Systemy Logistyczne Wojsk
Zeszyt 65(2026)
s.85 -114

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna w Warszawie

Military Logistics Systems
Volume 65(2026)
pp. 85-114

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology in Warsaw

DOI: 10.37055/slw/242081
Article type: Original research article

ISSN 1508-5430
eISSN 2719-7689

FROM INFRASTRUCTURE PROTECTION TO THE CONTINUITY OF ESSENTIAL SERVICES: EU POLICY ON INTERDEPENDENCE AND SUPPLY CHAINS

Krzysztof Szwarc
krzysztof.szwarc@wat.edu.pl; ORCID: 0000-0002-5964-691X
Military University of Technology in Warsaw, Poland
(Corresponding author)

Michał Wiśniewski
michal.wisniewski@pw.edu.pl; ORCID: 0000-0003-3435-3114
Warsaw University of Technology, Poland

Witold Skomra
witold.skomra@pw.edu.pl; ORCID: 0000-0002-2625-6683
Warsaw University of Technology, Poland

Abstract.
The growing dependence of states and societies on uninterrupted services, complex supply chains, and digitally connected infrastructures makes the continuity of essential services a key security and management problem. The research gap addressed in this article is the insufficient integration of the regulatory perspective with the service, logistics, and interdependency perspectives in studies on critical infrastructure protection in the EU. The purpose of the research was to assess how changes in EU policy affect the protection of critical infrastructure and the continuity of essential services in interdependent operational environments. The study was guided by research questions concerning the evolution of the EU governance model for critical infrastructure (CI) protection and essential services (ES) continuity, expert assessments of the current regulatory framework, the operationalisation of interdependencies and cascading risks, and methods for identifying interdependencies and assessing risk and resilience. The results show a clear shift from protecting single assets to ensuring service continuity, a stronger regulatory recognition of cascading, systemic, and cross-border risks, and a dynamic but methodologically fragmented research field. The conclusions indicate the need for network-level risk management

methods, better support for operators, and stronger integration of management and security perspectives. The research highlights an asymmetry between the issue of interdependence and systemic risk in EU policies and regulations, and the availability of methods for identifying interdependencies and carrying out joint risk assessments within networks of independent system operators.

Keywords:
critical infrastructure; essential services; supply chain continuity; protection policy; resilience

Introduction

The security of modern economies and societies increasingly depends on logistics systems' ability to ensure business continuity. In the face of geopolitical tensions, armed conflicts, disasters, technical failures, and cyber incidents, a nation's stability is no longer determined solely by the protection of individual facilities, but by the efficiency of entire supply, production, transport, storage, distribution, and data exchange systems. From this perspective, security has a distinct logistical dimension: it signifies the ability to sustain key flows and functions despite disruptions.

In this context, the management of the security of critical infrastructure (CI) and essential services (ES) in the European Union (EU) takes on particular significance. EU policy is shifting from protecting individual assets deemed critical to protecting the functions, processes, and services essential to citizens, the economy, and the state. From a systems logistics perspective, this means shifting the focus from protecting a facility to ensuring continuity of service delivery across the entire organisational ecosystem, including the operator, its suppliers, subcontractors, infrastructure partners, and digital service providers. In this context, the security of the ES should be understood as the ability to maintain operational continuity at an acceptable level of quality despite disruptions.

Adopting this perspective changes the way we understand risk. Disruption analysis cannot be limited to a single organisation, as the effects of a failure manifest throughout the entire value chain, from the sources of raw materials and components, through processing, transport, and storage, to distribution to the end user. Therefore, identifying critical entities requires taking into account not only the facility's criticality, but also its role in the supply chain or network, the scale of cross-border interdependencies, and the possibility of substituting a given supplier or service. This direction is evident in the Critical Entities Resilience Directive (CER Directive), Network and Information Systems Directive 2 (NIS2), and Digital Operational Resilience Act (DORA), but it still does not fully resolve the issue of methodically managing interdependencies among ES operators.

The purpose of this article is to assess how the evolution of EU policy in the area of CI protection affects the way in which the continuity of ES is ensured in the context of growing intersectoral, cross-border, digital, and supply-chain interdependencies. The research problem specifically concerns whether the transition from a model focused on the protection of individual assets to one oriented towards

service continuity is accompanied by the development of sufficient mechanisms to identify and manage interdependencies and cascading effects.

On this basis, the overarching research question was formulated as follows. How does the evolution of the EU model for managing CI protection and the continuity of ES address growing interdependencies, cascading effects, and supply chain dependencies, and what are the implications for assessing and strengthening resilience?

Answering the overarching research question requires addressing specific questions concerning:

Q1. How has the model for managing the protection of CI and ES evolved in EU policy and regulations?

Q2. How do experts in the field of CI and ES security assess the strengths and weaknesses of the current EU regulatory framework, as well as the opportunities and threats associated with its implementation?

Q3. To what extent does the current EU regulatory framework recognise interdependencies and the resulting cascading effects?

Q4. What methods, tools, and approaches described in the literature can support the identification of interdependencies and the assessment of risk and resilience?

Literature Review

A structured scoping review combined with bibliometric mapping and targeted thematic synthesis was conducted to identify the main issues emerging in the academic discourse. This design follows the broad literature-review typology discussed by Snyder (2019), but it is reported here as a scoping and bibliometric review rather than as an exhaustive systematic review. The selection of articles relevant to the study focused on constructing a search query that included various terms, synonyms, and abbreviations related to CI and ES, business continuity, and interdependencies. The selection of keywords was based on the scoping study approach (Arksey and O'Malley 2005).

The literature search was conducted using the Web of Science Core Collection (WoSCC) and Scopus scientific databases. A description of the procedure used to construct the bibliometric corpus, together with the search queries and derived bibliometric data, has been made available as a dataset (Skomra et al. 2026).

The purpose of this analysis was to define the scope and structure of the field and to identify the publications most relevant to Q4, rather than to conduct an exhaustive systematic review. The Global Citation Score (GCS) was calculated to identify groundbreaking publications (Knoke and Yang 2008). To capture the latest research with a potentially significant impact on the evolution of approaches to the protection of CI and ES, articles were ranked by the number of citations divided by the number of years that have elapsed since the year of publication. This allowed us to identify works with a potentially low GCS that have, however, recently gained significant attention from the scientific community.

An analysis of keyword co-occurrence networks (Lou and Qiu 2014) was conducted. The identified network of relationships divides the analysed body of work into thematic clusters. This allows for the identification of dominant research topics and the detection of knowledge gaps.

Table 1 ranks ten highly cited publications in the bibliometric corpus to identify influential and recent research relevant to interdependencies, business continuity, CI and ES.

Table 1. Ranking of 10 highly cited publications in the bibliometric corpus, including the time-normalised citation rate

Paper	Number of citations	Time-normalised citations per year
(Hosseini et al. 2016)	1792	163
(Linnenluecke 2017)	1373	137
(Ghobakhloo et al. 2025)	161	81
(Aljohani 2023)"container-title":"Sustainability"",""DOI":"10.3390/su152015088"",""ISSN":"-2071-1050"",""issue":"20"",""journalAbbreviation":"Sustainability"",""language":"en"",""page":"15088"",""source":"DOI.org (Crossref	311	78
(Sun et al. 2020)	436	62
(Leng et al. 2023)	249	62
(Gu and Liu 2025)	95	48
(Annarelli and Nonino 2016)	481	44
(Bui et al. 2021)	247	41
(Zio 2018)	369	41

Source: own elaboration based on the bibliometric dataset (Skomra et al. 2026)

The next stage of the study involved creating a map of the relationships between the keywords. The analysis included both keywords identified by the authors and those indexed by the SCOPUS database. Both sets were analysed together. The minimum number of keyword occurrences was set in accordance with proposals tested in previous studies (Ciano et al. 2019). The entry criterion was set at five occurrences of a given keyword. The total number of keywords in the analysed set of publications was 3,705. Using VOSviewer, a network (Figure 1) was generated comprising 186 nodes and six clusters (Table 2).

