Research and Science TODAY
www.rstjournal.com

OPEN ACCESS

Section: *Social Sciences and Humanities*
Issue: *1/2026*
Article number: *1.2026*

DOI
https://doi.org/10.38173/RST.2026.1.1

The Use of Intelligence in the Protection of Critical Infrastructure: From Reactive Protection to Anticipatory Resilience

Cătălin PEPTAN[1]

[1] Lecturer, PhD; "Constantin Brâncuși" University of Târgu-Jiu, Romania; catalinpeptantm@gmail.com

Received: *25 November 2025*
Revised: *7 January 2026*
Accepted: 28 January 2026
Available online: 2 February 2026

Suggested citation
C. Peptan, "The use of intelligence in the protection of critical infrastructure: From reactive protection to anticipatory resilience", Research and Science Today, vol. 2026, no. 1, art. no. 1.2026, pp. 1–23, 2026, doi: 10.38173/RST.2026.1.1.

Abstract
The study analyzes the role of intelligence in the protection and resilience of critical infrastructure within a dynamic security environment characterized by technological interdependencies, accelerated digitalization, and multidimensional threats. A qualitative, theoretical-analytical, and interdisciplinary approach was adopted, with the main objective of constructing an integrated conceptual framework that highlights the contribution of intelligence - across its operational, tactical, and strategic analytical dimensions - to the transition from a reactive security model to one of anticipatory resilience. The research demonstrates that the coherent integration of intelligence processes and products into infrastructural risk governance enhances the capacity to anticipate, detect, and prevent incidents with systemic potential, providing decision-making and operational support under conditions of heightened uncertainty. Furthermore, the study underscores the need to optimize the intelligence cycle, leverage emerging technologies, develop human capital, and standardize information dissemination. The general conclusion is that intelligence must be conceived as a central pillar of infrastructural resilience - not merely as an informational support tool - in order to ensure the continuity of the essential functions of the state and society.

Keywords: *Critical infrastructure; intelligence; protection; resilience; security*

1. INTRODUCTION

1.1. Context and relevance of the research topic

Over the past two decades, critical infrastructures have become central to discussions concerning national security and societal resilience, against the backdrop of increasing technical, logistical, and organizational interdependencies, accelerated digitalization, and the convergence between Information Technology (IT) and Operational Technology (OT) systems [1–2]. Infrastructures in the fields of energy, transport, communications, healthcare, finance, and food supply can no longer be examined merely as collections of physical assets, but rather as complex socio-technical systems, deeply interconnected, whose disruption may generate domino effects with systemic impact on the functioning of the state and society [3–6].

In parallel, the security environment is marked by a proliferation of threats - from sophisticated cyberattacks (ransomware, the compromise of Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA), attacks on digital supply chains) to hybrid threats, terrorism, sabotage, and natural disasters - alongside the emergence of new technological risks associated with the Internet of Things (IoT), 5G/6G networks, Artificial Intelligence (AI), or digital twins [7–14]. All these dynamics transform the protection of critical infrastructures into a continuous, adaptive, and anticipatory process that surpasses the traditional logic of reactive security.

In this context, intelligence - understood as informational product, operational process, and specialized agency - emerges as an essential strategic capability. Through the collection, analysis, and dissemination of relevant and actionable information concerning threats, vulnerabilities, actors, and evolving patterns, intelligence can support the transition from a model focused on physical and cyber protection to one grounded in resilience and integrated risk governance [15–20].

The research topic therefore lies at the intersection of security studies, Intelligence studies, and the literature on critical infrastructure governance, holding both theoretical relevance (by clarifying the conceptual framework) and practical relevance (for public policy and for operators of essential infrastructure).

1.2. Purpose, hypotheses, and research objectives

The purpose of this study is to analyze how intelligence can contribute to the protection and resilience of critical infrastructures within the context of threats and vulnerabilities specific to contemporary security.

Building on this direction, the ***main research question*** is: *How can intelligence support the strengthening of critical infrastructure protection and resilience through its coherent integration into the processes of assessment, prevention, and response to current threats?*

In accordance with this question, the research pursues the following ***main objectives***:

O1. Clarifying the conceptual and theoretical framework regarding critical infrastructures, resilience, and intelligence.

O2. Identifying the relevant types of intelligence and their roles in the risk management process.

O3. Analyzing the main threats and vulnerabilities targeting critical infrastructures in the current security environment.

O4. Assessing how intelligence can support early warning, risk assessment, decision-making, and operational response.

O5. Formulating an integrated analytical framework for the use of intelligence in the protection of critical infrastructures.

To guide the analysis, the following ***research hypotheses*** are formulated:

H1. The enhanced valorization of intelligence facilitates the transition from reactive protection to anticipatory resilience.

H2. Major vulnerabilities of critical infrastructures can be significantly reduced through robust intelligence capabilities oriented toward early warning and integrated risk assessment.

H3. A governance framework that prioritizes intelligence increases the capacity to anticipate and manage emerging threats.

H4. Inter-institutional cooperation and standardized mechanisms for information sharing are essential conditions for the resilience of critical infrastructures.

1.3. Research methodology and structure of the study

a.) Type of research and methodological approach. The research is predominantly qualitative, theoretical–analytical, and exploratory, focusing on the clarification of concepts, the systematization of the specialized literature, and the formulation of an integrated analytical framework. It does not constitute empirical research in the strict sense (i.e., involving the collection of primary data), but rather an in-depth analysis of relevant sources.

The approach is interdisciplinary, positioned at the intersection of security studies, Intelligence studies, and public policy concerning the protection of critical infrastructures.

b.) Methods used. The research employs primarily the following methods:

Documentary and content analysis of the relevant normative and strategic framework (European directives and strategies, national security documents, OECD, ENISA, UN, CISA reports etc.), with the aim of capturing conceptual and institutional developments in the protection and resilience of critical infrastructures.

Conceptual and theoretical analysis of the academic literature on critical infrastructures, resilience, and intelligence, in order to clarify concepts, typologies, and the relationships between them.

Analytical synthesis for the formulation of an integrated framework for understanding the role of intelligence in the protection of critical infrastructures, correlating intelligence levels of analysis, the diversity of threats and vulnerabilities, and governance functions.

c.) Research delimitations. The research focuses on: critical infrastructures in a broad sense, with emphasis on their cyber dimension; the role of intelligence in their protection, without developing in detail the technical–operational specificities of each sector (energy, health, transport etc.), but treating them at the level of general principles and mechanisms; the European and Euro-Atlantic framework, insofar as the literature provides relevant examples for conceptual analysis.

2. CONCEPTUAL AND THEORETICAL BENCHMARKS REGARDING THE PROTECTION OF CRITICAL INFRASTRUCTURE THROUGH INTELLIGENCE

2.1. The concept of critical infrastructure

The term *critical infrastructure* refers to the set of systems, installations, networks, and services whose serious disruption would affect essential functions of society, the economy, public health, public order, or national security. At the level of the European Union (EU), Directive (EU) 2022/2557 on the resilience of critical entities (CER) specifies that critical entities are those providers of essential services - from energy and transport to drinking water, healthcare, or digital infrastructures - whose inability to operate would have significant consequences for the state and the population [1].

In the United States of America, critical infrastructures are defined as “assets, systems, and networks that provide functions necessary for (...) our way of life,” structured into 16 sectors (energy, transport, communications, water, health, financial sector, chemical, food,

etc.) [21]. Similar approaches are adopted by private actors in the cybersecurity domain: IBM, for example, emphasizes that critical infrastructures include both physical systems (power grids, bridges, transport networks) and digital and industrial systems (IT/OT networks, SCADA systems, data centers), interconnected within a complex socio-technical ecosystem [22].

At the conceptual level, there is a notable shift from an approach centered on protection (Critical Infrastructure Protection) to one focused on resilience (Critical Infrastructure Resilience). The OECD report *Good Governance for Critical Infrastructure Resilience* (2019) proposes a governance model in which protection is no longer merely an exercise in fortification and security, but a broader process aimed at identifying essential functions, managing interdependencies, planning business continuity, and enabling rapid recovery to an acceptable level of functioning [2].

Recent studies on national-level cyber resilience extend this perspective, arguing that cyberspace has become a critical infrastructure of exceptional importance, since nearly all vital sectors depend on digital networks and systems, transforming cyber risks into systemic societal risks [23].

Furthermore, academic literature approaches the holistic evaluation of critical infrastructure resilience, conceptualizing resilience as a process composed of capacities for preparedness, shock absorption, adaptation, and restoration [3–4].

