UDC: 004:351.824.11(496.5)
DOI: 10.5937/PDSC26009N

Klejn Ngraçani, MSc
University of New York Tirana, Albania,
email: klejnngracani@unyt.edu.al,

Adela Danaj, PhD
University of New York Tirana, Albania,
email: adeladanaj@unyt.edu.al,
ORCID ID: https://orcid.org/0000-0001-5794-5804

CRITICAL INFRASTRUCTURE IN TIMES OF UNCERTAINTY: REGULATING THE DIGITAL WORLD

Abstract: Critical infrastructure encompasses all physical and virtual systems that are essential to the survival of a country, starting from electrical power grids up to digital networks and cloud environments. Given the current geopolitical events, where critical infrastructure across many countries has been targeted by physical and virtual attacks, this paper takes into analysis the resilience of the Albanian regulatory framework in relation to governing critical infrastructure systems within the country. Through a documentary analysis this paper analyses the extent in which critical infrastructure is protected by the current regulatory framework, focusing especially on the digital sphere, given its everchanging nature and emerging importance in relation to security issues. The documentary analysis uses as primary data the laws, bylaws, and other normative acts which are deemed important by the authors in the governing of the digital systems of critical infrastructure in Albania.

Keywords: *Critical infrastructure, documentary analysis, digital systems, regulatory framework*

1. INTRODUCTION

Critical Infrastructure (CI) refers to the "systems and assets, whether physical or virtual, so essential to the nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination of these" (Alcaraz & Zeadally, 2015, p. 1). These infrastructures—including sectors such as telecommunications, banking, transportation, energy, and healthcare—are fundamental to the functioning of modern society. Any disruption, whether caused by natural hazards, technical failures, or cyberattacks, can have serious economic, social, and security consequences. Moreover, critical infrastructures do not operate independently. As Alcaraz and Zeadally (2015) note, "a CI could require and depend on the services from another CI to work properly, and the latter might also need the output from the first infrastructure. This interdependence relationship could trigger a cascading effect when disruptions of services and functionalities appear within a CI" (p. 3). This interconnectedness is further reinforced within what Castells (2010) describes as the Network Society, where information and communication technologies connect institutions, services, and citizens through complex digital networks. As a result, protecting critical infrastructure is no longer only a technical challenge but also a governance issue requiring effective regulation, institutional coordination, and policies that ensure the security, resilience, and continuity of essential services.

The importance of these issues has grown considerably as cyber threats increasingly target digital infrastructures. The cyberattacks against Albanian government systems in July 2022 exposed significant vulnerabilities in public-sector cybersecurity and demonstrated the risks associated with growing digital dependence (European Union Agency for Cybersecurity [ENISA], 2023). These events highlighted the need for a robust legal and institutional framework capable of protecting digital critical infrastructure and strengthening national resilience. Against this background, this paper examines the extent to which Albania's current regulatory framework protects digital critical infrastructure. Using a documentary analysis approach, the study analyses four laws and three national strategies governing cybersecurity and digital critical infrastructure in Albania. The analysis evaluates the extent to which the existing regulatory framework addresses the challenges created by increasing digitalization, interconnected infrastructure systems, and emerging cyber threats.

The findings indicate that Albania has made significant progress in strengthening the governance of digital critical infrastructure, particularly

following the adoption of Law No. 25/2024 "On Cybersecurity." At the same time, the analysis identifies areas requiring further improvement, particularly the harmonization of legal terminology, clearer institutional coordination, and more effective implementation of regulatory requirements. These findings contribute to understanding Albania's progress in aligning its cybersecurity governance with evolving European standards while identifying priorities for future regulatory development.

2. LITERATURE REVIEW

2.1. Critical Infrastructure: Definitions and Evolution

The concept of critical infrastructure (CI) has evolved considerably over the past three decades in response to technological advances, changing security environments, and the growing interconnectedness of modern societies. Initially associated with physical assets such as transportation, energy, water supply, telecommunications, healthcare, and financial systems, CI now also encompasses cyber-physical systems and digital networks that are essential to national security, economic stability, and societal well-being (Lewis, 2006; European Commission, 2008). Although no universally accepted definition exists, international organizations consistently describe critical infrastructure as assets and services whose disruption would have serious societal consequences.

Digitalization has fundamentally transformed critical infrastructure. Traditional sectors such as energy, transportation, healthcare, and finance increasingly operate as interconnected cyber-physical systems integrating operational technologies, information systems, cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) (Alcaraz & Zeadally, 2015). While these developments have improved efficiency and service delivery, they have also expanded vulnerabilities to cyber threats, making cybersecurity, data governance, information resilience, and digital risk management integral components of critical infrastructure protection. Moreover, modern infrastructures are highly interdependent. As Rinaldi et al. (2001) argue, disruptions in one sector can rapidly cascade across others, complicating risk management, emergency response, and infrastructure governance.