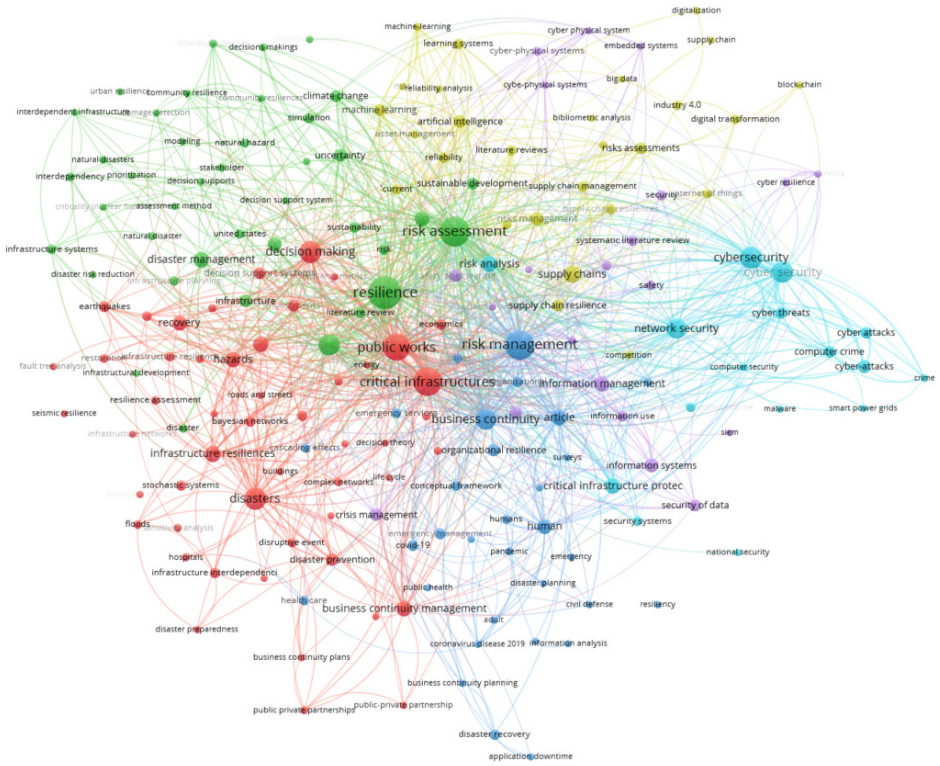


Figure 1. Co-occurrence network of author keywords (minimum occurrence threshold: five), generated in VOSviewer

Source: own elaboration based on the bibliometric dataset (Skomra et al. 2026)

Table 2. Clusters based on the keywords discovered in VOSviewer

Cluster	Colour	Cluster name
Cluster 1	red	Conceptualisation of resilience
Cluster 2	green	Impact of natural hazards on CI resilience
Cluster 3	blue	Impact of cyber threats on CI resilience
Cluster 4	yellow	CI security and resilience management
Cluster 5	violet	Business continuity management
Cluster 6	light blue	State of research on critical infrastructure

Source: own elaboration based on the bibliometric dataset (Skomra et al. 2026)

The thematic synthesis presented here is based on the 24 publications most relevant to the research problem, identified through citation rankings and thematic cluster analysis. Publications were selected on the basis of their direct relevance to Q4 and at least one of the analytical domains: CI and ES interdependencies, cascading and systemic effects, systems-of-systems approaches, network-level resilience, inter-organisational continuity management, and methods for mapping and assessing dependencies. It should therefore be understood as an analytical subset intended for substantive interpretation rather than an exhaustive thematic analysis of the entire bibliometric corpus.

Recent literature on the subject shows a clear shift away from viewing information security solely through the lens of protecting individual assets, towards an approach focused on service continuity within complex interdependent systems. A key reference point for this approach is the work of Petit et al. (2018), in which the authors argue that interdependencies should be integrated into risk and business continuity management processes and that CI itself should be analysed as a system of systems (SoS). This implies the need to expand the scope of analysis beyond a single facility to encompass relationships among entities, resources, processes, and services. From a SoS perspective, resilience is an emergent property of interactions among operationally autonomous constituent systems.

Interdependencies should also be distinguished analytically from cascading effects. Interdependencies describe structural, functional, informational, geographic, organisational, or logical relationships among infrastructures and service providers, whereas cascading effects concern the propagation of disruption through those relationships. The foundational classification proposed by Rinaldi et al. (2001), and subsequent modelling work by Dudenhoeffer et al. (2006) and Lee et al. (2007), established a basis for identifying dependency chains and analysing how failures can spread across systems. Recent reviews show that this research has advanced towards multilayer and network-level representations of infrastructure resilience, while data availability, uncertainty, model validation, and the representation of real operational dependencies remain significant limitations (Tong et al. 2025, Ghasemkhani et al. 2026).

The topic of interdependence was further explored in research on the resilience of critical entities in the context of the CER Directive (Rehak, Splichalova, Janeckova, et al. 2024). The authors proposed the CERA method, which enables a semi-quantitative assessment of the resilience of both the entity itself and the infrastructure it operates. In turn, the paper by Rehak, Splichalova, Hromada, et al. (2024) discusses the CERFI tool, which is used to identify the breaking point of a critical entity's resilience in relation to threat intensity and protective capabilities. This research is further developed in the study by Rehak et al. (2025), which classified 161 tools for strengthening the resilience of critical entities. Collectively, these studies have significant practical implications, as they translate general regulatory requirements

into tools for diagnosis and management improvement. At the same time, they focus primarily on the level of the individual entity, addressing coordination within networks of interdependent ES operators only to a lesser extent.

At the network level, recent methods increasingly combine graph representations with dynamic and probabilistic modelling. Schneider et al. (2025)such as floods or storms, can disrupt multiple critical infrastructures at once. In addition, a localized failure of one service can trigger a cascade of failures of other dependent services. This makes it challenging to anticipate and prepare adequately for direct and indirect consequences of such events. Existing methods that are spatially explicit and consider service dependencies currently lack practicality, as they require large amounts of data. To address this gap, we propose a novel method called\n DISruption-Map\n which analyzes complex disruptions to critical infrastructure services. The proposed method combines (i propose Dependent Infrastructure Service Disruption Mapping (DISruptionMap) to trace cascading service disruptions through dependency chains. Faraji et al. (2026)forming complex dependency networks where disruptions can propagate across sectors and amplify systemic risk. Conventional risk assessment methods are limited by evaluating components in isolation and neglecting how interdependencies shape cascading exposure. This paper introduces the Risk Impact Pathway Analysis (RIPA develop Risk Impact Pathway Analysis (RIPA) for dynamic risk assessment in interdependent CI networks, while Tong et al. (2025) combine Fault Tree analysis and Dynamic Bayesian Networks to assess resilience performance under propagated failures. These approaches complement semi-quantitative entity-level tools such as CERA and CERFI by making the propagation mechanism itself an object of analysis. Their practical use in networks of autonomous ES operators nevertheless depends on the availability of sufficiently detailed dependency data and on arrangements that allow such data to be exchanged across organisational and sectoral boundaries.

A major area of research also focuses on cyber resilience and the systemic nature of risk in digitally connected environments (Rios et al. 2023). The authors presented the DYNABIC concept, a framework for dynamic IT business continuity based on adaptation, automated response, collaboration, risk assessment, and continuous improvement. The value of this proposal lies in combining the business continuity perspective with cybersecurity and in accounting for cascading effects in multi-tiered environments. In turn, Aghazadeh Ardebili et al. (2024)their exposure to cyber threats has grown significantly. The complex and hyper-connected nature of these systems presents challenges for enhancing cyber resilience against adverse conditions, stresses, attacks, or compromises on cybersecurity resources. Integrating risk assessment with cyber resilience allows for adaptive approaches that can effectively safeguard critical infrastructures (CIs demonstrate that effective information and communication technology (ICT) cyber resilience requires integrating risk assessment methods, standards, and governance mechanisms. This picture is

complemented by the framework for systemic risk (Assenza et al. 2024). The authors point out that in highly networked environments, cyber risk is inherently shared, and its materialisation can rapidly propagate disruptions across supply chains and the ES. It is particularly important here to shift the focus from the risk of a single organisation to systemic risk, which requires inter-organisational coordination, a common conceptual language, and agreed-upon management practices.

