aimed at laying the foundation for the subsequent stages of designation and protection of critical infrastructures. It ensures a comprehensive understanding of systemic vulnerabilities and enables the implementation of public security policies based on risk assessment and resource prioritization. In the absence of a rigorous identification process, neither the effectiveness of protection measures nor the compatibility of the national framework with European standards and cooperation mechanisms in this field can be guaranteed. Therefore, the process of identifying critical infrastructures, as regulated by *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010) - with subsequent amendments -, represents the conceptual and operational foundation of the national policy for the protection of vital infrastructures, contributing to the maintenance of society's vital functions and to the strengthening of national security within the European framework.

The designation of critical infrastructures represents the subsequent and complementary stage of the identification process, through which an element, system, or component is granted the official legal status of national critical infrastructure or European critical infrastructure. This stage is regulated by Article 10 of *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), with later amendments presented in Chapter 2.2. This stage is of major importance, as only

designated infrastructures benefit from the legal protection regime established by the ordinance, including specific measures of security, control, and inter-institutional cooperation.

The designation is carried out based on the results of the identification process conducted by the public authorities responsible for each sector of activity. After completing the analysis and validating the impact criteria, these authorities formulate designation proposals, which are then submitted to the Government for approval. The designation of national critical infrastructures is thus made by Government Decision, an act that grants the respective infrastructure an official status within the national system for the protection of critical infrastructures.

In the case of European critical infrastructures, the designation procedure is more complex, as it involves a cross-border dimension and cooperation among EU Member States. Thus, after identifying a potentially critical infrastructure at the European level, the MAI, through the CNCPIC, notifies the Member States that could be significantly affected by a possible disruption of that infrastructure. This is followed by bilateral and/or multilateral consultations between Romania and the concerned Member States in order to reach a common agreement on the designation. If the competent national authorities consider that Romania may be affected by a potentially critical infrastructure located on the territory of another Member State, the competent authorities notify CNCPIC within the MAI, which in turn informs the Prime Minister. With the Prime Minister's approval, the MAI, through CNCPIC, notifies the European Commission regarding Romania's intention to participate in the bilateral or multilateral consultations necessary to obtain the agreement of the Member State on whose territory the infrastructure proposed for designation as European critical infrastructure is located. In this way, the principles of consensus and cooperation among Member States are ensured, avoiding the unilateral imposition of decisions that may generate significant cross-border implications. It should also be noted that CNCPIC annually informs the European Commission of the designated infrastructure and of the number of Member States dependent on it (*Government Emergency Ordinance No. 98/2010*, Art. 10, para. 1, amended by point 14, Art. I of *Law No. 225 of 1 August 2018*; Government of Romania, 2010; Parliament of Romania, 2018).

Another essential element of the designation process is the notification of operators. The responsible public authorities have the obligation to inform the owners, operators, or administrators of the respective infrastructure about its designation as national or European critical infrastructure. This notification triggers the legal responsibilities of the operators, particularly the development of the Critical Infrastructure Operator Security Plan (PSO), which must be completed within nine months from the designation (Government of Romania, 2010, Art. 11).

To ensure information security, all data and documents relating to the designated infrastructures are treated as sensitive information, classified in accordance with the legislation on the protection of classified information and distributed strictly on a "need-to-know" basis (Government of Romania, 2012).

The designation procedure is therefore a formal, governmental, and strategic one, based on objective criteria, institutional consultation, and, where applicable, international agreements. Through this mechanism, the official recognition of infrastructures vital to the functioning of the state and to maintaining the safety of citizens is ensured, as well as Romania's integration into a coherent European system for preventing and managing major risks.

In conclusion, the designation of critical infrastructures represents an act of strategic governance that marks the transition from the theoretical assessment of the importance of infrastructures to the assumption of institutional responsibility for their protection. It strengthens the legal and operational framework of national security and contributes to reinforcing European

solidarity in the protection of infrastructures essential to the economic, social, and institutional life of the Member States.

4.3. Risk Assessment and Vulnerability Analysis

Risk assessment and vulnerability analysis represent essential components of the critical infrastructure protection process, forming the basis for strategic and operational decision-making in the field of national security and the stability of socio-economic systems. According to the legislative framework established by Art. 3, letter c) of *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), with subsequent amendments provided in Point 2, Article I of *Law No. 225/2018* (Parliament of Romania, 2018), these activities are explicitly included within the scope of critical infrastructure protection, being defined as processes of identifying, analyzing, and assessing significant threats with the purpose of determining existing vulnerabilities and the potential impact of the disruption or destruction of a national or European critical infrastructure.

The risk assessment process has a continuous and multidimensional character, involving both the analysis of possible causes of disruptive events and the estimation of the consequences on society's vital functions. In a first stage, this involves identifying internal and external threats, whether natural or anthropogenic, that could affect the infrastructure. Threats may range from natural disasters and technological failures to cyberattacks, sabotage, or terrorist acts. Their evaluation is carried out through the development of risk scenarios, which allow the modeling of possible evolutions and the quantification of the likelihood of occurrence (Government of Romania, 2011a; Briceag, A. C., 2017).

The results of risk assessment and vulnerability analysis are used for the development of the PSO (Government of Romania, 2010, Art. 11), mandatory documents that establish the technical, organizational, and procedural measures necessary to prevent and limit the effects of incidents. Additionally, these assessments form the basis for decisions regarding resource allocation, the development of response capabilities, and the establishment of priorities at both national and European levels.

In a second stage, the analysis focuses on determining vulnerabilities, understood as the set of weaknesses of a system - whether technical, organizational, informational, or related to intersectoral dependencies - that can be exploited by a threat or that may amplify its effects. Vulnerability assessment has a diagnostic character, aiming to identify areas of major risk and establish intervention priorities (Government of Romania, 2011a; Briceag, A. C., 2017).

