BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

# Critical Infrastructure through a Securitization Theory Lens

**Sorina-Denisa POTCOVARU (DRAGNE), PhD Candidate***
**Marinel-Adi MUSTAȚĂ, PhD****

*Interdisciplinary Doctoral School, "Carol I" National Defence University, Bucharest, Romania
e-mail: dragne.sorina@adlunap.ro
**Security and Defence Faculty, "Carol I" National Defence University, Bucharest, Romania
e-mail: mustata.adi@unap.ro

## Abstract

Critical infrastructure has become a central focus of European security governance amid increasingly complex physical, digital, and hybrid threats. This article applies securitization theory, drawing on both the classical Copenhagen School and its sociological developments, to analyse how the EU constructs and governs critical infrastructure through the CER Directive and the NIS2 Directive. The comparison shows that these instruments articulate distinct, yet complementary, referent objects: the CER Directive securitizes the continuity of essential services in the physical and organisational domain, while the NIS2 Directive securitizes the security and reliability of network and information systems underpinning the internal market. Together, they reveal a dual securitization logic, physical operational continuity, and digital systemic integrity, embedded in a multi-level EU security architecture that operates through legal instruments, regulatory practices, and technical standards. By linking securitization theory with the material politics of infrastructure governance, the article demonstrates that critical infrastructure is not merely a technical domain, but a key arena through which contemporary European security is defined and enacted.

**Keywords:**
Securitization Theory; Critical Infrastructure; Resilience; Cybersecurity; CER Directive; NIS2 Directive; European Union Governance; Essential Services; Network and Information Systems.

**Article info**
Received: 12 October 2025; Revised: 3 November 2025; Accepted: 4 December 2025; Available online: 15 January 2026

Citation: Potcovaru (Dragne), S.D., and M.A. Mustață. . 2025. "Critical Infrastructure through a Securitization Theory Lens." *Bulletin of "Carol I" National Defence University*, 14(4): 169-182. https://doi.org/10.53477/2284-9378-25-65

## Introduction

The governance of critical infrastructure has become a central concern of contemporary security policy, driven by the increasing interdependence of European societies and the expansion of hybrid, cyber, and systemic risks (e.g., ransomware attacks, the sabotage of the Nord Stream pipelines (2022), and the disruption of satellite communications). While early approaches to critical infrastructure protection relied primarily on risk management and technical standards, recent European Union (EU) legislation reveals a profound restructuring of the way "criticality" is politically constructed and governed. The adoption of the Directive on the resilience of critical entities (CER Directive) and the Directive on measures for a high common level of cybersecurity (NIS2 Directive) marks a decisive shift from sectoral vulnerability assessments to a broader framework in which essential services, digital dependencies, and socio-technical systems are elevated to matters of existential importance.

Securitization theory, developed by the Copenhagen School and subsequently expanded through sociological and material-discursive perspectives, provides a robust conceptual lens to understand this transformation. Rather than treating infrastructures as neutral objects of technical management, securitization theory highlights the way in which political and regulatory actors construct essential services, digital infrastructures, and networked systems as existentially threatened entities whose protection justifies extraordinary governance arrangements. In this context, critical infrastructure is not merely a set of assets but a referent object produced through legal, institutional, and discursive practices that assign it a privileged status in the hierarchy of societal priorities. Applying securitization theory, therefore, enables a deeper understanding of how EU legislation mobilizes narratives of vulnerability, interdependence, and societal risk to expand regulatory authority and reshape the responsibilities of both states and operators.

The CER Directive and the NIS2 Directive offer a compelling basis for comparative analysis because they represent two distinct but interconnected forms of securitization. The CER Directive constructs the continuity of essential services, such as energy, transport, water, healthcare, and public administration, as indispensable to vital societal functions and economic stability. By contrast, the NIS2 Directive securitizes the reliability and integrity of network and information systems that underpin these functions, framing cybersecurity not as a technical domain but as a condition for the functioning of the internal market and the resilience of digitally dependent services. Despite substantial sectoral overlap, the two directives posit different referent objects, mobilize distinct threat imaginaries, and deploy separate governance mechanisms. Their comparison thus reveals how the EU articulates physical, organisational, and digital vulnerabilities across multiple layers of the socio-technical system.