Another important aspect of the literature concerns the challenge of implementing new EU regulations (Mentzelou et al. 2025)placing new demands on both essential and important entities. Despite its importance, organizations face multiple barriers that undermine compliance, including lack of awareness, technical complexity, financial constraints, and regulatory uncertainty. This study identifies and models these barriers to provide a clearer view of the systemic challenges of NIS2 implementation. Building on a structured literature review, fourteen barriers were defined and validated through expert input. The Decision-Making Trial and Evaluation Laboratory (DEMATEL. The authors identify barriers to compliance with the NIS2 Directive, pointing primarily to a lack of awareness, technical complexity, financial constraints, and regulatory uncertainty. The use of the DEMATEL method enabled the authors to demonstrate interdependencies among these barriers and distinguish causal factors from organisational effects, such as operational disruptions, high reporting costs, and inadequate risk assessment.

The network perspective is also increasingly visible in continuity-management research. Hassel and Cedergren (2024) argue that business continuity management, traditionally centred on a single organisation, is insufficient where critical societal functions are jointly delivered by networks of interdependent actors. The proposed multiactor perspective extends business impact analysis beyond the focal organisation by identifying ES, shared resources, upstream and downstream dependencies, and continuity measures whose effectiveness should be assessed for the wider actor network. This is particularly relevant to ES because service continuity may depend on autonomous suppliers, infrastructure partners, digital providers, and public authorities operating under different governance and regulatory arrangements. Inter-organisational continuity management therefore provides a bridge between organisational BCM and network-level resilience analysis.

Taken together, the literature identifies several complementary families of methods for mapping and assessing dependencies:

- network and multilayer graph models for representing structural relationships,
- network-flow, simulation, agent-based, and system-dynamics approaches for analysing propagation and recovery,
- probabilistic methods such as Bayesian and Dynamic Bayesian Networks for representing uncertainty and conditional failure,
- semi-quantitative resilience-assessment tools such as CERA and CERFI,

- service-disruption and dependency-mapping methods such as DISruptionMap and RIPA,
- business-impact/scenario approaches that can be extended to multiactor continuity management.

The literature highlights the fragmentation of available methods. Many tools support the assessment of individual entities' resilience, whereas network-oriented approaches frequently focus on technical infrastructures, specific sectors, or data-intensive models. Recent studies demonstrate that methods for mapping dependencies, cascading effects, and network resilience do exist. Therefore, the research gap should not be understood as an absence of methods. Rather, it concerns their integration and operationalisation for networks of autonomous ES operators, where joint assessment must combine service criticality, inter-operator and supply-chain dependencies, partner substitutability, uncertainty, information-sharing constraints, and cross-sector governance.

Methodology

Table 3 shows the relationship between the research questions and the methods used. Figure 2 provides an overview of the study.

Table 3. Relationship between research questions and research methods

Research question and method	Rationale for the Choice of Method	Principal empirical corpus	Evidence	Analytical procedure	Limitations	**Reporting of findings**
Q1 Desk research; regulatory analysis	Role: Reconstructing changes in the scope of protection, the obligations of entities, and risk management mechanisms. Rationale: This method allows for a comparison of successive generations of EU regulations and helps identify the direction of the shift from asset protection to service continuity and resilience.	EU legal acts and institutional documents concerning CI and ES, particularly EPCIP, NIS, NIS2, CER and DORA, together with documents on civil protection mechanisms and electronic communications	Object of protection; criteria for identifying critical entities; obligations of Member States and operators; requirements concerning risk management, business continuity, reporting and cross-border cooperation	Document identification → extraction of relevant provisions → coding by analytical category → comparison of successive regulatory frameworks → identification of the direction of change in the protection model	Reliance on public sources; lack of access to classified information, operator documentation, and national business continuity plans	Results
Q2 Qualitative expert CAWI survey; SWOT analysis	Role: Identification of practical assessments and interpretations of regulations. Rationale: It allows the normative analysis to be supplemented with perspectives from the administration, CI operators, and the academic community; open-ended questions make it possible to capture issues not addressed by closed-ended measurement scales.	Three groups of six respondents: public administration representatives, CI operators and academic experts	Responses to four open-ended questions concerning the strengths, weaknesses, opportunities and threats associated with CER, NIS2 and DORA	Anonymous data collection → grouping of semantically similar statements → comparison across the three respondent groups → synthesis of expert assessments	A small, purposive sample; lack of statistical representativeness; the results reflect expert assessments rather than the prevalence of problems in the population	Results; Table 4

Table 3 (continued)

Research question and method	Rationale for the Choice of Method	Principal empirical corpus	Evidence	Analytical procedure	Limitations	**Reporting of findings**
Q3 Desk research; regulatory analysis; case study analysis;	Role: A comparison of the normative conception of interdependencies with their actual manifestations. Rationale: Combining both methods makes it possible to verify whether the interdependencies defined in regulations correspond to the mechanisms observed during actual disruptions.	EU legal acts and documents: EPCIP, NIS, NIS2, CER and DORA; publicly available material concerning six incidents presented in Table 5	Provisions addressing interdependencies, cascading effects, systemic risk, supply chains, substitutability and cross-border cooperation; causes, course and consequences of incidents and the interdependencies revealed	Extraction of regulatory references → reconstruction of the causes and consequences of the cases → classification of interdependency types using categories established in the literature → comparison of regulatory recognition with operational manifestations of interdependencies	Purposeful selection of cases; use of public materials only; varying levels of detail in the documentation across cases; the cases serve an illustrative rather than a representative purpose	Results; Tables 5–6
Q4 Structured scoping review; bibliometric analysis; bibliometric mapping;	Role: Defining the structure of the research field and identifying families of methods. Rationale: Combining a scoping review with bibliometrics allows for both a broad overview of the field and an in-depth analysis of methods without claiming the comprehensiveness typical of a systematic review.	Scopus and WoSCC data: 553 records forming the bibliometric corpus; 24 publications relevant to the research problem selected for in-depth thematic synthesis	Methods reported in the literature for identifying interdependencies and assessing risk and resilience; citation counts; time-normalised citation rates; keywords	Database searching → consolidation and deduplication → keyword co-occurrence mapping in VOSviewer → cluster identification → targeted thematic synthesis of methods and tools	Results depend on databases, search terms, and terminology; bibliometric analysis does not measure the quality of methods; the 24 publications constitute a deliberately selected analytical subset, not a full systematic review.	Literature Review: Figure 1, Tables 1–2 and synthesis of methods; Results; synthesis of the answer to Q4 in the Discussion