Thus, we may conclude that critical infrastructure is not merely a set of physical assets, but a socio-technical system with multiple layers (technological, organizational, legislative, societal), whose protection requires the integration of intelligence into all phases of the risk management cycle.

2.2. The concept of Intelligence in security studies

Within the literature specific to Intelligence studies, there is no consensus regarding a single, universally accepted definition of the term intelligence. Most definitions reduce intelligence to information - knowledge about the surrounding world, clarification regarding an issue of novelty - while emphasizing, however, that for practitioners and decision-makers, “mere information is not intelligence,” as it must acquire a particular quality or value in order to become intelligence [15].

A quantitative–qualitative analysis of a set of academic and institutional definitions has revealed that the elements most frequently associated with intelligence are: “information,” “actionability,” and “knowledge.” In this context, intelligence is understood as “actionable knowledge about other states/actors, disseminated to decision-makers in the form of information,” thus underscoring its teleological dimension (action-oriented) and its relationship with the decision-making process [24].

More recently, a philosophical analysis of national security intelligence activity has been proposed, arguing that intelligence is, above all, an epistemic concept related to the notion of “knowledge,” endowed with a teleological character (defined by its purpose - the achievement of a collective good, namely security), and institutionally relative (military intelligence, police intelligence, financial intelligence, etc.) [25].

Given the absence of consensus on a single definition of the concept of intelligence, especially from an organizational and operational perspective, it is argued that the clear delineation, it is argued that the clear delineation - within the state’s institutional architecture - of the role and missions of Intelligence/Information Agencies, as well as the establishment of effective oversight mechanisms for intelligence communities, could substantially contribute to strengthening operational efficiency and the democratic legitimacy of activities in this field [26].

From the perspective of democratic governance, intelligence institutions are defined as specialized state agencies tasked with producing intelligence - in the sense of knowledge - relevant to the security of the state (national security information) and of the population, through the collection, analysis, and dissemination of information regarding security threats and risks [16]. This institutional approach emphasizes the public character of national security intelligence (serving the public interest) and the necessity of a rigorous framework of democratic oversight.

In summary, it may be concluded that contemporary literature in the field converges, despite terminological differences, on three main dimensions of intelligence: product (knowledge) - knowledge about the security environment, the actors involved, risks, and opportunities, with direct relevance for decision-making; process/activity - the set of activities of planning, collection, processing, analysis, production, and dissemination of information; organization/community - state institutions (or private entities) that carry out intelligence activities [18, pp. 22–25].

Building on these three dimensions and considering the specific nature of critical infrastructure protection, this study proceeds from the premise that, in this particular case, *intelligence represents the ensemble of institutional activities - predominantly secret and legally regulated - through which relevant and actionable information is collected, analyzed, and disseminated for the protection of critical infrastructures, as part of the broader endeavor of ensuring national security, as well as the products resulting from these activities.* This premise integrates both the epistemic character (knowledge) and the organizational and teleological dimensions (the orientation toward protecting a collective good: security, and in this specific case, the security of critical infrastructures).

2.3. Relevant types of Intelligence for the protection of critical infrastructures - the perspective of levels of analysis

The protection of critical infrastructures requires the coherent integration of the three levels of analysis specific to intelligence: operational, tactical, and strategic [18, p. 30; 27, pp. 21–28]. Each level contributes distinct types of specialized products, useful both for understanding threats and for adopting strategic decisions regarding the defense and resilience of infrastructures.

a.) Operational intelligence (operational level of analysis). Operational analysis is oriented toward identifying campaigns, actors, and threat vectors with direct relevance for critical infrastructures. The emphasis is placed on characterizing the behavior of the actors involved - from cybercriminal groups specializing in attacks on the energy or healthcare sectors to state actors conducting complex operations. Operational intelligence supports inter-institutional coordination, mission planning for response, and data sharing within communities responsible for threat management. Recent literature highlights that the development of this analytical level requires both detailed and continuously updated knowledge of actors, techniques, and attack vectors specific to a domain - particularly the energy sector [28] - as well as the use of advanced platforms capable of collecting and processing real-time data from the operational environment to deliver actionable intelligence necessary for rapid response [29].

b.) Tactical intelligence (tactical level of analysis). Tactical analysis focuses on identifying indicators of compromise, exploited vulnerabilities, the techniques and procedures of the actors involved, or vulnerable physical locations. The products delivered are particularly important for technical teams and intervention structures that directly manage incidents affecting critical infrastructures. Studies in the field show that this level of analysis supports early detection and immediate reaction to attacks by leveraging technical indicators and

patterns based on the tactics, techniques, and procedures of the actors involved, in order to inform immediate defensive actions [27, pp. 21–28; 30].

c.) Strategic intelligence (strategic level of analysis). At the strategic level, analysis seeks to highlight action trends that typically have medium- and long-term impacts on critical infrastructures, shaped by geopolitical, economic, and technological developments. Thus, strategic intelligence contributes significantly to the formulation of resilience policies on issues of interest. Risk anticipation at this level of intelligence is essential for supporting governance processes and coordinating long-term institutional responses. Moreover, the integration of advanced foresight tools and collaborative analytical methods enables a systemic perspective on disruptive threats and their implications for critical infrastructures [19; 31].

In conclusion, the protection of critical infrastructures requires the coherent articulation of all three levels of intelligence analysis. Tactical analysis must be supported by a solid operational understanding of the actors involved, while strategic decisions must be grounded in relevant information derived from the tactical and operational environments. Only through the integration of these levels can a resilient protection system be achieved -one capable not only of responding effectively to threats but also of anticipating developments with long-term impact.

3. THREATS AND VULNERABILITIES TO CRITICAL INFRASTRUCTURES IN THE CONTEXT OF CONTEMPORARY SECURITY

3.1. Introductory considerations

Critical infrastructures currently face a security environment marked by strategic uncertainty, technological interdependence, and the multiplication of threat vectors - factors that drive a paradigm shift from reactive protection to anticipatory resilience. Geopolitical developments, the acceleration of digitalization, the convergence of IT and OT systems, and the emergence of new technologies increase the exposure of critical infrastructures to diverse risks - physical, cyber, hybrid, or systemic [1–2; 32].

Threats to critical infrastructures in the current security climate are complex, multifactorial, and interdependent, resulting from the convergence of social, economic, and geopolitical factors, which continuously reshape how these threats must be managed within national and international security architectures [32].

In this context, the protection of critical infrastructures becomes a continuous, adaptable, and integrated process, with a direct impact on national security, socio-economic stability, and the functioning of the state.

3.2. Typologies of threats to critical infrastructures

Threats targeting critical infrastructures can be grouped into several main categories, depending on their nature and their impact on the functionality of the systems, as follows:

a.) Deliberate physical threats *(sabotage, terrorism, strategic violence)* - These are generated predominantly by actors motivated ideologically, politically, militarily, or economically, whose actions may aim to destroy, compromise, or interrupt the functioning of essential components of critical infrastructures, such as those in the fields of energy, transportation, communications, or health.

In the case of *sabotage*, actions seek to cause material or functional damage by destroying infrastructure, degrading operational capabilities, or compromising technical integrity, generally through covert means, with the aim of generating significant economic or logistical effects without explicit attribution [10–11].

In the case of *terrorism*, the motivation is associated with inducing public panic, eroding social trust, constraining political decision-makers, or achieving symbolic and visibility-related

gains. Critical infrastructures are preferred targets due to their major psychological impact and the domino effects they produce on communities and the economy [33].

With regard to *strategic violence*, this represents the intentional and planned use of force or physical coercion against critical infrastructures as an instrument of influence, intimidation, or pressure in specific geopolitical and military contexts, with the aim of altering the balance of power, disrupting the functioning of the state, or obtaining a strategic advantage in a hybrid, irregular, or conventional conflict [34–36].

b.) Accidental threats *(natural disasters, technological accidents)* - These are generated by natural factors or technological errors and can disrupt systemic functions without premeditation, affecting the performance and availability of public services [2; 32].

In the case of *natural disasters*, the disruption of critical infrastructures is caused by the manifestation of extreme natural phenomena - such as earthquakes, floods, severe drought, wildfires, or geomagnetic storms - which generate structural damage, operational interruptions, and the degradation of functional capacities, without any direct human intentionality. These events affect the availability, continuity, and performance of essential services at the societal level. The idea that risks to critical infrastructures are amplified by extreme natural phenomena is supported in reports on the resilience of essential infrastructures [2; 32].