This article uses securitization theory to analyse how critical infrastructure is constructed as an object of protection in EU law and to compare the CER and NIS2 Directives as complementary, yet conceptually distinct, frameworks. The analysis demonstrates that the EU now operates with a dual securitization logic: one centred on critical resilience and the uninterrupted provision of essential services, and another centred on cybersecurity and the integrity of network and information systems.

From a methodological perspective, the conceptual framework of this article is grounded in securitization theory, which provides the analytical tools for conducting a legislative and comparative examination of two European Union legal instruments concerning critical infrastructure. In this regard, the study investigates how the CER Directive and the NIS2 Directive construct their respective referent objects, securitizing actors, audiences, and threat imaginaries. The analysis is structured through a three-layered analytical grid, the value layer, the stakeholder/operator layer, and the physical–technical layer, applied symmetrically to both directives to ensure conceptual consistency. The insights generated through this framework are then integrated into a comparative assessment that identifies convergences, divergences, and complementarities in the EU's approach to governing critical infrastructure. The methodology adopted is therefore interpretive rather than empirical, focusing on how legislative instruments frame existential threats and authorize governance interventions within a multi-level European security architecture.

Nevertheless, this methodological approach carries certain inherent limitations. First, because it relies primarily on textual and conceptual analysis of EU legislation, the study does not capture the full diversity of national implementation practices or the sectoral variations across Member States.

## Securitization Theory and Its Relevance for Critical Infrastructure

Securitization theory, first developed by the Copenhagen School, conceptualizes security as a performative and intersubjective process in which political actors construct certain issues as existential threats that justify extraordinary measures (Buzan, Wæver, and de Wilde 1998; Taureck 2006, 54–55). Central to this framework is the claim that security is a *speech act*: by declaring an issue to be a matter of survival, an authoritative actor transforms it into one treated outside the bounds of normal politics. Classical securitization theory thus emphasises the role of elite actors, the referent object framed as under threat, the audience whose acceptance is necessary for securitization to succeed, and the shift from routine governance to exceptional political measures (Taureck 2006, 55; Balzacq 2019, 3–4).

Balzacq (2011) reformulates the theory beyond its linguistic foundations by distinguishing between a philosophical approach and a sociological approach,

which embeds securitization in broader practices, institutional contexts, and power relations. For Balzacq, securitization succeeds not simply through rhetorical performance but through the alignment of audience expectations, contextual resonance, and what he calls a dispositif of practices, tools, and cultural dispositions that render certain threat constructions meaningful. Security utterances, therefore, derive their force from their embeddedness in social and historical conditions rather than from semantics alone. This sociological turn shifts the theory from a narrow focus on language to a more comprehensive account of how threats are produced, circulated, and stabilized within political environments.

A further refinement is offered by Balzacq, Léonard, and Ruzicka (2016), who argue that securitization is best understood as a process that establishes the security character of public problems and shapes the policy options deemed legitimate in response. The authors reconceptualize securitization as a fusion of performativity and an "analytics of government," in which security is enacted through bureaucratic routines, professional practices, data systems, and legal instruments, not merely via discursive acts. They highlight four re-theorized dimensions (audience, context, power relations, and practices) demonstrating that securitization has evolved into a flexible research programme concerned with how threats are constructed and institutionalized across diverse domains, from migration and health to energy and cybersecurity.

Balzacq (2019) further deepens this trajectory by addressing key tensions that persist in the field: whether securitization derives primarily from elite performance or from co-constitutive interactions with audiences, and whether securitization depoliticizes or intensifies political struggle. To reconcile these debates, he proposes the idea of regimes of practices, which integrates discursive and material mechanisms that shape how threats become socially "sticky." Securitization, in this formulation, is inseparable from the politics of the extraordinary, a contest over legitimacy in which actors struggle to impose authoritative representations of danger. This approach situates securitization within the broader productive power of governance practices that structure visibility, expertise, and institutional responses to perceived threats.

Stritzel (2014) provides one of the most influential critiques of classical theory, arguing that the Copenhagen School's conceptual architecture is under-theorized and internally inconsistent, particularly regarding the relationship between speech acts, audiences, context, and power. He shows that the theory oscillates between an Austinian view of securitization as illocution, a poststructuralist focus on indeterminacy, and a Bourdieusian account of fields of power, without reconciling these positions. Stritzel therefore advocates a discursive-pragmatic and context-sensitive approach, in which the meaning of security emerges from historically situated practices of translation, negotiation, and power.