Source: own elaboration

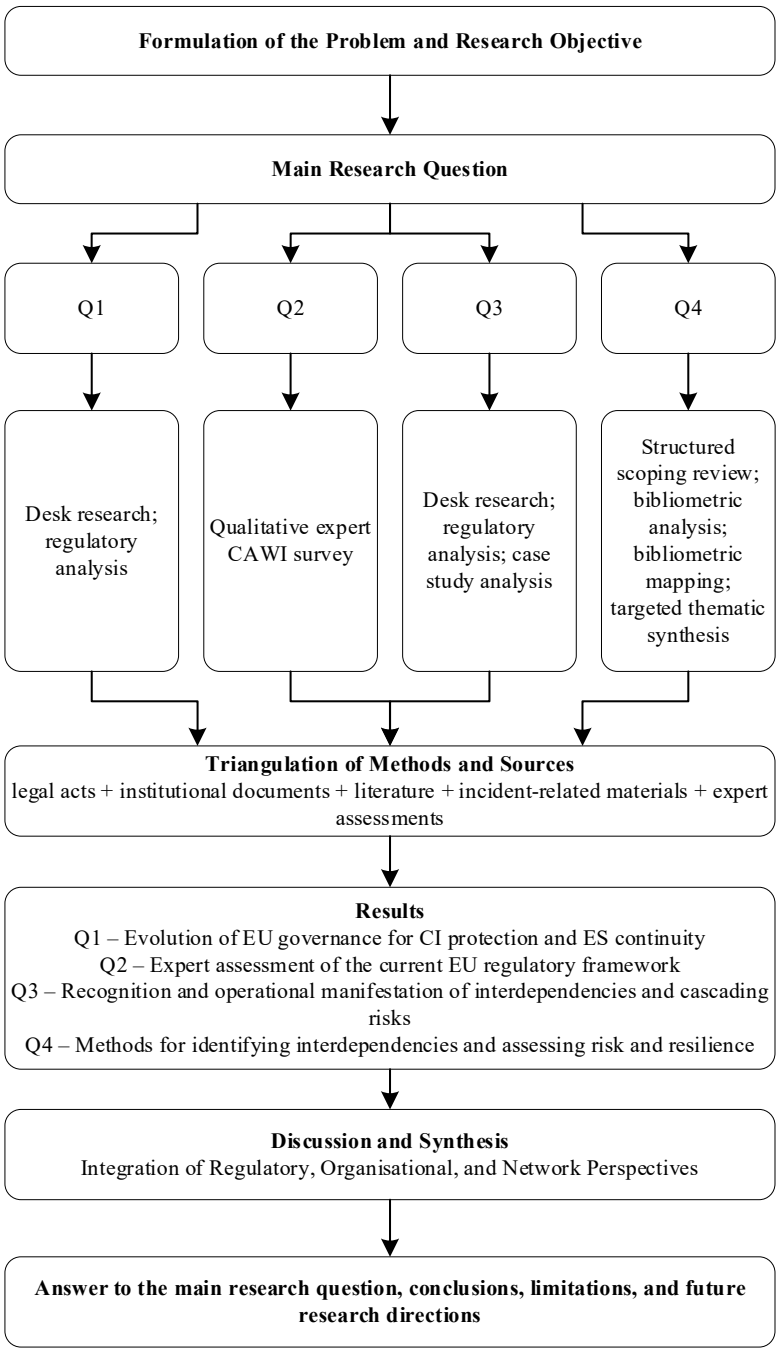


Figure 2. Overall multi-method research design
Source: own elaboration

The methods were integrated at the stage of results interpretation. The regulatory analysis was used to reconstruct the evolution of the CI protection and ES continuity model and to determine how interdependencies were addressed in EU regulations. The computer-assisted web interviewing (CAWI) survey provided expert assessments of the consequences of implementing the regulatory framework, while the case-study analysis enabled comparison between the normative treatment of interdependencies and the mechanisms observed in actual disruptions. The structured scoping review and bibliometric analysis were used to identify methods and tools for analysing interdependencies, risk and resilience. The findings were not aggregated as equivalent data; instead, they were integrated during the synthesis stage to assess their convergence, complementarity and divergence. Regulatory recognition of interdependencies was compared with their manifestations in the analysed incidents, regulatory requirements were compared with expert assessments, and the issues identified in the case studies were compared with methods reported in the literature. Methodological triangulation involved comparison of findings from the regulatory analysis, case studies, literature review and expert survey, while source triangulation involved comparison of EU legal and institutional documents, academic publications, publicly available incident materials and expert assessments. Interpretations were considered better supported when similar conclusions emerged from different methods or independent categories of sources.

The purpose of the desk research (Babbie 2016) was to reconstruct the evolution of the EU approach to CI protection, determine the scope of obligations imposed on **EU Member States and regulated entities**, and identify how EU regulations addressed sectoral, cross-border, digital and supply-chain interdependencies.

The scope of the analysis included EU legal acts and institutional documents concerning CI protection, cybersecurity, the resilience of ES, business continuity and the digital operational resilience of the financial sector. The analysis included European Commission documents, materials available in the EUR-Lex database, and documents issued by specialised institutions dealing with cybersecurity and CI protection, including European Union Agency for Cybersecurity (ENISA).

The regulatory scope of the study was primarily limited to the EU civilian regimes governing CI, ES, cybersecurity and digital operational resilience, in particular European Programme for Critical Infrastructure Protection (EPCIP), NIS/NIS2, CER and DORA. The analysis did not assume that defence-related infrastructure and activities are regulated by these instruments in the same manner as civilian CI and ES providers. Accordingly, references to military logistics and total defence were treated as analytical and operational implications of the identified interdependencies, particularly where defence capabilities depend on civilian ES, dual-use infrastructure, commercial supply chains or cross-border service networks, rather than as evidence of the direct applicability of the examined regulatory regimes to defence infrastructure.

A multiple-case study method (Yin 2012) was used to illustrate the practical significance of interdependencies for CI security and the continuity of ES and to compare the regulatory recognition of interdependencies with their operational manifestations. Six incidents were analysed. The documentary sources used for each case are specified in Table 5. The cases were selected purposively according to three criteria:

- the incident affected a sector or service important to the functioning of the state, economy or society,
- its consequences extended beyond the infrastructure or organisation directly affected and revealed inter-organisational, intersectoral or cross-border dependencies,
- sufficiently reliable public documentation was available to reconstruct the causes, course and consequences of the disruption.

The case analysis was conducted in four stages. First, the documentary material for each of the six cases was collected and reviewed against the case-selection criteria. Second, the causal sequence and operational context of each incident were reconstructed, including the initiating event, the directly affected infrastructure or service, the subsequent disruptions and the dependencies among infrastructure, service providers, suppliers and end users revealed by the incident. Third, the identified relationships and effects were classified using the categories of infrastructure interdependencies established in the literature. Fourth, a cross-case comparative synthesis was conducted using the same analytical dimensions for all six cases. Recurring and case-specific patterns were then identified and compared with the EU regulatory framework's treatment of interdependencies and cascading risks.

To complement the regulatory and case-study analyses, a qualitative expert survey was conducted using CAWI (Lozar Manfreda et al. 2002). The aim of this component was not to obtain statistically representative results but to collect structured expert assessments of the strengths, weaknesses, opportunities, and threats associated with the implementation of the CER Directive, the NIS2 Directive, and the DORA Regulation in the context of CI protection and ES continuity. The survey questionnaire was distributed to respondents, and the results obtained have been made available as a dataset (Skomra et al. 2026). The questionnaire was distributed via Microsoft Forms from 1 December 2024 to 28 February 2025.

The respondent group consisted of 18 experts divided into three analytical categories. The first group included six representatives of public authorities involved in the transposition or implementation of EU regulations in the area of CI, cybersecurity, civil protection, or crisis management. These respondents represented Poland, Austria, Croatia, Germany, Finland, and Ireland and were approached during the Organisation for Economic Co-operation and Development (OECD) High-Level Risk Forum held on 16 December 2024. The second group consisted

of six representatives of CI operators responsible for applying national security requirements at the organisational or facility level. They were contacted through the Government Centre for Security. The third group consisted of six academic experts specialising in security studies, legal sciences, CI protection, civil protection, or crisis management. They were identified based on academic output available in the knowledge bases of the Military University of Technology and the Warsaw University of Technology.

The CAWI survey was non-interventional and focused exclusively on expert assessments of the CER, NIS2, and DORA regulations. Before responding, participants were informed about the purpose of the survey, the institutions conducting it, and the planned use of their responses for publication. The form included a statement that completing it constituted consent to participate in the study and to the use of the responses for publication purposes. The data exported from MS Forms did not include respondents' names or email addresses, and responses were identified by ID codes in the analysis. The survey did not require respondents to provide personal data, classified information, or detailed information regarding vulnerabilities, security measures, or other operationally sensitive aspects of the functioning of critical infrastructure or essential services.

The qualitative responses were analysed using a coding procedure. Meaning units expressing similar issues were assigned provisional descriptive codes, and codes with overlapping or synonymous meanings were subsequently compared and merged into broader thematic categories. The final categories were therefore not defined in advance, but were developed from recurring patterns in the respondents' statements. To prevent more extensive responses from disproportionately influencing the synthesis, each thematic category was counted no more than once per respondent, irrespective of how many times the same issue was mentioned in that respondent's answer.

The coded responses were also analysed across the three expert categories to determine whether the main themes reflected materially different assessments. No consistent or analytically meaningful patterns of divergence were identified between public authorities, CI operators, and academic experts. Given the small, purposively selected subgroups and the qualitative nature of the study, the results are presented at the level of the entire expert sample rather than as separate subgroup comparisons.

