IJEMS | SCIENTIFIC ARTICLE

International Dimension of Critical Infrastructure Resilience: Challenges of the Mediterranean Security Environment

DENIS ČALETA
Institute for Corporative Security Studies, Slovenia
denis.caleta@gmail.com

The resilience of critical infrastructure (CI) has emerged as a defining challenge of the 21st century, accompanied by a growing recognition of its international and cross-border dimensions. Nowhere is this more evident than in the Mediterranean region, a region characterised by its strategic position at the crossroads of Europe, Africa, and the Middle East, its climatic vulnerability, and its socio-political diversity. This article explores the international dimension of CI resilience with a particular focus on the challenges and opportunities presented by the Mediterranean basin. The Mediterranean faces a convergence of threats that test the robustness and adaptability of infrastructures upon which societies depend. Climate-related hazards such as heatwaves, droughts, wildfires, and flooding increasingly disrupt energy, water, and transport systems. At the same time, cyber-physical threats associated with the digitalisation of energy grids, telecommunications networks, and maritime transport systems expose the region to sophisticated cyberattacks and cascading failures. These risks are further compounded by geopolitical instability, with conflicts, irregular migration flows, and the security of energy transit routes placing significant strain in national systems and cross-border cooperation. Drawing on European policy frameworks such as the CER Directive, the NIS2 Directive, the EU Civil Protection Mechanism, and the EU Strategy for Critical Infrastructure Resilience – as well as preparatory steps undertaken within the EU project ENDURANCE – this article argues that resilience in the Mediterranean requires both strategic integration and operational pragmatism. The analysis highlights the inadequacy of siloed, state-centric approaches and emphasises the need for cross-sectoral, cross-border, and community-level engagement. Case studies focusing on energy interconnectors, port infrastructures, and urban coastal resilience illustrate the interconnected vulnerabilities, as well as the opportunities for shared resilience building. The article concludes that enhancing CI resilience in the Mediterranean is not only a regional imperative but also a cornerstone of Europe's broader security and stability. It calls for harmonised strategies, stronger public-private partnerships, and innovative tools such as Digital Twins and regional stress-testing exercises, all embedded within a long-term vision of international cooperation.

Key Words: resilience, Mediterranean security environment, critical infrastructure, sectorial interdependences, international cooperation, ENDURANCE

CC BY-SA © 2025 Denis Čaleta

https://doi.org/10.70908/2232-6022/18.177-205

INTRODUCTION

The resilience of critical infrastructure (CI) has become a central concern for governments, industry, and society at large. In an era defined by accelerating climate change, growing geopolitical instability, and rapid technological transformation, the capacity of essential systems – such as energy, water, transport, telecommunications, and health – to withstand and recover from disruptions is both a strategic imperative and a societal necessity. The European Union (EU) has recognised this urgency through the adoption of the Critical Entities Resilience (CER) Directive (Directive (EU) 2022/2557) and the NIS2 (Directive (EU) 2022/2555) Directive, which together establish a comprehensive framework for strengthening both physical and cyber resilience across Member States.

The Mediterranean region provides a distinctive and complex context in which to examine these issues. Geographically positioned at the crossroads of Europe, Africa, and the Middle East, the Mediterranean basin functions as a strategic transit corridor for energy, trade, and communications. Its extensive coastlines, dense population centres, and critical maritime chokepoints render it particularly susceptible to natural hazards and security threats. Furthermore, the Mediterranean is one of the world's most climate-vulnerable regions, already experiencing a rise in extreme weather events such as wildfires, floods, droughts, and heatwaves, with profound implications for critical infrastructure systems (Vadnjal 2025).

At the same time, the Mediterranean is characterised by deep interdependencies and asymmetries (ATLANTIS 2022). European Union Member States in the northern Mediterranean share regulatory frameworks and resilience policies, while neighbouring countries in North

Africa and the Middle East operate under diverse governance systems and often face political instability. These differences complicate cross-border coordination but also underscore the importance of an international dimension in resilience planning.

This article therefore addresses two interrelated research questions:

1. What are the specific challenges to CI resilience in the Mediterranean environment, given its climatic, geopolitical, and technological characteristics?
2. How can international cooperation and harmonised strategies contribute to strengthening resilience across this heterogeneous region?

By combining policy analysis with selected case studies on energy, maritime, and urban infrastructure, the article seeks to illustrate both the vulnerabilities and the opportunities inherent in the Mediterranean context. It argues that traditional, centralised, and siloed approaches to infrastructure protection are increasingly inadequate, and that multilevel, cross-border, and community-driven approaches are required to ensure the continuity of essential services. Ultimately, the paper positions the resilience of Mediterranean critical infrastructures not merely as a regional concern but as a strategic pillar underpinning the stability and security of Europe as a whole.

To address the research questions outlined above, this article adopts a multi-layered methodological framework that combines policy analysis, case study research, and comparative assessment. This approach reflects the multidimensional nature of critical infrastructure (CI) resilience in the Mediterranean, where climatic, geopolitical, and technological factors interact across multiple levels of governance. Specifically, the study employs five complementary components: (1) Policy and Regulatory Analysis, (2) Case Study Selection and Analysis, (3) Comparative Cross-Border Assessment, (4) Integration of a Hybrid Threat Perspective and (5) Analytical Framework and Evaluation. The methodological framework integrates regulatory analysis, case-based evidence, and comparative evaluation, all interpreted through the lens of hybrid threats and cascading risks.

This allows the article not only to identify the specific challenges of CI resilience in the Mediterranean but also to assess the potential of international cooperation and harmonised strategies as pathways towards enhanced resilience.

Theoretical and Policy Background

Critical infrastructure (CI) refers to the assets, systems, and networks that provide essential services for the functioning of society and the economy. These include energy, transport, water supply, telecommunications, healthcare, and financial services. Resilience, in this context, extends beyond physical protection: it encompasses the capacity to anticipate, absorb, adapt to, and rapidly recover from disruptive incidents. This multidimensional perspective links resilience not only to engineering robustness but also to organisational adaptability, policy frameworks, and societal preparedness (Jovanović et al. 2021).

The concept of resilience has evolved in recent years from a narrow focus on protection – emphasising defensive measures against threats – to a broader systems-based approach, that recognises interdependencies, cascading risks, and the need for adaptive governance. For highly interconnected regions such as the Mediterranean, where risks are transboundary and often concurrent resilience cannot be confined within national or sectoral boundaries (Hosseini et al. 2016).