Complementing this debate, Taureck (2006) clarifies the distinction between securitization theory as an analytical framework and securitization studies as a

broader normative critique. She argues that many critiques misinterpret the theory by faulting it for lacking moral guidance, even though its purpose is diagnostic: it seeks to explain *how* actors construct threats and mobilize exceptional measures, not to evaluate whether they should do so. By drawing this boundary, Taureck repositions securitization theory as a methodologically neutral tool for tracing processes of securitization and desecuritization.

Despite these advancements, the application of securitization theory to critical infrastructure remains underdeveloped. Aradau (2010) highlights that much of the literature treats infrastructures as passive objects rather than as material–discursive assemblages actively constituted as "critical" through engineering standards, legal classifications, and risk assessment practices. This challenges the dominant tendency to privilege linguistic acts and audience acceptance while neglecting the material agency of infrastructures and the socio-technical practices that underpin their governance. As a result, securitization analyses often reproduce a managerial and depoliticized framing, overlooking how infrastructures co-produce security logics and how "criticality" itself is fabricated through institutional and technical work. Aradau's intervention, therefore, underscores the need for a more integrated perspective that bridges securitization theory with the material politics of infrastructure governance.

## A Securitization Theory Approach to the Resilience of Critical Entities

Applying securitization theory to the Directive on the resilience of critical entities (CER Directive) demonstrates that the primary referent object is not the physical infrastructure itself, but the continuity of essential services that sustain vital societal functions and economic stability. The Directive explicitly positions critical entities as indispensable for "the maintenance of vital societal functions or economic activities," establishing service continuity as the existential value at stake (European Union 2022b, Recitals 1–3). In securitization terms, it is the potential disruption of these essential services and the cascading societal and economic consequences that constitute the existential threat requiring exceptional governance measures.

This securitized framing is operationalized through a three-layered conception of the referent object: value, stakeholder, and physical layer. At the value layer, the Directive identifies essential services such as energy, transport, banking, healthcare, digital infrastructure, and water supply as the foundational societal functions whose uninterrupted provision must be safeguarded. These services underpin the stability of the internal market and public welfare and therefore justify harmonised EU intervention.

At the stakeholder or operator layer, the referent object comprises the critical entities, public and private operators, responsible for maintaining these essential services.

Article 1 asserts that the purpose of the Directive is to ensure the "resilience of critical entities, so that they can provide essential services "in an unobstructed manner," even under disruptive conditions (European Union 2022b, Art. 1). Operators thus become functional intermediaries whose failure would directly threaten the essential societal values securitized at the higher layer.

Finally, at the physical layer, the Directive encompasses the infrastructures, assets, and systems through which operators deliver essential services. These physical and digital components, networks, facilities, and technologies are framed as instrumental referent objects. Article 2 defines critical infrastructure as any asset or system "necessary for the provision of an essential service," underscoring its supporting role relative to the operator and value layers (European Union 2022b, Art. 2).

Viewed through securitization theory, the CER Directive therefore constructs a hierarchical referent object: the essential societal functions to be protected, the operators responsible for delivering them, and the infrastructures that enable their functioning. This multi-layered framing shifts attention away from traditional asset-based protection toward the safeguarding of service continuity as a matter of existential importance for the European Union, thereby legitimizing extensive regulatory and supervisory measures across Member States.

Applying securitization theory to the Directive on the resilience of critical entities (CER Directive) reveals a multi-layered and multi-level constellation of securitizing actors. Securitization unfolds both at the legal–institutional level, through authoritative legislative acts, and at the operational level, through the implementation and oversight practices that translate the Directive into everyday governance. Each layer operates simultaneously at the EU level and the national level, resulting in a complex architecture of distributed securitizing authority.

At the EU legal–institutional level, the primary securitizing actors are the European Parliament and the Council, acting on a proposal from the European Commission. Through the adoption of the Directive, these institutions perform the foundational securitizing move: they formally frame the continuity of essential services as indispensable to the functioning of vital societal and economic systems, identify a broad range of threats, from natural disasters and terrorism to hybrid attacks and interdependencies (threats such as the 2016 Italian earthquakes or cyber-enabled attacks on Ukraine's electricity grid), and justify the imposition of harmonised resilience obligations across Member States. In securitization terms, the act of legislating constitutes the authoritative speech act that elevates essential service continuity to an existential priority for the Union (European Union 2022b, Recitals 1–3).