Results

The regulatory analysis indicates that the EU governance model for CI and ES protection has evolved through successive and partly overlapping stages. EPCIP established an asset- and sector-based framework focused primarily on identifying and protecting CI and on cooperation between Member States. The NIS Directive introduced a stronger service-oriented and cybersecurity perspective, while NIS2 broadened the range of covered entities and strengthened requirements for risk

management, incident reporting, and supply chain security. The CER Directive further shifted the regulatory focus towards the resilience of critical entities and the continuity of essential services, including greater attention to cross-sectoral and cross-border dependencies. DORA complements this development with a sector-specific operational resilience framework that addresses, among other issues, dependencies on external third-party ICT providers and concentration risk. Taken together, these changes demonstrate a gradual transition from the protection of individual critical assets towards the continuity and resilience of services delivered through interdependent organisational, digital and supply-chain networks.

The survey assessed expert views on the impacts of implementing the CER and NIS2 Directives and the DORA Regulation (Table 4).

Table 4. Results of the analysis of the NIS2, CER, and DORA regulations based on survey data

Thematic category	Frequency (n = 18)	Relationship to regulatory analysis and the literature	Significance for the original contribution of the study
Increased resilience and security of CI/ES	9/18	Strong alignment with the stated objectives of CER, NIS2 and DORA	Empirical confirmation of the direction of regulatory change
Harmonisation of requirements and common EU standards	8/18	Directly consistent with the legal analysis indicating the harmonising nature of the new regulatory framework	Empirical confirmation that harmonisation is perceived as a practical benefit
Enhanced cooperation and information sharing	6/18	The regulatory framework establishes cooperation mechanisms, while the experts emphasise the importance of existing institutional capacities	Extends the regulatory analysis by demonstrating the importance of pre-existing cooperation structures
Improved risk management and corporate governance	6/18	Closely linked to obligations arising particularly from NIS2 and DORA	Empirical confirmation of changes in managerial accountability and organisational priorities
Supply-chain security as a new area of management	4/18	Directly consistent with NIS2 requirements and the broader direction of CER and DORA	Empirical confirmation that protection is shifting from the individual operator towards networks of entities jointly delivering a service
Costs and organisational burden	9/18	The issue has been partly identified in the literature on NIS2 implementation	Confirmation of a recognised implementation barrier

Table 4 (continued)

Thematic category	Frequency (n = 18)	Relationship to regulatory analysis and the literature	Significance for the original contribution of the study
Compliance formalism	6/18	The issue does not arise directly from the normative content of CER/NIS2/DORA; it reveals a potential consequence of the way in which the framework is implemented	Original contribution – formal compliance does not necessarily equate to an increase in actual resilience
Transposition delays and implementation uncertainty	6/18	The legal analysis identifies obligations and deadlines but does not capture the experience of entities awaiting national implementing measures	Original contribution – identifies a time lag between the adoption of EU rules and the achievement of operational effects
Transfer of costs and requirements to suppliers	5/18	The regulatory framework requires supply-chain risk management, but legal documents give limited attention to the possibility that compliance may alter the structure of the supplier market	Original contribution – regulation may indirectly reduce supplier substitutability and thereby create new dependencies or concentration risk
Inconsistent interpretations and insufficiently specific standards	4/18	Extends the issue, identified in the legal analysis, of national implementation and the operationalisation of general requirements	Demonstrates the distinction between normative harmonisation and operational harmonisation
Coordination problems across entities and sectors	3/18	Directly linked to the gap in managing interdependencies across networks of autonomous entities	A significant original finding linking Q2 with Q3 and Q4: regulating the obligations of individual entities does not in itself ensure coordination at network level
Skills gaps and shortages of specialists	4/18	Consistent with implementation barriers identified in the literature	Empirical confirmation of findings reported in the literature
Existing national security-of-supply mechanisms	2/18	The issue is reflected in the analysis of EU regulation	Empirical confirmation that implementation effectiveness may depend on pre-existing national structures and cooperation practices

Source: own elaboration based on the expert survey data (Skomra et al. 2026)

The issue of ES interdependence is not merely theoretical (Table 5).

Table 5. Examples of the effects of interdependencies on CI security

Incident	Initiating event	Types of interdependencies
Ice Storm, 1998, Canada (Chang et al. 2007)	Several waves of freezing rain damaged power distribution and transmission systems	Physical interdependence (power outages affected services such as emergency response, finance, food and water supply, healthcare, administration, transport and telecommunications) Geographic interdependence (results from the location of the disaster and the structure of the country's power system) Social interdependence (approximately 16% of the population was without power for hours, days or weeks)
The Buncefield Explosion, 2005, UK (Buncefield Major Incident Investigation Board 2008)	Explosion at the oil depot	Geographic interdependence (the explosion caused physical damage to numerous facilities, including IT infrastructure. Some roads were closed for months. According to estimates, local business losses were estimated at approximately £70 million). Physical interdependence (almost half of Heathrow Airport's fuel came from the depot).
Blackout, 2003, USA-Canada (U.S.-Canada Power System Outage Task Force 2004, Andersson et al. 2005)	Overloading of the network due to contact of the high-voltage line with the tree and defects in the control system	Social interdependence (power outages affected about 50 million citizens in both countries). Physical interdependence (reduced water pressure in water-supply networks in many cities; unavailability of telecommunications services due to power outages; restrictions on radio and television broadcasting - emergency power supply. Problems with cooling in homes and office/service areas. Disruption of transport services - electrically powered locomotives and signal systems. Closure of airports in the region - need to redirect flights to other airports. Logical interdependence (overloading of the telecommunications network and consequent disruption of its operation)
Disruption to urban bicycle-sharing services, 2013, Poland (Skomra 2021)	Flooding in Saxony, Brandenburg and Bavaria.	Information interdependence (the servers supporting the city bike-sharing service in many Polish metropolitan areas were located in Leipzig. As a result of the flood, the server room was inundated, and the service was unavailable in Poland.)
Disruption of telecommunications services, 2019, Poland (Skomra 2021)	Fire in a vegetable wholesaler	Geographic interdependence (smoke from a burning building was sucked into the air conditioning of a server room owned by a telecommunications company. The destroyed computers led to a reduction in the scope of service provision). Logical interdependence (the telecommunications disruption affected several sectors, including transport and finance).

Table 5 (continued)

Incident	Initiating event	Types of interdependencies
Reduction in fertiliser production, 2022, Poland (Polska Federacja Producentów Żywności Związek Pracodawców 2022)	Increase in electricity and gas prices; business decision to reduce production	Physical interdependence (in the production of fertilisers, carbon dioxide used in food and beverage production is a by-product of fertiliser production. As a result of the disruption of the supply of carbon dioxide, many food manufacturers **announced that they would cease** production.

Source: own elaboration

One of the fundamental weaknesses of the asset-based approach, which the EU policy revision was intended to address, is the failure to account for interdependencies. In response to this issue, Table 6 illustrates the evolution of the EU's approach to regulating protection processes, with a focus on recognising and addressing interdependencies.

Table 6. References to interdependence in the EU legal and institutional framework

Source	Recognition of interdependencies	Operational implications
EPCIP	Cross-border, physical and social dependencies	Identification of European critical infrastructure, bilateral and multilateral consultations, and information exchange
NIS	ICT-related and cross-border dependencies	Cooperation between Member States, exchange of incident-related information, and consideration of dependencies when identifying operators of essential services
NIS2	Supply-chain dependencies, cascading effects and systemic risk	Supply-chain risk management, expanded incident reporting, coordinated risk assessments, and enhanced situational awareness
CER	Cross-sectoral and cross-border interdependencies	National risk assessments, critical-entity risk assessments, resilience strategies, identification of critical entities, and cross-border cooperation
European Commission 2025 – Guidelines (C/2025/4990)	Dependencies, alternatives and cascading effects	Support for the identification of critical entities, assessment of disruption impacts, analysis of the availability of alternatives, and evaluation of the potential for cascading effects

Table 6 (continued)

