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 ON THE INTERNATIONAL COOPERATION FRAMEWORK FOR CRITICAL INFRASTRUCTURE PROTECTION

Cătălin PEPTAN

„Constantin Brâncuși" University of Târgu Jiu, Romania

Abstract: *The paper examines the framework of international cooperation for the protection of critical infrastructures within a context marked by growing interdependence, hybrid threats, and accelerated digitalization. The research objective is to assess the legal, institutional, and operational mechanisms developed at the levels of the EU, NATO, the UN, and the OSCE, with a focus on the energy, transport, healthcare, and communications/cyber sectors. The methodology combines documentary analysis of key instruments (NIS2, CER, NATO strategies, UN/OSCE initiatives), inter-institutional comparative analysis, and sectoral synthesis.*

The results highlight the EU's dual architecture (NIS2 - cyber pillar; CER - physical pillar), supported by ENISA and CERT-EU, NATO's approach centered on collective resilience and NATO-EU cooperation, as well as the UN and OSCE roles in standardization and confidence-building measures. Major challenges in this field include regulatory fragmentation, trust deficits, capacity asymmetries, and emerging risks linked to AI/5G technologies and climate change.

The paper proposes an international convention on critical infrastructures, enhanced EU-NATO interoperability, a rapid reaction mechanism, and the integration of cybersecurity into strategies addressing critical infrastructure issues. For Romania, recommendations include full alignment with NIS2 and CER, clarification of institutional responsibilities, and the strategic use of the Bucharest ECCC. The conclusion argues that the resilience of critical infrastructures depends on shared standards, secure information exchange, and sustained investment in education and innovation.

Keywords: *critical infrastructures; international cooperation; resilience; NIS2; CER; NATO; cybersecurity; Romania.*

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

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

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

1. INTRODUCTION

1.1. General Context

Critical infrastructures represent the backbone of modern society, ensuring the continuous functioning of essential services such as energy, transport, communications, healthcare, and financial systems. In an increasingly interconnected world, the vulnerabilities of these infrastructures can trigger cascading effects that rapidly transcend national borders, undermining collective security, economic stability, and social well-being (Kane et al., 2024; Sonesson, Johansson, & Cedergren, 2021).

Recent developments - ranging from the intensification of cyberattacks and risks associated with accelerated digitalization to the impact of armed conflicts and climate change - have prompted states and international organizations to place greater emphasis on international cooperation in the field of critical infrastructure protection (Kallenborn & Willis, 2025; United Nations Office for Disarmament Affairs, 2024). Without a coordinated approach, no state can effectively manage the systemic risks that threaten these vital infrastructures.

The European Union (EU), the North Atlantic Treaty Organization (NATO), the United Nations (UN), the Organization for Security and Co-operation in Europe (OSCE), and other regional structures have developed normative, institutional, and technical frameworks that facilitate information sharing, the alignment of security standards, and mutual support in times of crisis. Cooperation in this field is no longer optional, it has become a fundamental component of international resilience.

1.2. Motivation and Relevance of the Topic

The topic of this paper is particularly relevant in the current geopolitical and technological context. Against the backdrop of regional conflicts, the proliferation of hybrid threats, and the growing number of attacks on energy and digital infrastructures, transnational cooperation has become a strategic priority for governments and international organizations. For instance, the cyberattacks targeting Ukraine's energy networks (Abraham, Houmb, & Erdodi, 2025; Peptan, 2022) and incidents that disrupted global supply chains, such as the 2021 ransomware attack on Colonial Pipeline (Bellamkonda, 2024), have clearly demonstrated the cross-border nature of these threats. Such events underscore the urgent need for integrated cooperation mechanisms aimed at prevention, detection, and coordinated incident response.

For Romania, the issue of critical infrastructure protection carries increased significance in light of its membership in the EU and NATO, which set high standards for security, protection, and international cooperation. Moreover, the country's strategic geographical position and its emerging role as a regional energy and digital hub lend both practical and geopolitical weight to this topic.

1.3. Purpose and Objectives of the Research

Research Purpose

The primary purpose of this research is to analyze the framework of international cooperation in the field of critical infrastructure protection by identifying the main legal, institutional, and operational mechanisms that facilitate collaboration among states and international organizations. The study aims to highlight the importance of transnational cooperation in strengthening resilience and to propose directions for improving coordination in this domain, with particular reference to Romania's role within the European and global security architecture.

Research Hypotheses

Hypothesis 1: International cooperation is a determining factor for the effective protection of critical infrastructures, as contemporary threats are interdependent and transnational in nature.
Hypothesis 2: The existence of a unified and interoperable international regulatory framework significantly contributes to enhancing the resilience of critical infrastructures and improving the efficiency of crisis response.
Hypothesis 3: Legislative and institutional divergences between states hinder international cooperation and reduce the effectiveness of joint protection measures.
Hypothesis 4: A comprehensive sectoral approach - including energy, transport, healthcare, and communications - is essential for an integrated system of critical infrastructure protection.
Hypothesis 5: Romania has the potential to become a relevant regional actor in the field of critical infrastructure protection through the consolidation of its legislative framework and active participation in international initiatives.

Research Objectives

General Objective:

To analyze the framework of international cooperation in the field of critical infrastructure protection by assessing existing policies, institutions, and mechanisms at the European, Euro-Atlantic, and global levels.

Specific Objectives:

O1: To identify the main international documents and policies related to critical infrastructure protection (*NIS/NIS2 Directives, EU Resilience Strategy, NATO Security Strategy*, etc.).
O2: To analyze the mechanisms of cooperation and information exchange among states and international organizations (EU, NATO, UN, ENISA, CERT-EU etc.).
O3: To evaluate international cooperation in strategic sectors - energy, transport, healthcare, communications, and cybersecurity.
O4: To identify current challenges affecting the implementation of international cooperation policies, with an emphasis on legal, technical, and organizational barriers.
O5: To analyze Romania's role and contribution within international cooperation frameworks on critical infrastructure protection.
O6: To formulate recommendations for strengthening international cooperation in line with emerging technological and security trends (AI, 5G, IoT, digitalization).

Through its proposed hypotheses and objectives, the analysis seeks to provide both a theoretical and applied understanding of how international cooperation contributes to strengthening the resilience of critical infrastructures and safeguarding the strategic interests of EU and NATO member states.

1.4. Research Methodology

This research employs an interdisciplinary approach positioned at the intersection of security studies, international relations, and legal-institutional analysis. The purpose of the methodology is to establish a rigorous framework for identifying, assessing, and comparing international cooperation mechanisms in the protection of critical infrastructures by correlating the theoretical, normative, and applied dimensions of the field.

Research Methods

Documentary Analysis - Focused on examining the relevant legislative, strategic, and institutional frameworks at the international and European levels. This included the analysis of directives, treaties, strategies, and reports issued by key organizations (EU, NATO, UN,

OSCE), as well as specialized academic literature. This method enabled the identification of major trends and developments in the field of critical infrastructure protection.

Comparative Analysis - Used to highlight the convergences and differences between institutional cooperation models (EU, NATO, UN, OSCE) in order to assess their degree of interoperability and complementarity.

Sectoral Analysis - Applied to the energy, transport, healthcare, and communications sectors to capture the specific features of international cooperation and the functional interdependencies among these strategic domains.

Case Study - Focused on Romania's role and contribution within the Euro-Atlantic security architecture, through an examination of its participation in EU and NATO initiatives and the corresponding national legislative framework.

Sources and Methodological Criteria

The research focused on the period after 2008 - with the first significant European initiative in the field, *Directive 2008/114/EC* - and was based on primary sources (official documents, directives, treaties, institutional reports) and secondary sources (scientific studies, public policy analyses, and specialized materials), using their relevance as the main inclusion/exclusion criterion. The selection of documents was carried out according to their relevance to the established objectives, the timeliness of the information, and their level of academic or institutional recognition.

Methodological Limitations

The main limitations stem from the dynamic and interdisciplinary nature of the field, partial access to classified information, and national variations in the implementation of resilience policies. Nevertheless, the combination of qualitative analytical methods has made it possible to outline a coherent and comparable picture of international cooperation in critical infrastructure protection.

1.5. Conceptual Delimitations

The research focuses on international cooperation, analyzing the main institutional and policy frameworks that define relations among states and organizations in the field of critical infrastructure protection. While the emphasis is placed on the EU and NATO, references are also made to the UN, OSCE, and other relevant global initiatives.

2. INTERNATIONAL FRAMEWORK OF COOPERATION IN THE FIELD OF CRITICAL INFRASTRUCTURE PROTECTION

2.1. Introductory Considerations

In the context of global economic, technological, and strategic interdependence, the protection of critical infrastructures has become a major priority for governments and international organizations (Mottahedi, Sereshki, Ataei, Nouri Qarahasanlou, & Barabadi, 2021; Sathurshan, Saja, Thamboo, Haraguchi, & Navaratnam, 2022). Contemporary threats - ranging from cyberattacks and physical sabotage to natural disasters and armed conflicts - simultaneously affect multiple vital sectors, requiring a coordinated and multidimensional approach (Sonesson, Johansson, & Cedergren, 2021; Wells, Boden, Tseytlin, & Linkov, 2022).

International cooperation in this field entails not only the exchange of information and best practices but also the harmonization of legal and institutional frameworks, the development of joint response mechanisms, and the strengthening of infrastructure resilience against complex and interconnected risks (Pursiainen & Kytömaa, 2023; Markopoulou & Papakonstantinou, 2021). The main actors driving this cooperation are the EU, the NATO, the UN, and the OSCE.

2.2. The Framework of Cooperation within the European Union (EU)

2.2.1. Evolution of the European Legislative Framework

The EU has been one of the pioneers in recognizing the importance of critical infrastructures for the functioning of the internal market and for the collective security of its Member States. The first significant initiative was *Directive 2008/114/EC* (Council Directive 2008/114/EC, 2008) on the identification and designation of European critical infrastructures, which initially focused on the energy and transport sectors.

Subsequently, the growing complexity of new threats - particularly in the digital domain - led to the adoption of *Directive (EU) 2016/1148* (Directive (EU) 2016/1148, 2016) on the security of network and information systems (the *NIS Directive*), establishing a common framework for cybersecurity across critical infrastructures. In 2022, this directive was replaced by *Directive (EU) 2022/2555 (NIS2)* (Directive (EU) 2022/2555, 2022), which expanded its scope to include new sectors such as water, healthcare, transport, and public administration, while introducing stricter governance and reporting requirements.