The growing frequency and sophistication of cyber threats have further elevated critical infrastructure as a national and international security priority. Cyberattacks against energy systems, public institutions, transportation, finance, and healthcare demonstrate that severe disruptions can occur without physical destruction, producing substantial economic,

social, and political consequences (Lewis, 2006). Consequently, critical infrastructure protection has evolved into a multidimensional challenge requiring coordinated legal, institutional, technical, and organizational responses. Recent scholarship increasingly adopts resilience as the dominant governance paradigm, emphasizing the capacity of infrastructures to anticipate, absorb, recover from, and adapt to disruptions while maintaining essential services (Linkov et al., 2013). This perspective recognizes that complete protection against increasingly sophisticated cyber and hybrid threats is unrealistic and highlights the need for integrated regulatory frameworks capable of ensuring the continuity and resilience of critical infrastructure, including in the Albanian context.

2.2. Critical Infrastructure Resilience

As the complexity and interconnectedness of critical infrastructure (CI) systems have increased, scholarly attention has shifted from traditional infrastructure protection toward the broader concept of resilience. Although the terms *protection*, *security*, and *resilience* are often used interchangeably, they represent distinct yet complementary approaches to managing risks affecting critical infrastructure (Linkov et al., 2013). Protection focuses on preventing physical and cyber threats through defensive measures such as physical barriers, cybersecurity controls, surveillance, and legal safeguards (Lewis, 2006), whereas security adopts a broader perspective by integrating physical protection, cybersecurity, intelligence, risk management, emergency preparedness, and institutional coordination to safeguard essential services (Alcaraz & Zeadally, 2015). However, the increasing complexity of cyber threats, hybrid warfare, insider risks, and technological vulnerabilities has demonstrated that prevention alone is insufficient.

Consequently, resilience has become the dominant paradigm for governing critical infrastructure. Rather than aiming to eliminate all risks, resilience emphasizes the capacity of infrastructures to anticipate, absorb, respond to, recover from, and adapt to disruptive events while maintaining essential functions (Linkov et al., 2013). This shift reflects a move from asking how infrastructures can be fully protected to how they can continue operating under increasingly uncertain conditions. Expanding this perspective, Hollnagel (2011) argues that resilience is not merely recovery from failure but the continuous ability of socio-technical systems to anticipate, monitor, respond to, and learn from unexpected events.

As cyber threats become increasingly sophisticated and unpredictable, resilience has become a central objective of international cybersecurity

strategies and European critical infrastructure policies. Contemporary regulatory frameworks therefore emphasize risk management, business continuity planning, cybersecurity preparedness, incident reporting, and institutional cooperation to ensure the continuity of essential services. Overall, resilience extends beyond traditional notions of protection and security by providing the theoretical foundation for governing digital critical infrastructure and strengthening its long-term security and continuity.

2.3. Digital Critical Infrastructure and Cybersecurity Governance

The rapid digital transformation of public and private sectors has fundamentally reshaped the operation and governance of critical infrastructure. Technologies such as cloud computing, the Internet of Things (IoT), artificial intelligence (AI), big data analytics, and advanced communication networks have transformed traditional infrastructures into interconnected cyber-physical systems where operational technologies (OT) and information technologies (IT) continuously interact (European Commission, 2020). While digitalization has improved efficiency, automation, interoperability, and service delivery, it has also expanded the cyberattack surface, exposing critical infrastructures to increasingly sophisticated threats (Alcaraz & Zeadally, 2015; ENISA, 2023). As dependence on digital infrastructure has increased, cyber threats have become more frequent and sophisticated. Beyond data theft and financial fraud, attacks increasingly target the continuity of essential services through ransomware, distributed denial-of-service (DDoS) attacks, malware, phishing, supply-chain compromises, software vulnerabilities, and advanced persistent threats (APTs) (ENISA, 2023). At the same time, critical infrastructures have become targets of hybrid threats that combine cyber, political, economic, military, and informational actions to achieve strategic objectives (Bendiek, 2021).

These developments have made cybersecurity governance a central component of critical infrastructure protection. It encompasses the legal, institutional, organizational, and technical arrangements required to prevent, detect, respond to, and recover from cyber incidents. Consequently, contemporary governance frameworks emphasize institutional coordination, risk management, incident reporting, information sharing, and cooperation among governments, regulators, infrastructure operators, law-enforcement agencies, and international organizations (OECD, 2022). Within the European Union, cybersecurity governance has evolved through an integrated legislative framework. The NIS Directive established the first EU-

wide cybersecurity requirements for operators of essential services and digital service providers, introducing common rules on risk management, incident reporting, competent authorities, Computer Security Incident Response Teams (CSIRTs), and cross-border cooperation (European Parliament & Council of the European Union, 2016). These requirements were strengthened through the NIS2 Directive, which expanded its scope and reinforced obligations related to supervision, business continuity, supply-chain security, vulnerability management, and organizational accountability (European Parliament & Council of the European Union, 2022). Complementing these measures, the EU Cybersecurity Strategy for the Digital Decade promotes digital resilience through stronger cybersecurity capabilities, secure infrastructure, technological sovereignty, and international cooperation (European Commission, 2020). A central role within this governance framework is played by the European Union Agency for Cybersecurity (ENISA), which supports Member States through threat intelligence, cybersecurity guidance, risk assessments, cyber exercises, and implementation of the NIS and NIS2 Directives (ENISA, 2023). ENISA's *Threat Landscape* reports have become key references for identifying emerging cyber risks, while the broader literature emphasizes that effective cybersecurity governance depends on adaptive institutions, regulatory harmonization, cross-border cooperation, information sharing, and continuous investment in cybersecurity capabilities (OECD, 2022).