The European Union has significantly advanced its resilience agenda in response to rising geopolitical tensions, increasing climate-related risks, and the growing sophistication of cyber-physical threats. Three policy frameworks are particularly relevant:

- The Critical Entities Resilience (CER) Directive (Directive (EU) 2022/2557): Adopted in 2022, the CER Directive replaces the earlier European Critical Infrastructure Directive. It introduces a holistic, all-hazards approach to resilience across eleven essential sectors, including energy, transport, health, and digital infrastructure. It requires Member States to identify critical entities, conduct risk assessments, and support operators in strengthening resilience, while also ensuring EU-wide cooperation.
- The NIS2 Directive (Directive (EU) 2022/2555): NIS2 broadens and deepens the EU's cybersecurity framework by expanding the range of sectors and entities subject to mandatory requirements. It emphasises risk management, incident reporting within 24–72 hours, and the accountability of senior management. For CI operators, particularly in the energy and telecommunications sectors, NIS2 introduces stricter obligation regarding supply chain security, cross-border information sharing, and coordinated vulnerability disclosure.

- The Union Civil Protection Mechanism (UCPM): Complementing the CER and NIS2 Directives, the UCPM provides a cooperative framework for disaster prevention, preparedness, and response among EU Member States and neighbouring countries. Its role is particularly significant in the Mediterranean, where natural disasters (wildfires, floods, and earthquakes) frequently exceed national response capacities.

Together, these frameworks embody the EU's shift towards a resilience-based security model, integrating climate adaptation, cyber protection, and cross-border solidarity.

The Mediterranean basin exposes the limitations of national or sector-specific approaches. CI systems in the region are highly interdependent and transnational. Energy flows through cross-border grids and pipelines, maritime trade depends on shared sea routes and ports, and digital networks connect coastal cities across continents. Disruptions in one country or sector can therefor trigger cascading effects across the entire region (Molnár et al. 2021).

Moreover, the Mediterranean's heterogeneity in terms of governance structures, regulatory maturity, and socio-economic capacities makes policy harmonisation both challenging and essential. While the integration of the CER and NIS2 Directives provides EU Member States with robust instruments, the full benefits of resilience can only be realised if these extend beyond the EU's borders to include neighbouring states. This underscores the importance of international cooperation, regional governance frameworks, and trust-building mechanisms for effective CI resilience within the Mediterranean environment.

Grašič (2025) argues that in recent years, the concept of the smart city has evolved from a futuristic vision into a practical framework for urban development integrating digital technologies, data-driven governance, and sustainable infrastructure. As cities become increasingly interconnected and reliant on digital and energy systems, their vulnerability to natural hazards becomes more complex. The interplay between technological advancement and environmental risk necessitates a new paradigm for urban resilience: one that is multi-sectoral, dynamic, and adaptive.

Traditional risk assessment approaches often rely on static indicators and isolated sectoral analyses, failing to capture the cascading effects and temporal dynamics of disasters in smart urban environments. By contrast, a multi-sectoral model offers a holistic perspective, accounting for system interdependencies and the evolving nature of risk over time (Grašič 2025).

Resilience assessment is now widely recognised as a vital component in the management and protection of critical infrastructure systems (CI), including energy grids, transportation networks, water supply systems, and digital services. It involves evaluating a system's ability to absorb, adapt to, and recover from disruptions, such as cyberattacks, natural disasters, or technical failures, while maintaining the continuity of essential services.

The seminal work by Rinaldi et al. (2001) established a foundational understanding of infrastructure interdependencies, identifying four key dimensions of interconnection: physical, cyber, geographic, and logical. Their framework demonstrated how disruptions in one system – such as energy – can cascade into others, including telecommunications or water supply, thereby amplifying both risk exposure and the complexity of response. This conceptual model laid the groundwork for subsequent research on cross-sectoral vulnerabilities and cascading risk analysis.

From a policy perspective, international standards and EU directives define core principles of resilience, albeit often in general terms. ISO 22301:2012 addresses business continuity, framing resilience as robustness, adaptability, and recovery. ISO/IEC 27001:2013 focuses on protecting digital infrastructure through structured cybersecurity management.

At the EU level, the CER Directive strengthens the resilience of critical service providers, while the NIS2 Directive enhances cybersecurity across interconnected sectors. Together, these instruments support a systemic approach to managing risks within interdependent infrastructure networks.

Since Rinaldi's foundational work, numerous studies have sought to formalise the concepts of risk and resilience. For example, resilience has been introduced as a system property that complements risk by focusing on a system's ability to prepare for, absorb, recover from, and adapt to disruptions (Linkov and Trump 2014). This perspective provides a dynamic alternative to traditional, static risk metrics. Building on this foundation, a systematic literature review synthesised definition of infrastructure resilience, categorising them into engineering, ecological, and organisational perspectives (Hosseini et al. 2016). These studies emphasize that resilience must be dynamic and measurable over time, challenging conventional models that treat threats as isolated or singular events. Further development of the concept includes a systems-based resilience framework that contrasts with traditional risk assessment by emphasising adaptive management and decision-making under uncertainty (Linkov and Trump 2019), introducing robustness and adaptability as core performance indicators.

Much of the recent literature has shifted toward multi-sectoral analysis, particularly in the context of smart cities and critical infrastructure. A review of modelling and simulation techniques (Ouyang 2014) for interdependent infrastructures, which includes network models, agent-based simulation, and system dynamics, highlights the importance of hybrid approaches that combine physical network modelling with behavioural and systemic perspectives.

Several studies address cascading effects across sectors, particularly digital-physical interdependencies. Boldyrev et al. (2010) employed network theory to demonstrate how failures in one system can trigger abrupt, systemic collapse in interdependent networks.

Recent research by Mentges et al. (2023) provides a conceptual and interdisciplinary review of how resilience is defined across domains, particularly in the context of critical infrastructure. The authors offer a theoretical and cross-disciplinary lens that helps to unify and explain diverse, domain-specific understandings on resilience. Their work reflects the evolution of the concept and introduces a structured glossary that clarifies key terms, such as robustness, redundancy, adaptability, and resilience capacity, tailored to the needs of resilience engineering. This contribution enhances conceptual clarity and supports the integration of standardised terminology into practical assessment and decision-making models.

The following publicly accessible platforms, which represent existing solutions that monitor outages across internet services, telecommunications, and power systems. Within the resilience framework, they provide a foundation for situational awareness by offering real-time data on service disruptions and infrastructure performance. These tools already operate at scale and demonstrate the value of transparent reporting in identifying risks, tracking resilience, and highlighting patterns of disruption.

At the same time, these platforms have limitations: each focuses on a specific domain, often with fragmented coverage, and few fully capture cascading effects across sectors. In the context of this study, where the resilience of Critical Infrastructure (CI) and cross-sector interdependencies are central, these platforms form an important baseline. Building on their capabilities, improvements can be made to integrate data, model systemic risks, and strengthen coordinated responses across interconnected systems.