Complementing this, the EU adopted in 2022 the *Directive on the Resilience of Critical Entities (CER Directive - 2022/2557)* (Directive (EU) 2022/2557, 2022), which replaced the earlier *Directive 2008/114/EC*, establishing an integrated framework for the identification, protection, and monitoring of critical infrastructures at the European level.

As a result, the current European legislative system is structured around two complementary pillars: The digital - cyber pillar, represented by *NIS2*; The physical - operational pillar, represented by the *CER Directive.*

This dual approach reflects the EU's strategic vision that the resilience of critical infrastructures constitutes a shared responsibility among European institutions, Member States, and private operators.

2.2.2. Institutional and Cooperation Mechanisms within the EU

To implement its legislative framework, the EU has established a range of institutions and cooperation mechanisms:

- *ENISA - European Union Agency for Cybersecurity* (European Union Agency for Cybersecurity [ENISA], n.d.a) – Coordinates the EU's strategic and methodological efforts in the prevention, monitoring, and response to cyber incidents, providing support to Member States in protecting critical infrastructures.
- *CERT-EU - Computer Emergency Response Team for the EU* (Computer Emergency Response Team for the European Union [CERT-EU], n.d.) - Coordinates technical response and cooperation among EU institutions and agencies in major cyber incident situations, contributing to the strengthening of the collective resilience of Europe's digital infrastructure.
- *(ERNCIP) - European Reference Network for Critical Infrastructure Protection*, initiated by the *European Commission, Joint Research Centre* (European Commission, Joint Research Centre [JRC], n.d.), supports critical infrastructures through research, testing, methodological development, and the exchange of best practices.
- *EU Civil Protection Mechanism* (European Parliament & Council of the European Union, 2013) - Facilitates mutual assistance among Member States in emergency situations, including those affecting critical infrastructures, by coordinating civil protection operations, sharing resources, and ensuring cross-border assistance in the event of major disruptions.

- *SPOC - Single Points of Contact Network* (Directive (EU) 2022/2557, 2022, Art. 11) – Ensures coordination and information exchange between national authorities and the European Commission, facilitating cross-border cooperation in the event of disruptions to critical infrastructures.

Additionally, the EU promotes joint resilience-testing exercises, such as *Cyber Europe* (European Union Agency for Cybersecurity [ENISA], n.d.b), periodically organized by ENISA, as well as cooperation and innovation initiatives, such as the *EU-CIP Exercises* (European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection [EU-CIP], 2022-2025), which focus on energy and transport infrastructures.

According to the European Commission and its specialized agencies, European cooperation in the field of critical infrastructure protection is founded on key principles such as: solidarity and mutual support among Member States; legal and technological interoperability; shared responsibility between public and private actors; and a proactive approach to resilience rather than a merely passive approach to protection (European Commission, 2025; European Cyber Security Organisation [ECSO] & CEN-CENELEC, n.d.; European Union Agency for Cybersecurity [ENISA], n.d.c).

2.3. The Framework of Cooperation within NATO

2.3.1. Critical Infrastructures and the Concept of Collective Resilience

NATO addresses the protection of critical infrastructures through the lens of collective security and strategic resilience. The concept of resilience was formalized at the *NATO Warsaw Summit (2016)* with the adoption of the document *Commitment to Enhance NATO's Resilience* (NATO, 2016), which defines resilience as the combined civil and military ability to withstand and rapidly recover from major shocks such as natural disasters, armed attacks, or disruptions to critical infrastructures. The document underscores that resilience is an essential condition for collective defense.

This principle was reaffirmed in NATO's *New Strategic Concept* (NATO, 2022a), which defines resilience as a fundamental component of collective defense and a prerequisite for both national and allied security. The Concept highlights the need to adapt critical infrastructures, supply chains, and essential services to emerging hybrid, cyber, and energy-related risks. NATO also emphasizes that resilience is not solely a national responsibility but a shared objective, crucial for protecting populations and ensuring the continuity of governance in the face of complex crises.

It is important to note that NATO does not possess direct regulatory authority over national infrastructures; however, it supports member states through: Common standards for resilience and critical infrastructure protection; Periodic assessments of preparedness and vulnerability levels; Joint simulation and crisis-response exercises, such as the *Crisis Management Exercise (CMX)* (NATO, n.d.-a); Information sharing through the *NATO Intelligence Fusion Centre (NIFC)* (NATO Intelligence Fusion Centre, n.d.); Centres of Excellence, the most notable being the *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)* (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], n.d.).

In recent years, NATO has paid increasing attention to the protection of energy infrastructures, in light of strategic dependencies on resources and the growing number of attacks on energy networks in Ukraine and other member states.

2.3.2. NATO - EU Cooperation

The NATO - EU relationship represents a prime example of advanced institutional cooperation in the field of security and critical infrastructure protection. The two organizations signed *Joint Declarations on NATO-EU Cooperation in 2016, 2018, and 2023*, establishing concrete mechanisms for coordination, data exchange, and joint response to hybrid, cyber, and energy-related threats.

The *Joint Declaration adopted at the Warsaw Summit* (NATO, 2016) formalized cooperation in key areas such as cybersecurity, infrastructure resilience, and countering hybrid threats, emphasizing the strategic importance of protecting critical infrastructures as a cornerstone of collective defense. The document highlighted the need to harmonize security standards and coordinate civilian and military capabilities to strengthen the resilience of energy, transport, and communication infrastructures. Within this framework, NATO and the EU committed to developing joint mechanisms for prevention, information sharing, and response to cross-border threats, thus establishing critical infrastructure resilience as a central pillar of Euro-Atlantic security (European Union & NATO, 2016).

The *NATO-EU Joint Declaration of July 10, 2018*, signed at the NATO Summit in Brussels (European Union & NATO, 2018), reinforced the commitments made in 2016 and expanded cooperation in practical areas such as cybersecurity, military mobility, countering hybrid threats, and protecting critical infrastructures. The document reaffirmed the importance of strategic coordination between the two organizations, emphasizing information sharing and joint exercises, and explicitly underscoring the need to strengthen collective resilience and interoperability in the face of emerging risks to Euro-Atlantic security.

Furthermore, the *Joint Declaration signed in 2023* at the NATO Summit in Brussels (European Union & NATO, 2023) - the third of its kind following those of 2016 and 2018 - reaffirmed these objectives while extending cooperation to new areas, including energy security, supply chain protection, and the strengthening of critical infrastructure resilience. The document highlighted the need for an integrated transatlantic approach to address emerging risks, particularly hybrid, cyber, and technological threats, and reiterated that critical infrastructure resilience is a shared responsibility of both NATO and the EU. Through this declaration, the two organizations strengthened their mechanisms for strategic coordination and information exchange related to critical infrastructure protection, reaffirming that collective security depends on the stable functioning of the Euro-Atlantic region's energy, logistics, and digital networks.

This institutional synergy reflects an integrated approach to European security, in which critical infrastructures are regarded as shared strategic assets rather than purely national components.

2.4. The Cooperation Framework within the UN and the OSCE

2.4.1. UN Initiatives

The UN approaches critical infrastructure protection through the lens of global security governance and sustainable development, where human security, resilience, and sustainability are deeply interdependent. Although the UN system does not possess a single, dedicated legal framework for critical infrastructure protection, several sectoral initiatives contribute significantly to strengthening international cooperation and global resilience. These initiatives align closely with EU and NATO resilience policies, underscoring the UN's pivotal role in global coordination and standardization.

This set of initiatives reflects a cross-sectoral approach, in which infrastructures are regarded as foundational elements of sustainable development, security, and international stability.

Accordingly, the *2030 Agenda for Sustainable Development* (United Nations, 2015), through Goal 9 ("Industry, Innovation, and Infrastructure"), promotes the development of resilient,

sustainable, and inclusive infrastructures, recognizing their essential role in supporting economic growth and social cohesion. Complementing this effort, the *United Nations Institute for Disarmament Research (UNIDIR)* (United Nations Institute for Disarmament Research, n.d.) contributes to digital infrastructure security by analyzing cyber threats and the military implications of emerging technologies, providing technical and strategic expertise to help prevent conflicts in the digital domain.

The International Telecommunication Union (ITU) (International Telecommunication Union, n.d.) also plays a central role in establishing global standards for security and interoperability in communication infrastructures and digital networks, facilitating cooperation between states and the private sector in managing cyber risks.

In the field of civil protection, the *United Nations Office for Disaster Risk Reduction (UNDRR)* (United Nations Office for Disaster Risk Reduction, n.d.) promotes the resilience of infrastructures to both natural and man-made disasters through the implementation of the *Sendai Framework for Disaster Risk Reduction (2015-2030)* (United Nations Office for Disaster Risk Reduction, 2015) and by integrating disaster risk considerations into national development strategies.

2.4.2. The Role of the OSCE in Regional Cooperation

The OSCE complements the architecture of international cooperation through a comprehensive security approach that integrates political, economic, and human dimensions. In 2013, the organization adopted *Decision No. 1106 - Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies* (Organization for Security and Co-operation in Europe, 2013), representing the first multilateral politico-diplomatic framework aimed at reducing the risk of conflicts arising from the use of information and communication technologies.

The document promotes a cooperative approach to digital security, focusing particularly on preventing attacks on critical infrastructures by enhancing transparency, communication, and trust among participating states. Key measures include: the establishment of national points of contact for managing major cyber incidents; the voluntary notification of national cybersecurity strategies; and the exchange of information and technical cooperation in investigating attacks targeting digital infrastructures. This framework has established the OSCE as a global actor in promoting stability and predictability in cyberspace, integrating critical infrastructure protection into the broader architecture of regional cooperative security.

The OSCE also supports cooperation among participating states through information sharing, joint incident response exercises, and the harmonization of national standards for the protection of critical infrastructures. Through its network of national points of contact, the organization facilitates rapid communication and coordinated responses to major cyber incidents, promoting transparency and mutual trust (Organization for Security and Co-operation in Europe, 2013). Joint exercises strengthen institutional interoperability and regional response capacity, while standardization activities contribute to aligning national policies with international cooperation principles (Organization for Security and Co-operation in Europe, 2016). Through these instruments, the OSCE serves as a platform for regional coordination and stability, playing a vital role in strengthening the collective resilience of its member states.