2.4. Regulatory Frameworks for Critical Infrastructure

The effective protection and resilience of critical infrastructure depend not only on technological capabilities but also on comprehensive and enforceable regulatory frameworks. While technology can reduce vulnerabilities and support detection and recovery, only regulation can define institutional responsibilities, establish security standards, coordinate cross-sector responses, and ensure compliance. Effective regulatory frameworks therefore provide the legal and institutional architecture through which critical infrastructure risks are governed by clearly allocating responsibilities, establishing risk-management and reporting obligations, and creating mechanisms for supervision, cooperation, enforcement, and continuous improvement.

Effective regulation is closely linked to governance and institutional coordination. Because critical infrastructures operate across administrative and sectoral boundaries, fragmented governance may result in overlapping mandates, regulatory gaps, and delayed responses. Consequently, regulatory

frameworks must ensure coordination both vertically between national authorities and infrastructure operators and horizontally among ministries, regulators, law-enforcement bodies, civil-protection institutions, and sector-specific authorities. National strategies, competent authorities, Computer Security Incident Response Teams (CSIRTs), information-sharing platforms, crisis-management mechanisms, and joint exercises are therefore central components of effective governance. Legal clarity is another key characteristic of an effective regulatory framework. Clear definitions of critical infrastructure, critical entities, essential services, significant incidents, competent authorities, and digital service providers reduce legal uncertainty and facilitate supervision, while coherence among cybersecurity, sector-specific, emergency management, data protection, and criminal legislation ensures consistent obligations for infrastructure operators.

At the European level, the NIS2 Directive represents a major step forward in cybersecurity regulation. Replacing the original NIS Directive, it expands the scope of regulated sectors, requires Member States to establish national cybersecurity strategies, designate competent authorities and CSIRTs, strengthen cooperation and supervision, and introduce comprehensive cybersecurity risk-management and incident-reporting obligations (European Parliament & Council of the European Union, 2022a). NIS2 also reinforces organizational accountability through stronger management responsibilities, supervisory powers, and enforcement mechanisms. Complementing NIS2, the Critical Entities Resilience (CER) Directive adopts an all-hazards approach to protecting essential services by requiring Member States to identify critical entities, conduct risk assessments, develop national strategies, and ensure that operators implement technical, security, and organizational measures to prevent, respond to, and recover from disruptions (European Parliament & Council of the European Union, 2022b). Together, the two directives promote an integrated governance model recognizing that physical and digital risks are increasingly interconnected.

Public–private cooperation is another cornerstone of critical infrastructure governance. Since many essential services are privately owned or operated, governments rely on partnerships with infrastructure operators to exchange threat information, coordinate preparedness, report incidents, and develop security standards. The OECD emphasizes the importance of clearly defined responsibilities, institutional frameworks, trust-based partnerships, and international cooperation for protecting digitally dependent critical activities (OECD, 2019, 2021). At the same time, voluntary cooperation must be supported by mandatory reporting obligations,

confidentiality safeguards, supervisory powers, and proportionate sanctions.

Risk management forms the operational basis of modern regulation. Rather than prescribing identical technical measures, risk-based regulation requires organizations to assess threats, vulnerabilities, dependencies, and potential consequences while implementing measures proportionate to their risk profile. Similarly, the OECD views cybersecurity as an economic and social risk-management issue requiring leadership commitment, national strategies, stakeholder cooperation, and governance mechanisms that support digital transformation without compromising security (OECD, 2015, 2019). Nevertheless, legislation and standards alone do not guarantee resilience. Their effectiveness depends on implementation, compliance, and continuous adaptation. Competent authorities require sufficient expertise and resources to supervise regulated entities, while operators must demonstrate compliance through risk assessments, security policies, continuity plans, audits, incident reporting, and corrective actions. As cyber risks continue to evolve, regulatory frameworks must also incorporate mechanisms for periodic review, organizational learning, vulnerability management, and continuous improvement.

2.5. Research Gap

The existing literature provides a comprehensive understanding of critical infrastructure protection, resilience, cybersecurity governance, and regulatory frameworks. Studies have examined the evolution of critical infrastructure from predominantly physical assets to complex cyber-physical systems (Alcaraz & Zeadally, 2015; Rinaldi et al., 2001), the emergence of resilience-based governance (Linkov et al., 2013), and the contribution of European instruments such as the NIS2 Directive, the Critical Entities Resilience (CER) Directive, and the EU Cybersecurity Strategy to strengthening the security of essential services (European Commission, 2020; European Parliament & Council of the European Union, 2022a, 2022b).