In the case of *technological accidents*, regarded as a major vulnerability for critical infrastructures, disruptions are caused by internal malfunctions of technical systems, human errors, hardware or software failures, design flaws, non-compliant industrial processes, or lack of proper maintenance. These issues can lead to operational shutdowns, performance degradation, and the compromise of essential service continuity, without intentionality, but with potentially major impact on socio-economic stability [2].

c.) The cyber dimension currently represents the dominant component of the issue under analysis, as ransomware attacks, the compromise of industrial systems (ICS/SCADA), the exploitation of zero-day vulnerabilities, and attacks on digital supply chains constitute threats with systemic impact, capable of generating extensive and cascading effects [7; 8; 37; 38].

In *the case* of *ransomware attacks*, the disruption of critical infrastructures results from the unauthorized infiltration and encryption of essential data or operational systems, which leads to the blocking of functionalities, the compromise of service availability, and the generation of potentially major financial, operational, and psychological impacts on the affected entities. Ransomware is recognized as one of the most aggressive forms of contemporary cyber threat [7].

The compromise of industrial control and automation systems (ICS/SCADA) introduces critical risks through the possibility of manipulating technical processes, altering operational parameters, and causing direct physical effects on operated infrastructures, with the potential for rapid expansion beyond the digital sphere and for impacting physical and operational safety [8].

The exploitation of zero-day vulnerabilities generates a high level of systemic risk in the context of critical infrastructures, as it relies on security breaches unknown to the manufacturer or operator, which allows attackers to obtain privileged, persistent, and undetected access, nullifying the effectiveness of classical cyber-defense mechanisms [37].

Attacks on digital supply chains consist of the intentional compromise of a supplier, integrator, or technical service provider in order to facilitate the insertion of malicious code or unauthorized access into the target infrastructure, exploiting commercial and technical interdependencies and propagating risk in an undetectable and long-term manner [38].

d.) At the strategic level, ***hybrid threats*** combine cyber, informational, and economic tactics to influence the security of critical infrastructures, frequently being associated with

coordination between kinetic and cyber actions or with Advanced Persistent Threat (APT) campaigns of a political-strategic nature.

Coordination between *kinetic and cyber actions* involves the simultaneous and synchronized integration of physical and digital effects on critical infrastructures, through the use of cyberattacks to degrade technical, communication, or command-and-control capabilities, in parallel with physical operations designed to maximize tactical-strategic impact and the degree of systemic disruption, thereby increasing the effectiveness of a military or destabilization campaign [39].

Politico-strategic APT campaigns are based on persistent, clandestine, long-term operations carried out by advanced actors supported or tolerated by states, with the aim of infiltrating, maintaining access to, and exploiting the informational or operational components of critical infrastructures, in order to obtain geopolitical, economic, or military advantages without military escalation [40].

e.) Emerging technological threats to critical infrastructures are becoming increasingly complex, as accelerated digitalization, hyperconnectivity, and the integration of intelligent technologies generate new risk vectors that are difficult to anticipate and manage through traditional security paradigms [31]. Prospective analyses highlight that *IoT ecosystems, 5G/6G networks, autonomous systems, AI, and the industrial cyber domain* are converging into a vulnerable technological architecture, prone to interdependent attacks with potential systemic and cross-border impact [14].

At the same time, the rapid development of *quantum computers* may compromise current cryptographic foundations, generating major risks for the security of critical infrastructures and underscoring the need for an accelerated transition toward post-quantum solutions [41]. In parallel, the widespread use of *digital twins* in the operationalization and optimization of industrial processes introduces new attack surfaces, as the compromise of digital components may simultaneously lead to software disruptions and physical effects on real infrastructures, through the manipulation of data, simulations, and automated commands [42].

3.3. Specific vulnerabilities of critical infrastructures

In the context of accelerated digital transformation and the increasing interconnectivity of essential systems, critical infrastructures face a complex spectrum of vulnerabilities, as follows:

a.) Interdependencies and domino effect / cascading failures. Technical, logistical, and organizational interdependencies among critical infrastructure sectors (energy, transport, telecommunications, finance, etc.) amplify the risk that a local disruption - whether caused by a cyberattack, technological malfunction, or natural hazard - may propagate throughout the system in the form of cascading failures, generating systemic “perfect storms” that rapidly exceed the response capacity of operators and authorities, as highlighted in recent literature on the resilience of interdependent infrastructures [5–6].

b.) IT-OT convergence and ICS/SCADA exposure. The increasingly close convergence between IT and OT networks exposes industrial control systems (ICS/SCADA), traditionally isolated, to attack vectors specific to the IT environment - sophisticated malware, ransomware, compromised remote access - expanding the attack surface and complicating security governance. As a result, the compromise of an IT segment can directly lead to the degradation or shutdown of essential physical processes [43–44].

c.) Human capacity shortages and advanced skills gaps. The structural shortage of cybersecurity specialists - particularly in advanced competence areas such as malware analysis, threat hunting, ICS/SCADA security, and cloud security engineering - limits the ability of critical infrastructures to implement proactive measures, continuously monitor complex

environments, and respond rapidly to incidents. This issue is also reflected in recent studies showing that skill gaps represent a major risk factor for the preparedness and resilience of critical sectors [45].

d.) Dependence on suppliers and digital supply chains. The dependence of critical infrastructures on technology vendors, cloud service providers, software, and hardware components distributed across a global network of digital supply chains introduces vulnerabilities that are difficult to control - from compromised software updates and backdoors in equipment to poor security practices among third parties. As a result, supply chain breaches can be exploited to indirectly penetrate the most sensitive entities [9; 46].

e.) Legislative fragmentation and insufficient standardization. The fragmentation of the regulatory framework - across European, national, and sectoral levels, as well as across different jurisdictions (EU–USA, etc.) - combined with technical and certification standards that are still unevenly implemented, generates compliance gaps, high alignment costs, and difficulties in achieving a uniform level of protection. Consequently, some infrastructures remain significantly more exposed compared to other sectors or countries [47–48].

f.) Difficulties in sharing classified data between institutions. The exchange of classified information and indicators of compromise between authorities, private operators of critical infrastructures, and other relevant entities is often hindered by legal constraints, organizational barriers, lack of trust, and the absence of standardized information-sharing mechanisms. This results in delayed detection of attack campaigns and reduces the collective ability to build an accurate picture of the security situation [49].

4. THE FUNCTIONS AND ROLE OF INTELLIGENCE IN PROTECTING CRITICAL INFRASTRUCTURES

4.1. Introductory considerations

In recent years, intelligence has become a fundamental component of critical infrastructure protection due to its ability to provide validated, integrated, and operationalizable information on threatening actors, their intentions, capabilities, tactics, and possible attack actions, in an anticipatory and prevention-oriented manner [19]. Thus, intelligence is shaping itself as a strategic capability in the governance of risks and threats to critical infrastructures, through the use of diverse tools designed to anticipate medium- and long-term trends and to support public decision-making in a dynamic and uncertainty-driven technological context.

In this regard, the specialized literature highlights the need for a conceptual and practical transition from a reactive model - focused mainly on physical and cyber security - to a proactive and adaptive model grounded in resilience and anticipatory analysis [2; 50]. At the same time, intelligence is no longer viewed solely as an informational product but as a dynamic, inter-institutional, and multisectoral process in which the collection, analysis, and dissemination of information constitute integrated stages within a decision-making cycle that is critically relevant to the functioning of critical infrastructures [51].

Therefore, the role of intelligence in critical infrastructure protection extends beyond simple observation and reporting/informing activities. It represents a mechanism of anticipation, prevention, and adaptation - capable of reducing decision-making uncertainty, optimizing operational response, and enhancing societal, institutional, and technological resilience.