Although the concept of resilience has gained prominence in academic, policy, and operational discourse, significant dilemmas remain in establishing a common understanding of resilience as a distinct process. These dilemmas are particularly evident in the Mediterranean, where diverse governance systems, socio-economic conditions, and institutional capacities complicate harmonisation.

1. *The conceptual dilemma.* Resilience is often interpreted differently across disciplines and sectors. Engineers may define it in terms of system robustness and redundancy, policymakers emphasise governance frameworks and risk management, while social scientists highlight adaptability, inclusiveness, and community capacity (Bertoncelj 2017). These perspectives are not mutually exclusive, yet the absence of a unified definition leads to fragmented practices. In the context of CI, this raises a critical question: should resilience be viewed primarily as technical continuity, institutional capacity, or societal adaptability?
2. *The sectoral dilemma.* Critical infrastructures are interconnected, yet each sector has its own operational logic, regulatory environment, and priorities. Energy operators, for instance, prioritise supply continuity and grid stability; telecommunications stakeholders focus on data security and availability; transport authorities focus on physical safety and mobility. Attempting to impose a one-size-fits-all resilience framework risks overlooking sectoral nuances, whereas excessive sector-specific fragmentation undermines interoperability and coordinated response.
3. *The governance dilemma.* Resilience processes often extend across multiple jurisdictions and governance levels. At the EU level, directives such as CER and NIS2 aim to harmonise approaches, yet their implementation is mediated by national legislation and local practices. In the Mediterranean, this dilemma is particularly acute for the EU Member States, candidate countries, and neigh-

bouring regions must negotiate between European standards, national sovereignty, and local needs. The key challenge lies in balancing supranational harmonisation with context-sensitive flexibility.

4 *The temporal dilemma.* Resilience is inherently dynamic, it must account for short-term incident response, medium-term recovery, and long-term adaptation to systemic changes such as climate change or digital transformation. However, political and financial cycles often prioritise immediate measures over long-term investment. This temporal misalignment increases the risk of resilience being treated as a finite project deliverable rather than a continuous and adaptive process.

5 *The trust dilemma.* Effective resilience depends on information sharing and coordination between public and private actors. Yet competitive pressures, security sensitivities, and regulatory constraints frequently inhibit data exchange. In the Mediterranean, where political trust between certain states remains fragile building a shared resilience framework is particularly complex. Without overcoming these trust deficits, resilience efforts risk remaining confident within national or sectoral boundaries.

The dilemmas surrounding resilience as a unique process reveal that, while the concept provides a unifying language, its translation into practice remains contested. For the Mediterranean environment, resilience cannot be understood as a uniform or static condition but must instead be approached as a plural, negotiated, and evolving practice that integrates technical, organisational, and societal dimensions across borders.

MEDITERRANEAN CONTEXT AND SPECIFICITIES

The Mediterranean basin presents a particularly complex environment for the resilience of critical infrastructure (CI). Fabijan et al. (2025) argue that its significance lies not only in its geographical position linking Europe, Africa, and the Middle East but also in the interplay of environmental, political, and socio-economic dynamics that shape both its vulnerabilities and capacities. This section outlines the distinctive characteristics of the Mediterranean context and explores how they intersect with the dilemmas associated with developing a common understanding of resilience.

Geostrategic Importance

The Mediterranean functions as a strategic transit hub for global trade, energy flows, and digital communications. Submarine cables across the basin carry a significant share of Europe's internet traffic, while oil and gas pipelines connect North Africa and the Middle East with European markets. Major maritime chokepoints such as the Strait of Gibraltar and the Bosporus are essential for global supply chains. Disruption of any of these nodes whether by accident, conflict, or cyberattack can have cascading effects far beyond the region (Čaleta and Powers 2020). This underscores the need for resilience as a cross-border and multi-sectoral priority, however, differences in governance structures and levels of trust continue to complicate the development of joint strategies.

Environmental and Climatic Vulnerabilities

The Mediterranean is one of the world's most climate-sensitive regions. It faces rising temperatures, prolonged droughts, water scarcity, wildfires, sea-level rise, and extreme flooding events. These environmental pressures directly threaten energy grids, water supply systems, transport infrastructure, and urban environments. The dilemma of temporal resilience is particularly evident in this context: while long-term adaptation to climate change is essential, political and financial cycles often prioritise short-term crisis management. The lack of investment in preventive measures amplifies existing vulnerabilities (Pelling 2011).

Political and Socio-Economic Heterogeneity

The Mediterranean is characterised by deep political asymmetries. On the northern shore, EU Member States operate within shared legal and regulatory frameworks (CER Directive, NIS2, and the Civil Protection Mechanism), while the southern and eastern shores are marked by greater instability, weaker institutions, and divergent priorities. This creates a governance dilemma: EU states are obliged to harmonise resilience policies, yet regional interdependencies require cooperation with neighbouring countries that may not share equivalent standards or capacities. Socio-economic inequalities further complicate resilience-building, as some states lack the resources to invest in robust infrastructure or cybersecurity (Brožič 2024).

Sectoral Interdependencies

Mediterranean CI systems are highly interdependent. Energy networks rely on telecommunications for monitoring and control; maritime transport relies on digital platforms for logistics and customs management; and water supply systems require stable energy provision (Gabrijelčič et al. 2000). These interdependencies render the sectoral dilemma particularly acute: each sector defines resilience differently, yet disruptions in one can propagate rapidly across others. Without shared methodologies and interoperable standards, resilience efforts remain fragmented and inconsistent.

Migration and Humanitarian Pressures

The Mediterranean also represents a frontline for migration flows and humanitarian crises, which can place sudden and severe demands on CI systems, particularly health, water, and emergency services. Here, the trust dilemma becomes evident: resilience depends on coordinated response mechanisms between countries, yet political sensitivities surrounding migration often inhibit the trust and data sharing needed for effective action (Čaleta and Robinson 2018). The Mediterranean environment thus illustrates why resilience cannot be treated as a uniform or static process. Its geostrategic position, environmental fragility, political heterogeneity, and sectoral interdependencies make it a laboratory of resilience dilemmas, where the need for international cooperation is both most urgent and most difficult to achieve. Addressing these specificities requires moving beyond centralised, siloed approaches towards flexible, adaptive, and multilevel strategies that integrate local communities, national systems, and regional frameworks.

KEY CHALLENGES FOR CI RESILIENCE IN THE MEDITERRANEAN

The Mediterranean basin faces a convergence of risks that intensify the vulnerabilities of critical infrastructures. These challenges are not isolated; they are multi-dimensional, cross-sectoral, and often transboundary in nature. Building resilience in this environment requires recognising the complexity of these threats and the ways in which they reinforce one another.