Despite these advances, four important gaps remain. *First*, most studies adopt an international or comparative perspective, focusing on European Union policy, NATO strategies, or highly developed digital economies. Considerably less attention has been devoted to Western Balkan countries, where digital transformation, institutional capacity, and regulatory development follow different political and administrative trajectories, leaving the applicability of broader European governance models insufficiently explored. *Second*, research on Albania has primarily examined

individual aspects of cybersecurity, including digital transformation, e-government, cyber incidents, and institutional reforms. Although the 2022 cyberattacks against Albanian public institutions increased attention to cybersecurity preparedness and governmental responses, relatively few studies have assessed the country's legal and strategic framework governing digital critical infrastructure. Consequently, there is limited evidence on whether Albania's regulatory framework clearly defines institutional responsibilities, promotes inter-agency coordination, and incorporates internationally recognized principles of resilience and risk management. *Third*, relatively few studies investigate how EU candidate countries translate evolving European cybersecurity legislation into domestic legal and institutional frameworks. As Albania continues to align its legislation with the European Union acquis, assessing its compliance with instruments such as the NIS2 Directive and the CER Directive is both academically and practically relevant. Unlike EU Member States, candidate countries must strengthen national resilience while simultaneously adapting to rapidly evolving European standards. The Albanian case is particularly significant because the 2022 cyberattacks transformed cybersecurity from a technical issue into a matter of national security and public governance, exposing vulnerabilities in one of the region's most digitalized public administrations and accelerating discussions on regulatory reform and institutional resilience. *Fourth*, a methodological gap persists. Existing studies have predominantly focused on cyber incidents, policy developments, or institutional reforms, while relatively few have systematically examined Albania's legal and strategic framework through documentary analysis. Analysing the principal laws, bylaws, and national strategies governing digital critical infrastructure provides a structured assessment of how cybersecurity governance is embedded within the national regulatory framework and complements the predominantly technical and policy-oriented literature.

To address these gaps, this study employs a qualitative documentary analysis of Albania's regulatory framework governing digital critical infrastructure. By examining the principal laws, bylaws, and national strategies, it evaluates the extent to which the framework incorporates internationally recognized principles of governance, institutional coordination, legal clarity, risk management, resilience, and regulatory compliance. It also assesses the degree to which Albania's approach aligns with contemporary European standards while identifying legal and institutional areas requiring further development. Based on the literature reviewed, an effective regulatory framework for digital critical

infrastructure can be assessed through six interrelated dimensions: (1) legal clarity; (2) governance and institutional responsibilities; (3) inter-agency coordination; (4) cybersecurity risk management; (5) resilience and business continuity; and (6) compliance and enforcement mechanisms. These dimensions constitute the analytical framework applied in the documentary analysis presented in the following sections.

3. METHODOLOGY

In order to assess the extent in which critical infrastructure is protected and governed within the digital sphere by the current regulatory framework in Albania, this article employs a Qualitative Research approach based on Documentary Analysis. The documentary corpus consists of a purposive sample of four laws and three national strategies, based on their direct relevance to cybersecurity governance. The analysed legal documents include Law No. 25/2024 "On Cybersecurity", Law No. 54/2024 "On Electronic Communications in the Republic of Albania", Law No. 9887 "On Protection of Personal Data" (as amended), and Law No. 107/2015 "On Electronic Identification and Trust Services" (Republic of Albania, 2008, 2015, 2024a, 2024b). In addition, the analysis incorporates three strategic documents: the National Cybersecurity Strategy of the Republic of Albania 2020–2025, the National Security Strategy of the Republic of Albania 2023–2028, and the National Cybersecurity Strategy of the Republic of Albania 2025–2030 (Assembly of the Republic of Albania, 2023; Council of Ministers of the Republic of Albania, 2020; National Authority for Cyber Security, 2025).

The analysis followed a 10-step approach, namely: (i) Identify the research problem or issue; (ii) Devise a list of possible aims and research questions; (iii) Identify the relevant theoretical and methodological frameworks; (iv) Develop a list of key words or themes from the literature; (v) Locate physical (library, archives) and electronic documents; (vi) Classify documents; (vii) Collect and collate data; (viii) Identify emerging themes from the data; (ix) Interpret evidence and link with research questions and literature themes; (x) Structure and write a report (Fitzgerald, 2012, p. 298).

Following this methodological framework, the selected documents were examined through a thematic analysis approach, focusing on key areas relevant to the governance and protection of digital critical infrastructure in Albania. More specifically, the analysis was guided by six main thematic categories: *(1) legal clarity; (2) governance and institutional*

responsibilities; (3) inter-agency coordination; (4) cybersecurity risk management; (5) resilience and business continuity; and (6) compliance and enforcement mechanisms. These categories were selected based on their relevance to the protection of digitally dependent critical infrastructure and their significance within contemporary cybersecurity governance debates. Even though the Documentary Analysis offers valuable insights on the current state of protection and governing of critical infrastructure in the digital world within the Albanian context, it has certain limitations as well. While the study examines the legal framework as well as the strategic vision for the protection of digital critical infrastructure, it lacks on evaluation of practical implementation or operational effectiveness of these measures. Therefore, the findings should be understood solely as an examination of the regulatory framework, and not its implementation in practice.