A defining element of the process is the estimation of the potential impact of a risk materializing. The impact is analyzed based on the severity of the consequences on population security, the continuity of essential services, the economic environment, and social stability. In this regard, *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010) introduces the concept of critical thresholds, representing limit values established according to the severity of the impact, which determine the qualification of an infrastructure as critical. These thresholds allow for the objective comparison of risks and the prioritization of protection measures.

In conclusion, risk assessment and vulnerability analysis constitute the fundamental pillars of critical infrastructure protection. By applying these processes, authorities and operators can understand the nature and magnitude of threats, identify weaknesses within vital systems, and develop effective protection policies and plans. In the current context of economic and technological interdependencies, these activities are no longer merely a legal obligation but a strategic necessity for ensuring the resilience of critical infrastructures and, implicitly, national and European security.

4.4. Critical Infrastructure Operator Security Plan (PSO)

PSO are essential instruments within the national system for the protection of critical infrastructures, being regulated by *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010, Art. 11) - approved by *Law No. 18/2011* (Parliament of Romania, 2011) - and, indirect, by *Government Decision No. 718/2011* (Government of Romania, 2011a). Their purpose is to ensure the functionality and resilience of national and European critical infrastructures, prevent major disruptions, and guarantee the rapid resumption of activities in crisis situations.

According to the aforementioned legislation, operators, owners, or administrators of designated critical infrastructures are required to develop PSOs within nine months from designation. This plan must identify the critical elements of the infrastructure, analyze risks and vulnerabilities, and specify existing or necessary security measures for its protection. The minimum requirements regarding the content of the PSO include: risk analysis, preventive measures, intervention procedures, responsibilities, communication, interinstitutional cooperation, and evaluation mechanisms.

The plans have a dynamic character, being periodically evaluated, tested, and updated in order to reflect technological changes and new types of threats. Thus, the PSO becomes a living document that evolves together with the infrastructure and its operational environment. The approval and monitoring of PSOs are carried out by the responsible public authorities in each sector, which may request its revision or the adoption of additional protection measures.

From a strategic perspective, these plans have a dual function: preventive - by establishing security measures and reducing the likelihood of incidents; and reactive - by defining the mode of action and coordination in case of disruption. They reflect the transition from a reactive to a proactive approach in the field of critical infrastructure protection, based on the principles of resilience and continuity.

In conclusion, security and operational continuity plans represent the practical pillars of the critical infrastructure protection system. They translate risk and vulnerability assessments into actionable measures, providing a coherent framework for managing emergency situations and restoring the functionality of vital infrastructures. Through their development and implementation, in accordance with *Government Emergency Ordinance No. 98/2010* and *Government Decision No. 718/2011*, Romania strengthens its capacity for prevention, response, and recovery in the face of complex risks, contributing to the maintenance of economic, social, and institutional stability, as well as fulfilling its European obligations in the field of critical infrastructure security.

4.5. Mechanisms of Interinstitutional Cooperation

Interinstitutional cooperation constitutes the functional foundation of the national system for the protection of critical infrastructures, serving to ensure the unified coordination of institutional efforts, informational integration, and interoperability of security measures. The legal framework regulating these mechanisms is structured through a series of complementary normative acts: *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010) - with subsequent amendments- , *Government Decision No. 718/2011* (Government of Romania, 2011a), and, more recently, *Law No. 294/2024* (Parliament of Romania, 2024a) on the resilience of critical entities, as well as *Government Emergency Ordinance No. 155/2024* (Government of Romania, 2024), approved by *Law No. 124/2025* (Parliament of Romania, 2025a). Together, these define a complex and adaptable system capable of responding to modern threats and the interdependencies among vital infrastructures.

Based on Art. 3, letter k; Art. 5; and Art. 6^1 para. (1) of *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), interinstitutional cooperation is carried out at two levels:

strategic and operational. At the strategic level, overall coordination of activities related to identifying, designating, and protecting critical infrastructures lies with the Prime Minister, through a designated State Counselor. This role ensures the integration of critical infrastructure protection policies within the broader framework of national security policies and coordinates cooperation among ministries and institutions.

At the operational level, the central role is exercised by the MAI, through the National CNCPIC. This institution functions as the national point of contact and liaison structure between national public authorities, the European Commission, NATO, and other EU Member States. It also manages, at the national level, the CIWIN network, the European secure communication system used for exchanging information regarding vulnerabilities and the protection measures applied across Member States.

In accordance with Strategic Objective No. 4 of *Government Decision No. 718/2011* (Government of Romania, 2011a), interinstitutional cooperation is strengthened through the establishment of the Interinstitutional Working Group for the Protection of Critical Infrastructures (Art. 5, para. 1 of *Government Emergency Ordinance No. 98/2010*, as amended by point 2 of *Art. I of Law No. 18/2011*; Government of Romania, 2010; Parliament of Romania, 2011), a structure operating under the coordination of the Government. This group has the role of coordinating the actions of the responsible public authorities, developing common methodological guidelines, and periodically evaluating the stage of implementation of protection measures. The group brings together representatives of key ministries, emergency services, defense and security structures, as well as other relevant authorities depending on the sector concerned.

Furthermore, the issue of cooperation in the field of critical infrastructure protection also emerges from the provisions of *Law No. 294/2024* (Parliament of Romania, 2024a): Art. 1 para. (1) establishes the objective of improving cross-border cooperation; Art. 9 para. (3) designates CNCPIC as the single point of contact for cooperation with other states and with the Critical Entities Resilience Group; para. (4) creates the interinstitutional working group; and paras. (10)-(11) provide for cooperation and information exchange with other national and cyber authorities. This law expresses the European dimension of cooperation, granting Romania the legal framework to participate in information exchanges, joint exercises, training programs, and coordinated planning activities, thereby strengthening its integration into the European system for the protection of essential infrastructures.