In addition, the OSCE, in cooperation with the UN and the EU, contributes to the development of a shared security culture grounded in dialogue, transparency, and technical cooperation (Organization for Security and Co-operation in Europe, 2019; Organization for Security and Co-operation in Europe, 2021). Through its mechanisms for conflict prevention, information exchange,

and confidence-building, the organization promotes an integrated approach to security that combines political, economic, and human dimensions. This cooperation enables the harmonization of regional and global initiatives related to critical infrastructure protection, cybersecurity, and cross-border risk management. Within this framework, the OSCE acts as a platform for strategic dialogue and normative standardization, facilitating the transfer of best practices and interinstitutional coordination with the overarching goal of enhancing collective resilience and ensuring the stability of the Euro-Atlantic area.

2.5. Comparative Summary

Table 1 summarizes the main distinctive elements of international cooperation in the field of critical infrastructure protection.

Organization	Type of Cooperation	Main Domains	Key Instruments
EU	Normative and Operational	Energy, Transport, Health, IT&C	NIS2 Directive, CER Directive, ENISA, CERT-EU
NATO	Strategic and Military	Energy, Communications, Defense, Cybersecurity	CCDCOE, CMX, Resilience Assessments
ONU	Global and Multidimensional	Digital Infrastructures, Communications, Sustainable Development	ITU, UNDRR, 2030 Agenda
OSCE	Regional and Preventive	Cybersecurity, Energy, Political Cooperation	CBMs, Regional Dialogue

Table 1. Distinctive Elements of International Cooperation in the Field of Critical Infrastructure Protection

The EU stands out through its advanced regulatory framework and dedicated institutions, while NATO provides strategic support and mechanisms for military coordination and resilience. The UN and the OSCE complement this system through global governance initiatives and regional cooperation, fostering dialogue and prevention.

Thus, the protection of critical infrastructures can no longer be conceived without structured international cooperation, grounded in interoperability, solidarity, and knowledge sharing.

3. INTERNATIONAL SECTORAL COOPERATION IN THE PROTECTION OF CRITICAL INFRASTRUCTURES

3.1. General Considerations

International cooperation in the field of critical infrastructure protection cannot be analyzed solely from a general or institutional perspective. It manifests differently in each strategic sector, depending on technological characteristics, applicable regulations, and the actors involved. Today, critical infrastructures are deeply interconnected and interdependent, meaning that a disruption in one domain - such as energy or communications - can trigger cascading effects across other vital sectors (Li & Zhang, 2025).

A sectoral approach to international cooperation enables a deeper understanding of how states and organizations collaborate to prevent risks, respond to incidents, and strengthen collective resilience. The most developed cooperation frameworks are found in the sectors of energy, transport, health, communications, and cybersecurity, which together constitute the strategic backbone of the modern world.

The sectoral analysis of international cooperation highlights a paradigm shift - from the traditional concept of critical infrastructure protection to that of integrated resilience, focused on the capacity of interdependent systems to anticipate, absorb, and recover rapidly from complex disruptions (Wells et al., 2022).

3.2. International Cooperation in the Energy Sector

The energy sector represents one of the most critical components of both national and international security. Energy powers all other infrastructures, and its disruption can directly impact the economy, transport, healthcare, and defense. Recent energy crises, such as the one triggered by the Russia-Ukraine conflict, have demonstrated the vulnerability of transport and distribution networks to both physical and cyberattacks.

The vulnerabilities of the energy sector are further amplified by cross-border dependencies - such as interconnected power grids, gas pipelines, and global supply chains - as well as by accelerated digitalization, including smart grids and SCADA systems (Kreso, n.d.). Consequently, international cooperation in this field has become an essential condition for stability and resilience.

At the European level, the main cooperation framework is represented by:

- *ENTSO-E - European Network of Transmission System Operators for Electricity* (European Network of Transmission System Operators for Electricity, n.d.) - responsible for coordinating the operation of interconnected power grids, ensuring energy security, and supporting the integration of the European energy market;
- *ACER - Agency for the Cooperation of Energy Regulators* (Agency for the Cooperation of Energy Regulators, n.d.) - oversees European energy markets, ensuring the safe, transparent, and integrated functioning of electricity and gas networks;
- *Energy Community Treaty* (European Union, 2006) - establishes the legal framework for the integration of the energy markets of the European Union with those of South-Eastern Europe and the Black Sea region, promoting energy security, investment, and alignment with EU standards on infrastructure and environmental protection;
- *European Energy Security Strategy* (European Commission, 2014) - aims to ensure the EU's energy security through the diversification of supply sources and routes, increased interconnectivity of energy networks, reduction of import dependency, and the strengthening of the resilience of critical energy infrastructures against geopolitical, technical, and cyber risks.

It is also worth noting that the EU promotes the green transition and climate resilience as essential pillars of energy security, through initiatives such as *REPowerEU* (European Commission, 2022c) and the *European Green Deal* (European Commission, 2019). These initiatives aim to reduce dependence on fossil fuels, accelerate investment in renewable energy, and strengthen sustainable infrastructures.

Furthermore, under the *NIS2 Directive* and the *CER Directive,* the EU has established a common framework for cybersecurity resilience and the protection of critical infrastructures, including those in the energy sector, focusing on the prevention, detection, and management of cross-border cyber incidents.

These policies reinforce an integrated approach to resilience - encompassing energy, cyber, and climate dimensions - reflecting the interdependence between technological security, economic stability, and environmental protection.

Transatlantic cooperation in the energy sector is carried out through the *EU-U.S. Energy Council* (U.S. Department of Energy, 2022), established in 2009, which serves as the principal transatlantic forum for strategic dialogue on energy. Its objectives include strengthening energy

security, diversifying energy sources, and protecting critical infrastructures through technological cooperation and policy coordination between the EU and the United States.

In 2023, this cooperation was expanded through the *Joint Task Force on Energy Security* (European Commission, 2022b), established in response to the energy crisis triggered by the war in Ukraine. The Task Force was created to diversify liquefied natural gas (LNG) supplies and develop alternative energy sources for Europe, thereby reducing the EU's dependence on fossil fuels from the Russian Federation and enhancing transatlantic energy security.

It is also worth noting that the *International Energy Agency (IEA)* (International Energy Agency, n.d.), founded in 1974 within the framework of the OECD, is the leading global actor in coordinating energy policies, promoting security, sustainability, and resilience of energy systems through strategic analysis, international cooperation, and energy crisis management.

A significant example of international cooperation is the interconnection of Ukraine's and Moldova's electricity grids with ENTSO-E, achieved in 2022 - a measure that strengthened regional energy security and reduced dependence on the Russian power system (European Network of Transmission System Operators for Electricity, 2022).

3.3. International Cooperation in the Transport Sector

Transport systems - land, air, maritime, and rail - represent critical infrastructures essential to the functioning of the global economy and the maintenance of social stability. Any major disruption in transport flows can generate systemic effects on international trade, food security, medical assistance, and even on the ability of states to provide basic public services.

Currently, the transport sector is exposed to a complex spectrum of threats, including cyberattacks targeting traffic control and logistics systems, physical sabotage of critical infrastructures (such as ports, railways, and road networks), and the use of transport systems for terrorist purposes (O'Kelly, 2025).

In this context, international cooperation relies on fundamental principles of standardization, interoperability, and coordinated response, aimed at ensuring the resilience and security of transport systems.

At the level of the EU, the main instruments of cooperation and governance in the transport sector are:

- *TEN-T - Trans-European Transport Network* (European Commission, 2020a, 2021a) - represents the EU's strategic framework for developing an integrated, safe, and sustainable transport infrastructure, designed to connect member states through rail, road, maritime, and air corridors, thereby facilitating mobility, trade, and European territorial cohesion;
- *EASA - European Union Aviation Safety Agency* (European Union Aviation Safety Agency, n.d.) and *EMSA - European Maritime Safety Agency* (European Maritime Safety Agency, n.d.) - responsible for risk monitoring, crisis management, and the protection of critical infrastructures in the air and maritime transport sectors;
- *CEF - Connecting Europe Facility* (European Commission, 2021c) - the EU's main financial instrument dedicated to the development of strategic transport, energy, and digital infrastructures, aimed at enhancing the connectivity, competitiveness, and resilience of trans-European networks.

The *EU Strategy for Sustainable and Smart Mobility* (European Commission, 2020a) also provides the framework for the transition toward a safe, green, and digital transport system, including concrete measures to protect transport infrastructures against physical and cyber risks. In addition, the *NIS2 Directive* and the *CER Directive* establish a common framework for cybersecurity

resilience and the protection of critical infrastructures, including those in the transport sector, thereby strengthening the EU's capacity to prevent, detect, and manage cross-border incidents.

At the global level, cooperation in the field of transport is carried out through specialized UN agencies, such as:

- *ICAO - International Civil Aviation Organization* (International Civil Aviation Organization, n.d.) - establishes global standards for the safety, security, and efficiency of international air transport;
- *IMO - International Maritime Organization* (International Maritime Organization, n.d.) - responsible for regulating maritime navigation safety, protecting the marine environment, and ensuring port security, while maintaining uniform international standards for global maritime transport;
- *UNECE - United Nations Economic Commission for Europe* (United Nations Economic Commission for Europe, n.d.) - coordinates international standards for road, rail, and multimodal transport infrastructures, promoting connectivity, safety, and sustainability within European and Eurasian transport networks.

These structures support the implementation of the *Sustainable Development Goals (SDGs)* from the *2030 Agenda* (United Nations, 2015), particularly SDG 9 ("Industry, Innovation, and Infrastructure") and SDG 11 ("Sustainable Cities and Communities"), which promote the development of resilient and safe infrastructures.

In light of the above, it should also be noted that military and logistical transport represents a shared dimension of EU-NATO cooperation, essential for ensuring strategic mobility. The *Military Mobility Project* (European External Action Service, 2023), launched in 2017 under the framework of *Permanent Structured Cooperation (PESCO)* (European External Action Service, n.d.), aims to harmonize civilian and military infrastructure to enable the rapid movement of troops and equipment across Europe. This initiative strengthens the link between civilian and defense infrastructure, reflecting the „dual-use" approach promoted by the EU.