4.2 The Functions and role of Intelligence in the field of critical infrastructure protection

4.2.1 For the protection of critical infrastructures, ***the functions of intelligence*** are articulated primarily along four main directions:

a.) The Early Warning Function - enables the timely identification of trends and intentions of involved actors and the prompt dissemination of information to relevant beneficiaries. The effectiveness of intelligence's early warning function in protecting critical infrastructures is supported by recent research findings, which highlight both the necessity of early detection and prediction of ransomware attacks targeting industrial and control systems [7], and the essential role of integrating threat information and operational data sharing in the energy sector through dedicated Early Warning systems [52].

b.) The Risk Assessment Support Function - essential for underpinning impact analysis models, it relies on the systematic provision and integration of data regarding actors, capabilities, and operational attack patterns. This is emphasized in recent studies demonstrating the importance of correlating information on cyber threats with standardized risk assessment methodologies in critical infrastructures [3; 53].

c.) The Strategic Decision-Support *Function* - grounded in the capability of intelligence to deliver relevant analytical products for the formulation of security policies, a point sustained by the specialized literature, which underlines the role of cyber threat information in strengthening sectoral resilience and aligning national strategies with international security directives [50; 53].

d.) The Operational Support Function - consists in providing actionable intelligence to operational structures (incident response teams, infrastructure operators) to enable rapid incident response and the dynamic adaptation of protection measures. Recent studies highlight that the Integration of advanced technologies such as AI and Digital Twin platforms allows intelligence to be transformed into a directly operational tool for intervention structures, through the rapid detection of threats, simulation of possible scenarios, and reduction of response time in the event of incidents affecting critical infrastructures [12–13].

In the context of the aspects presented above, we consider that without the optimal valorization of intelligence, the protection of critical infrastructures risks becoming reactive - based on knowledge of incidents that have already occurred - rather than proactive, oriented toward prevention and resilience.

4.2.2. It is also ***relevant that Intelligence plays a central role in both preventing and countering threats to critical infrastructures***, through specific actions at each level of analysis, as follows:

a.) From the perspective of ***operational analysis*****,** the role of intelligence in the case of the analyzed threats is reflected in the monitoring of the groups involved, their logistical flows, routes used, funding sources, and intentions, based on multi-source analysis, interinstitutional cooperation, and structured information exchange. The aim is to identify early indicators of hostile actions and to enable the timely activation of prevention and counteraction measures through mechanisms adapted to the specific features of the targeted infrastructure sectors [28-29].

b.) From the perspective of ***tactical analysis***, intelligence provides precise and near–real-time information regarding potential targets, modes of operation, behavioral profiles, techniques used in sabotage actions, and other early warning indicators with immediate relevance for intervention. This facilitates the direction of operational forces, the optimization of reaction procedures, and the reduction of the time between detection and threat neutralization, including through the integration of advanced surveillance technologies and AI-assisted analysis [27].

c.) From the perspective of ***strategic analysis***, intelligence enables the identification and examination of geopolitical trends, interstate competition, and transnational risks, thus offering a solid foundation for anticipating vulnerable sectors and the actors involved. In this regard,

strategic analysis integrates political, economic, military, and ideological developments with destabilizing potential, assessing the evolution of interests and capabilities of hostile actors, as well as the possible effects on the security of critical infrastructures. This supports the formulation of prevention-oriented policies and priorities for the medium and long term [19; 31].

Through the coherent integration of the three levels of analysis - operational, tactical, and strategic - Intelligence supports critical infrastructure protection measures and strengthens system resilience by ensuring operational continuity.

5. ENHANCING THE IMPACT OF INTELLIGENCE IN CRITICAL INFRASTRUCTURE PROTECTION

5.1. Premises and limitations of the current use of Intelligence

Although the previous chapters highlighted the central role of intelligence in the protection of critical infrastructures, its practical impact often remains below its potential. In many states and sectors, intelligence is still perceived more as a "support component" than as a constitutive pillar of risk governance and infrastructural resilience. This situation is determined by a combination of factors: the fragmentation of responsibilities among institutions and sectors, which generates grey areas of competence and difficulties in interinstitutional coordination [2]; the gap between the intelligence production cycle and the "temporality" of operational processes within critical infrastructures, where the decision window is often extremely narrow [20]; the structural tension between the need to protect classified information and the need to rapidly share relevant information with critical infrastructure operators, including private actors [54]; the deficit of analytical understanding between the technical language (cybersecurity, ICS/SCADA, etc.) and the strategic/decision-making language (public policy, investments, budgetary priorities) [20].

Enhancing the impact of intelligence therefore requires not only the technical improvement of collection and analysis, but also a recalibration of how intelligence is integrated into: the governance architectures of critical infrastructures; risk management cycles; and strategic, operational, and tactical decision-making processes [55].

This chapter aims to explore the major directions of action through which the added value of intelligence in critical infrastructure protection can be amplified, with emphasis on governance, processes, technology, human capital, and cooperation.

5.2. Strengthening the governance framework and the integration of Intelligence into public policies

An important pillar in increasing the impact of Intelligence is ***strengthening the governance framework*** within which it is produced and used [56]. In line with European directives on the resilience of critical entities and cybersecurity, the protection of critical infrastructures can no longer be conceived as a succession of isolated sectoral measures, but as an integrated public policy in which intelligence plays a transversal role. To achieve this objective, the following are required:

a.) Clarifying institutional mandates and roles, through the explicit definition of the responsibilities of intelligence institutions in relation to sectoral regulatory authorities, national critical infrastructure coordination structures, and private operators. Such clarification reduces overlaps, gaps, and ambiguities in threat management. Although, in general, international cooperation (both at the political level and between agencies) has increased the capacity of national intelligence institutions, it has not been sufficient to fully ensure the clarification of mandates, the transparent definition of legal beneficiaries, and the strengthening of democratic oversight [57].

b.) The integration of Intelligence into national security and resilience strategies, with its role needing to be defined not merely as a generic tool but as a specific mechanism in the development of strategies for energy, transport, health, communications, space, etc., with clear responsibilities in risk assessment, investment prioritization, and implementation monitoring. Recent studies generally address the role of intelligence as a pillar of national security in the face of hybrid warfare, cyberattacks, and other risks, integrated into the institutional architecture and strategic documents [58].

c.) The creation of formal mechanisms for dialogue between the Intelligence Community and political/sectoral decision-makers with responsibilities in the field, through interministerial committees, permanent working groups, and public–private dialogue forums, which can function as entities that harmonize intelligence analyses with public policy decisions. This prevents intelligence products from remaining isolated within classified channels without operational impact, an issue also highlighted in the specialized literature [59].

d.) Aligning the national framework with European and Euro-Atlantic standards on critical infrastructure protection [60] and intelligence utilization, through normative and conceptual coherence that facilitates cross-border cooperation, the exchange of best practices, and interoperability in crisis situations.

In the absence of such strengthened governance, even highly capable intelligence risks being underused, fragmented, or out of sync with the real needs of critical infrastructures.

5.3. Optimizing the Intelligence cycle for the needs of critical infrastructures

Another major vector for improving ***the impact of intelligence concerns the concrete way in which the Intelligence cycle*** (planning - collection - processing - analysis - dissemination - feedback) is carried out, both in general terms [17; 18, pp. 37-38] and with regard to the specific characteristics of critical infrastructures.

To increase its impact, we believe several adjustment directions are necessary, as follows:

a.) Risk- and essential-function-oriented planning, which should be based not only on general security agendas, but also on: the essential functions identified in critical infrastructures (continuity of energy supply, provision of medical services, functioning of communication networks, etc.); risk scenarios with systemic impact (cascading failures, major disruptions in supply chains, coordinated attacks on multiple sectors). This approach aligns with studies in the field of intelligence that highlight the importance of planning and direction as a fundamental stage for the efficiency of the entire process, showing that the setting of priorities, the definition of requirements, and the allocation of resources must be strictly oriented toward risk assessment and the essential functions of the state, so that intelligence products genuinely meet the decision-making needs of legal beneficiaries [16]. This requires a direct correlation between intelligence planning and the risk assessment exercises carried out by authorities and operators.

b.) Multi-source collection and integration of technical sources (sensors, telemetry, etc) with human and open sources (information on hostile groups, underground forums, geopolitical or economic developments), which would allow for the integration of large volumes of heterogeneous information and their transformation into relevant situational pictures regarding security issues across various domains [7], and in particular for critical infrastructures.

c.) Actionability- and scenario-oriented analysis, which should go beyond the descriptive level and produce: predictive assessments (trends regarding attacks, shifts in the tactics of the actors involved, possible technological developments with an impact on vulnerabilities); impact scenarios for critical infrastructures (for example, the consequences of

a coordinated attack on an energy operator and a cloud service provider on which other sectors depend), as is likewise concluded in other academic studies [61].

d.) Rapid, segmented, and secure dissemination, so that intelligence products reach sufficiently quickly the specific beneficiaries with responsibilities in managing critical infrastructures (response teams, executive leadership, sectoral authorities), in a format adapted to their access level and degree of expertise. This approach is also reflected in recent studies that highlight the necessity of rapid and secure dissemination mechanisms, the use of differentiated channels (beneficiary segmentation), and issues related to confidentiality, trust, and access classes in intelligence sharing [20].

e.) Systematic feedback and lessons learned, through: periodic evaluation of the extent to which intelligence products were useful in preventing or managing incidents; adjusting collection requirements and analytical methodologies based on the lessons learned; creating an institutional culture of continuous learning between the Intelligence Community and critical infrastructure operators [16].