Source	Recognition of interdependencies	Operational implications
European Commission 2026 – Guidelines (C/2026/3712)	Bidirectional sectoral, supply-chain and cross-border dependencies	Linking national and entity-level risk assessments with the selection of resilience measures; supply-chain mapping, redundancy, alternative suppliers, mutual-aid arrangements, and recovery prioritisation. The Guidelines do not, however, establish a single methodology for joint risk assessment across networks of interdependent operators
DORA	Dependence on external ICT third-party providers and concentration risk	Business impact analysis, identification of critical ICT third-party providers, assessment of provider substitutability, oversight of third-party risk, and operational resilience testing
ENISA NIS360 2026	Sectoral ecosystem and systemic relevance	Support for sector-level maturity and criticality assessment and for analysing systemic consequences; the material supports an ecosystem-based approach but does not constitute a mandatory methodology for mapping or jointly assessing interdependencies between operators

Source: own elaboration based on European Parliament and Council of the European Union (2016), European Parliament and Council of the European Union (2022a), European Parliament and Council of the European Union (2022b), European Parliament and Council of the European Union (2022c), European Commission (2006), European Commission (2025), European Commission (2026), ENISA (2026)

Discussion

Regarding Q1, it should be noted that not only have the protection objectives changed, but the very logic of regulatory intervention has changed as well. EPCIP and the NIS Directive laid the groundwork for coordination and information exchange, but left EU Member States with broad discretion in interpretation and implementation. The regulatory package comprising CER, NIS2 and DORA, however, aims to narrow this scope by introducing more precise minimum standards, expanded reporting obligations, greater management accountability, and broader supply-chain coverage. It is therefore more accurate to speak of reducing the scope of divergent transposition rather than simply limiting the independence of EU Member States.

The governance implication of the regulatory evidence is that implementation should not be confined to compliance by individual entities. National resilience strategies should identify dependencies between essential services and sectors, connect national risk assessments with critical-entity risk assessments, and define arrangements for cross-sector and, where relevant, cross-border information exchange.

Incident-reporting arrangements should also support learning about interdependencies by recording not only the initiating event but, where feasible, the affected service, cascading consequences and recovery requirements. These implications primarily operationalise directions already visible in CER, NIS2, DORA and the Commission guidance. They should therefore be treated as an extension of the regulatory analysis rather than as new empirical findings of the survey.

Regarding Q2, the expert evidence adds an implementation-level perspective that is not directly observable from the regulatory texts themselves. In particular, respondents highlighted the risk that compliance requirements may produce formalistic behaviour and that transferring regulatory obligations to suppliers may reduce the pool of eligible or willing providers, thereby increasing concentration and reducing substitutability within critical-service supply networks. The survey therefore suggests that measures intended to strengthen supply-chain security may, under certain implementation conditions, generate new organisational dependencies that should themselves be considered in resilience management.

The evidential status of these observations should be differentiated. High implementation costs, skills shortages and implementation complexity largely confirm barriers already identified in the academic literature. By contrast, compliance formalism, the possibility that transferred requirements may contract the pool of willing suppliers, and coordination difficulties across autonomous entities are the clearest original empirical signals generated by the expert survey. Because the survey is qualitative and based on a purposive expert sample, these findings should be interpreted as plausible implementation mechanisms requiring further testing rather than as estimates of their prevalence across the EU. From a governance perspective, supply-chain security should therefore include not only the assessment of individual suppliers but also supplier substitutability, concentration risk, switching time and the possibility that regulatory costs themselves may reduce the availability of alternatives. Supervisory and support measures should likewise assess substantive resilience outcomes rather than formal compliance alone.

Regarding Q3, an analysis of the results indicates that the issue of interdependence has been clearly recognised in EU law but has so far been only partially translated into operational solutions. The CER emphasises the role of EU Member States in national risk assessments and resilience strategies, NIS2 strengthens operators' obligations regarding supply chain security and incident reporting, and DORA presents a more developed, sector-specific model for managing dependence on ICT suppliers.

The case-study evidence provides a different and more limited form of support for Q3. The six incidents demonstrate mechanisms through which physical, geographical, informational and logical dependencies can propagate disruptions beyond the initially affected asset or operator. They therefore confirm the practical relevance of cascading risk, but they should not be interpreted as a basis for deterministic

prediction of future cascading events. The cases are retrospective and reconstructed from publicly available material, whereas the topology of current dependencies can change as a result of supplier replacement, outsourcing, digitalisation, route reconfiguration, redundancy measures, market concentration and organisational change. Moreover, public sources rarely disclose the level of operational detail required to reconstruct current inter-operator dependencies. Historical incident data are consequently valuable for identifying mechanisms and plausible propagation pathways, but their predictive capacity is limited when the underlying network of dependencies has changed.

The results for Q4 indicate that research on critical-infrastructure interdependencies and resilience constitutes an established and rapidly developing field, but remains methodologically fragmented. The large body of publications and the six identified thematic clusters indicate that the issues of interdependence, resilience, cyber threats, and business continuity are already firmly established in academic discourse. At the same time, solutions focused on a single entity or sector dominate. Proposals such as the SoS approach (Petit et al. 2018), the use of scenario-based methods to analyse defence industry logistics (Owczarczyk 2025), the CERA and CERFI methods (Rehak, Splichalova, Hromada, et al. 2024), and the classification of resilience-enhancing tools (Rehak et al. 2025) or the DYNABIC framework (Rios et al. 2023) demonstrate significant progress in application within a single enterprise, but do not address the gap regarding inter-organisational coordination within ES operator networks. At the same time, recent network-oriented approaches, including DISruptionMap (Schneider et al. 2025)such as floods or storms, can disrupt multiple critical infrastructures at once. In addition, a localized failure of one service can trigger a cascade of failures of other dependent services. This makes it challenging to anticipate and prepare adequately for direct and indirect consequences of such events. Existing methods that are spatially explicit and consider service dependencies currently lack practicality, as they require large amounts of data. To address this gap, we propose a novel method called\n DISruptionMap\n which analyzes complex disruptions to critical infrastructure services. The proposed method combines (i, RIPA (Faraji et al. 2026)forming complex dependency networks where disruptions can propagate across sectors and amplify systemic risk. Conventional risk assessment methods are limited by evaluating components in isolation and neglecting how interdependencies shape cascading exposure. This paper introduces the Risk Impact Pathway Analysis (RIPA, and probabilistic and dynamic network models, demonstrate that methods for mapping dependencies, modelling cascading effects, and assessing network-level resilience are increasingly available. The multiactor continuity-management perspective proposed by (Hassel and Cedergren 2024) further shows that business continuity can be extended beyond a single organisation to networks jointly delivering critical societal functions. The remaining methodological gap therefore does not concern the absence

of methods for analysing dependencies or cascading effects. Rather, it concerns the limited availability of integrated and operationally applicable approaches that simultaneously identify ES, map inter-operator and supply-chain dependencies, assess partner substitutability, and support joint network-level risk assessment across autonomous organisations and regulatory domains. This gap is exacerbated by findings on cyber resilience and systemic risk (Aghazadeh Ardebili et al. 2024, Assenza et al. 2024)their exposure to cyber threats has grown significantly. The complex and hyper-connected nature of these systems presents challenges for enhancing cyber resilience against adverse conditions, stresses, attacks, or compromises on cybersecurity resources. Integrating risk assessment with cyber resilience allows for adaptive approaches that can effectively safeguard critical infrastructures (CIs and by the barriers to NIS2 compliance (Mentzelou et al. 2025)placing new demands on both essential and important entities. Despite its importance, organizations face multiple barriers that undermine compliance, including lack of awareness, technical complexity, financial constraints, and regulatory uncertainty. This study identifies and models these barriers to provide a clearer view of the systemic challenges of NIS2 implementation. Building on a structured literature review, fourteen barriers were defined and validated through expert input. The Decision-Making Trial and Evaluation Laboratory (DEMATEL. It is precisely this gap that constitutes one of the most important findings of this article. Against this backdrop, the present article adds value by linking the regulatory, organisational, and network perspectives. It demonstrates that the shift in the EU's security paradigm is not merely about expanding the list of operators' obligations, but about changing the unit of risk analysis, from the risk faced by a single entity to the risk of disruption to functions delivered by a network of interdependent entities.

Conclusions

The most important finding of the study is therefore the existence of an asymmetry between the relatively advanced regulatory recognition of interdependencies and systemic risk in EU policies and regulations and the still-limited availability of integrated, operationally applicable methods for identifying interdependencies and conducting joint risk assessments across networks of autonomous ES providers.