It is also worth mentioning that the accelerated digitalization of transport, through the implementation of Logistics 4.0 concepts and *Intelligent Transport Systems (ITS),* has optimized operational efficiency while simultaneously increasing the cyber vulnerability of logistics chains. This has exposed transport infrastructures to risks such as disruption, data manipulation, and attacks on control systems - a context in which the role of international cooperation in this field has become increasingly crucial (Santos & Tavasszy, 2025).

3.4. International Cooperation in the Health Sector

The COVID-19 pandemic revealed the vulnerability of medical and pharmaceutical infrastructures in the face of global crises. The shortage of equipment, dependence on transnational supply chains, and cyberattacks targeting healthcare systems have underscored the urgent need for enhanced international cooperation.

In 2021, the EU established the *Health Emergency Preparedness and Response Authority (HERA)* (European Commission, n.d.) as a permanent structure for coordinating responses to health emergencies. HERA works closely with the *European Centre for Disease Prevention and Control (ECDC)* (European Centre for Disease Prevention and Control, n.d.) and the *European Medicines Agency (EMA)* (European Medicines Agency, n.d.) to ensure rapid crisis response and the protection of critical healthcare infrastructures.

At the global level, the World Health Organization (WHO) coordinates the *Global Outbreak Alert and Response Network (GOARN)* (World Health Organization, n.d.), which facilitates

cooperation among states in the prevention and control of epidemics. In parallel, the UN promotes the strengthening of health infrastructures through the *2030 Agenda for Sustainable Development* (United Nations, 2015), specifically Goal 3: "Good Health and Well-Being for All."

After 2021, the concept of „health resilience" was integrated into the *Security strategies of the European Union (EU)* (European Union External Action Service, 2022) and *NATO* (NATO, 2022a), being recognized as an integral part of critical infrastructure. In December 2023, the European Commission launched the initiative *"European Health Union: A New EU Health Security Framework Is in Motion"* (European Commission, 2022a), which establishes a revised EU-level health security framework designed to strengthen cooperation among European health agencies, enhance preparedness for health emergencies, and harmonize the collective response to cross-border threats.

The digital component of health infrastructures has been strengthened through the *European Health Data Space (EHDS)* initiative (European Commission, 2024), launched in 2024, which aims to create a unified framework for the secure sharing of medical data across the European area, facilitating cross-border cooperation, innovation in digital health, and rapid responses to health crises.

Although significant progress has been made toward a more coherent global governance of health security, international cooperation continues to face multiple structural limitations.

First, institutional bureaucracy and the complex decision-making procedures of international organizations slow down collective responses to major crises, thereby reducing operational flexibility (Sommerer, Squatrito, Tallberg, & Lundgren, 2022).

Second, significant disparities among member states - both in terms of financial resources and administrative and technological capacities - lead to uneven implementation of health resilience policies (EU Expert Group on Health Systems Performance Assessment [HSPA], 2020).

Third, interoperability challenges between the mechanisms of the WHO, EU, and NATO result in overlapping competences, data redundancies, and the absence of a shared real-time information exchange platform (Lucarelli, Moro, & Marrone, 2022).

These challenges demonstrate that the effectiveness of the global response to public health crises depends on overcoming institutional fragmentation and strengthening mutual trust among actors.

3.5. International Cooperation in the Field of Communications and Cybersecurity

Communication networks, data centers, and IT&C infrastructures form the foundation of all other sectors' functioning. Today, the vast majority of public services and industrial infrastructures depend on digital networks. Consequently, cyberattacks can have systemic effects, potentially triggering large-scale crises.

At the EU level, cooperation in the field of cybersecurity is governed by the *NIS2 Directive*, the *EU Cybersecurity Strategy* (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2020), and the mandate of *ENISA*. The Union has also established the *European Cybersecurity Competence Centre (ECCC)* (European Cybersecurity Competence Centre, n.d.), headquartered in Bucharest, which is tasked with coordinating research and innovation in the field of cyber resilience.

At the international level, the main instruments are:

- *Council of Europe Convention on Cybercrime* (Council of Europe, 2001) - the first international treaty establishing a common legal framework for combating cybercrime, promoting the harmonization of national legislation, international cooperation, and mutual assistance among states in the investigation and prosecution of cyberattacks;

• *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)* (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], n.d.) - supports the Alliance and its member states through research, training, and doctrinal development in the field of cyber defence, while also serving as the main coordinator of the Tallinn Manual project on the application of international law in cyberspace;
• *Tallinn Manual 2.0* (Schmitt, 2017) - the most comprehensive academic analysis of the application of international law to cyber operations, providing detailed interpretations of principles such as sovereignty, state responsibility, and the use of force in cyberspace, developed under the auspices of the *CCDCOE;*
• *Global Forum on Cyber Expertise (GFCE)* (Global Forum on Cyber Expertise, n.d.) - a multi-stakeholder international initiative launched in 2015, bringing together governments, international organizations, academia, and the private sector to promote global cooperation, capacity building, and the exchange of best practices in the field of cybersecurity.

Romania holds a strategic position in international cooperation on cybersecurity, hosting the *ECCC* and actively participating in the *CCDCOE*. Additionally, the *National Cybersecurity Directorate (DNSC)* (National Cyber Security Directorate, n.d.) coordinates national efforts to integrate into European and international networks dedicated to protecting digital infrastructures

Although international cooperation in cybersecurity has advanced considerably, the harmonization of technical standards among the EU, NATO, and other global organizations remains a major challenge. Differences in regulatory frameworks and strategic priorities create interoperability gaps that may hinder coordinated responses to cross-border incidents (Mishra, 2024).

Moreover, global data supply chains, dominated by infrastructures and providers outside the European space, expose critical networks to systemic vulnerabilities and risks of unauthorized access or information manipulation (Aarland & Gjøsæter, 2022). On a geopolitical level, the normative fragmentation among the jurisdictions of the EU, the United States, and Asia leads to divergent standards in data protection, encryption, and digital sovereignty, complicating the establishment of a coherent global governance framework for cyberspace (Organisation for Economic Co-operation and Development [OECD], 2021).

A comparative sectoral synthesis of the issues related to the four analyzed domains is presented in Table 2.

Domain	Main Actors	Cooperation Mechanisms	Examples of Good Practices
Energy	EU, NATO, IEA, Energy Community	ENTSO-E, ACER, EU–US Energy Council	Interconnection of EU–Ukraine grids (2022)
Transport	EU, ICAO, IMO, NATO	TEN-T, EASA, Military Mobility	EU–NATO military mobility
Health	EU, WHO, UN	HERA, ECDC, GOARN	Coordinated COVID-19 response
Communications & Cyber	EU, NATO, CCDCOE, ITU	NIS2, ECCC, GFCE, Tallinn Manual	EU–NATO cooperation in cyber defence

Table 2. Comparative sectoral synthesis of sectoral issues

The analysis of sectoral international cooperation highlights that no critical domain can be protected in isolation - energy infrastructures depend on digital networks, transport relies on communications and energy, and healthcare systems depend on logistics and cybersecurity. The EU is at the forefront of developing cooperation mechanisms; however, their effectiveness depends on the active participation of Member States and on interoperability with NATO, the UN, and other

international organizations. The expansion of global cooperation, the integration of the physical and digital dimensions of security, as well as public–private partnerships, are key elements for protecting critical infrastructures in the 21st century.

4. CHALLENGES AND GOOD PRACTICES IN INTERNATIONAL COOPERATION IN THE FIELD OF CRITICAL INFRASTRUCTURE PROTECTION

4.1. Introductory Considerations

The development of an effective framework for international cooperation in the field of critical infrastructure protection faces a number of structural, institutional, and operational challenges. Although the European and global regulatory frameworks have evolved significantly over the past two decades, differences in vision, administrative capacity, and mutual trust among states continue to limit the uniform implementation of resilience measures.

At the same time, the accelerated dynamics of emerging technologies - such as digitalization, artificial intelligence (AI), the Internet of Things (IoT), and 5G systems - amplify the interdependencies and complexity of critical infrastructures. These trends give rise to new transnational vulnerabilities that require adaptive cooperation and flexible governance mechanisms.

4.2. Institutional and Political Challenges

One of the most persistent challenges in international cooperation is ***normative fragmentation and overlapping competences***, which hinder interinstitutional collaboration and reduce the efficiency of coordinated responses to major incidents - especially when an event has both physical and digital components (Mikac, 2023). At the global level, there is no unified legal framework for the protection of critical infrastructures; instead, there exists a plurality of instruments - directives, regional agreements, sectoral conventions - that partially overlap.

For example, within the EU, the *NIS2 Directive* and the *CER Directive* create a coherent framework for digital and physical infrastructures; however, their implementation varies among Member States depending on national capacities. Outside the EU, the approaches of NATO, the UN, or the OSCE are complementary but not perfectly harmonized, leading to interoperability gaps. This underscores the need for deeper strategic coordination and highlights the importance of harmonizing standards and interoperability mechanisms to strengthen collective security (Debuysere & Blockmans, 2021; European Commission & NATO, 2023).

This fragmentation has direct consequences for information sharing and joint crisis response, as standards and terminology are not always compatible.

On the other hand, ***the lack of trust and the difficulties associated with information sharing*** represent another significant challenge, given that cooperation in the field of critical infrastructures involves managing sensitive information related to technical vulnerabilities, strategic resources, and security policies. Many states hesitate to share such information due to concerns about sovereignty, confidentiality, or economic security. Recent studies show that the level of trust between public and private actors remains limited, and information sharing often occurs only in emergency situations (Sedenberg & Dempsey, 2018; Paulusson & Widman, 2024).

Moreover, geostrategic competition among major powers can undermine multilateral cooperation, turning critical infrastructures into instruments of geopolitical influence — thereby weakening traditional multilateral collaboration and reshaping the global order around the concept of the "infrastructure state" (DiCarlo & Schindler, 2022).

Lastly, ***divergences in priorities and resources*** in the field of critical infrastructure protection mean that some EU and NATO member states face difficulties in implementing technical standards and allocating the necessary funds for resilience. Significant disparities among EU member states regarding political priorities, financial resources, and administrative capacity to meet resilience requirements create structural differences that lead to challenges in the coherent application of technical standards, gaps in interinstitutional coordination, and inequities in funding allocation for critical infrastructure protection (Alexopoulos et al., 2024). This structural asymmetry limits the coherence of collective responses to cross-border threats and may create „weak points" exploitable by hostile actors.