4. RESULTS

4.1 Legal Clarity

Albania's legal framework for cybersecurity and digital critical infrastructure has evolved considerably in recent years, particularly following the adoption of Law No. 25/2024 "On Cybersecurity" (Republic of Albania, 2024a). While the framework demonstrates a clear commitment to strengthening cybersecurity governance, the analysis also identifies inconsistencies in terminology and the distribution of provisions across multiple legal and strategic documents. At the strategic level, the National Security Strategy of the Republic of Albania 2023–2028 recognizes cybersecurity as a core component of national security and identifies digital infrastructure as increasingly vulnerable to state and non-state threats (Assembly of the Republic of Albania, 2023). Although it establishes cybersecurity resilience as a national priority, the Strategy primarily defines policy objectives rather than legally binding obligations, providing limited guidance on the specific responsibilities of public institutions and infrastructure operators. The principal legal foundation is Law No. 25/2024 "On Cybersecurity", which clearly defines key concepts, including cybersecurity, cyber incidents, critical and important information infrastructures, operators, and competent authorities (Republic of Albania, 2024a). It specifies the sectors within its scope, establishes obligations for entities operating critical digital services, and creates a coherent relationship between legislation, secondary legislation, and national cybersecurity policy. Compared with the previous framework, the law substantially improves legal certainty by introducing a common legal vocabulary and

reducing ambiguity regarding institutional responsibilities.

This framework is complemented by the National Cybersecurity Strategy 2025–2030, which translates the objectives of the Cybersecurity Law into strategic priorities and implementation measures (National Authority for Cyber Security, 2025). The Strategy focuses on strengthening digital infrastructure resilience, enhancing institutional capacity, and aligning Albania's cybersecurity governance with European Union standards, particularly the principles reflected in the NIS2 Directive. Additional legislation strengthens specific components of the digital ecosystem. Law No. 107/2015 "On Electronic Identification and Trust Services" establishes the legal basis for electronic identification, electronic signatures, trust services, and authentication mechanisms, supporting secure digital transactions and public services (Republic of Albania, 2015). Similarly, Law No. 54/2024 "On Electronic Communications in the Republic of Albania" regulates electronic communications networks and services, clarifying the obligations of network operators and service providers (Republic of Albania, 2024b). Although neither law specifically governs critical infrastructure protection, both provide essential legal foundations for secure digital infrastructure. The Law on Protection of Personal Data further complements the framework by regulating the processing, storage, and security of personal data (Republic of Albania, 2008). While primarily intended to protect privacy and fundamental rights, it reinforces cybersecurity governance by requiring appropriate organizational and technical safeguards for personal information.

Overall, these legal and strategic documents demonstrate that Albania has progressively developed a more coherent framework for governing digital critical infrastructure. The Cybersecurity Law provides the principal legal basis, while the National Security Strategy and the National Cybersecurity Strategy establish the strategic direction for implementation (Assembly of the Republic of Albania, 2023; National Authority for Cyber Security, 2025; Republic of Albania, 2024a). Sector-specific legislation on electronic communications, electronic identification, and personal data protection further strengthens the regulatory framework, reflecting Albania's efforts to align with European cybersecurity standards. Nevertheless, the analysis also identifies areas requiring further improvement. Terminology is not always applied consistently across legal and strategic documents. Concepts such as *critical infrastructure*, *critical information infrastructure*, *important information infrastructure*, and *digital infrastructure* are used in different contexts without clearly defining their relationship. In addition, the regulatory framework remains dispersed across several laws and strategies,

requiring considerable cross-referencing to understand the full legal landscape. Greater harmonization of terminology and further consolidation of the legal framework would enhance legal clarity and facilitate more consistent implementation.

4.2 Governance and Institutional Responsibilities

A clearly defined governance structure is essential for ensuring the effective protection of digital critical infrastructure. Beyond establishing legal obligations, the regulatory framework must allocate responsibilities among institutions, define their respective mandates, and provide mechanisms for accountability. The reviewed legislation shows that Albania has made considerable progress in this area, particularly through the adoption of Law No. 25/2024 "On Cybersecurity", which consolidates institutional roles and strengthens the governance of national cybersecurity (Republic of Albania, 2024a).

At the strategic level, the National Security Strategy 2023–2028 presents cybersecurity as a shared national responsibility involving state institutions, critical infrastructure operators, the private sector, and international partners (Assembly of the Republic of Albania, 2023). The Strategy recognises that protecting critical infrastructure requires coordinated action across multiple sectors and emphasises the need to strengthen institutional capacities to address evolving cyber threats. However, as a strategic document, it outlines general policy objectives without assigning detailed operational responsibilities to individual institutions.

The allocation of institutional responsibilities becomes much clearer in Law No. 25/2024 "On Cybersecurity", which establishes the governance architecture for cybersecurity in Albania (Republic of Albania, 2024a). The law designates the National Authority for Cyber Security (AKSK) as the principal competent authority responsible for implementing national cybersecurity policy, supervising compliance, coordinating incident response, and overseeing the protection of critical and important information infrastructures. At the same time, the law clearly defines the obligations of operators of essential and important entities, requiring them to implement appropriate cybersecurity measures, conduct risk assessments, report significant incidents, and cooperate with the competent authorities. This distribution of responsibilities reflects a governance model in which public authorities perform regulatory and supervisory functions, while infrastructure operators bear primary responsibility for managing cybersecurity risks within their own systems.