For Q1, the study shows that EU governance has evolved from a predominantly asset- and sector-focused model towards a service- and resilience-oriented model characterised by more explicit minimum requirements, stronger managerial accountability, broader reporting duties, and greater attention to supply-chain and cross-border dependencies. For Q2, the expert survey indicates that CER, NIS2 and DORA are perceived as capable of strengthening harmonisation, resilience, cooperation and risk management, while their implementation may be constrained by

costs, skills gaps, implementation uncertainty and coordination difficulties. The most distinctive survey-based empirical signals concern compliance formalism, possible supplier-market contraction caused by transferred requirements, and coordination problems across autonomous entities. For Q3, interdependencies and cascading risks are explicitly recognised in the current EU framework, but their operationalisation remains partial because consistent dependency mapping, supplier-substitutability assessment, joint risk assessment and protected cross-sector information exchange are not yet implemented through a single coherent operational approach. For Q4, the literature provides multiple methods for mapping dependencies and assessing risk and resilience, but the field remains methodologically fragmented. The principal gap is therefore not the absence of methods, but their integration and operational application across networks of autonomous ES providers.

The added value of this study lies in its integration of regulatory, organisational, and network perspectives. The article traces the evolution of EU policy while demonstrating that ensuring the continuity of the ES is a matter of managing logistics, risk, and resilience across networks of multiple autonomous actors. Thus, it contributes to management science by expanding the discussion of continuity management in networks of interdependent organisations, and to security studies by shifting the focus from the protection of individual facilities to the protection of ES, public value, and national resilience.

However, when interpreting the above findings, the study's limitations must be taken into account. The analysis was based exclusively on publicly available sources. The literature review was based on a structured search of Scopus and WoSCC using a specific set of keywords. The survey component included 18 respondents. These limitations constrain the generalisability and predictive scope of the findings. The purposive expert sample supports qualitative interpretation of implementation mechanisms but does not provide a basis for estimating their prevalence across the EU. The publicly available documentary corpus and retrospective case-study material also provide only partial insight into current operational dependencies, many of which are commercially sensitive, security-relevant or dynamically changing. However, they indicate that further research should include in-depth studies of national implementations and the development and validation of integrated operational tools supporting the identification, assessment, and management of interdependencies across critical-service networks.

Future research should combine comparative studies of national CER and NIS2 implementation with access to operator-level or otherwise protected dependency data, longitudinal updating of dependency maps, cross-sector pilot applications of joint risk assessments, scenario exercises and stress tests. A particularly relevant direction is the development and validation of minimum shared datasets for interdependency analysis that improve situational awareness and network-level assessment without creating disproportionate confidentiality, security or compliance burdens.

References

Aghazadeh Ardebili, A., Lezzi, M., and Pourmadadkar, M., 2024. Risk assessment for cyber resilience of critical infrastructures: methods, governance, and standards. *Applied Sciences*, 14(24), 11807. DOI: 10.3390/app142411807.

Aljohani, A., 2023. Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. *Sustainability*, 15(20), 15088. DOI: 10.3390/su152015088.

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., and Vittal, V., 2005. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20(4), 1922–1928. DOI: 10.1109/TPWRS.2005.857942.

Annarelli, A. and Nonino, F., 2016. Strategic and operational management of organizational resilience: current state of research and future directions. *Omega*, 62, 1–18. DOI: 10.1016/j.omega.2015.08.004.

Arksey, H. and O'Malley, L., 2005. Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19–32. DOI: 10.1080/1364557032000119616.

Assenza, G., Ortalda, A., and Setola, R., 2024. Redefining systemic cybersecurity risk in interconnected environments. *Applied Cybersecurity & Internet Governance*, 3(2), 144–169. DOI: 10.60097/ACIG/192119.

Babbie, E.R., 2016. *The practice of social research*. 14th ed. Boston, MA: Cengage Learning.

Bui, T.-D., Tsai, F.M., Tseng, M.-L., Tan, R.R., Yu, K.D.S., and Lim, M.K., 2021. Sustainable supply chain management towards disruption and organizational ambidexterity: a data driven analysis. *Sustainable Production and Consumption*, 26, 373–410. DOI: 10.1016/j.spc.2020.09.017.

Buncefield Major Incident Investigation Board, 2008. *The Buncefield incident, 11 December 2005: the final report of the Major Incident Investigation Board. Volume 1*. Sudbury: Health and Safety Executive. Available from: https://www.icheme.org/media/13707/buncefield-miib-final-report-volume-1.pdf [Accessed: 6 October 2026].

Chang, S.E., McDaniels, T.L., Mikawoz, J., and Peterson, K., 2007. Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. *Natural Hazards*, 41(2), 337–358. DOI: 10.1007/s11069-006-9039-4.

Ciano, M.P., Pozzi, R., Rossi, T., and Strozzi, F., 2019. How IJPR has addressed 'lean': a literature review using bibliometric tools. *International Journal of Production Research*, 57(15–16), 5284–5317. DOI: 10.1080/00207543.2019.1566667.

Dudenhoeffer, D.D., Permann, M.R., and Manic, M., 2006. CIMS: a framework for infrastructure interdependency modeling and analysis. In: *Proceedings of the 2006 Winter Simulation Conference*. Piscataway, NJ: IEEE, 478–485. DOI: 10.1109/WSC.2006.323119.

ENISA, 2026. *ENISA NIS360: latest insights in the cybersecurity maturity and criticality of NIS sectors of high criticality*. European Union Agency for Cybersecurity. Available from: https://www.enisa.europa.eu/enisa-nis360-2026 [Accessed: 6 October 2026].

European Commission, 2006. Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM(2006) 786 final, 12 December 2006. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:52006DC0786 [Accessed: 6 October 2026].

European Commission, 2025. Communication from the Commission - Commission guidelines and reporting template developed pursuant to Articles 5(5), 6(6) and 7(3) of Directive (EU) 2022/2557 on the resilience of critical entities. *Official Journal of the European Union*, C/2025/4990, 12 September 2025. Available from: https://data.europa.eu/eli/C/2025/4990/oj [Accessed: 6 October 2026].

European Commission, 2026. Communication from the Commission - Guidelines on the application of Article 13(5) of Directive (EU) 2022/2557 on the resilience of critical entities. *Official Journal of the European Union*, C/2026/3712, 13 July 2026. Available from: https://data.europa.eu/eli/C/2026/3712/oj [Accessed: 6 October 2026].

European Parliament and Council of the European Union, 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194, 19 July 2016, 1–30. Available from: https://data.europa.eu/eli/dir/2016/1148/oj [Accessed: 6 October 2026].

European Parliament and Council of the 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. *Official Journal of the European Union*, L 333, 27 December 2022, 80–152. Available from: https://data.europa.eu/eli/dir/2022/2555/oj [Accessed: 6 October 2026].

European Parliament and Council 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 and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L 333, 27 December 2022, 164–198. Available from: https://data.europa.eu/eli/dir/2022/2557/oj [Accessed: 6 October 2026].

European Parliament and Council of the European Union, 2022c. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. *Official Journal of the European Union*, L 333, 27 December 2022, 1–79. Available from: https://data.europa.eu/eli/reg/2022/2554/oj [Accessed: 6 October 2026].

Faraji, F., Mouratidis, H., and Al Zakwani, A., 2026. Risk impact pathway analysis (RIPA): a dynamic risk assessment framework for interdependent critical infrastructures. *International Journal of Information Security*, 25, 26. DOI: 10.1007/s10207-025-01201-1.

Ghasemkhani, A., Basiri, M.A., and Nicholson, C., 2026. Interdependency and uncertainty in the resiliency of infrastructure networks: a comprehensive review. *International Journal of Critical Infrastructure Protection*, 54, 100866. DOI: 10.1016/j.ijcip.2026.100866.

Ghobakhloo, M., Iranmanesh, M., Foroughi, B., Tseng, M.-L., Nikbin, D., and Khanfar, A.A.A., 2025. Industry 4.0 digital transformation and opportunities for supply chain resilience: a comprehensive review and a strategic roadmap. *Production Planning & Control*, 36(1), 61–91. DOI: 10.1080/09537287.2023.2252376.