In essence, normative fragmentation, institutional mistrust, and resource asymmetry undermine the effectiveness of international cooperation in critical infrastructure protection, generating interoperability gaps and systemic vulnerabilities. To strengthen resilience, deeper strategic coordination between international organizations, harmonization of standards, and sustainable information-sharing mechanisms based on mutual trust are required.

4.3. Technological and Operational Challenges

The integration of digital technologies across all areas of critical infrastructure - from energy and transport to healthcare - brings major benefits but also increased risks, making interconnected and automated systems vulnerable to complex cyberattacks with significant disruptive potential. According to the *Global Risks 2024* report (World Economic Forum, 2024), risks related to attacks on digital critical infrastructures are considered among the most likely and high-impact threats globally. Therefore, international cooperation in the cyber domain must include real-time information sharing, the standardization of security protocols, and joint response exercises.

Another major obstacle is represented by ***the complex interdependencies among infrastructures***. For example, a disruption in the energy network can affect communications, transportation, and medical services. The lack of a systemic vision and cross-sectoral coordination mechanisms reduces the effectiveness of international cooperation. Modeling these interdependencies and simulating crisis scenarios require advanced analytical tools, such as multi-agent models or network analysis. However, many states still lack the technical capacity for such integrated assessments (Lewis & Petit, 2019).

Hybrid infrastructures, formed through the combination of civilian and military functions - for example, energy networks also used for strategic purposes - represent new technological and operational challenges, as the protection of infrastructures cannot be separated from defense and security policy, potentially generating critical interdependencies and vulnerabilities in the context of contemporary conflicts (Capone, 2025). NATO-EU cooperation on military mobility and the protection of cross-border energy networks reflects a dual (civil–military) approach to resilience. However, the integration of these domains raises complex legal issues related to jurisdiction, responsibility, and operational control.

4.4. Good Practices in International Cooperation

Multinational simulation exercises represent one of the most effective forms of strengthening cooperation. Relevant examples include *Cyber Europe* (European Union Agency for Cybersecurity [ENISA], 2022), organized by ENISA, which simulates complex attacks on European digital infrastructures; and *Locked Shields* (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2023), CCDCOE's annual exercise, considered the largest cyber defense exercise in the

world. These exercises provide opportunities to test response capabilities and to strengthen trust among partners.

Additionally, ***public–private partnerships*** highlight success in institutional cooperation, as most critical infrastructures are operated by private entities, meaning that their protection depends on close collaboration between the public and private sectors. The EU has developed platforms such as the *European Public-Private Partnership for Resilience (EP3R)* (European Union Agency for Cybersecurity [ENISA], 2015), which promotes the exchange of information and best practices among governments, companies, and international organizations.

In the United States, the *Information Sharing and Analysis Centers (ISACs)* model (National Council of ISACs, n.d.) provides a solid foundation for data sharing between companies and authorities - a model partially adopted by some European states as well. Such partnerships enhance the collective capacity for threat detection and response.

Another example of good practice is the ***development of training programs and centers of excellence***, as is the case with the network of centers of excellence established within NATO and the EU. Centers such as the *CCDCOE Tallinn* (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], n.d.), the *Energy Security COE Vilnius* (NATO Energy Security Centre of Excellence, n.d.), and the *Crisis Management COE Sofia* (Crisis Management and Disaster Response Centre of Excellence, n.d.) contribute to the training of specialists, the development of standards, and the dissemination of knowledge.

In addition, the EU supports training programs within the *ECCC and the European Security and Defence College (ESDC)* (European Security and Defence College, n.d.), facilitating educational cooperation in the field of critical infrastructure protection.

Romania represents an interesting case of progressive integration into international cooperation networks, due to its dual status as an EU and NATO member and its hosting of the *ECCC*. At the regional level, initiatives such as the *Black Sea Cyber Cooperation Forum* (Black Sea and Balkans Security Forum, n.d.) and the *Eastern Partnership: Recovery-Reform-Resilience* (Council of the European Union, 2021) demonstrate the potential of multilateral cooperation in strengthening infrastructure security. These initiatives reflect the complementarity between EU and NATO efforts in the fields of cyber and energy security, highlighting Romania's role as a bridge actor between Euro-Atlantic structures and the Eastern neighborhood.

The analysis of challenges and good practices shows that the success of international cooperation in the field of critical infrastructure protection depends on three main factors: *trust* - between states, organizations, and private actors; *interoperability* - legal, technological, and operational; and *collective learning capacity* - through exercises, training, and exchange of experience.

4.5. Critical Analysis: Between Security and Sovereignty

One of the major dilemmas of international cooperation in the field of critical infrastructures is the balance between collective security and national sovereignty. In a globalized world, infrastructures are increasingly interconnected, yet states remain reluctant to relinquish control over strategic sectors. For example, the implementation of the *NIS2 Directive* has sparked debates regarding the competences of European versus national authorities (Ruohonen, 2024, p. 12). Similarly, within NATO, cooperation on energy infrastructures raises questions about the division of responsibility between the allied and national levels (Atanasov, 2024, p. 92).

Thus, a constant tension emerges between the need for coordination and the pressure to maintain strategic autonomy - a tension that must be managed through mechanisms of dialogue,

transparency, and shared governance. Despite these obstacles, good practices developed within the EU, NATO, and transatlantic partnerships provide functional models of cooperation. Strengthening these through investments in resilience, digitalization, and education represents an essential direction for the future.

5. FUTURE DIRECTIONS AND RECOMMENDATIONS IN INTERNATIONAL COOPERATION ON CRITICAL INFRASTRUCTURE PROTECTION

5.1. Introductory Considerations

The geopolitical, technological, and economic transformations of the past decade have redefined the very concepts of security and resilience in relation to critical infrastructures. In an environment marked by global interdependencies, hybrid threats, and accelerated technological progress, international cooperation has become not merely a strategic option, but an existential necessity for the stability of states and the functioning of essential systems.

This new reality calls for the development of innovative cooperation mechanisms grounded in real-time information sharing, legislative interoperability, and cross-sectoral coordination. At the same time, emerging trends - such as full digitalization, artificial intelligence, 5G networks, and smart infrastructures - bring forth not only new opportunities, but also significant risks that demand an adapted framework of global governance.

5.2. Emerging Trends in Critical Infrastructure Protection

The accelerated digitalization and the integration of artificial intelligence (AI) into the domain of critical infrastructures enhance operational efficiency but also amplify the risks associated with cyberattacks and technological failures (Yigit et al., 2025). In this context, the development of international standards for the ethical and technological governance of AI under the auspices of the UN, EU, and OECD becomes imperative. It is worth noting that the European Union has taken a significant step forward with the *AI Act (2024)* (European Parliament & Council of the European Union, 2024), which establishes rules for the responsible use of artificial intelligence, including within critical infrastructure systems.

Moreover, as ***5G networks - and the forthcoming 6G - evolve to form the „digital nervous system"*** of global economies, connecting billions of devices and supporting critical applications such as autonomous transport, telemedicine, and smart industrial networks, new vulnerabilities will emerge, particularly in the areas of supply chain attacks and technological espionage. Consequently, the protection of communication infrastructures must become a shared strategic priority.

In this regard, the EU launched in 2021 the *EU Toolbox for 5G Security* (European Commission, 2020b), a set of coordinated measures designed to mitigate technological and dependency risks associated with suppliers that do not comply with European standards. In parallel, NATO has integrated 5G security considerations into its strategy on *Emerging and Disruptive Technologies (EDTs)* (NATO, n.d.b), emphasizing the importance of interoperability and transatlantic standardization in safeguarding critical communications networks.

Another major challenge in the field of critical infrastructures is ***climate resilience and the green transition***, as climate crises and natural disasters are increasingly affecting these systems - from energy and transport networks to water and communication systems. In response, the European Union promotes the concept of green resilience, which entails integrating climate objectives into infrastructure protection policies. The *Green Deal* (European Commission, 2019) and the *Climate Adaptation Strategy* (European Commission, 2021b) set forth investments in sustainable and smart

infrastructures capable of withstanding climate-related risks. At the global level, the UN and the World Bank support cooperation through the *Global Facility for Disaster Reduction and Recovery* (Global Facility for Disaster Reduction and Recovery, n.d.), which provides technical assistance to vulnerable states.

Amid these international developments, ***critical infrastructures have been redefined as a collective defense objective***. Since 2022, NATO has incorporated critical infrastructure protection into the broader framework of collective defense (NATO, 2022b), particularly in light of attacks targeting European energy infrastructure (e.g., the Nord Stream incident, 2022). In this regard, NATO has established the *Critical Undersea Infrastructure Coordination Cell (CUICC)* (NATO, 2023) to monitor and safeguard submarine cables and maritime pipelines - a clear sign of the growing militarization of strategic infrastructure protection. Consequently, there is an urgent need to strengthen coordination between NATO, the EU, and member states concerning dual-use infrastructures - those serving both civilian and military purposes.

5.3. Strategic Recommendations at the International Level

Based on the analysis of the current framework, the following strategic directions can be proposed to strengthen international cooperation in the protection of critical infrastructures:

Establishing a global governance framework for critical infrastructures. Given the absence of a unified international legal instrument in this field, a viable solution would be the development - under the auspices of the UN - of an *International Convention on the Protection of Transnational Critical Infrastructures*. Such an instrument would define common standards regarding security, information sharing, and state responsibility in the event of major incidents.

Enhancing EU-NATO interoperability to ensure more effective coordination of critical infrastructure protection mechanisms and to prevent duplication of efforts. This objective could be achieved through: the alignment of resilience standards; the creation of a joint risk assessment platform for energy, cyber, and transport infrastructures; and the organization of regular joint hybrid exercises designed to test interoperability in complex, multi-domain scenarios.

Promoting global public-private partnerships, in which international organizations should support the creation of transnational information-sharing platforms between operators and governments. These platforms could contribute to the early detection of threats and rapid response in the event of coordinated attacks on global infrastructures.

Developing a shared culture of resilience, recognizing that the protection of critical infrastructures extends beyond technical measures and requires a common culture of security and resilience. This involves continuous professional training, regular simulation exercises, academic cooperation, and awareness campaigns. European institutions, together with NATO and the OSCE, should invest in resilience education through joint university programs, expert exchange initiatives, and the integration of critical infrastructure topics into public administration training.