We also note that each responsible public authority and each designated operator must establish specialized units in the field of critical infrastructures, headed by a security liaison officer. These structures function as contact points and communication instruments between the public and private actors involved, facilitating the exchange of data, reports, and risk assessments. Cooperation is thus formalized both at the institutional level and at the technical level through mechanisms of reporting, consultation, and continuous coordination (Government of Romania, 2010, Art. 8 para. (1)-(4)).

Through *Law No. 225/2018* (Parliament of Romania, 2018), the institutional framework of cooperation was modernized, introducing early-warning and communication mechanisms (MeCAT) for the real-time management of events that may affect critical infrastructures (Parliament of Romania, 2018, Art. 6^3 para. (1)-(2)). This law expanded the responsibilities of CNCPIC, strengthening its role as a national center for information and coordination and ensuring a permanent flow of data between the local, national, and European levels. At the same time, the law imposed the obligation of cooperation between CNCPIC, the Department for Emergency Situations (DSU), and

national security and intelligence structures, in order to integrate crisis management into the system for the protection of critical infrastructures.

We also note that *Government Emergency Ordinance* No. *155/2024* (Government of Romania, 2024), approved by *Law No. 124/2025* (Parliament of Romania, 2025a), contains provisions referring to cooperation - particularly at the national, European, and international levels - in the field of cybersecurity, as specified in Table 2.

In conclusion, the mechanisms of interinstitutional cooperation regarding the protection of critical infrastructures have evolved from a national model of administrative coordination - established by *Government Emergency Ordinance No. 98/2010* (Government of Romania, 2010), approved by *Government Decision No. 718/2011* (Government of Romania, 2011a) - toward a complex, multidimensional, and Europeanized system, strengthened by *Law No. 225/2018* (Parliament of Romania, 2018), *Law No. 294/2024* (Parliament of Romania, 2024a), and *Government Emergency Ordinance No. 155/2024* (Government of Romania, 2024), approved by *Law No. 124/2025* (Parliament of Romania, 2025a). These instruments configure an institutional architecture based on partnership, interoperability, and resilience, enabling Romania to actively participate in the EU's efforts to strengthen collective security and the protection of critical infrastructures within an international context marked by interdependencies and emerging threats.

4.6. The Use of Modern Technologies in the Protection of Critical Infrastructures

The accelerated technological developments of recent decades have redefined both the concept of critical infrastructure and the methods used to protect it. In a global context characterized by digital interconnection, increasing dependence on information networks, and the complex risks associated with cyberspace, the use of modern technologies has become an essential pillar of national and European security strategies. In this regard, Romania has begun implementing a set of innovative tools and solutions designed to enhance the resilience and response capacity of national and European critical infrastructures.

A significant first step is the implementation of real-time monitoring systems for physical and digital infrastructures. These systems use intelligent sensors, IoT (Internet of Things) devices, and secure communication networks to continuously collect data on equipment functioning, energy flows, environmental parameters, and operating conditions. The information is processed through advanced analytical platforms, which enable the rapid detection of deviations from normal parameters and the issuance of early warnings (Szentesi, Cuc, Lile, & Cuc, 2021). Thus, a transition is made from a reactive approach to a preventive one, reducing the risk of major failures or attacks on vital systems, as also targeted in the national strategy for artificial intelligence (Authority for the Digitization of Romania, 2024).

A second emerging area is the use of artificial intelligence (AI) and machine learning techniques for the predictive analysis of infrastructure behavior. Algorithmic models can identify abnormal operating patterns, forecasting the occurrence of technical failures, security breaches, or attempted cyberattacks. In the energy and transport sectors, AI is already used for the dynamic management of networks and for optimizing flows of energy, traffic, or data, contributing to increased operational efficiency and safety (Transelectrica, 2024-2025; Ministry of Energy, 2024; Ioanid & Palade, 2023). Through the integration of artificial intelligence, decision-making processes become automated, reducing the dependence on human intervention in critical situations and enabling rapid responses in the event of an incident.

In parallel, Romania is exploring the application of blockchain technologies in the protection of critical infrastructures, particularly for securing the flow of sensitive data and communications

between public institutions. Through its characteristics - transparency, immutability, and decentralization - blockchain offers a reliable solution for ensuring data integrity, preventing unauthorized access, and verifying the authenticity of informational transactions. In the financial, energy, and public administration sectors, the implementation of such solutions contributes to strengthening trust in digital infrastructures, reducing vulnerabilities generated by cyberattacks or human errors (Vevera & Vasiloiu, 2024; Sbîrneciu & Florea, 2023).

An essential component of the modernization of critical infrastructures is the development of resilient data centers and secure communication platforms for inter-institutional use (Vevera, 2024; Petcu, Candet, Ștefănescu, Gruia, & Craioveanu, 2021). These centers, built in accordance with European standards of redundancy and security, ensure the continuity of government digital services in the event of major incidents. They integrate distributed backup solutions, advanced encryption, and automated data recovery mechanisms. The secure communication platforms used by institutions such as the MAI the Special Telecommunications Service (STS), and CNCPIC enable the rapid exchange of classified information, the simultaneous alerting of relevant structures, and the efficient coordination of national-level response.

At the European level, the use of these technologies is supported through international cooperation and funding programs. Romania actively participates in the Digital Europe Programme (European Commission, 2024a), which supports the development of data infrastructures, artificial intelligence competence centers, and cybersecurity mechanisms, as well as in the Horizon Europe Programme (European Commission, 2024b), dedicated to research and innovation in the field of critical infrastructure resilience. Through these programs, Romania collaborates with other Member States in pilot projects on the digitalization of essential infrastructures, risk management, and the improvement of cross-border interoperability of protection systems.