At the national legal–institutional level, Member States and their designated competent authorities become secondary securitizing actors. They are required to adopt national strategies, conduct national risk assessments, and identify critical

entities whose disruption would have significant societal effects (European Union 2022b, Arts. 3–6). Through these designations and the domestic translation of EU rules, national authorities reproduce and embed the EU-level securitizing move within their territorial governance structures, thereby extending its authority across multiple administrative and regulatory domains.

At the EU operational level, securitization is further enacted by bodies such as the Critical Entities Resilience Group, which coordinates implementation, develops guidance, and facilitates cross-border information exchange. Although these bodies do not produce binding law, they operationalize and stabilize the securitized framing by shaping how resilience obligations are interpreted, monitored, and integrated into ongoing administrative routines. Their work ensures that the exceptional framing introduced by the EU legislator is sustained through continuous practices of supervision and coordination.

At the national operational level, competent authorities, supervisory bodies, and the critical entities themselves enact securitization through day-to-day compliance activities. National authorities carry out inspections, impose corrective measures, and oversee adherence to resilience obligations, while critical entities implement risk assessments, adopt organisational and physical resilience measures, and report disruptive incidents (European Union 2022b, Arts. 18–21). These practices embed the securitized logic in the routine operations of infrastructure operators, transforming the abstract framing of essential service continuity into concrete organisational and behavioural requirements.

Taken together, the CER Directive establishes a dual-layered securitizing architecture operating across the EU and national levels. The EU institutions initiate and institutionalize securitization through law and high-level coordination, while national authorities and critical entities concretize, implement, and enforce it through regulatory and operational practices. Through this distributed configuration of actors, essential service continuity becomes constructed and maintained as a matter of existential concern for the Union, thereby legitimizing extensive oversight and resilience-building interventions.

Applying securitization theory to the Directive on the resilience of critical entities (CER Directive) shows that the primary audience of the securitizing move is the Member States, which act as the principal legal and political authorities responsible for giving effect to the Directive. Formally, the Directive is "addressed to the Member States" (European Union 2022b, Art. 29), requiring them to transpose its provisions, adopt the necessary national strategies, identify critical entities, and conduct national risk assessments. In securitization-theory terms, their acceptance is juridical and administrative: by incorporating these obligations into domestic law, Member States confirm that essential service continuity constitutes an existential concern that warrants harmonised and intrusive resilience measures.

A second key audience consists of the critical entities themselves, public and private operators directly subject to the obligations set out in Chapter III of the Directive. Article 1(b) stipulates that the Directive "lays down obligations for critical entities" to ensure their ability to provide essential services under all conditions, while Article 6 requires that designated entities be formally notified of their status and informed of the specific obligations applicable to them (European Union 2022b, Arts. 1(b), 6). Operational securitization thus hinges on these entities' acceptance of their elevated role: no longer ordinary service providers, they become actors whose performance is framed as crucial to societal stability, and whose failure could generate cascading and cross-border disruptions.

Finally, the Directive implicitly addresses a broader societal and economic audience, including investors, companies, and service users. Recital 6 emphasises that a resilient system of critical entities fosters "reliance and trust," which are portrayed as essential for a well-functioning internal market. Although this audience does not bear direct obligations, the Directive seeks to reassure it by signalling that essential services are being protected through coordinated resilience measures. In this sense, securitization extends beyond regulatory actors and operators to encompass the wider public whose expectations of stable and reliable essential services underpin societal confidence.

Taken together, the CER Directive establishes a multi-layered audience structure. Member States form the primary legal-political audience responsible for institutionalizing the securitizing move; critical entities constitute the operational audience tasked with implementing resilience obligations; and a broader societal and economic audience represents the diffuse public whose trust the Directive aims to secure. This layered configuration reinforces the Directive's framing of essential service continuity as a matter of existential importance for the European Union.