5.4. Leveraging emerging technologies in the production and use of Intelligence

Another determining factor in improving the impact of intelligence is ***the integration of emerging technologies*** into all phases of the intelligence cycle, through the following action directions:

a.) Use of Artificial Intelligence and machine learning, for the early detection of anomalies in operational and cyber data flows; identification of attack patterns and subtle correlations between seemingly unrelated events; prioritization of alerts and reduction of informational "noise" [7; 29; 52]. In this way, intelligence becomes more scalable and more capable of managing the complexity of the security environment of critical infrastructures.

b.) Integration of Big Data analytics and fusion platforms, which facilitates: the integration of large volumes of data from multiple sources (technical logs, surveillance data, economic and geopolitical information, OSINT); the execution of complex network analyses on the connections among actors, attack vectors, infrastructures, and supply chains; the modeling and simulation of scenarios involving the propagation of effects (cascading failures) [5; 6; 19].

c.) Use of Digital Twins and advanced simulations, which, in the case of critical infrastructures, allows for: testing in a virtual environment the impact of attack scenarios or technical malfunctions; experimenting with response measures and business continuity plans without disrupting real systems [12]. Thus, operational intelligence that can be directly used in exercise planning and in the preparation of intervention teams can be generated.

d.) Implementation of standards and protocols for automated information sharing, which would: increase the speed at which tactical and operational intelligence is distributed to specific beneficiaries; reduce interpretation errors; facilitate the integration of external feeds into the situational pictures of critical infrastructures [49].

Leveraging these technologies does not replace the analyst's judgment and human decision-making, but it significantly amplifies detection, analysis, and response capabilities, thereby enhancing the overall impact of intelligence.

5.5. Developing human capital and an Intelligence culture in critical infrastructures

Any technological and institutional progress is limited by the level of development of human capital and organizational culture. In the context of the need to protect critical infrastructures, increasing the impact of intelligence involves:

a.) Specialized training at the intersection of Intelligence and technical domains, through training and professional development programs designed to create: intelligence

analysts with a solid understanding of the specificities of critical infrastructures (energy, health, transport, communications, etc.); technical specialists familiar with the logic and processes of intelligence, capable of formulating information requirements and using analytical products in decision-making. This direction aligns with current recommendations, according to which, in the digital technology era, the effectiveness of intelligence activities depends decisively on training hybrid-profile professionals capable of integrating advanced technical competencies with analytical and strategic interpretation skills [62].

b.) Mixed teams - bringing together intelligence analysts, technical experts, legal specialists, and public policy professionals - and ***"hybrid profiles"***, consisting of practitioners capable of translating technical problems into strategic risk terms and vice versa [19; 62].

c.) An organizational culture oriented toward prevention and learning, characterized by: proactive reporting of incidents; voluntary participation in exercises and simulations; openness to sharing relevant information with authorities and sectoral partners; acceptance of intelligence as a legitimate tool in the strategic design of the organization, not merely as a "crisis alarm." This recommended direction is consistent with recent European approaches emphasizing that the resilience of critical infrastructures depends on an organizational culture oriented toward prevention, in which incident reporting, information sharing, participation in exercises, intersectoral collaboration, and continuous learning are essential institutional mechanisms [2].

5.6. Shifting the approach from "information support" to "resilience architecture"

Improving the impact of intelligence in the protection of critical infrastructures requires a shift in logic - from an approach in which intelligence is perceived as a simple provider of information, to a vision in which intelligence is understood as a structural element of the resilience architecture [63].

This transformation involves: strengthening the governance framework and integrating intelligence into public policies and sectoral strategies; adapting the intelligence cycle to the specificities of critical infrastructures, with an emphasis on actionability, scenarios, and feedback; leveraging emerging technologies (AI, big data, digital twins, automated information-sharing standards) to increase the speed and depth of analysis; investing in human capital and intelligence culture through specialized training and the formation of mixed teams; developing cooperation and information-sharing mechanisms at national and international levels (see Chapters 5.2–5.5).

By integrating these directions, intelligence can shift from a predominantly reactive, incident-centered function to an anticipatory and adaptive capability, able to reduce uncertainty, support informed decision-making, and strengthen the resilience of critical infrastructures in the face of an increasingly complex and volatile security environment.

5.7. Integrated model for the use of Intelligence in critical infrastructure resilience

Based on conceptual analyses, typologies of threats and vulnerabilities, as well as the functions of intelligence in the protection of critical infrastructures, an integrated model is proposed that describes how intelligence contributes to the transition from reactive protection to anticipatory resilience. The model is structured into four main components: (1) risk context, (2) intelligence architecture, (3) key intelligence functions, and (4) governance mechanisms and resilience outcomes (Figure 1).

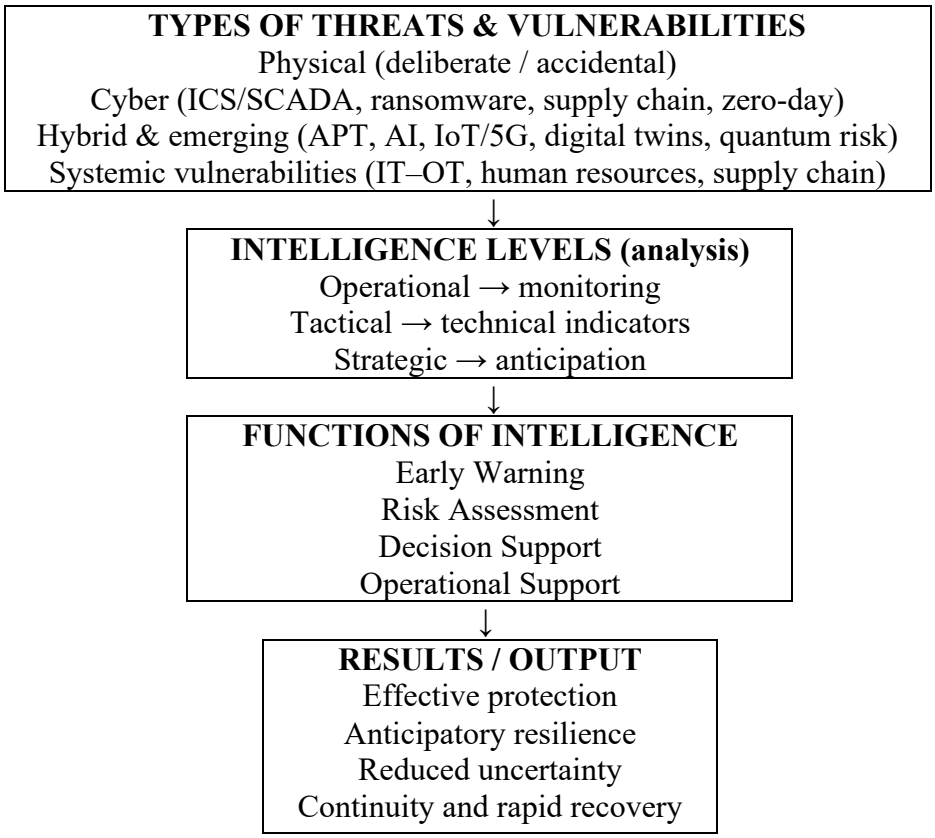

Figure 1. Integrated model on the use of Intelligence in the protection and resilience of critical infrastructures.

Overall, the model conveys a vision in which the risk context is filtered through the intelligence architecture, transformed into concrete functions (early warning, risk assessment, decision-making and operational support), and integrated into governance and resilience mechanisms, the final outcome being the shift from reactive protection to anticipatory resilience of critical infrastructures.

6. DISCUSSIONS

This chapter aims to place the results of the analysis within a broader interpretative framework, by relating them to the formulated hypotheses, the specialized literature, and the theoretical and practical implications for the governance of critical infrastructures and for the intelligence community. The discussion also highlights the structural tensions and dilemmas associated with using intelligence as a pillar of infrastructural resilience.

6.1. Interpretation of the results in relation to the research hypotheses

The analysis conducted in the previous chapters theoretically supports the validity of the four research hypotheses.