The integration of modern technologies into the national system for the protection of critical infrastructures therefore carries a dual significance. On the one hand, it strengthens the preventive and response capabilities of institutions, enabling coordinated and efficient incident management. On the other hand, it raises new challenges related to cybersecurity, data protection, and dependence on digital technologies, which require the continuous adaptation of the legal framework and the development of the technical competencies of the personnel involved.

In conclusion, the use of modern technologies in the protection of critical infrastructures represents a strategic priority for Romania, aligned with European objectives for digitalization and resilience. The implementation of intelligent systems, artificial intelligence, blockchain solutions, and secure data centers contributes to building an adaptive and collaborative security ecosystem capable of anticipating threats, reducing vulnerabilities, and protecting the vital functions of the state in an increasingly interconnected and technology-driven world.

5. CURRENT ISSUES AND CHALLENGES IN THE FIELD OF CRITICAL INFRASTRUCTURE PROTECTION IN ROMANIA

5.1. General Premises

Although Romania has a well-defined legislative and institutional framework for the protection of critical infrastructures, its practical implementation is often hindered by a series of systemic problems and emerging challenges generated by recent technological, economic, and geopolitical transformations.

The developments of the last decade - from health and energy crises to regional conflicts and the intensification of cyberattacks - have shown that the vulnerability of critical infrastructures does

not stem solely from a lack of physical protection, but also from the increasing interdependence of systems and the insufficiency of strategic coordination mechanisms.

In the *National Defence Strategy for the period 2020-2024* (Parliament of Romania, 2020), critical infrastructures are mentioned as vital elements for the functioning of the state and for national security, the document highlighting the need to strengthen their resilience in the face of hybrid, cyber, and asymmetric threats. Nevertheless, a significant gap persists between the existing normative framework and the actual level of implementation.

5.2. Deficient Interinstitutional Coordination

One of the most persistent problems of the national system is institutional fragmentation. Although CNCPIC has coordination responsibilities, many operational competences remain dispersed among ministries and sectoral authorities, each applying its own procedures. This situation generates overlaps of responsibilities between institutions; the absence of a unified mechanism for communication and information exchange; and delays in joint responses to complex incidents.

For example, in the case of a cyberattack on an energy operator, the MAI, the DNSC, the Ministry of Energy, the DSU, and possibly the SRI are involved simultaneously - yet the absence of a single decision-making center often results in partial or delayed responses.

The need for an integrated national center for coordination and strategic analysis of critical infrastructures thus becomes evident. One solution would be to expand the responsibilities of CNCPIC and transform it into a structure with strengthened executive and analytical competences, capable of managing multisectoral information in real time.

5.3. Shortcomings in the Current Public-Private Cooperation Framework

Most critical infrastructures in Romania are owned by private operators, particularly in the energy, financial, transport, and IT&C sectors. However, cooperation between the state and the private sector remains insufficiently structured, despite the recent adoption of *Government Emergency Ordinance No. 155/2024* (Government of Romania, 2024), approved by *Law No. 124/2025* (Parliament of Romania, 2025a). There is a lack of clear mechanisms for the exchange of classified information on risks and incidents; joint training and simulation exercises; and accountability and monitoring of the implementation of security measures.

Although the legislation relevant to critical infrastructure protection establishes clear obligations for essential service operators, the level of compliance varies significantly across sectors. In the absence of economic incentives and a mature security culture, some companies treat legal requirements merely as formalities, which undermines the overall effectiveness of the system.

A potential direction for development would be the institutionalization of public-private partnerships through a distinct legislative framework that clearly regulates responsibilities, confidentiality, and mutual benefits. This could include mechanisms for financial compensation, risk-sharing, and governmental technical assistance for strategic private operators. It is worth noting that *the National Defence Strategy for the period 2025-2030* (Parliament of Romania, 2025b) - a document under public debate at the time of drafting this study (15 November 2025) - highlights the role of the "public–private partnership" as an essential instrument for strengthening national resilience, mentioned generally but with direct applicability in strategic sectors such as critical infrastructures, where cooperation between the state and the private sector becomes indispensable for protecting and modernizing vital systems. Implementing the above-mentioned instrument would be capable of eliminating some of the shortcomings in the public–private cooperation framework with regard to the issue under analysis.

5.4. Insufficient Integration of the Cyber Dimension

A major challenge is the full integration of cyber protection into the national critical infrastructure system. Although *Law No. 362/2018* (Parliament of Romania, 2019) and the activity of the National Cybersecurity Directorate (DNSC) have strengthened this component, and more recently a new institutionalized civil cybersecurity framework has been adopted through *Government Emergency Ordinance No. 155/2024* (Government of Romania, 2024), approved by *Law No. 124/2025* (Parliament of Romania, 2025a), with subsequent norms and practical instruments, coordination between physical protection (MAI and CNCPIC) and digital protection (managed by DNSC) remains incomplete.

The existence of two parallel institutional chains leads to: the absence of a shared picture of hybrid threats; difficulties in correlating data on physical and cyber incidents; and overlaps of competences in risk analysis.

Recent examples of cyberattacks on hospitals and payment systems in Romania (2023-2024) have demonstrated the need for an integrated approach. One viable solution would be the creation of a joint MAI-DNSC platform to centralize information on incidents, vulnerabilities, and response measures, similar to models implemented in Nordic states or Germany.

5.5. Limited Resources and Shortage of Specialized Personnel

The protection of critical infrastructures is a highly complex technical field requiring expertise in risk analysis, security engineering, emergency management, and cybersecurity. However, many Romanian institutions involved in critical infrastructure protection face a shortage of qualified personnel and insufficient financial resources. CNCPIC, DNSC, and sectoral authorities operate with relatively small teams compared to the complexity of their missions. The lack of continuous training and professional motivation affects reaction capacity and innovation. In addition, lower salaries in the public administration compared to the IT or energy private sectors lead to the migration of specialists to the private sector.