Climate-Related and Environmental Threats

The Mediterranean is recognised as a climate change hotspot, warming faster than the global average. Rising sea levels threaten coastal infrastructure, while increasingly frequent and severe storms, floods, and wildfires directly affect power grids, transport networks, water supply systems, and urban centres. Droughts and water scarcity strain hydropower generation and agriculture, creating knock-on effects for food and energy security. The temporal dilemma of resilience is clearly visible here: immediate crisis management often dominates political agendas, while long-term investments in adaptation (e.g., flood defences, resilient grid design) remain underfunded (Pelling 2011).

Cyber-Physical Vulnerabilities

Digitalisation and the expansion of smart infrastructure are advancing rapidly across the Mediterranean region, from smart energy grids to automated port logistics. While these technologies enhance efficiency, they also enlarge the attack surface for cyber threats. Critical infrastructures such as energy interconnectors, maritime systems, and water management facilities rely heavily on supervisory control and data acquisition (SCADA) systems, which are vulnerable to ransomware, denial-of-service, and state-sponsored cyberattacks. The sectoral dilemma emerges here: operators may prioritise efficiency over security, while uneven cyber capacities across states hinder coordinated defence (Mikac 2023).

Geopolitical Instability and Security Risks

The Mediterranean is a zone of geopolitical contestation, marked by conflicts in the Middle East and North Africa, disputes over maritime boundaries, and competition for energy resources. Infrastructure such as pipelines, subsea cables, and shipping routes constitute potential targets for sabotage, coercion, or hybrid warfare. This reality underscores the governance dilemma: whereas EU Member States are bound by CER and NIS2 Directives, neighbouring states may lack equivalent regulatory frameworks, creating uneven levels of protection along shared infrastructure corridors.

Cross-Sectoral and Cross-Border Interdependencies

The Mediterranean's CI systems are deeply interconnected: power networks depend on telecommunications for grid management; ports rely on digital systems for cargo and customs operation: health systems depend on both energy and transport. Disruption in one sector can therefore cascade rapidly across others, producing consequences that extend far beyond national borders. For instance, a cyberattack on a telecommunications hub can paralyse port operations, and disruption supply across Europe. The absence of harmonised resilience metrics and standards exacerbates this sectoral dilemma, leaving resilience efforts fragmented and inconsistent.

Migration and Humanitarian Pressures

The Mediterranean is also the epicentre of migration flows and humanitarian challenges, which impose sudden demands on health, water, and energy infrastructures, especially in southern Europe. Refugee arrivals, for instance, can overwhelm local hospitals, municipal water supplies, and emergency shelters. These pressures highlight the trust dilemma: effective resilience requires cross-border cooperation and data sharing between states, yet political sensitivities and divergent national interests often undermine collaborative approaches (Brožič 2024).

The key challenges for CI resilience in the Mediterranean can be categorised as climatic, cyber-physical, geopolitical, interdependent, and socio-humanitarian. Each is significant, but their intersections create a complex risk environment that no single state or sector can address in isolation. The following section illustrates these challenges through selected case studies, providing concrete examples of vulnerabilities and emerging responses within the Mediterranean context.

CASE STUDIES/ILLUSTRATIVE EXAMPLES

To demonstrate how the aforementioned challenges manifest in practice, this section presents selected case studies from across the Mediterranean basin. Each highlight both existing vulnerabilities and innovative approaches to strengthening resilience.

Energy Interconnectors and Grid Resilience

The Mediterranean energy landscape is highly interconnected. The Italy–Greece interconnector, the Euro Africa Interconnector (Egypt–Cyprus–Greece), and the Euro Asia Interconnector (Israel–Cyprus–Greece) are strategic projects designed to enhance energy security and diversification. Yet, these subsea cables and transmission systems are exposed to multiple risks: physical damage from earthquakes or maritime accidents, sabotage during periods of geopolitical tensions, and cyberattacks targeting SCADA systems. These interconnectors exemplify both the cross-border and sectoral dilemmas. Resilience requires harmonised standards, real-time data exchange, and coordinated contingency planning across jurisdictions. Success depends not only on technical redundancy but also on trust-based cooperation between operators and states.

Maritime and Port Infrastructure

[190] The Mediterranean accounts for nearly 20% of global maritime trade. Major ports such as Piraeus, Barcelona, Genoa, and Marseille are vital nodes within global supply chains. Increasing digitalisation – through smart logistics systems, automated cranes, and integrated customs management –has boosted efficiency but also heightened exposure to cyber-physical threats, as demonstrated by global incidents such as the 2017 ransomware attack on Maersk. Furthermore, physical disruptions (severe storms, labour strikes and blockades) can propagate rapidly through regional and global supply chains. Consequently, resilience strategies in ports now combine enhanced cybersecurity protocols, redundancy in logistics chains, and crisis coordination mechanisms involving both port authorities and international shipping alliances.

Urban Coastal Resilience

Mediterranean coastal cities such as Barcelona, Athens, Dubrovnik, and Alexandria are highly vulnerable to climate-related hazards, including flooding, storm surges, and heatwaves. Their dense populations and reliance on tourism amplify the consequences of disruptions to water, electricity, and health infrastructures. Efforts to build resilience increasingly involve urban Digital Twins and simulation-based planning, enabling authorities to test responses to extreme scenarios. Local communities are also engaged as frontline actors in resilience, reflecting the growing recognition that top-down, centralised models are insufficient to address complex risks in urban environments.

Together, these case studies illustrate the layered nature of resilience challenges in the Mediterranean. Energy interconnectors reveal the geopolitical and technical complexities of cross-border cooperation; ports highlight the dual risks of physical and cyber disruption in globalised logistics; and coastal cities demonstrate the urgency of climate adaptation. Across all three domains, the need for integrated, multi-actor, and cross-sectoral approaches emerges as the common denominator of effective resilience.

STRATEGIES FOR ENHANCING RESILIENCE

Building resilience in the Mediterranean environment requires moving beyond reactive, sector-specific measures toward integrated, anticipatory, and collaborative strategies. The following approaches provide pathways for addressing the vulnerabilities identified in the preceding sections (Fošner et al. 2024).

Strengthening Cross-Border Cooperation and Data Sharing

Given the transnational nature of Mediterranean critical infrastructures, resilience cannot be achieved without systematic cross-border cooperation. Critical infrastructures such as energy grids, transport corridors, digital networks, and port systems extend well beyond national borders, meaning that disruption in one state can have cascading effects across the entire region. To address this, cooperation must begin with the establishment of secure data-sharing platforms among CI operators and relevant authorities. These platforms should enable real-time information exchange, ensure technical interoperability, and at the same time respect strict data protection and confidentiality rules to preserve trust among participants. Such initiatives align closely with EU programmes such as the Connecting Europe Facility (CEF Digital) (European Commission 2021a), which promotes secure cross-border data exchange and supports the development of digital corridors across the Union.