In light of the above, it can be argued that the future directions of international cooperation in critical infrastructure protection will be shaped by three essential factors: Integrated global governance, based on common norms and inter-institutional cooperation; Digital transformation and the green transition, which redefine the risks and opportunities associated with infrastructures; and the strategic role of regional actors, such as Romania, in the practical implementation of international standards.

5.4. Specific Recommendations for Romania

Considering Romania's membership in the EU and NATO, as well as its strategic commitments within the Euro-Atlantic values and standards, the following points can be noted:

Romania's institutional framework in the field of critical infrastructure protection and cybersecurity is the result of a gradual evolution, adapted to European requirements and transatlantic commitments. The current architecture includes a set of public authorities, regulatory bodies, and technical structures that contribute complementarily to ensuring national resilience, as follows:

The *National Cyber Security Directorate (DNSC)* plays a central role in coordinating cybersecurity policies, implementing the *NIS2 Directive,* and managing *CERT-RO.* DNSC represents Romania within the *ENISA* and the *ECCC*, headquartered in Bucharest.

In parallel, the *Ministry of Internal Affairs (MAI)* manages the physical protection dimension of critical infrastructures through its specialized structures, in accordance with *LAW No. 18 of March 11, 2011on the approval of Government Emergency Ordinance No. 98/2010 regarding the identification, designation, and protection of critical infrastructures*, (Parliament of Romania, 2011) and coordinates the process of implementing the *CER Directive.*

The *National Authority for Management and Regulation in Communications (ANCOM)* holds direct competences in regulating and supervising the security of electronic communications networks and services, contributing to the application of resilience requirements imposed by the *NIS2 Directive.*

Sectoral CSIRTs - established in essential fields such as energy, finance and banking, transport, and healthcare - provide operational and technical support, ensuring coordination with *DNSC* and *CERT-EU*. At the strategic level, the *Supreme Council of National Defence (CSAT)* (Supreme Council of National Defence [CSAT], n.d.) sets the main directions in the field of security and resilience, while the *National Committee for the Protection of Critical Infrastructures* (National Committee for the Protection of Critical Infrastructures, n.d.) coordinates, at the inter-ministerial level, policies of prevention, response, and recovery.

Regarding the ***status of transposing the NIS2 and CER directives***, Romania has made significant progress through the adoption of *Law No. 362/2018 on the security of network and information systems* (Parliament of Romania, 2018) and *Emergency Ordinance 155/2024* (Government of Romania, 2024), approved through *Law 124/2025* (Parliament of Romania, 2025), but it is still in an advanced yet incomplete stage of the transposition process for the two fundamental directives - *NIS2* and *CER*. The MAI is coordinating the update of the national framework for the protection of critical infrastructures and the risk assessment methodology in order to align with the *CER Directive*. The full completion of this process is estimated for the period 2025–2026, alongside the adoption of a unified legislative framework and the establishment of sectoral supervisory authorities.

A comparative assessment of the current framework against EU and NATO requirements highlights significant progress, but also a series of structural and operational challenges:

- *Legislative and regulatory framework* - Although the transposition projects for the *NIS2* and *CER Directives* are advanced, overlaps in institutional competences persist, as well as the absence of a unified law on the resilience of critical infrastructures.
- *Interinstitutional coordination* - Cooperation among DNSC, MAI, ANCOM, and private actors remains only partially formalized; effective mechanisms for operational coordination and real-time information exchange are still lacking.
- *Technical and operational capacities* - Sectoral CSIRTs are uneven in terms of development; the absence of an integrated national platform for incident reporting and a real-time monitoring center is evident.

- *Professional training and awareness* - Existing programs represent an important step forward but do not yet provide full coverage; the development of a national standardized framework for training and simulation across all critical sectors is necessary.
- *Financial resources and strategic sustainability* - The implementation of strategies depends largely on European funding, highlighting the need for the creation of a dedicated domestic budget line for critical infrastructure resilience projects.

Consequently, we ***consider that Romania's strategic directions*** may focus on the following:

- *Strengthening analytical and response capacities* through investments in real-time risk monitoring platforms, research centers in the field of infrastructure security (in partnership with the *ECCC*), and university and postgraduate training programs in the field.
- *Expanding regional cooperation* by initiating a *Resilience Partnership for the Western Balkans and the Black Sea,* focused on energy and cybersecurity, active participation in the *Energy Community* (Energy Community, n.d.), and the periodic organization of multinational exercises for incident response.

Through these directions, Romania can strengthen its position as a pillar of regional stability and innovation, contributing to the strategic objectives of the EU and NATO.

6. LIMITATIONS OF THE RESEARCH

Although grounded in a rigorous and interdisciplinary methodological approach, the present research exhibits a series of limitations inherent to the analyzed field and the nature of the available data.

First, restricted access to sensitive or classified information regarding incidents affecting critical infrastructures represented a major constraint. The analysis relied exclusively on public sources - official documents, institutional reports, and academic literature - which may result in gaps in assessing the actual level of operational preparedness and the practical experiences of crisis management.

Another limitation stems from the rapidly evolving legislative and institutional framework, particularly during the 2022-2025 period. The European directives *NIS2* and *CER*, as well as the new NATO-EU arrangements concerning critical infrastructure resilience, are still in the process of implementation. Consequently, some conclusions have a prospective character, being based on the estimated future impact of these policies, which may affect the long-term stability of interpretations.

Moreover, international comparability is limited by significant differences among states in terms of institutional capacities, terminology used, and levels of data reporting. This factor reduces the possibility of a fully homogeneous assessment of the effectiveness of cooperation mechanisms. At the same time, the research's focus on major international organizations (EU, NATO, UN, OSCE) and on the sectors of energy, transport, health, and communications has led to a certain underrepresentation of other regions or strategic domains, such as financial infrastructure or water supply systems.

From a methodological perspective, the predominant use of qualitative analyses and the illustrative single-case study - Romania - introduces an inevitable degree of subjectivity. The absence of standardized quantitative datasets that are comparable at the transnational level limits the possibility of empirically validating the identified causal relationships.

Nevertheless, these limitations do not diminish the theoretical relevance or practical value of the research, which provides a solid foundation for future developments. Overcoming these constraints could be achieved through expanded cooperation with specialized institutions, controlled

access to operational data, the integration of quantitative methods, and the use of simulation models to analyze interdependencies among critical infrastructures.

7. CONCLUSIONS

This study has systematically examined the framework of international cooperation in the field of critical infrastructure protection from a multidimensional perspective - legal, institutional, technological, and strategic.

Starting from the proposed hypotheses, the research has demonstrated that the protection of critical infrastructures can no longer be conceived solely at the national level. Instead, it requires an integrated approach founded on transnational cooperation, solidarity, and collective resilience.

The main findings can be summarized as follows:

• *Confirmation of cooperation as an essential factor of resilience (Hypothesis 1).* International cooperation has proven to be the cornerstone of critical infrastructure protection, as modern threats - whether cyber, energy-related, climatic, or health-related - are inherently transnational and interdependent. The EU, NATO, and the UN play complementary roles in strengthening global security, and the alignment of their efforts has generated a coherent and adaptable framework for action.

• *The need for a unified and interoperable international regulatory framework (Hypothesis 2).* The research highlights that such a framework, in which technology acts as a transformative factor, can significantly enhance the resilience of critical infrastructures and improve the efficiency of crisis response mechanisms.

• *Identification of major challenges in international cooperation (Hypothesis 3).* The study has identified several key difficulties, including regulatory fragmentation, lack of trust among actors, capacity asymmetries, and the complexity of technological interdependencies. Nevertheless, these obstacles can be mitigated through mechanisms promoting transparency, interoperability, and joint training.

• *Emphasis on cross-sectoral interdependence (Hypothesis 4).* Sectoral analysis has shown that energy, transport, healthcare, and communication infrastructures are deeply interconnected. This interdependence calls for integrated governance and coordinated response mechanisms at the international level.

• *Romania's relevance as a regional actor (Hypothesis 5).* Romania holds significant strategic potential due to its geographic position, membership in the EU and NATO, and its hosting of the ECCC. With clearer institutional coordination and greater investment in research and training, the country could evolve into a regional hub for expertise and cooperation in the field of critical infrastructure protection.

From a theoretical perspective, the study has validated the following premises:

• *International cooperation represents an advanced form of global governance*, grounded in interdependence and shared responsibility. It transcends the classical dimension of security, becoming an expression of solidarity among states and organizations.

• *The resilience of critical infrastructures possesses a systemic dimension*, encompassing not only physical or cyber protection but also adaptability, learning capacity, and the rapid restoration of functionality after a crisis.

• *Critical infrastructures constitute a global public good*, whose protection goes beyond the traditional logic of national sovereignty. In this regard, the development of a coherent global framework under the auspices of the UN is necessary to standardize principles and responsibilities.

At a practical level, the research has led to the formulation of the following conclusions and strategic recommendations:

- *Strengthening the international regulatory framework*. It is recommended to initiate a Global *Convention on the Protection of Critical Infrastructures*, aimed at unifying standards and procedures under the auspices of the UN, thereby ensuring a coherent and harmonized global approach.
- *Full alignment between the EU and NATO.* The two organizations should develop advanced interoperability mechanisms, including the establishment of a joint risk analysis system and a unified database for incidents affecting critical infrastructures.
- *Creation of a permanent transnational response system.* The proposal envisions the development of a *Rapid Response Mechanism for Critical Infrastructures (RRMCI),* designed to provide technical, operational, and logistical support to member states in the event of a major attack or systemic disruption. *Integration of cybersecurity and climate security into resilience strategies.* Emerging climate and digital risks must be addressed in a unified manner. It is recommended to develop national collective resilience plans that combine energy, cyber, and climate protection within a comprehensive strategic framework.
- *Strengthening Romania's role within the regional architecture.* In this context, it is proposed that Romania should: adopt a *National Strategy for Critical Infrastructures 2025–2030*; strengthen the roles of the DNSC and the Ministry of Internal Affairs (MAI) in coordinating cross-sectoral policies; promote regional cooperation within the *Black Sea Resilience Partnership*; and develop a *Regional Training and Simulation Centre for Infrastructure Protection* under the auspices of the *ECCC* in Bucharest, serving as a platform for training, research, and coordinated crisis response.