To counter this phenomenon, it is necessary to professionalize the field through: master's programs and postgraduate training dedicated to critical infrastructure protection; interdisciplinary courses in collaboration with universities and defense institutions; and the creation of a nationally accredited body of experts, following the model of European CERT teams.

5.6. Lack of an Updated National Strategy

The last *National Strategy for the Protection of Critical Infrastructures* dates back to 2011 (Government of Romania, 2011a). Since then, the security environment has changed radically: digitalization has accelerated, energy dependencies have diversified, and hybrid and cyber threats have become dominant. The absence of an updated version of the strategy generates a lack of coherence in national policies and in the prioritization of investments.

Given that new legislative frameworks have been adopted at the European level - *Directive (EU) 2022/2557 (CER)* and *Directive (EU) 2022/2555 (NIS2)* - Romania is obligated to rapidly harmonize its national legislation.

A new national strategy should include: a clear definition of the concept of "critical resilience"; the integration of physical, cyber, and social dimensions; the prioritization of investments in vital infrastructures; and the strengthening of interinstitutional and international cooperation mechanisms. Updating this strategy is essential for shifting from a static, reactive approach to a proactive and anticipatory one.

5.7. Emerging Risks and Future Challenges

In the medium and long term, Romania faces a series of emerging risks that will redefine the field of critical infrastructure protection: hybrid threats - combinations of cyberattacks, disinformation, and physical sabotage; cross-border dependencies of supply chains (energy, transport, IT&C); the impact of climate change on energy and water infrastructures; information warfare and attacks on strategic communication infrastructures; automation and artificial intelligence, which, although they increase efficiency, may introduce new vulnerabilities (Parliament of Romania, 2025b).

Addressing these risks requires an integrated vision of resilience, based on interinstitutional cooperation, scientific research, investment in technological security, and public education.

6. LIMITATIONS OF THE RESEARCH

The analysis of the institutional framework for the protection of critical infrastructures in Romania encountered several limitations inherent to the nature of the field, which is characterized by a high degree of confidentiality and intersectoral complexity.

First, the *research relied exclusively on public sources* - normative documents, strategies, institutional reports, and academic studies - without access to classified data or operational information from infrastructure operators. This restricted the possibility of conducting a direct empirical evaluation of the effectiveness of cooperation mechanisms and incident-response capabilities.

Second, *the predominantly qualitative methodology* enabled an interpretative analysis of the legal and institutional framework, but not a rigorous quantification of performance, maturity indicators, or the actual degree of implementation of European directives. Moreover, the *absence of an empirical component* (interviews, questionnaires, applied case studies) limited the understanding of how institutional and private actors perceive the applicability of resilience measures.

Additionally, *the legislative and institutional dynamics* - generated by the transposition of the CER and NIS2 directives - mean that some findings reflect an intermediate stage that may undergo further developments. Furthermore, *the European comparative dimension* was limited to conceptual references, without a systematic analysis of the models applied in other Member States.

Lastly, *the interdisciplinary nature of the topic* - situated at the intersection of security, technology, and public administration - required a transversal approach, without an exhaustive exploration of the specificities of each critical sector.

Overall, these limitations do not undermine the validity of the conclusions but highlight the need to expand future research through the inclusion of empirical tools, comparative analyses, and quantitative performance indicators that would enable a more comprehensive assessment of Romania's institutional and operational resilience.

7. CONCLUSIONS

The study on Romania's institutional framework for the protection of critical infrastructures has demonstrated that the national architecture in this field is well-grounded from a normative and strategic standpoint, yet it remains in a process of consolidation and operational maturation. Overall, the analysis confirmed *the hypotheses formulated* and achieved *the proposed objectives*, revealing a significant degree of coherence between public policy directions and institutional mechanisms, while also highlighting a series of structural challenges that affect the system's effectiveness.

The first hypothesis (*Hypothesis 1*), according to which the institutional framework is coherent at the level of principles but presents overlapping competences and coordination dysfunctions, was confirmed. Although the responsibilities of the MAI/CNCPIC and sectoral authorities are clearly defined in legislation, in practice there are insufficiently delineated interface areas, especially in cooperation with the DNSC and in the management of incidents with mixed impact (physical-cyber). This aspect was also reflected in the research objective regarding the assessment of interinstitutional coordination mechanisms, which was only partially achieved.

The second hypothesis (*Hypothesis 2*), concerning the incomplete and uneven transposition of the CER and NIS2 directives, was also confirmed. Romania has made significant progress in aligning its legislative framework with European standards; however, the practical application and operationalization of requirements - particularly reporting, performance indicators, and compliance auditing - are still in a transitional phase. In this regard, the research objective related to assessing the degree of compliance with EU regulations was fully met.

The third hypothesis (*Hypothesis 3*), regarding the uneven nature of public–private cooperation, was confirmed by highlighting a significant discrepancy between mature sectors (energy, finance, telecommunications) and those in the early stages of development. Despite the existence of formal cooperation frameworks, the level of trust and information sharing remains limited, which affects the effective implementation of PSO and continuity measures.

The hypotheses relating to the correlation between the clarity of institutional roles, interinstitutional exercises, and the level of resilience (*Hypothesis 4*), as well as to the role of integrating the cyber dimension into the management of critical infrastructures (*Hypothesis 5*), were confirmed on the basis of documentary analysis and sector-specific examples. The results showed that where processes are standardized, competences are clearly defined, and regular joint exercises exist, the capacity for reaction and adaptation increases significantly. Moreover, integrating cybersecurity into the planning and monitoring of critical infrastructures decisively contributes to reducing systemic vulnerabilities.