Resilience also requires strengthening and expanding the role of regional mechanisms such as the Union Civil Protection Mechanism (UCPM). While the UCPM already provides vital support for disaster response, its mandate could be broadened to include systematic cross-border stress-testing of critical infrastructures, joint simulation exercises, and coordinated preparedness measures. Embedding CI resilience into the UCPM framework would help institutionalise cooperation and ensure that resilience planning extends beyond ad hoc crisis management. This approach is in line with the CER Directive, which emphasises systemic and cross-sectoral resilience. The approach is also in line with the preparation process of the EU Strategy for Critical Infrastructure Resilience, which is being developed under the framework of the EU INFRA 01-01/2023 project ENURANCE (Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe).

Equally essential is the development of trust networks between EU and non-EU Mediterranean states. Differences in governance structures, political priorities, and resource capacities can complicate cooperation, but trust-building initiatives such as joint training programmes, bilateral agreements, and shared risk assessments help reduce fragmentation. These networks are particularly important for overcoming the dilemmas of information sharing and joint decision-making identified earlier, and they support broader efforts under NATO–EU cooperation on resilience (NATO 2016), which stresses the importance of engaging partner states beyond the EU's borders. At the

energy level, EU-supported interconnection projects in the Mediterranean, such as electricity links between Greece, Cyprus, and Israel (Great Sea Interconnector, https://www.great-sea-interconnector.com) or between Greece and Egypt (GREGY, https://gregy-interconnector.gr), provide concrete examples of how cross-border cooperation enhances both operational capacity and political trust.

Ultimately, building resilience in Mediterranean critical infrastructures is only possible if cross-border cooperation is institutionalised, technologically supported, and politically reinforced. By linking secure information exchange, regional mechanisms, and trust networks with concrete EU programmes such as CEF Digital, the UCPM, the CER Directive, and major energy interconnection projects, the region can create a shared foundation for resilience. This foundation not only acknowledges the deep interdependence among Mediterranean states but also prepares them to face the hybrid and cascading threats that will increasingly define the regional security landscape.

Integrating Climate Adaptation into CI Protection

With the Mediterranean recognised as a climate hotspot, resilience strategies must explicitly and systematically incorporate climate change adaptation to address both current vulnerabilities and future risks. This requires moving beyond short-term protective measures and embedding climate resilience into the very design and operation of critical infrastructures. Investments in climate-resilient infrastructure are essential, including flood-proof substations capable of withstanding rising sea levels and extreme precipitation, as well as transport systems built with heat-resistant materials that can endure prolonged heatwaves. By integrating such measures into long-term planning cycles, operators can significantly reduce the likelihood of service disruptions and cascading failures during climate-related events. In addition to technological and engineering solutions, resilience strategies should increasingly adopt nature-based approaches. Restoring and expanding coastal wetlands, rein-forcing natural riverbanks, and preserving forests in vulnerable areas can help mitigate storm surges, control flooding, and reduce the risk of landslides. These solutions provide multiple benefits: they not only protect infrastructure but also strengthen biodiversity and improve the quality of life in local communities.

Equally important is ensuring that critical infrastructure resilience planning is not carried out in isolation but closely aligned with broader policy frameworks. Linking CI resilience with the EU Climate Adaptation Strategy (European Commission 2021b) and national adaptation plans ensures coherence, avoids duplication, and promotes access to European funding and technical support. It also strengthens accountability by requiring operators and authorities to embed climate considerations into compliance and reporting mechanisms. Ultimately, climate adaptation for critical infrastructures in the Mediterranean must be seen as a dynamic and ongoing process. The increasing frequency of extreme events – ranging from wildfires and droughts to flash floods and coastal erosion – demands strategies that are proactive, cross-sectoral, and forward-looking. By combining climate-resilient infrastructure, nature-based solutions, and alignment with EU and national adaptation frameworks, Mediterranean stakeholders can create a holistic resilience model capable of protecting societies and economies against the intensifying impacts of climate change (Comfort et al. 2010).

Building Local and Community-Level Preparedness

Local communities are the first responders in crisis situations, especially in coastal cities and rural areas affected by flooding, drought, or wildfires, and their role is indispensable for ensuring timely and effective action. Strategies should therefore place strong emphasis on building local capacity through systematic training of municipal authorities, civil protection services, and civil society organisations in critical infrastructure continuity planning. Such training equips local actors with the knowledge and procedures needed to maintain essential services even under severe stress.

Comfort et al. (2010) state that equally important is the involvement of local populations in resilience exercises, which not only strengthens situational awareness but also fosters a culture of preparedness and collective responsibility. When citizens understand the risks and are familiar with emergency procedures, the overall community response becomes faster, more coordinated, and less dependent on external assistance. In addition, promoting community-based early warning systems provides an essential layer of protection that complements national and regional frameworks. Localised monitoring of environmental conditions, supported by sensors and digital platforms, can generate rapid alerts tailored to community needs, ensuring that warnings are both timely and actionable. By combining local knowledge with national capabilities, these systems enhance trust and ensure that responses are adapted to the realities on the ground.

Ultimately, empowering local communities through training, engagement, and early warning mechanisms creates a bottom-up resilience structure that strengthens the effectiveness of national strategies. It bridges the gap between high-level policies and on-the-ground realities, ensuring that resilience is not only a matter of state-level preparedness but also a shared responsibility across society.

Developing Regional Digital Twins and Simulation Exercises

To anticipate cascading risks, Mediterranean stakeholders can increasingly rely on Digital Twins and advanced simulation models as practical and strategic tools for resilience. Regional Digital Twins of energy networks, port infrastructures, and urban systems enable virtual stress-testing under complex multi-hazard conditions, such as floods coinciding with cyberattacks and widespread blackouts. By mirroring real-world infrastructures in digital environments, these models allow stakeholders to identify vulnerabilities, test the robustness of systems, and evaluate different mitigation measures in a safe and controlled way, without putting actual operations at risk.

Cross-border simulation exercises further extend these benefits by engaging multiple countries and sectors in coordinated testing and preparedness activities. Such exercises strengthen interoperability, enhance trust between authorities, and develop shared decision-making capacities that are vital in a region where interdependencies are strong and crises often transcend national borders. For example, a Digital Twin of a port could model how flooding in one location might disrupt energy supplies or transport corridors across the region, while simultaneously simulating how a cyberattack could exacerbate the disruption and delay recovery efforts.

The use of these technologies also goes beyond immediate response. They support forward-looking resilience strategies by enabling decision-makers to explore hidden interdependencies, anticipate cascading effects, and design contingency plans that are more realistic and effective. In this way, Digital Twins and advanced simulations become not only a testing environment for preparedness but also a planning instrument that guides investment decisions and policy development. For Mediterranean stakeholders, they represent a vital capability to cope with increasing hybrid threats and the growing impact of climate-related hazards, ensuring that resilience planning remains dynamic, evidence-based, and regionally coordinated.