The National Cybersecurity Strategy 2025–2030 reinforces this governance model by identifying institutional capacity building as one of its central objectives (National Authority for Cyber Security, 2025). The Strategy emphasises strengthening the operational capabilities of AKSK, improving cooperation among public institutions, and promoting partnerships with academia and the private sector. In doing so, it extends the governance framework beyond regulatory oversight and recognises cybersecurity as a whole-of-society responsibility requiring continuous collaboration across sectors.

The complementary legislation also contributes to the institutional framework, although within more specialised domains. The Law on Electronic Communications assigns regulatory responsibilities for the oversight of electronic communications networks and services, while the Law on Electronic Identification and Trust Services establishes the legal responsibilities of trust service providers and competent supervisory bodies (Republic of Albania, 2015; Republic of Albania, 2024b). Similarly, the Law on Protection of Personal Data defines the responsibilities of data controllers, processors, and the supervisory authority responsible for ensuring compliance with data protection requirements (Republic of Albania, 2008). Together, these laws allocate responsibilities within their respective sectors while supporting the broader governance framework established by the Cybersecurity Law.

The data analysis process revealed a well-defined distribution of institutional responsibilities, with Law No. 25/2024 (Republic of Albania, 2024a) serving as the central instrument that integrates cybersecurity governance across critical sectors. Despite this, the governance responsibilities remain dispersed across several legal instruments and institutions, requiring continuous coordination to avoid overlaps and ensure effective implementation.

4.3 Inter-agency Coordination

Effective governance depends on the ability of public authorities, infrastructure operators, and other stakeholders to coordinate their actions. Given the cross-sectoral nature of cyber threats, effective regulatory frameworks require mechanisms for information sharing, joint response, and cooperation across institutional boundaries. The analysis indicates that inter-agency coordination has become a central feature of Albania's cybersecurity framework, particularly following the adoption of Law No. 25/2024 "On Cybersecurity" (Republic of Albania, 2024a). The National Security

Strategy 2023–2028 recognizes cybersecurity as a shared responsibility requiring coordinated action among government institutions, law-enforcement agencies, intelligence services, critical infrastructure operators, and international partners (Assembly of the Republic of Albania, 2023). While it establishes institutional cooperation as a strategic priority for strengthening national resilience, it provides only broad policy guidance, leaving operational coordination to sector-specific legislation.

A more comprehensive governance framework is established by Law No. 25/2024 "On Cybersecurity", which assigns the National Authority for Cyber Security (AKSK) a central coordinating role within Albania's cybersecurity system (Republic of Albania, 2024a). The law requires cooperation among competent authorities, public institutions, and operators of critical and important entities in preventing, detecting, and responding to cyber incidents. It also introduces formal obligations for incident reporting and information sharing, creating structured mechanisms for institutional collaboration rather than simply allocating responsibilities. The National Cybersecurity Strategy 2025–2030 further reinforces this approach by identifying inter-institutional cooperation as a key priority (National Authority for Cyber Security, 2025). It promotes greater information exchange among public institutions, stronger cooperation with the private sector and academia, and increased participation in regional and international cybersecurity initiatives, recognizing that effective cybersecurity governance requires collaboration beyond public administration. Sector-specific legislation complements this framework. The Law on Electronic Communications requires cooperation between regulatory authorities and communications providers to ensure the security and continuity of electronic communications networks (Republic of Albania, 2024b), while the Law on Protection of Personal Data promotes cooperation between supervisory authorities and organizations processing personal data, particularly in the event of security incidents affecting individual rights (Republic of Albania, 2008). Although pursuing different regulatory objectives, both laws reinforce the broader coordination framework established by cybersecurity legislation.

4.4 Cybersecurity Risk Management

Cybersecurity risk management is a core component of protecting digital critical infrastructure, shifting the focus from responding to incidents to preventing and mitigating risks. The analysis shows that Albania's regulatory framework increasingly adopts a risk-based approach, particularly through

Law No. 25/2024 "On Cybersecurity", which aligns national legislation with contemporary European cybersecurity standards (Republic of Albania, 2024a). The National Security Strategy 2023–2028 identifies cyber threats as a major national security risk and calls for stronger capabilities to anticipate, prevent, and respond to attacks affecting public services, economic stability, and national resilience (Assembly of the Republic of Albania, 2023). However, as a strategic document, it does not establish specific obligations for infrastructure operators. These obligations are introduced by Law No. 25/2024, which requires operators of critical and important entities to implement appropriate technical, operational, and organisational measures, conduct regular risk assessments, apply security measures proportionate to identified risks, report significant cyber incidents, and continuously monitor vulnerabilities (Republic of Albania, 2024a). This reflects a preventive approach in which cybersecurity risk management is understood as a continuous rather than a one-time process.