Overall, *the research objectives* - identifying the institutional structure, assessing the degree of European compliance, analyzing interinstitutional cooperation, and formulating proposals for improvement - were fulfilled. The study provides a coherent picture of the current state of critical infrastructure protection and of the necessary directions for strengthening national resilience.

The general conclusion is that Romania benefits from a credible institutional framework compatible with European standards; however, to transform it into an integrated resilience system, convergent actions are required: clarifying operational coordination, professionalizing human resources, strengthening the public–private partnership, and ensuring constant investment in monitoring and analytical technologies. Implementing these directions will enable the state to ensure the continuity of vital functions and to respond effectively to the complex threats of the contemporary strategic environment.

REFERENCES

Authority for the Digitalization of Romania (2024). *Strategia națională în domeniul inteligenței artificiale*. [*National Strategy in the Field of Artificial Intelligence.* Bucharest: Government of Romania]. https://www.adr.gov.ro/wp-content/uploads/2024/03/Strategie-Inteligenta-Artificiala-22012024-1.pdf

Briceag, A. C. (2017). *Elemente fundamentale ale managementului riscurilor – Studiu de caz: managementul riscurilor asociate infrastructurilor critice.* [*Fundamental Elements of Risk Management – Case Study: Risk Management Associated with Critical Infrastructures*]. Intelligence Review, 39(2). https://intelligence.sri.ro/elemente-fundamentale-managementul-riscurilor-studiu-de-caz-managementul-riscurilor-asociate-infrastructurilor-critice

Dănilă, V. B. (2012). *Critical Infrastructure. Danger, Threats to Them. Protection Systems.* Administratio, (13–14), "Danubius" University of Galați. https://journals.univ-danubius.ro/index.php/administratio/article/download/1013/1023

Directive 2008/114/EC of the European Parliament and of the Council (2008, December 8). On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJ L 345/75–82. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

European Commission. (2024a). *Digital Europe Programme (DIGITAL).* Europa.eu. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Commission. (2024b). *Horizon Europe – The EU Research and Innovation Programme (2021–2027).* Europa.eu. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/horizon-europe_en

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.* Official Journal of the European Union, L 194, 1–30. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

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 (NIS 2 Directive).* Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Government of Romania. (2010). *Ordonanță de urgență nr. 98 din 3 noiembrie 2010 privind identificarea, desemnarea și protecția Infrastructurilor critice. Guvernul României.* [*Emergency Ordinance No. 98 of 3 November 2010 on the Identification, Designation and Protection of Critical Infrastructures.* Government of Romania]. Official Gazette of Romania, No. 757 of 12 November 2010.

Government of Romania. (2011a). *Hotărârea Guvernului nr. 718 din 13 iulie 2011 pentru aprobarea Strategiei naționale privind protecția infrastructurilor critice*. [*Government Decision No. 718 of 13 July 2011 on the Approval of the National Strategy on the Protection of Critical Infrastructures*]. Official Gazette of Romania, No. 555 of 4 August 2011.

Government of Romania. (2011b). *Hotărârea Guvernului nr. 1.154 din 16 noiembrie 2011 pentru aprobarea pragurilor critice aferente criteriilor intersectoriale ce stau la baza identificării potențialelor infrastructuri critice naționale, precum și pentru aprobarea Metodologiei de aplicare a acestor praguri și de stabilire a nivelului de criticitate.* [*Government Decision No. 1.154 of 16 November 2011 on the Approval of the Critical Thresholds for the Cross-Sectoral Criteria Underlying the Identification of Potential National Critical Infrastructures, as well as the Approval of the Methodology for Applying These Thresholds and Establishing the Level of Criticality*]. Official Gazette of Romania, No. 849 of 30 November 2011. https://legislatie.just.ro/Public/DetaliiDocument/133279

Government of Romania. (2012). *Hotărârea Guvernului nr. 1198 din 4 decembrie 2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 1198 of 4 December 2012 on the Designation of National Critical Infrastructures*]. Official Gazette of Romania, No. 854 of 18 December 2012.

Government of Romania. (2014). *Ordonanța de urgență nr. 1 din 29 ianuarie 2014 privind unele măsuri în domeniul managementului situațiilor de urgență, precum și pentru modificarea și completarea unor acte normative*. [*Emergency Ordinance No. 1 of 29 January 2014 on Certain Measures in the Field of Emergency Management, as well as on the Amendment and Completion of Certain Normative Acts*]. Official Gazette of Romania, No. 88 of 4 February 2014. https://legislatie.just.ro/Public/DetaliiDocumentAfis/155216 Art. 1.

Government of Romania. (2015). *Hotărârea Guvernului nr. 639 din 19 august 2015 pentru modificarea și completarea Hotărârii Guvernului nr. 1198/2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 639 of 19 August 2015 amending and supplementing Government Decision No. 1198/2012 on the designation*

of national critical infrastructures]. Official Gazette of Romania, No. 653 of 28 August 2015. https://legislatie.just.ro/Public/DetaliiDocument/170951

Government of Romania. (2016). *Hotărârea Guvernului nr. 557 din 3 august 2016 privind managementul tipurilor de risc*. [*Government Decision No. 557 of 3 August 2016 on the management of risk types*]. Official Gazette of Romania, No. 615 of 11 August 2016.

Government of Romania. (2018). *Hotărârea Guvernului nr. 276 din 3 mai 2018 pentru modificarea anexelor la Hotărârea Guvernului nr. 1198/2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 276 of 3 May 2018 amending the annexes to Government Decision No. 1198/2012 on the designation of national critical infrastructures*]. Official Gazette of Romania, No. 401 of 10 May 2018. https://legislatie.just.ro/Public/DetaliiDocument/200565

Government of Romania. (2019a). *Ordonanța de urgență nr. 61 din 27 august 2019 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice*. [*Emergency Ordinance No. 61 of 27 August 2019 amending and supplementing Government Emergency Ordinance No. 98/2010 on the identification, designation and protection of critical infrastructures*]. Official Gazette of Romania, No. 717 of 30 August 2019.