Promoting Public–Private Partnerships and Harmonised Standards

As much of critical infrastructure is privately owned and operated, effective resilience depends on strong and well-structured public–private partnerships. This requires aligning investment incentives for resilience upgrades through EU funding instruments such as Horizon Europe and the Connecting Europe Facility, ensuring that private operators have both the resources and motivation to strengthen their systems. It also involves promoting harmonised standards and certification schemes for critical infrastructure resilience across the Mediterranean, creating a level playing field and facilitating cross-border cooperation. At the same time, public–private partnerships should encourage private sector innovation in resilience technologies, including AI-based monitoring systems and blockchain-secured data exchange, which can provide advanced tools to anticipate risks, enhance situational awareness, and secure critical operations (Linkov and Trump 2019).

The strategies for enhancing CI resilience in the Mediterranean must be multi-scalar (local, national, regional), multi-sectoral (energy, transport, telecom, water, health), and multi-actor (public, private, community). The integration of climate adaptation, cyber protection, and international cooperation is not optional but a prerequisite for ensuring the continuity of essential services in an environment defined by complexity and interdependence (Ouyang 2014).

Role of EU and International Cooperation

The resilience of critical infrastructure (CI) in the Mediterranean cannot be achieved in isolation. Given the deeply interconnected nature of infrastructures and risks, it depends on multi-level governance, EU frameworks, regional partnerships, and global cooperation.

The European Union's Strategic Role

The EU has developed a comprehensive body of legislation and strategies that shape the resilience of CI, with direct implications for the

Mediterranean. The CER Directive establishes an all-hazard, cross-sector framework requiring Member States to identify critical entities and ensure the continuity of essential services across eleven sectors. Complementing this, the NIS2 Directive strengthens cybersecurity obligations, supply chain security, and incident reporting, measures that are particularly crucial for Mediterranean energy grids, ports, and telecommunications networks. The Union Civil Protection Mechanism (UCPM) further enhances resilience by providing joint disaster prevention and response capacity, which has already been mobilised in the past for floods and wildfires in southern Europe.

In addition, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) ensures that resilience efforts involving cross-border data flows, such as critical infrastructure monitoring, incident reporting, and the deployment of Digital Twins, comply with strict standards of data protection and privacy. GDPR compliance is essential for maintaining trust in regional cooperation. The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) introduces a risk-based framework for trustworthy AI, and as AI tools are increasingly applied to CI resilience – including predictive maintenance, situational awareness, and anomaly detection – compliance with the Act will be vital for ensuring safety and accountability.

Finally, the EU Climate Adaptation Strategy (European Commission 2021b) provides the overarching framework for integrating climate resilience into infrastructure planning, which is particularly relevant for Mediterranean coastal cities and water systems. Together with the EU Green Deal and the REPowerEU initiative, which emphasise energy transition, diversification, and decarbonisation, these measures reshape the resilience landscape by expanding renewable energy systems and strengthening cross-border interconnectors.

Together, these instruments illustrate that CI resilience is not a siloed policy area but sits at the intersection of security, digital, climate, and fundamental rights frameworks.

Regional and Cross-Border Cooperation

Beyond EU law, resilience in the Mediterranean requires regional approaches that reflect the area's unique geographic, political, and socio-economic context. The interconnected nature of energy, water, transport, and digital infrastructures in the region means that disruptions rarely stop at national borders, making cooperation across jurisdictions indispensable. The Union for the Mediterranean (UfM) provides a critical institutional framework for this cooperation, fostering dialogue and practical initiatives on energy transition, environmental protection, and civil protection that involve both EU and non-EU states. By acting as a neutral platform, the UfM enables the alignment of strategies and priorities in a region where governance systems, levels of development, and security concerns can vary considerably (Union for the Mediterranean 2022).

Large-scale cross-border projects such as the EuroAsia Interconnector and the EuroAfrica Interconnector showcase the opportunities of shared infrastructures, offering the potential for enhanced energy security, diversification of supply, and regional integration of renewable sources. At the same time, these projects also highlight new vulnerabilities: a failure, cyberattack, or natural disaster affecting one segment of the network can have cascading consequences across multiple countries. This duality underscores the need for regional resilience strategies that combine infrastructure investment with joint preparedness and risk management. Strengthening resilience therefore requires not only technical measures but also trust-building and capacity development. Joint training programmes, shared simulation exercises, and collaborative risk assessments can help bridge governance asymmetries between states with differing institutional capacities. They also promote a culture of interoperability, ensuring that, when crises occur, national authorities and critical infrastructure operators can act together effectively and without hesitation.

Ultimately, resilience in the Mediterranean cannot be secured solely through EU-level directives or isolated national efforts. It demands regional solidarity and coordinated action, where the benefits of integration are matched by a shared responsibility for managing risks. By embedding resilience into regional cooperation frameworks, linking infrastructure projects with common security protocols, and investing in trust-building across borders, Mediterranean stakeholders can establish a more robust foundation for withstanding the complex challenges posed by climate change, hybrid threats, and increasing interdependencies.

NATO, UN, and Global Governance

Broader international frameworks complement EU instruments and provide additional layers of resilience, which are particularly relevant for the Mediterranean region. NATO's Resilience Baselines, which focus on civil preparedness, cyber defence, and energy security, reinforce the protection of dual-use infrastructures and ensure that both civilian and military dimensions of resilience are addressed. The United Nations' Sendai Framework for Disaster Risk Reduction promotes a global all-hazard resilience approach, which is directly applicable to Mediterranean risks such as wildfires, earthquakes, and floods. Financial institutions such as the World Bank, the European Investment Bank (EIB), and the European Bank for Reconstruction and Development (EBRD), also play a critical role by supporting resilience investment, especially in areas of climate adaptation and the deployment of smart infrastructure.

The European Union itself plays a central role in framing resilience through a multidimensional policy mix spanning several domains: security measures under the CER Directive, the NIS2 Directive, and the Union Civil Protection Mechanism; digital and data governance through the GDPR and the AI Act; and climate and energy transition policies such as the EU Climate Adaptation Strategy and the European Green Deal. Yet, in the Mediterranean context, these frameworks alone are insufficient. They must be extended and reinforced through broader regional and international partnerships to effectively address the unique combination of climatic, cyber, geopolitical, and humanitarian risks that increasingly define the resilience landscape of the Mediterranean.

CONCLUSIONS

The resilience of critical infrastructure (CI) in the Mediterranean environment is both a regional necessity and a European strategic priority. This article has shown that the Mediterranean functions as a laboratory of resilience dilemmas, concentrating climatic vulnerabilities, cyber-physical risks, geopolitical contestation, and socio-economic asymmetries in ways that test existing governance frameworks. The region demonstrates that resilience cannot be understood as a static or uniform process, but rather as a dynamic, multi-layered, and negotiated practice spanning technical, organisational, and societal domains.