First, *hypothesis H1* - according to which the coherent valorization of the three levels of intelligence analysis (operational, tactical, and strategic) facilitates the transition from reactive protection to anticipatory resilience - is supported by demonstrating the differentiated ways in which each level contributes to managing risks to critical infrastructures. Thus, at the operational level, knowledge is structured regarding the actors involved and the campaigns carried out; at the tactical level, concrete and immediately usable indicators are provided for incident response; and at the strategic level, the anticipation of trends and the shaping of relevant policies are ensured. The integrated model proposed in section 5.7 shows that only the

articulation of these levels within a common governance framework allows the shift from an incident-centered logic to one oriented toward prevention, adaptation, and continuity.

Secondly, *hypothesis H2* - according to which the major vulnerabilities of critical infrastructures can be significantly reduced through robust intelligence capabilities oriented toward early warning and integrated risk assessment - is confirmed by correlating the typologies of threats and vulnerabilities (physical, cyber, hybrid, emerging, systemic) with the functions of early warning and risk evaluation. Vulnerabilities such as IT–OT convergence, ICS/SCADA exposure, dependence on digital supply chains, or shortages in human capital can be managed more effectively when intelligence processes provide advance warnings, impact scenarios, and comprehensive views of interdependencies.

Hypothesis H3 - which posits that a governance framework that systematically employs intelligence increases the ability to anticipate and manage emerging threats - is supported by the argument that intelligence cannot remain a technical subsystem but must be explicitly integrated into national strategies, institutional architectures, and sectoral decision-making processes. The discussions on strengthening governance (section 5.2) show that, in the absence of a clear framework of roles, processes, and responsibilities, even high-performing intelligence risks being undervalued or misaligned with the real needs of critical infrastructure protection.

Finally, *hypothesis H4* - according to which interinstitutional cooperation and standardized information-sharing mechanisms constitute essential conditions for resilience - is supported by the analysis of current difficulties related to classified data exchange, normative fragmentation, and challenges in building an environment of mutual trust. The major interpretative conclusion is that intelligence can support infrastructural resilience only if it is embedded within a collaborative governance ecosystem that transcends the logic of isolated institutions.

6.2. Theoretical implications: Intelligence as architecture, not just as product

From a theoretical perspective, the study contributes to reconfiguring the way the role of intelligence is understood in security studies and in the literature on critical infrastructures. Traditionally, intelligence has been conceptualized either as an informational product (actionable knowledge), as a process (the intelligence cycle), or as an organization (specialized agencies) [64, pp. 12–14]. The proposed analysis adds an additional dimension: *Intelligence as a resilience architecture*, meaning a set of relationships, mechanisms, and functions that structure the way society manages systemic risks.

The integrated model presented in section 5.7 marks the shift from a "linear" representation of the intelligence cycle to a systemic vision, in which: the risk context (threats + vulnerabilities) is filtered through the levels of intelligence analysis; the levels are operationalized through functions (early warning, risk assessment, decision support, operational support); and the functions are anchored in multi-actor governance, generating outcomes in terms of protection and resilience.

Thus, intelligence is positioned explicitly at the intersection of resilience theories, security studies, and critical infrastructure governance, suggesting the need for conceptual frameworks that approach intelligence not merely as informational "input," but as a structural element of critical socio-technical systems.

6.3. Practical and Public Policy Implications

In practical terms, the results of the study indicate that the effectiveness of technical and regulatory protection measures is conditioned by the quality and integration of intelligence. Several essential implications can be outlined:

a.) For policy makers, the conclusions suggest that investments in the resilience of critical infrastructures cannot be limited to technological modernization or regulatory adjustments; they must also include strengthening intelligence capabilities, clarifying mandates, and establishing formal mechanisms for intelligence–public policy dialogue.

b.) For critical infrastructure operators, the proposed model highlights the need to: create internal structures or partnerships capable of translating intelligence products into operational decision-making; develop an organizational culture oriented toward prevention, reporting, and learning; and participate actively in information-sharing networks, especially in sectors with strong interdependencies.

c.) For the technical community, the discussion reveals the importance of better articulation between technical and strategic language, as well as the need for "hybrid profiles" able to operate simultaneously with concepts such as risk, vulnerability, interdependence, and political decision-making.

d.) In addition, ***the integration of emerging technologies*** (AI, big data, digital twins) into the intelligence cycle has direct implications for how security operations centers, training exercises, continuity plans, and reporting architectures to authorities are designed.

6.4. Tensions, paradoxes, and grey areas

The results of the study also reveal a set of structural tensions that must be acknowledged and managed in order to avoid an overly normative vision of the role of intelligence:

a.) The tension between secrecy and sharing: the protection of classified information is essential for security, yet insufficient sharing with private operators reduces the practical relevance of intelligence and leads to the late detection of complex campaigns. The balance between "need to know" and "need to share" remains difficult to achieve, even though in the digital age the activity of Intelligence Agencies no longer means "total isolation" but a process of "shared secrecy," which involves mutual trust among the actors engaged in the process [65].

b.) The tension between speed (time pressure) and analytical rigor: critical infrastructures operate in an almost real-time environment, while the intelligence cycle requires verification, corroboration, and evaluation. Adapting intelligence processes to the micro-decisional temporality of critical infrastructures is a major challenge. This finding is confirmed by recent studies arguing that, to meet the high time-pressure demands of intelligence activities without compromising analytical rigor, it is necessary to optimize analytical processes and enhance human capabilities (through psychology, education, statistics), in parallel with the use of digital technologies [66].

c.) The tension between centralization and distribution/dissemination: on the one hand, the governance of systemic risks requires central coordination and a unified vision; on the other hand, resilience requires a diversity of actors, redundancy, and local adaptive capacity. Intelligence must serve both of these apparently opposing logics simultaneously - finding a balance between centralization, which provides control and strategic direction, and distribution/dissemination, which enables agility and information sharing - thus highlighting the advantages and challenges of both approaches [67].

d.) The tension between technology and human capital: although emerging technologies can exponentially enhance detection and analytical capabilities, they cannot substitute the sound judgment of intelligence analysts or the responsibility inherent in decision-making. Despite technological advances in data collection and analysis, human resources retain an essential role in intelligence due to the unique human ability to contextualize, recognize patterns, and connect information - an environment in which investments in technology must be balanced with support for human capital [62]. Investment in human resources remains the

fundamental condition for technological investment to produce real effects in terms of resilience.

These tensions do not diminish the utility of intelligence; rather, they indicate that its role in the protection of critical infrastructures cannot be understood as a simple technical solution, but as part of a complex process of institutional, cultural, and political negotiation.

6.5. Directions for development and further research

Based on the discussions above, several avenues for further exploration can be outlined:

a.) Operationalizing the integrated model: applying the proposed logical framework to one or more sectors (energy, healthcare, transport, space) would allow for the validation and refinement of the model by identifying sector-specific patterns and transferable best practices.

b.) Comparative governance study: a comparative analysis between states or regions could highlight how different institutional intelligence architectures influence the level of infrastructural resilience.

c.) Exploring the ethical dimension and democratic oversight: the intensive integration of intelligence into economic and social life, under the pretext of protecting critical infrastructures, raises sensitive questions regarding democratic oversight, data protection, and the balance between security and liberties.

d.) Research on organizational culture: qualitative studies at the level of critical infrastructure operators could clarify how internal culture facilitates or hinders the effective use of intelligence in day-to-day practice.

Overall, the discussions show that for intelligence to truly become a pillar of infrastructural resilience, it must be conceived and analyzed not merely in terms of information flows, but as a mechanism that articulates technology, institutions, and decision-making within an environment characterized by systemic risks and high uncertainty.

7. LIMITS OF THE RESEARCH

The chapter on the limits of the research highlights the conditions under which the conclusions of the study on the role of intelligence in the protection of critical infrastructures can be understood and used.

In *thematic terms*, the research operates at a macro, cross-sectoral level: critical infrastructures are analyzed as interconnected socio-technical systems, with an emphasis on the cyber dimension and on the convergence between Information Technology (IT) and Operational Technology (OT), without addressing the technical-operational details specific to each sector (energy, healthcare, transport, etc.). The study focuses on governance, institutional architecture, and intelligence processes (early warning, risk assessment, decision-making and operational support), not on the technical design of security solutions based on intelligence.

Methodologically, the study is predominantly qualitative, theoretical-analytical, and exploratory. It relies on documentary, conceptual, and content analysis of regulations, strategies, and specialized literature, without the collection of primary data (access to internal data of operators or intelligence services) and without systematic quantitative or empirical testing of the hypotheses.