From the perspective of the points presented above, international cooperation in the field of critical infrastructure protection represents a fundamental premise of global security and stability. The success of this cooperation depends on three key conditions: the political will to share responsibilities and information; the harmonization of standards and institutional interoperability; and sustained investment in education, research, and innovation as the foundation of long-term resilience.

The study demonstrates that the protection of critical infrastructures is not merely a matter of security, but a true project of civilization - one that defines the international community's ability to cooperate, to adapt, and to safeguard its functional foundations in the face of global uncertainty.

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

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

REFERENCES

Aarland, M., & Gjøsæter, T. (2022). Digital supply chain vulnerabilities in critical infrastructure: A systematic literature review on cybersecurity in the energy sector. *ICISSP*, 326–333.

Abraham, D., Houmb, S. H., & Erdodi, L. (2025). Cyber-attacks on energy infrastructure: A literature overview and perspectives on the current situation. *Applied Sciences, 15*(17), 9233.

Agency for the Cooperation of Energy Regulators. (n.d.). *About ACER*. Retrieved November 1, 2025, from https://www.acer.europa.eu/

Alexopoulos, M. J., Niemi, A., Skobiej, B., & Sll Torres, F. (2025). Examination of the Critical Infrastructure Resilience Directive from the maritime point of view. *JCMS: Journal of Common Market Studies, 63*(2), 667–678.

Atanasov, D. D. (2024). Too many cooks in the kitchen? EU–NATO overlap in safeguarding European critical energy infrastructure post-2022. *Bezbednosni dijalozi, 15*(2), 87–96.

Bellamkonda, S. (n.d.). Ransomware attacks on critical infrastructure: A study of the Colonial Pipeline incident.

Black Sea and Balkans Security Forum. (n.d.). *Event programme 2025*. Retrieved November 1, 2025, from https://2bsecurityforum.ro/programme/

Capone, F. (2025). *Dual-use objects under international humanitarian law: Towards a paradigm shift*. T. M. C. Asser Press.

Computer Emergency Response Team for the European Union [CERT-EU]. (n.d.). *About CERT-EU*. Retrieved November 1, 2025, from https://cert.europa.eu/

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, pp. 75–82. Retrieved November 2, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)* (ETS No. 185). Retrieved November 3, 2025, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of the European Union. (2021, January 28). *Eastern Partnership: Recovery – Reform – Resilience* [Infographic]. November 3, 2025, from https://www.consilium.europa.eu/en/infographics/the-eastern-partnership-recovery-reform-resilience/

Crisis Management and Disaster Response Centre of Excellence. (n.d.). *About us*. Retrieved November 3, 2025, from https://www.cmdrcoe.org/menu.php?c_id=89&m_id=40

Debuysere, L., & Blockmans, S. (2021). The EU's integrated approach to crisis response: Learning from the UN, NATO and OSCE. In *The EU and crisis response* (pp. 86–114).

DiCarlo, J., & Schindler, S. (2022). Introduction: geopolitics, infrastructure, and the emergent geographies of us–China competition. In *The Rise of the Infrastructure State* (pp. 1-10). Bristol University Press.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems across the Union, *Official Journal of the European Union*, L 194, 19 July 2016, pp. 1-30. Retrieved November 5, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

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, *Official Journal of the European Union*, L 333, 27 December 2022, pp. 80–152. Retrieved November 5, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, *Official Journal of the European Union*, L 333, 27 December 2022, 164–198. Retrieved November 5, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557

Energy Community. (n.d.). *Who we are*. Energy Community Secretariat. Retrieved November 5, 2025, from https://www.energy-community.org/aboutus/whoweare.html

EU Expert Group on Health Systems Performance Assessment [HSPA]. (2020). *Assessing the resilience of health systems in Europe: An overview of the theory, current practice and strategies for improvement*. Publications Office of the European Union. Retrieved November 5, 2025, from https://health.ec.europa.eu/system/files/2021-10/2020_resilience_en_0.pdf

European Centre for Disease Prevention and Control. (n.d.). *About us*. Retrieved November 5, 2025, from https://www.ecdc.europa.eu/en/about-us

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020, December 16). *The EU's cybersecurity strategy for the digital decade*. European Union. Retrieved November 5, 2025, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commission, & NATO. (2023, June). *EU–NATO Task Force on the resilience of critical infrastructure: Final assessment report*. Retrieved November 5, 2025, from https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

European Commission, Joint Research Centre [JRC]. (n.d.). *European Reference Network for Critical Infrastructure Protection (ERNCIP)*. Retrieved November 5, 2025, from https://erncip-project.jrc.ec.europa.eu

European Commission. (2014, May 28). *European energy security strategy* (COM (2014) 330 final). Publications Office of the European Union. Retrieved November 5, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0330

European Commission. (2019, December 11). *The European Green Deal* (COM(2019) 640 final). Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0640

European Commission. (2020a, December 9). *Sustainable and smart mobility strategy – Putting European transport on track for the future*. Publications Office of the European Union. Retrieved November 5, 2025, from https://transport.ec.europa.eu/transport-themes/mobility-strategy_en

European Commission. (2020b, January 29). *Cybersecurity of 5G networks – EU toolbox of risk-mitigating measures* (NIS Cooperation Group Report). Publications Office of the European Union. Retrieved November 5, 2025, from https://op.europa.eu/en/publication-detail/-/publication/a9d278f6-4637-11ea-b81b-01aa75ed71a1

European Commission. (2021a, December 14). *Regulation (EU) No 1315/2013 on Union guidelines for the development of the trans-European transport network (TEN-T)* (consolidated, COM (2021) 812 final). Publications Office of the European Union. Retrieved November 7, 2025, from https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european-transport-network-ten-t_en

European Commission. (2021b, February 24). *Forging a climate-resilient Europe: The new EU strategy on adaptation to climate change* (COM (2021) 82 final). Retrieved November 7, 2025, from https://climate.ec.europa.eu/eu-action/adaptation-and-resilience-climate-change/eu-adaptation-strategy_en

European Commission. (2021c, June 9). *Regulation (EU) 2021/1153 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014. Official Journal of the European Union, L 249*, 38. Retrieved November 7, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1153

European Commission. (2022a, December 12). *European Health Union: A new EU health security framework is in motion*. Retrieved November 7, 2025, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7871

European Commission. (2022b, March 25). *United States and European Commission announce task force to reduce Europe's dependence on Russian fossil fuels and strengthen European energy security* [Fact sheet]. Retrieved November 7, 2025, from https://www.energy.gov/sites/default/files/2023-12/EX43FA~1_0.PDF

European Commission. (2022c, May 18). *REPowerEU plan: Joint European action for more affordable, secure and sustainable energy* (COM (2022) 230 final). Publications Office of the European Union. Retrieved November 8, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0230

European Commission. (2024). *European Health Data Space [EHDS]*. Publications Office of the European Union. Retrieved November 8, 2025, from https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

European Commission. (2025, March 26). *Joint communication on a new EU Preparedness Union*. Retrieved November 8, 2025, from https://commission.europa.eu/document/download/526806b6-c4e1-43d1-81b7-947308efbab1_en?filename=Joint+Communication.pdf

European Commission. (n.d.). *Health Emergency Preparedness and Response Authority* [HERA]. Retrieved November 8, 2025, from https://health.ec.europa.eu/health-emergency-preparedness-and-response-hera_en

European Cyber Security Organisation [ECSO], & CEN-CENELEC. (n.d.). *Memorandum of Understanding*. Retrieved November 8, 2025, from https://ecs-org.eu/ecso-and-cen-cenelec-sign-memorandum-of-understanding/

European Cybersecurity Competence Centre. (n.d.). *About the European Cybersecurity Competence Centre (ECCC)*. Retrieved November 9, 2025, from https://cybersecurity-centre.europa.eu

European External Action Service. (2023, July 20). *Military mobility*. European Union. Retrieved November 9, 2025, from https://www.eeas.europa.eu/eeas/military-mobility_en

European External Action Service. (n.d.). *Permanent Structured Cooperation [PESCO]*. Retrieved November 9, 2025, from https://www.pesco.europa.eu/

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection [EU-CIP]. (2022–2025). *EU-CIP – European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection*. Retrieved November 9, 2025, from https://www.eucip.eu/

European Maritime Safety Agency. (n.d.). *About EMSA*. Retrieved November 9, 2025, from https://www.emsa.europa.eu/

European Medicines Agency. (n.d.). *About the European Medicines Agency*. Retrieved November 9, 2025, from https://www.ema.europa.eu/en/about

European Network of Transmission System Operators for Electricity. (n.d.). *About ENTSO-E*. Retrieved November 9, 2025, from https://www.entsoe.eu/

European Network of Transmission System Operators for Electricity. (2022, March 16). *Continental Europe successful synchronisation with Ukraine and Moldova power systems*. Retrieved November 9, 2025, from https://www.entsoe.eu/news/2022/03/16/continental-europe-successful-synchronisation-with-ukraine-and-moldova-power-systems/

European Parliament & Council of the European Union. (2013, December 17). *Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism* (OJ L 347, pp. 924-947). Retrieved November 9, 2025, from https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32013D1313

European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L [2024/1689], 12 July 2024). Retrieved November 9, 2025, from http://data.europa.eu/eli/reg/2024/1689/oj

European Security and Defence College. (n.d.). *European Security and Defence College* [*ESDC*]. Retrieved November 9, 2025, from https://www.esdc.europa.eu/index_en?prefLang=ro

European Union & NATO. (2016, July 8). *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. Retrieved November 10, 2025, from https://www.nato.int/cps/en/natohq/official_texts_133163.htm

European Union & NATO. (2018, July 10). *Joint declaration on EU–NATO cooperation*. Retrieved November 10, 2025, from https://www.nato.int/cps/en/natohq/official_texts_156626.htm

European Union & NATO. (2023, January 10). *Joint declaration on EU–NATO cooperation*. Retrieved November 10, 2025, from https://www.nato.int/cps/en/natohq/official_texts_210549.htm

European Union Agency for Cybersecurity [ENISA]. (2015, April 15). *EP3R 2009–2013: Future of NIS public–private cooperation*. Retrieved November 10, 2025, from https://www.enisa.europa.eu/publications/ep3r-2009-2013

European Union Agency for Cybersecurity [ENISA]. (2022). *Cyber Europe 2022 – After action report*. ENISA. Retrieved November 10, 2025, from https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