We could summarize key insights as follows: (1) Resilience is inherently international. In the Mediterranean, no state can secure its infrastructures in isolation. Energy interconnectors, maritime ports, submarine cables, and urban supply chains all across national boundaries. Disruptions are therefore regional in scope, requiring regional and cross-border strategies. (2) Resilience requires integration. Traditional siloed approaches are insufficient. Effective resilience must integrate climate adaptation, cybersecurity, physical protection, and community preparedness. (3) Resilience depends on trust and cooperation. Information sharing and joint preparedness are essential but politically sensitive. The trust dilemma is especially acute in the Mediterranean, where governance capacities and political priorities differ widely.

We would like also to present some important lessons from Key EU Projects: (1) ATLANTIS: demonstrated how advanced modelling and simulation can be used to predict cascading failures across interdependent infrastructures (energy, transport, ICT), offering a roadmap for regional Digital Twins in the Mediterranean. (2) SUNRISE: focused on pandemic resilience of CI, analysing how health crises (e.g., COVID-19) disrupt supply chains, workforce availability, and service continuity. Its outputs underscore the need for CI operators to integrate biosecurity, public health coordination, and demonstrate continuity of operations planning into resilience frameworks. (3) ENDURANCE: developed the EU Strategy for Critical Infrastructure Resilience, building stakeholder communities of CI operators, policymakers, and researchers, stressing that resilience is not only technical but also institutional, requiring multi-actor coordination frameworks. (4) PRECINCT: pioneered co-creation platforms where CI operators, public authorities, and citizens jointly design resilience strategies. This participatory approach could strengthen trust networks in politically sensitive Mediterranean settings. (5) InfraStress: advanced stress-testing tools for CI resilience under hybrid threats, integrating cyber, physical, and climate hazards directly relevant to ports, interconnectors, and energy hubs in the region.

Together, these projects demonstrate that resilience requires the integration of digital tools, community engagement, and cross-sectoral coordination, while also providing practical methodologies (e.g., co-creation, Digital Twins, and stress-testing) ready for application in the Mediterranean.

Policy recommendations are important for resilience, particularly in the context of critical infrastructure (CI). They translate research into actionable. Scientific projects and case studies often generate technical findings and best practices. Without clear policy recommendations, these insights remain confined to academic or operational silos. Recommendations bridge the gap between research and decision-making, ensuring that new insights inform actual governance and practice. It is essential to enable harmonisation across sectors and borders because resilience is not confined to one sector or country. CI systems

(energy, transport, telecom, and health) are interconnected and often cross-border. Policy recommendations promote standardisation, interoperability, and cooperation, helping stakeholders align on shared priorities and coordinated responses. It is also very important to support legal and regulatory frameworks as an important base for common operation and understanding. Recommendations provide a foundation for common operational standards and understanding. They inform new laws, directives, or standards (e.g., CER Directive, NIS2, AI Act). They highlight gaps in existing rules and suggest concrete adjustments to strengthen resilience against evolving threats. Prioritise resources and investment is strongly connected with policy advice which helps governments and operators identify where to invest limited resources (e.g., in flood defences, cyber monitoring, or redundancy). By framing resilience as a policy priority, recommendations increase the likelihood that funding is directed towards long-term adaptation rather than solely short-term crisis management.

The fundamental answers to the two research questions posed in the introduction can be summarized as follows.

1. *What are the specific challenges to CI resilience in the Mediterranean environment, given its climatic, geopolitical, and technological characteristics?* The Mediterranean environment presents a unique convergence of risks that complicates critical infrastructure (CI) resilience. Climatically, the region is a hotspot, experiencing intensifying wildfires, floods, droughts, and heatwaves that directly affect the stability of energy, water, and transport systems. Geopolitically, the Mediterranean is characterised by fragmented governance structures, unequal economic capacities, and tensions between EU and non-EU states, which hinder coordinated responses and trust-building. Technologically, rapid digitalisation and interconnection of infrastructures, for example energy interconnectors, cross-border port logistics, and 5G-enabled services create both opportunities for efficiency and vulnerabilities to cyberattacks and cascading failures. The heterogeneity of the region means that risks do not manifest uniformly: Southern

and Eastern Mediterranean states often face resource and governance gaps, while Northern states must manage highly complex, interdependent infrastructure systems. Combined these climatic, geopolitical, and technological characteristics generate hybrid risk environments where natural hazards, cyber threats, and political instability interact to increase the likelihood of large-scale disruptions.

2 *How can international cooperation and harmonised strategies contribute to strengthening resilience across this heterogeneous region?* International cooperation and harmonised strategies are vital because no single Mediterranean state can address these challenges in isolation. The EU provides a core framework through instruments such as the CER Directive, NIS2, the Union Civil Protection Mechanism, the Climate Adaptation Strategy, and the Green Deal, collectively promoting a comprehensive approach to resilience. These frameworks need to be complemented by regional initiatives, such as those under the Union for the Mediterranean, which facilitate dialogue between EU and non-EU states and support projects like the EuroAsia and EuroAfrica interconnectors. Cooperation extends to global frameworks as well: NATO's Resilience Baselines, the UN Sendai Framework for Disaster Risk Reduction, and investments by institutions such as the World Bank and EIB reinforce resilience by providing standards, funding, and shared methodologies. Harmonisation of risk assessment methodologies, early warning systems, and incident reporting procedures is particularly important for overcoming governance asymmetries and ensuring interoperability. Ultimately, international cooperation enables the creation of trust networks, joint simulations, and cross-border data exchange platforms, which are indispensable for managing cascading risks and hybrid threats in a highly interdependent Mediterranean environment.

The findings of this article suggest that the challenges to critical infrastructure resilience in the Mediterranean – arising from its climatic volatility, geopolitical fragmentation, and technological interdependencies – cannot be effectively addressed by individual states acting alone. The very characteristics that define the region generate hybrid risks and cascading effects that transcend national boundaries.

This makes international cooperation and harmonised strategies not merely desirable but essential. By embedding resilience into EU policy frameworks, aligning them with regional initiatives such as those of the Union for the Mediterranean, and reinforcing them through global mechanisms like the UN Sendai Framework and NATO's Resilience Baselines, Mediterranean stakeholders can address governance asymmetries and resource gaps. Harmonisation of risk assessments, data-sharing mechanisms, and crisis response procedures provides the foundation for operational interoperability, while trust networks and joint investment initiatives strengthen long-term resilience. In this way, the specific regional challenges identified in the first research question directly justify the cooperative and harmonised approaches outlined in the second, demonstrating that resilience in the Mediterranean is achievable only through collective, multi-level, and cross-border efforts.