A fundamental limitation stems from the *secret nature of intelligence activities*: access is restricted to public or unclassified information. This can generate a partial, sometimes normatively idealized image of how intelligence is integrated into the protection of critical infrastructures and does not allow the inclusion of sensitive operational examples or detailed descriptions of internal procedures.

There are also *geographical and normative limitations*: the analysis focuses on the European and Euro-Atlantic framework, on the directives and strategies in force at the time of

writing. The rapid dynamics of the technological and regulatory environment may render the extrapolation of the conclusions to other regions with different institutional architectures only partially valid.

Regarding the *sources*, the literature and documents from the Western and institutional sphere predominate. Limited access to "grey" literature and the heterogeneity of the sources used may introduce a Euro-Atlantic bias and underrepresent alternative approaches.

The assumptions regarding the *valorization of intelligence*, the role of early-warning capabilities, the importance of governance and cooperation are plausible, but their generalization is conditioned by context: resources, political will, organizational culture, and technological maturity.

8. CONCLUSIONS

The study highlights the important role of intelligence in the conceptual and operational transition from a traditional, reactive model of critical infrastructure protection to one based on anticipatory, integrated, and adaptive resilience. In the context of growing technological interdependencies, accelerated digitalization, and an increasingly complex security environment, critical infrastructures can no longer be protected solely through technical, physical, or regulatory measures. They require a systemic, interinstitutional, and proactive approach in which intelligence becomes an instrument of strategic governance.

The conceptual analysis demonstrated that critical infrastructures are socio-technical systems with multiple layers of vulnerability, simultaneously exposed to physical, cyber, hybrid, and emerging risks, and that their disruption has the potential to generate cascading effects at the societal level. Against this backdrop, intelligence can contribute to reducing decision-making uncertainty, anticipating threats, and supporting the decision-making process by providing actionable, relevant, and timely knowledge.

The research hypotheses were confirmed at the theoretical and analytical level: optimal valorization of intelligence strengthens the shift toward anticipatory resilience (H1); robust intelligence capabilities focused on early warning reduce exposure to major vulnerabilities (H2); intelligence-based governance enhances the ability of states and operators to anticipate and manage emerging risks (H3); and interinstitutional collaboration and standardized information-sharing mechanisms constitute critical elements for an effective and adaptive protection system (H4).

The overall conclusion is that intelligence must be understood as a structural pillar of infrastructural resilience, with a transversal role in governance, decision-making, planning, and response. Without such integration, protection remains fragmented, reactive, and vulnerable to multidimensional threats.

At the same time, the study emphasized a set of strategic directions for strengthening the impact of intelligence: reinforcing the governance framework and the role of intelligence in public policy; optimizing the intelligence cycle in relation to the specificities of critical infrastructures; capitalizing on emerging technologies (AI, big data, digital twins); developing human capital through specialized training and multidisciplinary teams; and standardizing and accelerating information-sharing across institutions, sectors, and states.

Therefore, the future architecture of critical infrastructure protection must evolve toward an integrated, collaborative, and anticipatory vision in which intelligence is conceived as a strategic resource, an operational mechanism, and a tool for continuous adaptation in a volatile, uncertain, complex, and ambiguous security environment.

In conclusion, the effectiveness of critical infrastructure protection depends on the ability of states, institutions, and private operators to transform intelligence into an architecture of

resilience rather than merely a reaction mechanism, thereby strengthening national security and societal functionality in an era of systemic risks.

REFERENCES

[1]. European Union. (2024, February 19). *Making critical entities more resilient: Summary of Directive (EU) 2022/2557 on the resilience of critical entities*. EUR-Lex. https://eur-lex.europa.eu/EN/legal-content/summary/making-critical-entities-more-resilient.html#
[2]. Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience* (OECD Reviews of Risk Management Policies). OECD Publishing. https://doi.org/10.1787/02f0e5a0-en
[3]. Irankunda, G., Zhang, W., Fernand, M., & Zhang, J. (2024). Assessing the resilience of critical infrastructure facilities toward a holistic and theoretical approach: A multi-scenario evidence and case study. *Sustainability, 16*(20), 8735. https://doi.org/10.3390/su16208735
[4]. Rathnayaka, B., Robert, D., Adikariwattage, V., Siriwardana, C., Meegahapola, L., Setunge, S., & Amaratunga, D. (2024). *A unified framework for evaluating the resilience of critical infrastructure: Delphi survey approach*. International Journal of Disaster Risk Reduction, 110, 104598. https://doi.org/10.1016/j.ijdrr.2024.104598
[5]. Sarker, P., Lohar, B., Walker, S., Patch, S., & Wade, J. T. (2024). Recovery Resiliency Characteristics of Interdependent Critical Infrastructures in Disaster-Prone Areas. *Infrastructures*, *9*(11), 208.
[6]. Hoff, R., Sparks, R., Chester, M., Mustafa, A., Johnson, N., Birchfield, A., ... & Searles, I. (2025). Cascading Failure Propagation and Perfect Storms in Interdependent Infrastructures. *ASCE OPEN: Multidisciplinary Journal of Civil Engineering*, *3*(1), 04025001.
[7]. Gazzan, M., & Sheldon, F. T. (2023). *Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems*. Future Internet, 15(4), 144. https://doi.org/10.3390/fi15040144
[8]. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & security*, *125*, 103028.
[9]. Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers & Security*, *108*, 102324.
[10]. Ringbom, H., & Lott, A. (2024). *Sabotage of Critical Offshore Infrastructure: a Case Study of the Balticconnector Incident.* In A. Lott (Ed.), *Maritime Security Law in Hybrid Warfare* (pp. 155). Brill. https://urn.fi/URN:NBN:fi-fe2025022614432
[11]. Skomra, W., & Wojtasik, K. (2025). *Critical infrastructure as a target for hybrid operations. Case studies of attacks against the facilities and systems of CI. Terrorism – Studies, Analyses, Prevention (Edycja specjalna)*, (7), 13–34. https://doi.org/10.4467/27204383TER.25.013.21516
[12]. Kampourakis, K. E., Gkioulos, V., Kavallieratos, G., & Lin, J. C. (2025). Digital Twin-Enabled Incident Detection and Response: A Systematic Review of Critical Infrastructures Applications. *International Journal of Information Security*, *24*(5), 1-42.
[13]. Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems*, *12*(5), 165. https://doi.org/10.3390/systems12050165
[14]. European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA Foresight Cybersecurity Threats for 2030*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-2030
[15]. Warner, M. (2002). *Wanted: A definition of "Intelligence"*. Central Intelligence Agency. https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf
[16]. DCAF – Geneva Centre for Security Sector Governance. (2022, July). *Intelligence services: Roles and responsibilities in good security sector governance (SSR Backgrounder BG 12)*. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_IntelligenceServices_EN_Jul2022.pdf
[17]. Weissmann, M., & Nilsson, N. (2024). *Current Intelligence and Assessments: Information Flows and the Tension between Quality and Speed. The International Journal of Intelligence and CounterIntelligence, 37*(4), 1351-1367. https://doi.org/10.1080/08850607.2023.2296886
[18]. Nițu, I. (2012). *Analiza de intelligence*. Editura RAO.