Applying securitization theory to the NIS2 Directive reveals that the primary referent object is the security and continuity of network and information systems (NIS) that underpin essential and important services across the European Union. Rather than treating cybersecurity as an end in itself, the Directive frames digital infrastructures as indispensable to the functioning of the internal market and to the stability of critical societal and economic activities. Thus, the existential threat is understood as the potential disruption, degradation, or compromise of digital systems whose failure would produce systemic and cross-border effects.

At the value layer, the Directive identifies the functioning of the internal market and the continuity of digitally dependent societal and economic activities as the foundational objects of protection. Article 1(1) explicitly states that the objective is to ensure "a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market" (European Union 2022a, Art. 1(1)). These systemic values, market stability, economic resilience, and the reliability

of essential digital services, constitute the existential goods whose protection justifies harmonised cybersecurity obligations.

At the stakeholder or operator layer, the Directive designates essential entities as indirect referent objects. These include operators in sectors such as energy, transport, banking, digital infrastructure, health, drinking water, ICT services, and public administration (European Union 2022a, Art. 3). Their operations are securitized because their digital dependence renders them pivotal to maintaining societal stability. The failure of these entities to protect or ensure the integrity of their digital systems is framed as a threat that could cascade across multiple sectors.

At the physical–technical layer, the Directive treats network and information systems themselves as the direct operational referent object. Article 6 defines NIS as interconnected digital and data-processing systems whose compromise can undermine confidentiality, integrity, authenticity, and availability (European Union 2022a, Art. 6). The obligations imposed on operators, ranging from risk-management measures to incident reporting (Arts. 20–21), are intended to secure these digital infrastructures as the material substrate through which threats manifest. In securitization terms, it is the vulnerability of these systems that anchors the Directive's logic of exceptional regulatory intervention.

Taken together, the NIS2 Directive constructs a layered referent object centred on the continuity and reliability of digital infrastructures that make essential services possible. At the macro level, the internal market and societal stability constitute the existential values to be safeguarded; at the meso level, essential entities function as operators whose cybersecurity posture is crucial to that protection; and at the micro level, network and information systems form the material basis of securitization. The Directive thus elevates digital continuity to a matter of existential importance for the European Union and legitimizes extensive cybersecurity governance as a necessary response.

## Comparative Analysis of the Referent Object in the CER Directive and NIS2 Directives

A comparative analysis of the Directive on the resilience of critical entities (CER Directive) and the NIS2 Directive through the lens of securitization theory shows that, although both instruments aim to safeguard the continuity of essential societal and economic functions, they construct different referent objects at the core of their respective securitizing logics. In the CER Directive, the primary referent object is the continuity of essential services, including energy, transport, water, health, digital infrastructure, and public administration, whose uninterrupted provision is portrayed as indispensable for vital societal functions and the functioning of the internal market. These essential services constitute the existential values at stake, as their disruption is expected to generate cascading, cross-sectoral consequences.

Supporting this value layer is a secondary referent object: the critical entities responsible for delivering these services. Their organisational and operational resilience is framed as crucial to maintaining societal stability. At the operational level, the CER Directive treats the physical and organisational infrastructures used by these entities as instrumental referent objects, relevant insofar as they enable service continuity.

By contrast, the NIS2 Directive constructs its referent object within a digital and systemic register. Its primary concern is the security and reliability of network and information systems (NIS) that underpin essential and important services across the European Union. The value layer is therefore articulated around the functioning of the internal market and the stability of digitally dependent societal and economic activities, which are increasingly exposed to cyber threats. At the stakeholder layer, the Directive identifies essential entities whose cybersecurity posture directly shapes the integrity and trustworthiness of the wider digital ecosystem. At the operational level, NIS2 focuses on technical infrastructures, such as data-processing systems, electronic communications networks, and ICT platforms, that form the material foundation of digital continuity.

Taken together, the two directives reveal complementary but distinct securitization logics. The CER Directive securitizes the continuity of essential services within the physical and organisational domain, whereas the NIS2 Directive securitizes the digital conditions that enable those services to function. In the CER framework, criticality arises from the potential disruption of vital societal functions; in NIS2, it arises from the compromise of digital infrastructures essential to the internal market. Although both aim to protect the resilience of European society, they identify different layers of the socio-technical system as their core referent objects, producing two parallel yet interconnected forms of securitization: one grounded in physical operational continuity, the other in digital systemic reliability.