The National Cybersecurity Strategy 2025–2030 complements these legal requirements by identifying risk management as a strategic priority and promoting threat monitoring, early warning, incident detection, capacity building, and the adoption of internationally recognised cybersecurity standards (National Authority for Cyber Security, 2025). Sector-specific legislation further supports this approach. The Law on Electronic Communications requires providers to ensure the security and integrity of electronic communications networks (Republic of Albania, 2024b), while the Law on Protection of Personal Data obliges controllers and processors to implement appropriate technical and organisational safeguards for personal data (Republic of Albania, 2008). Although these measures primarily address communications and data protection, they also strengthen the resilience of digital critical infrastructure.

4.5 Resilience and Business Continuity

The ability of critical infrastructure to continue operating during and after a cyber incident is a key indicator of effective cybersecurity governance. As digital systems become increasingly interconnected, resilience extends beyond preventing attacks to ensuring the continuity of essential services, rapid recovery, and adaptation to emerging threats. The analysis indicates that resilience has become a central element of Albania's cybersecurity framework, particularly through Law No. 25/2024 "On Cybersecurity" and the National Cybersecurity Strategy 2025–2030 (Republic of Albania, 2024a; National Authority for Cyber Security, 2025).

The National Security Strategy 2023–2028 identifies resilience as a strategic objective for protecting national security and critical infrastructure from physical and cyber threats (Assembly of the Republic of Albania, 2023). It recognizes that disruptions to essential digital services can have cascading effects across sectors and calls for strengthening national capacities to prevent, withstand, and recover from cyber incidents. However, the Strategy defines broad policy objectives, leaving operational measures to sector-specific legislation.

These measures are primarily established by Law No. 25/2024 "On Cybersecurity", which requires operators of critical and important entities to implement technical and organisational measures ensuring service continuity, incident management, vulnerability mitigation, and recovery planning (Republic of Albania, 2024a). By requiring organizations to prepare for, respond to, and recover from cyber incidents, the law promotes a resilience-based approach focused on maintaining essential services. The National Cybersecurity Strategy 2025–2030 reinforces this approach by promoting preparedness, institutional capacity building, crisis response mechanisms, regular testing of response capabilities, and stronger cooperation among public institutions and critical infrastructure operators (National Authority for Cyber Security, 2025). Complementary legislation further supports resilience. The Law on Electronic Communications requires providers to ensure the availability, integrity, and security of electronic communications networks (Republic of Albania, 2024b), while the Law on Electronic Identification and Trust Services strengthens trust in digital transactions through secure electronic authentication and trust services (Republic of Albania, 2015).

4.6 Compliance and Enforcement Mechanisms

The analysis indicates that Albania has strengthened its compliance and enforcement framework in recent years, particularly through Law No. 25/2024 "On Cybersecurity", which introduces more structured supervisory and accountability mechanisms (Republic of Albania, 2024a). The National Security Strategy 2023–2028 highlights the importance of institutional capacity and effective governance for protecting national assets and critical infrastructure from cyber threats (Assembly of the Republic of Albania, 2023). However, as a strategic document, it establishes policy objectives rather than specific compliance obligations or sanctions. A more comprehensive compliance framework is provided by Law No. 25/2024 "On Cybersecurity", which requires critical and important entities to implement

cybersecurity measures, report significant incidents, and cooperate with competent authorities (Republic of Albania, 2024a). The law assigns the National Authority for Cyber Security (AKSK) supervisory responsibilities, including monitoring compliance, issuing binding requirements, and taking measures in cases of non-compliance. This marks a significant shift from a predominantly advisory approach to a more regulated and accountable system.

The National Cybersecurity Strategy 2025–2030 reinforces this framework by promoting stronger supervision, institutional maturity, and compliance with cybersecurity requirements (National Authority for Cyber Security, 2025). It emphasizes enhanced monitoring capacities, closer cooperation between authorities and regulated entities, and the adoption of internationally recognised cybersecurity standards, presenting compliance as both a legal obligation and a key element of national cyber resilience. Sector-specific legislation further strengthens the compliance framework. The Law on Electronic Communications establishes security obligations for communications providers and provides for regulatory oversight (Republic of Albania, 2024b). Similarly, the Law on Electronic Identification and Trust Services introduces supervisory mechanisms to ensure the reliability and security of electronic identification and trust services (Republic of Albania, 2015), while the Law on Protection of Personal Data establishes obligations for data controllers and processors together with oversight by the competent data protection authority (Republic of Albania, 2008).

CONCLUSIONS

This paper examined the extent to which Albania's regulatory framework provides effective governance and protection for digital critical infrastructure through a qualitative documentary analysis of relevant laws and national strategies. Using six analytical dimensions derived from the literature—legal clarity, governance and institutional responsibilities, inter-agency coordination, cybersecurity risk management, resilience and business continuity, and compliance and enforcement—the study assessed Albania's capacity to address the security challenges associated with increasing digital dependence. The findings indicate that Albania has made significant progress in strengthening cybersecurity governance, particularly following the adoption of Law No. 25/2024 "On Cybersecurity" (Republic of Albania, 2024a). Together with the National Cybersecurity Strategy 2025–2030, the law establishes a more coherent, coordinated, and risk-based framework by defining key concepts, assigning institutional

responsibilities, and introducing obligations for operators of critical and important entities (National Authority for Cyber Security, 2025).