Government of Romania. (2019b). *Hotărârea nr. 35 din 30 ianuarie 2019 pentru desemnarea autorităţilor publice responsabile în domeniul protecţiei infrastructurilor critice naţionale şi europene*. [*Government Decision No. 35 of 30 January 2019 on the designation of public authorities responsible for the protection of national and European critical infrastructures*]. Official Gazette of Romania, No. 82 of 1 February 2019.

Government of Romania. (2020). *Hotărârea Guvernului nr. 1017 din 27 noiembrie 2020 pentru modificarea și completarea anexelor la Hotărârea Guvernului nr. 1198/2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 1017 of 27 November 2020 amending and supplementing the annexes to Government Decision No. 1198/2012 on the designation of national critical infrastructures*]. Official Gazette of Romania, No. 1162 of 1 December 2020. https://legislatie.just.ro/Public/DetaliiDocument/234344

Government of Romania. (2021). *Hotărârea Guvernului nr. 300 din 12 martie 2021 pentru completarea anexelor la Hotărârea Guvernului nr. 1198/2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 300 of 12 March 2021 supplementing the annexes to Government Decision No. 1198/2012 on the designation of national critical infrastructures*]. Official Gazette of Romania, No. 280 of 19 March 2021. https://legislatie.just.ro/Public/DetaliiDocument/239294

Government of Romania. (2022a). *Hotărârea Guvernului nr. 1.076 din 31 august 2022 pentru modificarea Hotărârii Guvernului nr. 1.198/2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 1,076 of 31 August 2022 amending Government Decision No. 1,198/2012 on the designation of national critical infrastructures*]. Official Gazette of Romania, No. 867 of 2 September 2022. https://legislatie.just.ro/Public/DetaliiDocument/258813

Government of Romania. (2022b). *Hotărârea Guvernului nr. 1.436 din 29 noiembrie 2022 pentru modificarea și completarea Hotărârii Guvernului nr. 1.198/2012 privind desemnarea infrastructurilor critice naționale*. [*Government Decision No. 1,436 of 29 November 2022 amending and supplementing Government Decision No. 1,198/2012 on the designation of national critical infrastructures*]. Official Gazette of Romania, No. 1,174 of 7 December 2022. https://legislatie.just.ro/Public/DetaliiDocument/262271

Government of Romania. (2022c). *Hotărârea Guvernului nr. 733 din 02 iunie 2022 privind aprobarea Normelor metodologice pentru identificarea obiectivelor strategice de interes național, aflate în stadiu de proiectare.* [*Government Decision No. 733 of 2 June 2022 approving the Methodological Norms for identifying strategic national interest objectives in the design phase*]. Official Gazette of Romania, No. 553 of 7 June 2022. https://legislatie.just.ro/Public/DetaliiDocument/255995

Government of Romania. (2024). *Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil*. [*Government Emergency Ordinance No. 155/2024 establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace*]. Official Gazette of Romania, No. 1332/31.12.2024. https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121

International Organization for Standardization. (2019). *ISO 22301:2019 — Security and Resilience — Business Continuity Management Systems — Requirements.* Geneva, Switzerland: ISO. https://www.iso.org/standard/75106.html

Ioanid, A., & Palade, D. (2023). *Role of Artificial Intelligence and Smart Grids in Energy Companies in the European Union Member States.* European Journal of Sustainable Development, 12(4), 589–589.

Mărcău, F. C., Peptan, C., Iliuta, F. P., Cojoaca, M. E., Musetescu, A. M., Holt, A. G., ... & Gheorman, V. (2025, January). *The Impact of the Ukraine Conflict on the Quality of Life of the Young Population in Romania from a Societal Security Perspective.* In *Healthcare* (Vol. 13, No. 2, p. 156). MDPI.

Ministry of Energy / Strategie energetică – capitolul „Digitalizarea și dezvoltarea rețelelor inteligente". [Energy Strategy – Chapter "Digitalization and Smart Grid Development"]. Bucharest, 2024.

Mitrescu, S. (2025). *Critical Infrastructure Study.* New Strategy Center. https://newstrategycenter.ro/wp-content/uploads/2025/02/Critical-Infrastructure-Study-WEB.pdf

Năstase, C., et al. (2022). *Public–private partnership and economic development in Romania.* Ovidius University Annals – Economic Sciences Series, 22(1), 353–367. https://stec.univ-ovidius.ro/html/anale/RO/2022-2/Section%203/24.pdf

National Centre for the Protection of Critical Infrastructures. (n.d.). *Institutional Presentation.* Bucharest: Ministerul Afacerilor Interne. [Ministry of Internal Affairs]. https://cncpic.mai.gov.ro/

National Cybersecurity Directorate. (n.d.). *Instrumentul NIS2@RO v. 01-2025*. [NIS2@RO Tool v. 01-2025]. https://www.dnsc.ro/vezi/document/instrumentul-nis2ro-v-01-2025

Nemoianu, I. D. (2025). *Addressing Cyber Vulnerabilities in Critical Sectors: The Health Sector.* Bulletin of the National Defence University "Carol I", 14(2), 31–40.

Organisation for Economic Co-operation and Development (OECD). (2019). *Good Governance for Critical Infrastructure Resilience: Policy Toolkit on the Governance of Critical Infrastructure Resilience.* OECD Publishing. https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html

Panteli, M., & Mancarella, P. (2015). *The Grid: Stronger, Bigger, Smarter? Presenting a Conceptual Framework of Power System Resilience.* IEEE Power and Energy Magazine, 13(3), 58–66.