## Comparative Analysis of Essential Service Sectors (CER) and Infrastructure Categories (NIS2)

The CER Delegated Regulation defines *essential services* as those necessary to maintain *vital societal functions, economic activity, public safety, and public health*. These essential services are grouped across eleven broad sectors, including energy, transport, digital infrastructure, banking, health, drinking water and wastewater, food, space, public administration, and environmental services such as waste management. The determining factor for inclusion is whether the interruption of these services would generate severe societal or economic consequences. Thus, the CER framework centres on service continuity as the core object of protection, and it identifies sectors according to their societal indispensability.

**TABLE no. 1.** Comparison of Essential Service Sectors under the CER Framework and Critical Digital Infrastructure Categories under NIS2

| Sector/Category | CER Delegated Regulation: Essential Services | NIS2 Directive: Categories of Critical Digital Infrastructure |
|---|---|---|
| **Energy** | Electricity, district heating, oil, and gas are essential for society | Electricity, oil, and gas operators as digital-dependent entities; the network and information systems of energy operators |
| **Transport** | Rail, air, maritime, and road transport services | Transport operators where ICT systems are critical; digital systems supporting air traffic, rail signaling, maritime operations |
| **Digital Infrastructure** | Included as essential services (e.g., IXPs, DNS, cloud under CER list) | A core NIS2 sector: DNS, cloud, data centres, CDNs, trust services, electronic communications networks |
| **Banking & Financial Markets** | Treated as essential services due to economic indispensability | Treated as essential because of cyber risk to financial stability |
| **Health** | Hospitals, medical care, and pharmaceutical supply | Healthcare providers are cyber-dependent entities whose systems must be secured |
| **Drinking Water & Wastewater** | Essential for public health and survival | Included due to reliance on SCADA systems and digital process control |
| **Food** | Production and distribution of essential food products | Not explicitly a NIS2 core digital category unless part of manufacturing with critical ICT systems |
| **Waste Management** | Essential for environmental and public health protection | Covered in NIS2 only indirectly when digital systems are central to waste operations |
| **Public Administration** | Core societal governance functions | Central governments are explicitly included as essential digital entities |
| **Space** | Satellite operations supporting essential services | Included under NIS2 only when space services depend on critical ICT providers (e.g., ground stations) |
| **Environmental & Chemical Sectors** | Essential for safety, environment, and chemical handling | Included in NIS2 manufacturing sectors when cybersecurity risks are high |

The NIS2 Directive, by contrast, identifies sectors not based on the essentiality of physical services, but on the criticality of digital infrastructures and ICT dependencies. The Directive's Annex I (essential entities) and Annex II (important entities) categorize entities whose network and information systems are fundamental to the functioning of the internal market and the resilience of digital-dependent activities. These categories include digital infrastructure (DNS service providers, data centres, cloud computing, content delivery networks), ICT service management, electronic communications networks, as well as sectors such as energy, transport,

drinking water, wastewater, health, banking, financial market infrastructures, and public administration. While there is broad sectoral overlap with CER, NIS2 reframes these sectors through a cybersecurity prism: what becomes "critical" is not the service itself, but the network and information systems that support or operate these services.

The key difference lies in the logic of classification. CER protects *services essential for societal functioning*, regardless of their digital intensity, while NIS2 protects *digital infrastructures and ICT-dependent operators* whose disruption could compromise cybersecurity, market stability, and digital continuity. In many sectors, energy, transport, health, water, and public administration, the same entities appear in both frameworks, yet they are securitized for different reasons. Under CER, they are essential due to their physical and organisational importance for society; under NIS2, they are essential because they rely on digital infrastructures whose compromise can create systemic risks. Thus, while the sectoral scope partially overlaps, the referent objects and mechanisms of criticality differ: CER focuses on essential services as such, whereas NIS2 focuses on the digital networks and infrastructures enabling them.

Although both CER and NIS2 cover many of the same sectors, the rationale behind their inclusion diverges significantly.
This demonstrates that the two directives protect different layers of the European socio-technical system: CER guards the *physical and organisational continuity* of essential services, whereas NIS2 guards the *cybersecurity and integrity of the digital systems* that make those services possible.