The analysis shows that the regulatory framework has become more coherent, with the Cybersecurity Law serving as its central legal instrument. The National Security Strategy 2023–2028 provides the strategic direction, while legislation on electronic communications, electronic identification, trust services, and personal data protection complements the framework by regulating key components of the digital ecosystem (Assembly of the Republic of Albania, 2023; Republic of Albania, 2008; Republic of Albania, 2015; Republic of Albania, 2024b). At the institutional level, the designation of the National Authority for Cyber Security (AKSK) as the competent authority has strengthened governance, accountability, and cooperation between public institutions and infrastructure operators (Republic of Albania, 2024a).

The findings also demonstrate a clear shift towards integrated cybersecurity governance. Mechanisms for information sharing, incident reporting, and inter-agency cooperation have improved national coordination (Assembly of the Republic of Albania, 2023; Republic of Albania, 2024a), while the regulatory framework increasingly adopts a preventive and risk-based approach by requiring operators to conduct risk assessments, implement technical and organisational measures, and report significant cyber incidents (Republic of Albania, 2024a; National Authority for Cyber Security, 2025). Greater emphasis is also placed on resilience and business continuity through requirements for incident management, recovery planning, and preparedness, recognising that the continuity of essential services is as important as preventing cyberattacks (Assembly of the Republic of Albania, 2023; Republic of Albania, 2024a). Furthermore, strengthened supervisory powers, reporting obligations, and compliance mechanisms contribute to a more accountable cybersecurity environment, supported by sector-specific legislation governing electronic communications, electronic identification, and personal data protection (Republic of Albania, 2008; Republic of Albania, 2015; Republic of Albania, 2024b).

Despite these advances, the analysis identifies several areas requiring further development. Terminology is not always harmonised across legal and strategic documents, particularly regarding the concepts of critical infrastructure, critical information infrastructure, and digital infrastructure. In addition, responsibilities remain dispersed across multiple legislative instruments, making effective implementation dependent on strong institutional coordination, technical expertise, and consistent enforcement.

REFERENCES

1. Alcaraz, C., & Zeadally, S. (2015). *Critical infrastructure protection: Requirements and challenges for the 21st century*. *International Journal of Critical Infrastructure Protection, 8*, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002
2. Assembly of the Republic of Albania. (2023). *National security strategy of the Republic of Albania 2023–2028.*
3. Bendiek, A. (2021). *European cyber security policy*. Stiftung Wissenschaft und Politik (SWP Research Paper).
4. Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
5. Council of Ministers of the Republic of Albania. (2020). *National cybersecurity strategy of the Republic of Albania 2020–2025.*
6. European Commission. (2008). *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. *Official Journal of the European Union, L 345*, 75–82.
7. European Commission. (2020). *The EU's cybersecurity strategy for the digital decade*. JOIN(2020) 18 final.
8. European Parliament & Council of the European Union. (2016). *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*. *Official Journal of the European Union, L 194*, 1–30.
9. European Parliament & Council of the European Union. (2022a). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.
10. *Official Journal of the European Union, L 333*, 80–152.
11. European Parliament & Council of the European Union. (2022b). Directive (EU) 2022/2557 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*, 164–198.
12. European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Publications Office of the European Union. https://doi.org/10.2824/782573
13. Fitzgerald, T. (2012). Documents and documentary analysis: A matter of record. In M. Coleman, A. R. J. Briggs, & M. Morrison (Eds.), *Research methods in educational leadership and management* (pp. 296–308). SAGE Publications.
14. Hollnagel, E. (2011). *Prologue: The scope of resilience engineering*.

In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice: A guidebook* (pp. xxix–xxxix). Ashgate.

15. Lewis, J. A. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation*. Wiley.
16. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y
17. National Authority for Cyber Security. (2025). *National cybersecurity strategy of the Republic of Albania 2025–2030.*
18. OECD. (2019). *Artificial intelligence in society*. OECD Publishing. https://doi.org/10.1787/eedfee77-en
19. OECD. (2022). *OECD digital economy outlook 2022*. OECD Publishing. https://doi.org/10.1787/b1e3b2a7-en
20. Organisation for Economic Co-operation and Development. (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. OECD Publishing. https://doi.org/10.1787/9789264245471-en
21. Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on digital security of critical activities* (OECD/LEGAL/0456). OECD.
22. Organisation for Economic Co-operation and Development. (2021). *Enhancing the digital security of critical activities: Going digital toolkit note*. OECD.
23. Republic of Albania. (2008). *Law No. 9887, dated 10.03.2008, "On protection of personal data" (as amended).* Official Publication Center.
24. Republic of Albania. (2015). *Law No. 107/2015, "On electronic identification and trust services"*. Official Publication Center.
25. Republic of Albania. (2024a). *Law No. 25/2024, "On cybersecurity"*. Official Publication Center.
26. Republic of Albania. (2024b). *Law No. 54/2024, "On electronic communications in the Republic of Albania"*. Official Publication Center.
27. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25. https://doi.org/10.1109/37.969131