Parliament of Romania. (2004). *Legea nr. 481 din 8 noiembrie 2004 privind protecția civilă. (2023, 7 martie).* [*Law No. 481 of 8 November 2004 on Civil Protection.* (2023, March 7)]. Official Gazette of Romania, No. 192. https://legislatie.just.ro/Public/DetaliiDocument/56923

Parliament of Romania. (2011). *Legea nr. 18 din 11 martie 2011 pentru aprobarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice.* [*Law No. 18 of 11 March 2011 for the Approval of Government Emergency Ordinance No. 98/2010 on the Identification, Designation and Protection of Critical Infrastructures*]. Official Gazette of Romania, No. 183 of 16 March 2011. https://legislatie.just.ro/Public/DetaliiDocument/126829

Parliament of Romania. (2018). *Legea nr. 225 din 1 august 2018 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice*. [*Law No. 225 of 1 August 2018 amending and supplementing Government Emergency Ordinance No. 98/2010 on the identification, designation and protection of critical infrastructures*]. Official Gazette of Romania, No. 677 of 3 August 2018.

Parliament of Romania. (2019). *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și de modificare și completare a unor acte normative.* [*Law No. 362/2018 on ensuring a high common level of security of network and information systems and amending and supplementing certain normative acts*]. Official Gazette of Romania, No. 21 of 9 January 2019.

Parliament of Romania. (2020). *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*. [*National Defence Strategy for the period 2020–2024*]. Official Gazette of Romania, Part I, No. 574 of 1 July 2020.

Parliament of Romania. (2021). *Ordonanța de urgență nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică*. [*Emergency Ordinance No. 104 of 22 September 2021 on the establishment of the National Cybersecurity Directorate.* Official Gazette of Romania, No. 918 of 24 September 2021.

Parliament of Romania. (2023a). *Legea nr. 344 din 10 noiembrie 2023 pentru completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice*. [*Law No. 344 of 10 November 2023 supplementing Government Emergency Ordinance No. 98/2010 on the identification, designation and protection of critical infrastructures*]. Official Gazette of Romania, No. 1029 of 13 November 2023.

Parliament of Romania. (2023b). *Lege nr. 58 din 14 martie 2023privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*. [*Law No. 58 of 14 March 2023 on the cybersecurity and cyber defence of Romania, and amending and supplementing certain normative acts*]. Official Gazette of Romania, No. 214 of 15 March 2023.

Parliament of Romania. (2024a). *Legea nr. 294 din 27 noiembrie 2024 privind reziliența entităților critice, precum și pentru modificarea unor acte normative*. [*Law No. 294 of 27 November 2024 on the resilience of critical entities and amending certain normative acts*]. Official Gazette of Romania, No. 1189 of 29 November 2024. https://legislatie.just.ro/Public/DetaliiDocumentAfis/291491

Parliament of Romania. (2024b). *Ordonanța de urgență nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil*. [*Emergency Ordinance No. 155 of 30 December 2024 establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace*]. Official Gazette of Romania, No. 1332 of 31 December 2024.

Parliament of Romania. (2025a). *Legea nr. 124/2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil*. [*Law No. 124/2025 approving Government Emergency Ordinance No. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace*]. Official Gazette of Romania, No. 638 of 7 July 2025.

Parliament of Romania. (2025b). *Strategia Națională de Apărare a Țării pentru perioada 2025–2030*. [*National Defence Strategy for the period 2025–2030*]. https://cdn.edupedu.ro/wp-content/uploads/2025/11/SNAT-2025-2030.pdf

Petcu, I., Candet, I. B., Ștefănescu, C., Gruia, C. I., & Craioveanu, V. (2021). *Security Risks of Cloud Computing Services from the Perspective of New Cybernetics Threats.* Romanian Cyber Security Journal, 3(1), 89–97.

Romanian Intelligence Service [SRI]– official website. Retrieved on 10 November 2025 from https://www.sri.ro/

Roshanaei, M. (2021). *Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies.* Journal of Computer and Communications, 9(8), 80–102.

Sbîrneciu, C., & Florea, N. V. (2023). *An Exploratory Case Study: Romania's Digital Innovation Opportunities Due to the Rise of Digital Currencies.* Journal of Financial Studies, 8(14), 143–164.

Seppänen, H., Luokkala, P., Zhang, Z., Torkki, P., & Virrantaus, K. (2018). *Critical Infrastructure Vulnerability—A Method for Identifying Infrastructure Service Failure Interdependencies.* International Journal of Critical Infrastructure Protection, 22, 25–38.

Szentesi, S. G., Cuc, L. D., Lile, R., & Cuc, P. N. (2021). *Internet of Things (IoT), Challenges and Perspectives in Romania: A Qualitative Research.* Amfiteatru Economic, 23(57), 448–464.

Transelectrica. *Planul de dezvoltare a Rețelei Electrice de Transport 2024–2033.* [*Development Plan for the Electricity Transmission Network 2024–2033*]. Bucharest. https://web.transelectrica.ro/noutati/noutati/word/PPDRET%202024-2028-2033.pdf

Vevera, A. V. (2024). *Digitalization of Critical Infrastructures – Systemic Considerations, the Evolution of Governance, and Elements of a National Research Agenda.* Gândirea Militară Românească, 2024(3), 106–127. https://doi.org/10.55535/GMR.2024.3.06

Vevera, A. V., & Vasiloiu, I. C. (2024). *E-Government in Romania and Estonia: Comparative Analysis and Future Directions.* Romanian Cyber Security Journal, 6(2), 73–83.

Zmădu, R. (2021). *Protection of Critical Infrastructure from Emerging Threats.* STRATEGIES XXI – Command and Staff College, 17(1), 377–384.