All of this is fundamental for strengthening stakeholder trust and legitimacy. Clear evidence-based recommendations increase trust among citizens, operators, and policymakers, showing that resilience planning is systematic rather than arbitrary. This enhances the legitimacy of decisions and encourages multi-actor buy-in. Ultimately, this approach addresses the 'resilience dilemmas' by building awareness of the strategic and operational actions required to safeguard critical infrastructure. As we outlined earlier, resilience is contested across sectors (technical vs. organisational vs. societal). Policy recommendations help find common ground by offering pragmatic compromises e.g., balancing cybersecurity needs with privacy (GDPR) or reconciling climate adaptation with economic feasibility.

Strengthening CI resilience in the Mediterranean is therefore not only about protecting infrastructure but also about safeguarding the continuity of essential services, fostering trust among diverse actors, and embedding lessons from EU projects into practical governance and operations. By aligning EU frameworks with project outcomes, national policies, industry practices, and community engagement, the Mediterranean can transition from a region of vulnerability to a regional model of integrated, international resilience.

ACKNOWLEDGMENTS

ENDURANCE project has received funding by the European Union's Horizon Europe, under grant agreement no. 101168007.

REFERENCES

ATLANTIS. 2022. 'ATLANTIS Aims at Enhancing Resilience and Cyber-Physical-Human (CPH) Security of the key EU Critical Infrastructures.' https://www.atlantis-horizon.eu.

Bertoncelj, B. 2017. 'Zanesljivost posameznika pri delovanju kritične infrastrukture sodobne države.' *Contemporary Military Challenges* 19 (4): 111–31.

Brožič, L. 2024. 'EU Actorness in a Mirror: The War in Ukraine.' *International Journal of Diplomacy and Economy* 10 (2): 153–68.

Boldyrev, A., G. Kupovykh, and A. Redin. 2010. 'Surface Layer Electrodynamic Structure According to the Meteorological State.' Paper presented at the 2nd International Conference on Electronic Computer Technology, Kuala Lumpur, 7–10 May.

Čaleta, D., and J. F. Powers, Jr., eds. 2020. *Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection.* Ministry of Defence of the Republic of Slovenia; Joint Special Operations University.

Čaleta, D., and C. A. Robinson, eds. 2018. *Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats.* Ministry of Defense of the Republic of Slovenia; Joint Special Operations University.

Comfort, L. K., A. Boin, and C. C. Demchak. 2010. *Designing Resilience: Preparing for Extreme Events.* University of Pittsburgh Press.

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 (NIS 2 Directive) (Text with EEA Relevance). 2022. *Official Journal of the European Union.* https://eur-lex.europa.eu /eliqnewline /dir/2022/2555/oj/eng

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 (Text with EEA Relevance). 2022. *Official Journal of the European Union.* https:// eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

European Commission. 2020. 'Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities.' COM/2020/829 final. https://eur-lex.europa.eu/legal -content/EN/TXT/?uri=CELEX%3A52020PC0829

European Commission. 2021a. 'Connecting Europe Facility.' https:// commission.europa.eu/funding-tenders/find-funding/eu-funding -programmes/connecting-europe-facility_en

European Commission. 2021b. 'Forging a Climate-Resilient Europe –

The New EU Strategy on Adaptation to Climate Change.' COM(2021) 82 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0082&from=EN

European Union. 2025. 'EU Civil Protection Mechanism.' https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/union-civil-protection-mechanism_en

Fabijan, J., J. Vadnjal, and D. Veselinovič. 2025. 'Economic Integration of Mediterranean States.' *International Journal of Euro-Mediterranean Studies* 18 (1): 103–27.

Fošner, A., B. Bertoncelj, T. Poznič, and L. Fink. 2024. 'Risk Analysis of Critical Infrastructure with the MOSAR Method.' *Heliyon* 10 (4): e26439.

Gabrijelčič, D., D. Čaleta, T. Zahariadis, F. Santori, C. De Santis, and Gasparini. 2020. 'Securing Critical Infrastructures of the Energy Sector: Security Challenges for the Critical Infrastructures of the Energy Sector.' In *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures,* edited by J. Soldatos, J. Philpot, and G. Giunta. Now Publishers.

Grasič, V. 2025. 'Development of a Multi Sectoral Risk and Resilience Assessment Model for Smart City: Case Study of Floods in 2023 in the North Eastern Part of Slovenia.' In *8th International Scientific Conference on Digital Economy DIEC 2025*. 'Internacionalna poslovno-informaciona akademija' Tuzla.

Hosseini, S., K. Barker, and J. E. Ramirez-Marquez. 2016. 'A Review of Definitions and Measures of System Resilience.' *Reliability Engineering & System Safety* 145:47–61.

Jovanović, A., M. Jeličić, P. Klimek, S. Chakravarty, D. Čaleta, M. Gerbec, and M. T. Nguyen. (2021). 'Modelling Interdependencies within and among Critical Infrastructures/Entities Exposed to Cyber-Physical Threats.' In *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures,* edited by J. Soldatos, J. Philpot, and G. Giunta. Now Publishers.

Linkov, I., and B. D. Trump. 2019. *The Science and Practice of Resilience.* Springer.

Mentges, A., L. Halekotte, M. Schneider, T. Demmer, and D. Lichte. 2023. 'A Resilience Glossary Shaped by Context: Reviewing Resilience-Related Terms for Critical Infrastructures.' *International Journal of Disaster Risk Reduction* 96:103893.

Mikac, R. 2023. 'Protection of the EU's Critical Infrastructures.' *Applied Cybersecurity & Internet Governance* 2 (1): 1–5.

Molnár, A., I. Szászi, and L. Takács (2021). 'Security Sector Reform by Intergovernmental Organisations in Libya.' *International Journal of Euro-Mediterranean Studies* 14 (1): 7–48.

NATO. 2016. 'Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.' https://www.nato.int/cps/en/natohq/official_texts_133163.htm

Ouyang, M. (2014). 'Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems.' *Reliability Engineering & System Safety* 121:43–60.

Pelling, M. 2011. *Adaptation to Climate Change: From Resilience to Transformation.* Routledge.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance). 2016. *Official Journal of the European Union.* https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance). 2024. *Official Journal of the European Union.* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.' *IEEE Control Systems Magazine* 21 (6): 11–25.

Union for the Mediterranean. (2022). *Regional Climate Change Adaptation Framework in the Mediterranean.* Union for the Mediterranean.

Vadnjal, J. 2025. 'Interdisciplinary Perspectives on Sustainability, Development, and Culture in the Mediterranean and Beyond.' *International Journal of Euro-Mediterranean Studies* 18 (1): 5–7.