## Conclusion

This article examines how the European Union constructs and governs critical infrastructure through securitization processes embedded in two key legislative frameworks: the Directive on the resilience of critical entities (CER Directive) and the NIS2 Directive. Drawing on securitization theory, both in its classical and sociologically expanded forms, the analysis has shown that these instruments articulate distinct yet interconnected securitizing logics that operate across multiple institutional and operational layers.

The CER Directive establishes a securitization dynamic centred on the continuity of essential services, positioning vital societal functions as existential goods whose disruption necessitates harmonised and intrusive resilience measures. This construction foregrounds critical entities and their infrastructures as indispensable intermediaries in the protection of societal stability. In contrast, the NIS2 Directive securitizes the digital conditions underpinning essential services, identifying the security and reliability of network and information systems as the referent object.

Here, the internal market and digital-dependent activities are framed as existentially threatened by cyber incidents, motivating stringent cybersecurity obligations for essential and important entities.

The comparative analysis demonstrates that these directives enact parallel but complementary forms of securitization. The CER Directive addresses vulnerabilities within the physical and organisational domain of essential services, whereas NIS2 targets the digital infrastructures that enable those services to function. Together, the two instruments reveal a layered EU security architecture in which physical continuity and digital integrity are mutually reinforcing dimensions of critical infrastructure resilience. This dual governance structure illustrates how the EU increasingly governs risk not through isolated sectoral measures but through integrated, cross-sectoral frameworks that reflect the material and socio-technical complexity of contemporary infrastructure systems.

More broadly, the findings contribute to securitization theory by showing how security logics extend beyond discursive acts into regulatory practices, technical standards, and institutional routines. The directives illustrate how threats are constructed, circulated, and operationalized through legal instruments, administrative procedures, and requirements imposed on public and private operators. They also underscore the need for securitization scholarship to account for the material agency of infrastructures and the centrality of socio-technical systems in contemporary modes of governance.

The analysis of the CER and NIS2 Directives also carries important implications for the Member States, whose role is central in operationalizing the EU's dual securitization logic. At the practical level, Member States must translate the legal framing of essential service continuity and digital-system integrity into coherent national strategies, institutional reforms, and sector-specific regulatory measures. This requires strengthening national risk-assessment capacities, improving cooperation between civil, military, and private actors, and ensuring that competent authorities possess sufficient technical expertise and resources to supervise compliance.

In sum, the CER and NIS2 Directives demonstrate that the EU's approach to critical infrastructure is marked by a multi-layered, multi-level, and materially grounded securitization process. By differentiating yet interlocking the protection of essential services and digital infrastructures, the EU constructs resilience as both a physical and a cyber-systemic imperative. This analysis highlights not only the growing complexity of critical infrastructure governance but also the expanding scope of securitization as a framework for understanding how modern polities define, prioritise, and protect what they deem existential to their societal and economic order.

## References

**Aradau, Claudia.** 2010. "Security That Matters: Critical Infrastructure and Objects of Protection." *Security Dialogue* 41 (5): 491–514. https://doi.org/10.1177/0967010610382687.

**Balzacq, Thierry.** 2011. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1–30. London: Routledge.

**___.** 2019. *Securitization Theory: Past, Present, and Future*. London: Routledge.

**Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka.** 2016. "Securitization: Toward a Theory of the Making of Security." *European Journal of International Relations* 22 (4): 493–516.

**Buzan, Barry, Ole Wæver, and Jaap de Wilde.** 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

**European Union.** 2022a. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*.

**___.** 2022b. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*.

**European Commission.** 2024. Commission Delegated Regulation (EU) 2023/503 supplementing Directive (EU) 2022/2557 by establishing a list of essential services. *Official Journal of the European Union*.

**Stritzel, Holger.** 2014. *Security in Translation: Securitization Theory and the Localization of Threat*. London: Palgrave Macmillan.

**Taureck, Rita.** 2006. "Securitization Theory and Securitization Studies." *Journal of International Relations and Development* 9 (1): 53–61.

**Taureck, Rita.** 2006. "Securitization – An Analytical Tool." In *Approaches to Security*, edited by Kai Michael Kenkel, 53–72. London: Routledge. *(If needed; optional depending on whether both texts were used.)*

**Wæver, Ole.** 1995. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz, 46–86. New York: Columbia University Press.