Gu, B. and Liu, J., 2025. A systematic review of resilience in the maritime transport. *International Journal of Logistics Research and Applications*, 28(3), 257–278. DOI: 10.1080/13675567.2023.2165051.

Hassel, H. and Cedergren, A., 2024. A framework for business continuity management in a multiactor context. *Journal of Contingencies and Crisis Management*, 32, e12573. DOI: 10.1111/1468-5973.12573.

Hosseini, S., Barker, K., and Ramirez-Marquez, J.E., 2016. A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145, 47–61. DOI: 10.1016/j.ress.2015.08.006.

Knoke, D. and Yang, S., 2008. *Social network analysis*. 2nd ed. Los Angeles, CA: SAGE Publications. DOI: 10.4135/9781412985864.

Lee, E.E., II, Mitchell, J.E., and Wallace, W.A., 2007. Restoration of services in interdependent infrastructure systems: a network flows approach. *IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews*, 37(6), 1303–1317. DOI: 10.1109/TSMCC.2007.905859.

Leng, J., Zhong, Y., Lin, Z., Xu, K., Mourtzis, D., Zhou, X., Zheng, P., Liu, Q., Zhao, J.L., and Shen, W., 2023. Towards resilience in Industry 5.0: a decentralized autonomous manufacturing paradigm. *Journal of Manufacturing Systems*, 71, 95–114. DOI 10.1016/j.jmsy.2023.08.023.

Linnenluecke, M.K., 2017. Resilience in business and management research: a review of influential publications and a research agenda. *International Journal of Management Reviews*, 19(1), 4–30. DOI 10.1111/ijmr.12076.

Lou, W. and Qiu, J., 2014. Semantic information retrieval research based on co-occurrence analysis. *Online Information Review*, 38(1), 4–23. DOI: 10.1108/OIR-11-2012-0203.

Lozar Manfreda, K., Batagelj, Z., and Vehovar, V., 2002. Design of web survey questionnaires: three basic experiments. *Journal of Computer-Mediated Communication*, 7(3), JCMC731. DOI: 10.1111/j.1083-6101.2002.tb00149.x.

Mentzelou, K., Chountalas, P.T., Kitsios, F.C., Magoutas, A.I., and Dasaklis, T.K., 2025. Identifying and modeling barriers to compliance with the NIS2 Directive: a DEMATEL approach. *Journal of Cybersecurity and Privacy*, 5(4), 97. DOI: 10.3390/jcp5040097.

Owczarczyk, P., 2025. Determinants of business continuity in the logistics processes of the armaments industry amid the current economic and military environment. *Systemy Logistyczne Wojsk*, 62(1), 23–42. DOI: 10.37055/slw/211037.

Petit, F., Verner, D., Phillips, J., and Lewis, L.P., 2018. Critical infrastructure protection and resilience: integrating interdependencies. In: A.J. Masys, ed. *Security by design: innovative perspectives on complex problems*. Cham: Springer International Publishing, 193–219. DOI: 10.1007/978-3-319-78021-4_10.

Polska Federacja Producentów Żywności Związek Pracodawców, 2022. Produkcja żywności i napojów w Polsce jest zagrożona. Available from: https://datki.pfpz.pl/produkcja-zywnosci-i-napojow-w-polsce-jest-zagrozona-20228 [Accessed: 6 October 2026].

Rehak, D., Splichalova, A., Hromada, M., Walker, N., Janeckova, H., and Ristvej, J., 2024. Critical entities resilience failure indication. *Safety Science*, 170, 106371. DOI: 10.1016/j.ssci.2023.106371.

Rehak, D., Splichalova, A., Janeckova, H., Oulehlova, A., Hromada, M., Kontogeorgos, M., and Ristvej, J., 2024. Critical entities resilience assessment (CERA) to small-scale disasters. *International Journal of Disaster Risk Reduction*, 111, 104748. DOI: 10.1016/j.ijdrr.2024.104748.

Rehak, D., Splichalova, A., Janeckova, H., Ryska, O., Oulehlova, A., Michalcova, L., Hromada, M., Kontogeorgos, M., and Ristvej, J., 2025. Critical entities resilience strengthening tools to small-scale disasters. *International Journal of Critical Infrastructure Protection*, 49, 100766. DOI: 10.1016/j.ijcip.2025.100766.

Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25. DOI: 10.1109/37.969131.

Rios, E., Iturbe, E., Rego, A., Ferry, N., Tigli, J.-Y., Lavirotte, S., Rocher, G., Nguyen, P., Song, H., Dautov, R., Mallouli, W., and Cavalli, A.R., 2023. The DYNABIC approach to resilience of critical infrastructures. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23)*. New York, NY: Association for Computing Machinery, Article 136, 1–8. DOI: 10.1145/3600160.3605055.

Schneider, M., Halekotte, L., Mentges, A., and Fiedrich, F., 2025. Dependent Infrastructure Service Disruption Mapping (DISruptionMap): a method to assess cascading service disruptions in disaster scenarios. *Scientific Reports*, 15, 5736. DOI: 10.1038/s41598-025-89469-0.

Skomra, W., 2021. Zagrożenia wynikające ze współzależności na przykładzie pożaru serwerowni w Strasburgu. Rządowe Centrum Bezpieczeństwa. Available from: https://archiwum.rcb.gov.pl/zagrozenia-wynikajace-ze-wspolzaleznosci-na-przykladzie-pozaru-serwerowni-w-strasburgu/ [Accessed: 6 October 2026].

Skomra, W., Szwarc, K., and Wiśniewski, M., 2026. *From infrastructure protection to the continuity of essential services: EU policy on interdependence and supply chains* [dataset]. Zenodo. Available from: https://doi.org/10.5281/zenodo.22640607 [Accessed: 6 October 2026].

Snyder, H., 2019. Literature review as a research methodology: an overview and guidelines. *Journal of Business Research*, 104, 333–339. DOI: 10.1016/j.jbusres.2019.07.039.

Sun, W., Bocchini, P., and Davison, B.D., 2020. Applications of artificial intelligence for disaster management. *Natural Hazards*, 103(3), 2631–2689. DOI: 10.1007/s11069-020-04124-3.

Tong, W., Li, H.X., Nasirzadeh, F., Yao, F., and Ji, Y., 2025. Resilience of interdependent infrastructure networks: review and future directions. *International Journal of Critical Infrastructure Protection*, 51, 100793. DOI: 10.1016/j.ijcip.2025.100793.

U.S.-Canada Power System Outage Task Force, 2004. *Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations*. Washington, DC and Ottawa: U.S.-Canada Power System Outage Task Force. Available from: https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf [Accessed: 6 October 2026].

Yin, R.K., 2012. *Applications of case study research*. 3rd ed. Thousand Oaks, CA: SAGE Publications.

Zio, E., 2018. The future of risk assessment. *Reliability Engineering & System Safety*, 177, 176–190. DOI: 10.1016/j.ress.2018.04.020.

Author Contributions

Research concept and design: K.S., M.W. and W.S.; data collection and assembly: K.S., M.W. and W.S.; data analysis and interpretation: K.S. and M.W.; writing – original draft: K.S., M.W. and W.S.; writing – review and editing: K.S., M.W. and W.S. All authors have read and approved the final version of the manuscript.

Funding

This research received no external funding.

Data Availability Statement

The data supporting the findings of this study are available in Zenodo at DOI 10.5281/zenodo.22640607.

Conflict of Interest Statement

The authors declare no conflict of interest.

Use of AI Tools

The authors did not use generative AI tools in preparing this manuscript.

Ethics Approval / Consent
Formal institutional ethical review was neither sought nor obtained. The CAWI component was designed as a non-interventional, minimal-risk expert opinion survey. Participants were informed of the purpose of the study, the institutions conducting it and the intended use of their responses. Completion of the questionnaire constituted informed consent to participate and to the use of the responses for research and publication purposes. No directly identifying, classified or operationally sensitive data were collected, and the responses were analysed and reported in anonymised, aggregated form.

Received: 17.06.2026
Accepted: 24.10.2026

© Krzysztof Szwarc, Michał Wiśniewski, Witold Skomra, 2026. This article is published in "*Systemy Logistyczne Wojsk*" / "*Military Logistics Systems*" under the Creative Commons Attribution 4.0 International licence (CC BY 4.0).