[19]. Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. *Sensors*, *25*(14), 4272. https://doi.org/10.3390/s25144272
[20]. Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., & Foo, E. (2024). *Current approaches and future directions for Cyber Threat Intelligence sharing: A survey*. Journal of Information Security and Applications, 83, 103786.
[21]. Cybersecurity and Infrastructure Security Agency. (n.d.). *Critical infrastructure security and resilience*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
[22]. IBM. (n.d.). *What is critical infrastructure?* IBM Think. Retrieved [data accesării], from https://www.ibm.com/think/topics/critical-infrastructure
[23]. Hubbard, G. (2023). State-level cyber resilience: A conceptual framework. *Applied Cybersecurity & Internet Governance, 2*(1), 1–14. https://doi.org/10.60097/ACIG/162859
[24]. Dokman, T. (2019). *DEFINIRANJE POJMA „OBAVJEŠTAJNO“ - UVID U POSTOJEĆE OBAVJEŠTAJNO ZNANJE* [“Defining the term ‘Intelligence’ – insight into existing Intelligence knowledge”]. *Informatologia*, 52(3-4), 194-205. https://doi.org/10.32914/i.52.3-4.7
[25]. Miller, S. R. M. (2022). *National security Intelligence activity: A philosophical analysis*. *Intelligence and National Security, 37*(6), 791-808. https://doi.org/10.1080/02684527.2022.2076329
[26]. Baron, F. (2024, March 28). *Why define Intelligence?* https://www.ni-u.edu/wp-content/uploads/2024/04/Why-Define-Intelligence.pdf
[27]. Petcu, G. (2011). Tipuri de analiză în activitatea de intelligence. În Ionel, Nițu (coordonator), *Ghidul analistului de intelligence. Compendiu pentru analiști debutanți* (pp. 21-28), București: Editura ANI „Mihai Viteazul”.
[28]. 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.
[29]. Balasubramanian, P., Nazari, S., Kholgh, D. K., Mahmoodi, A., Seby, J., & Kostakos, P. (2024). Tstem: A cognitive platform for collecting cyber threat Intelligence in the wild. *arXiv preprint arXiv:2402.09973*.
[30]. Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. (2022). Key requirements for the detection and sharing of behavioral indicators of compromise. *Electronics, 11*(3), 416. https://doi.org/10.3390/electronics11030416
[31]. Robinson, D. K. R., & Doherty, D. (2025). *Strategic Intelligence tools for emerging technology governance: A policy primer* (OECD Science, Technology and Industry Working Papers, No. 2025/22). OECD Publishing. https://doi.org/10.1787/02c05775-en
[32]. European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA Threat Landscape 2023*. Publications Office of the European Union. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdfEuropean Commission. (2023). *Cybersecurity and resilience of critical infrastructure guidelines*. European Union Publication Office. https://ec.europa.eu
[33]. Peptan, C. (2019). Terrorism-Security threat in the context of globalization. *Analele Universitatii „Constantin Brancusi” din Targu Jiu–Seria Litere si Stiinte Sociale*, (01), 126-142.
[34]. Jones, S. G. (2025, March 18). *Russia’s shadow war against the West*. Centre for Strategic and International Studies. https://www.csis.org/analysis/russias-shadow-war-against-west
[35]. Owuondo, J. O. (2025, August). *Kenya’s Hybrid Warfare Threats and National Security Infrastructure*. *Journal of National Defence University-Kenya*, 3(1), 107-123. https://doi.org/10.64403/bzte1n38
[36]. 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 Universităţii Constantin Brâncuşi din Târgu-Jiu. Seria Inginerie*, (1).
[37]. Augustine, A. S. (2025). Zero-day exploits and their impact on critical infrastructure. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5213418
[38]. Kern, E., & Szanto, A. Cyber Supply Chain Attacks. *Brandenburgisches Institut für Gesellschaft und Sicherheit. BIGS Policy Paper*, *10*.
[39]. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Profile Books.
[40]. Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Vintage.
[41]. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

[42]. Soudan, B. "Cybersecurity of Digital Twins in Industrial IoT Environments," *2024 Advances in Science and Engineering Technology International Conferences (ASET)*, Abu Dhabi, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/ASET60340.2024.10708640.
[43]. Maleh, Y. (2021). IT/OT convergence and cyber security. *Computer Fraud & Security*, *2021*(12), 13-16.
[44]. SANS Institute. (2022, October). *The state of ICS/OT cybersecurity in 2022 and beyond*. https://uploads-ssl.webflow.com/645a4534705010e2cb244f50/64920fe14944579cf72f874c_SANS-Survey-2022-OT-ICS-Cybersecurity-Nozomi-Networks.pdf
[45]. World Economic Forum. (2025, January 13). *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
[46]. United Nations Office for Disarmament Affairs. (2024). *Protecting the cybersecurity of critical infrastructures and their supply chains*.
[47]. Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: On drivers of convergence. *Journal of European Integration*, *46*(7), 1073-1088.
[48]. Georgescu, A., & Dinu, A. (2025). *Cybersecurity governance for critical space infrastructures – The European framework*. *International Journal of Cyber Diplomacy, 6*, 81-95. https://doi.org/10.54852/ijcd.v6y202505
[49]. Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*, *16*(3), 172-196.
[50]. European Commission. (2023). *Guidance on the implementation of Directive (EU) 2022/2557 on the resilience of critical entities (CER)*. Publications Office of the European Union. https://commission.europa.eu/system/files/2023-06/cer-directive-guidance_en.pdf
[51]. Peptan, C. (2019). Information and Intelligence in security equation. *Analele Universitatii „Constantin Brancusi" din Targu Jiu–Seria Litere si Stiinte Sociale*, (02), 39-45.
[52]. Rajamäki, J., Tikanmäki, I., Knowlton, R., & Korhonen, S. (2025). *AI and Cyber Threat Intelligence Management in the Energy Sector*. In Proceedings of the 26th European Conference on Knowledge Management. https://doi.org/10.34190/eckm.26.2.3781
[53]. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. *Applied Sciences, 14*(24), 11807. https://doi.org/10.3390/app142411807
[54]. Jančárková, T., & Wolthusen, S. D. (2020). Legal Issues Related to Cyber Threat Information Sharing: Challenges in the EU and US - with Implications for Critical Infrastructure Protection. *CyCon 2020 Proceedings*. Retrieved from https://ccdcoe.org/uploads/2020/05/CyCon_2020_4_Nweke_Wolthusen.pdf
[55]. Obreja, C., & Rusu, C. (2009). *Protejarea și promovarea intereselor firmei prin activități de intelligence*. Editura Expert.
[56]. Kacker, S. (2024, December 5). *AI Governance: Key Benefits and Implementation Challenges*. ISACA Now Blog. https://www.isaca.org/resources/news-and-trends/ai-governance-key-benefits-and-implementation-challenges
[57]. Ioniță, E. A. (2021). *Intelligence sector reform in Romania: The impact of international cooperation*. Romanian Journal of Society and Politics, 15(2), 42–65. https://www.rjsp.politice.ro/sites/default/files/2022-04/Intelligence%20sector%20reform%20in%20Romania.%20The%20impact%20of%20international%20cooperation_Emilian%20Alexandru%20Ionita%20-%20RJSP%20v.%2015%2C%20no.%202.pdf
[58]. Kovač, S., & Ćutić, D. (2025). *Intelligence activities in the function of national security in Croatia*. National Security and the Future, 26(2), 71–106. https://doi.org/10.37458/nstf.26.2.2
[59]. Gideon, K. (2017). *A cooperative approach between intelligence and policymakers at the national level*. Institute for National Security Studies (INSS) Publication Series: Cyber, Intelligence and Security. Retrieved from https://www.inss.org.il/publication/cooperative-approach-intelligence-policymakers-national-level-chance/
[60]. Vevera, A. V., & Georgescu, A., & Cirnu, D. (2022). *A critical infrastructure perspective and the Romanian framework*. Revista Militară de Teorie şi Strategie, 1(1), pp. 57-73. https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2022/1/VEVERA,%20GEORGESCU,%20CIRNU.pdf
[61]. Dimitriadis, A., Papoutsis, A., Kavalieros, D. *et al.* EVACTI: evaluating the actionability of cyber threat Intelligence. *Int. J. Inf. Secur.* 24, 123 (2025). https://doi.org/10.1007/s10207-025-01033-z
[62]. Frascà, D., Venturi, G., Ustenko, M., Zanasi, A., Staniforth, A., & Fortune, D. (2024). *The role of human intelligence in the age of digital technology*. Revista de Intelligence și Securitate (RISR), 1(31), 5–20.

[63]. Rossbach, N. H. (2024). *Intelligence and data resilience – A small state perspective on digitalisation and national defence towards the 2030s* (Swedish Defence University Report Series 2024:09). Swedish Defence University. https://doi.org/10.62061/iibr1180
[64]. Shulsky, A. N., & Schmitt, G. S. (2008). *Războiul tăcut: Privire asupra lumii informațiilor* (Ediția a 3-a). Potomac Books.
[65]. Bigo, D. (2019). Shared secrecy in a digital age and a transnational world. *Intelligence and National Security, 34*(3), 379–394. https://doi.org/10.1080/02684527.2019.1553703
[66]. Mandel, D. R., & Irwin, D. (2024). *Beyond bias minimization: Improving intelligence with optimization and human augmentation*. *International Journal of Intelligence and CounterIntelligence, 37*(2), 649-665. https://doi.org/10.1080/08850607.2023.2253120
[67]. Pokrajčić, I. (2025). Examining the Transformation of the US National Security System after 2001. Strategos, 9(1), 11-32. https://hrcak.srce.hr/336535