European Union Agency for Cybersecurity [ENISA]. (n.d.-a). *About ENISA*. Retrieved November 10, 2025, from https://www.enisa.europa.eu

European Union Agency for Cybersecurity [ENISA]. (n.d.-b). *Cyber Europe*. Retrieved November 10, 2025, from https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe

European Union Agency for Cybersecurity [ENISA]. (n.d.-c). *EU cybersecurity policies | Shaping Europe's digital future*. Retrieved November 9, 2025, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Union Aviation Safety Agency. (n.d.). *About EASA*. Retrieved November 10, 2025, from https://www.easa.europa.eu/

European Union External Action Service. (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*. Council of the European Union. Retrieved November 9, 2025, from https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence_en

European Union. (2006). *Energy Community Treaty*. Energy Community. Retrieved November 9, 2025, from https://www.energy-community.org/legal/treaty.html

Global Facility for Disaster Reduction and Recovery. (n.d.). *About GFDRR*. The World Bank. Retrieved November 9, 2025, from https://www.gfdrr.org/en

Global Forum on Cyber Expertise. (n.d.). *About the GFCE*. The Hague: Global Forum on Cyber Expertise. Retrieved November 5, 2025, from https://thegfce.org

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. Retrieved November 5, 2025, from https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121

International Civil Aviation Organization. (n.d.). *About ICAO*. Retrieved November 9, 2025, from https://www.icao.int/

International Energy Agency. (n.d.). *About the IEA*. Retrieved November 9, 2025, from https://www.iea.org/about

International Maritime Organization. (n.d.). *About IMO*. Retrieved November 3, 2025, from https://www.imo.org/

International Telecommunication Union. (n.d.). *About ITU*. United Nations. Retrieved November 5, 2025, from https://www.itu.int/

Kallenborn, Z., & Willis, H. H. (2025). *Globally critical infrastructure: The unique risks and challenges*. Risk Analysis. Advance online publication. Retrieved November 5, 2025, from https://doi.org/10.1111/risa.70147.

Kane, B. R., Webber, S., Tucker, K. H., Wallace, S., Chang, J., McCarthy, D., Murphy, D., Egel, D., & Wingfield, T. (2024). *Threats to critical infrastructure: A survey* (RR-A2397-2). Santa Monica, CA: RAND Corporation. Retrieved November 5, 2025, from https://doi.org/10.7249/RRA2397-2

Kreso, I. (n.d.). *Cyber threats and vulnerability mapping in the energy sector: Laying the groundwork for smart grid resilience*. *Applied Cybersecurity & Internet Governance*.

Lewis, L. P., & Petit, F. (2019). *Critical infrastructure interdependency analysis: Operationalising resilience strategies*. Argonne National Laboratory. Retrieved November 5, 2025, from https://www.researchgate.net/publication/382480432_Critical_Infrastructure_Interdependency_Analysis_Operationalising_Resilience_Strategies

Li, Y., & Zhang, M. (2025). Cascading failure analysis of interdependent water-power networks based on functional coupling. *Reliability Engineering & System Safety, 259*, 110950.

Lucarelli, S., Moro, F., & Marrone, A. (2022). Pandemics and international security: The outlook for NATO.

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges—The case of the health sector in particular. *Computer Law & Security Review, 41*, 105502.

Mikac, R. (2023). Protection of the EU's critical infrastructures: Results and challenges. *Applied Cybersecurity & Internet Governance, 2*(1), 1–25.

Mishra, N. (2024). Regulatory interoperability in the digital economy. SSRN.

Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies, 14*(6), 1571.

National Committee for the Protection of Critical Infrastructures. (n.d.). General information. Retrieved November 6, 2025, from https://cncpic.mai.gov.ro/

National Council of ISACs. (n.d.). *About Information Sharing and Analysis Centers (ISACs)*. Retrieved November 6, 2025, from https://www.nationalisacs.org/about-isacs

National Cyber Security Directorate. (n.d.). *Despre DNSC*. [About DNSC]. Government of Romania. Retrieved November 3, 2025, from https://dnsc.ro/

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023). *Locked Shields 2023 – After action report*. NATO CCDCOE. Retrieved November 6, 2025, from https://ccdcoe.org/exercises/locked-shields

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (n.d.). *About us*. Retrieved November 6, 2025, from https://ccdcoe.org/

NATO Energy Security Centre of Excellence. (n.d.). *About us*. Retrieved November 8, 2025, from https://www.enseccoe.org/about-us/

NATO Intelligence Fusion Centre. (n.d.). *About us – Who we are*. Retrieved November 10, 2025, from https://web.ifc.bices.org/about-us/who-we-are

NATO. (2016, July 9). *Commitment to enhance NATO's resilience: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016*. North Atlantic Treaty Organization. Retrieved November 10, 2025, from https://www.nato.int/cps/en/natohq/official_texts_133180.htm

NATO. (2022a, June 29). *Strategic concept 2022*. NATO. Retrieved November 6, 2025, from https://www.nato.int/strategic-concept

NATO. (2022b, June). *Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization*. NATO. Retrieved November 10, 2025, from https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2023, February 15). *NATO stands up undersea infrastructure coordination cell*. Retrieved November 5, 2025, https://www.nato.int/cps/en/natohq/news_211919.htm

NATO. (n.d.-a). *Crisis Management Exercise (CMX)*. North Atlantic Treaty Organization. Retrieved November 5, 2025, from https://www.nato.int/cps/en/natolive/topics_49192.htm

NATO. (n.d.-b). *Emerging and disruptive technologies*. North Atlantic Treaty Organization. Retrieved November 2, 2025, from https://www.nato.int/cps/en/natohq/topics_184303.htm

O'Kelly, M. E. (2025). Transportation security at hubs: Addressing key challenges across modes of transport. *Journal of Transportation Security, 18*(1), 4.

Organisation for Economic Co-operation and Development. (2021, December). *Interoperability of privacy and data protection frameworks*. OECD Publishing. Retrieved November 2, 2025, from https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/12/interoperability-of-privacy-and-data-protection-frameworks_8c0b32f4/64923d53-en.pdf

Organization for Security and Co-operation in Europe. (2013, December 3). *Permanent Council Decision No. 1106: Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. Retrieved November 2, 2025, from https://www.osce.org/pc/109168

Organization for Security and Co-operation in Europe. (2016, March 10). *Permanent Council Decision No. 1202: OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. Retrieved November 2, 2025, from https://www.osce.org/pc/227281

Organization for Security and Co-operation in Europe. (2019, December 10). *Joint statement to supplement the framework for cooperation and coordination between the United Nations Secretariat and the OSCE*. Retrieved November 2, 2025, from https://www.osce.org/files/f/documents/1/c/441808.pdf

Organization for Security and Co-operation in Europe. (2021). *Physical security considerations for protecting critical infrastructure from terrorist attacks.* Organization for Security and Co-operation in Europe. November 2, 2025, https://www.osce.org/files/f/documents/e/6/597756_0.pdf

Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction, 60*, 102316.

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. Retrieved November 6, 2025, from https://legislatie.just.ro/Public/DetaliiDocument/126829

Parliament of Romania. (2018, December 28). *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*. [*Law No. 362/2018 on ensuring a high common level of security of network and information systems*]. Official Gazette, nr. 21/9 ianuarie 2019.

Parliament of Romania. (2025). *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.

Paulusson, J., & Widman, E. (2024). Private–public information sharing for cybersecurity: Exploring private actors' perspective in the Swedish banking sector. *Stockholm University Working Paper*. Retrieved November 5, 2025, from https://su.diva-portal.org/smash/get/diva2%3A1955729/FULLTEXT01.pdf

Peptan, C. (2022). Considerations on some aggressions against critical infrastructure on the territory of Ukraine during the „special military operation" conducted by the Russian Federation. *Annals of'Constantin Brancusi'University of Targu-Jiu. Engineering Series/Analele Universității Constantin Brâncuși din Târgu-Jiu. Seria Inginerie*, (1).

Pursiainen, C., & Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure, 8*(4), 270–285.

Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. *arXiv*. https://arxiv.org/abs/2412.08084.

Santos, B. F., & Tavasszy, L. A. (2025). Cyber resilience in Logistics 4.0: Managing vulnerabilities in intelligent transport systems and digital supply chains. *Transportation Research Part E: Logistics and Transportation Review, 188*, 103613.

Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures, 7*(5), 67.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Sedenberg, E. M., & Dempsey, J. X. (2018). Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs. *arXiv*.

Sommerer, T., Squatrito, T., Tallberg, J., & Lundgren, M. (2022). Decision-making in international organizations: Institutional design and performance. *The Review of International Organizations, 17*(4), 815–845.

Sonesson, T. R., Johansson, J., & Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety Science, 142*, 105383.

Supreme Council of National Defence. (n.d.). *Consiliul Suprem de Apărare a Țării [Supreme Council of National Defence]*. Retrieved November 6, 2025, from https://csat.presidency.ro

U.S. Department of Energy. (2022, February 7). *Joint statement on the U.S.–EU Energy Council*. Retrieved November 6, 2025, from https://www.energy.gov/articles/joint-statement-us-eu-energy-council

United Nations Economic Commission for Europe. (n.d.). *About UNECE*. Retrieved November 8, 2025, from https://unece.org/

United Nations Institute for Disarmament Research. (n.d.). *About UNIDIR*. United Nations. Retrieved November 8, 2025, from https://www.unidir.org/

United Nations Office for Disarmament Affairs. (2024). *Protecting the cybersecurity of critical infrastructures and their supply chains*. UNODA. Retrieved November 8, 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf?

United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030*. United Nations. Retrieved November 8, 2025, from https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

United Nations Office for Disaster Risk Reduction. (n.d.). *About UNDRR*. United Nations. Retrieved November 10, 2025, from https://www.undrr.org/

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1). Retrieved November 6, 2025, from https://sdgs.un.org/2030agenda

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science, 15*, 100244.

World Economic Forum. (2024). *The Global Risks Report 2024*. World Economic Forum. Retrieved November 9, 2025, from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

World Health Organization. (n.d.). *Global Outbreak Alert and Response Network (GOARN)*. Retrieved November 9, 2025, from https://goarn.who.int/

Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., … Janicke, H. (2025). Generative AI and LLMs for critical infrastructure protection: Evaluation benchmarks, agentic AI, challenges, and opportunities. *Sensors, 25*(6), 1666.