ATLANTIS

In collaboration with

SUNRISE

Resilient by Design:
Integrating Standards, Tools and Partnerships to Secure Critical Infrastructure in Europe

Policy Brief - August 2025

Co-funded by
the European Union

Executive Summary

As critical infrastructure (CI) in Europe becomes increasingly interdependent, it is also more vulnerable to cascading disruptions triggered by cyberattacks, physical sabotage, and climate-related hazards. These vulnerabilities are further amplified by persistent fragmentation across national, regional and local frameworks, divergent sectoral protocols, and varied risk management (RM) approaches, i.e. compounded by limited coordination mechanisms, particularly between public and private actors. The EU Strategic Foresight Report 2023 [1] has already flagged CI vulnerabilities as one of the top systemic risks to European stability, alongside digital dependencies and geopolitical shocks. Despite recent legislative advances, most notably the second version of the Directive on Network and Information Systems (NIS2) and Critical Entities Resilience (CER) Directives, the European Union (EU) still lacks a cohesive and interoperable model to secure its most vital systems.

This policy brief outlines a strategic roadmap to address these vulnerabilities through the integration of harmonized standards, advanced RM tools, and effective public-private partnerships (PPPs) in order to embed resilience into the design and governance of CI across the EU. Grounded in the findings of the ATLANTIS project and aligned with the EU's broader resilience agenda, this policy brief offers targeted and actionable recommendations to reinforce CI protection across Member States (MSs). Specifically, this brief proposes the following tangible actions:

- Establishing EU-wide interoperability standards for CI protection
- Deploying AI-based threat forecasting platforms

This brief is intended for EU policymakers, national authorities, CI operators, and strategic decision-makers across crucial sectors such as civil protection, cybersecurity, space, and infrastructure resilience, all of which shape the design, governance, security, and continuity of Europe's critical systems. The brief addresses the urgent need to strengthen the resilience of CIs in Europe in the face of increasingly complex and interconnected threats, and as these CIs become more

interdependent, it also addresses CIs' vulnerability to cascading disruptions, which are amplified by climate change, geopolitical instability, as well as technological and systemic risks.

Recent advances in EU legislation, such as the NIS2 and CER Directives, which are the current frameworks for CI protection and resilience, remain fragmented across MSs and sectors. Divergent security standards, inconsistent RM practices and limited interoperability hinder coordinated responses and leave systemic vulnerabilities unaddressed. Moreover, PPPs, which are crucial for sharing threat intelligence and best practices, face persistent challenges related to trust, legal frameworks and liability concerns.

Drawing on the findings from the ATLANTIS project and other Horizon Europe initiatives to chart a strategic roadmap for a more cohesive, interoperable and forward-looking CI protection system, the following three core priorities are highlighted:

- **Integration of standards of practice:** Harmonizing traditional, cyber, physical and natural hazard protections through EU-wide interoperability standards, drawing on best global practices and multi-stakeholder engagement with a tiered approach while incorporating short-, medium- and long-term targets and goals.

- **Advance the understanding and capacity for RM:** Leveraging AI-based threats forecasting, Big Data, and predictive analytics to enhance early warning, scenario planning, and dynamic risk scenarios across borders and sectors.

- **Effective public-private collaboration:** Fostering efforts towards building trusted national 'Points of Contact' and frameworks for regional, sub-regional and cross-border coordination, enabling rapid information sharing and joint crisis response.

As the EU stands at a crossroads of digital, geopolitical and climate-driven transitions, the message is clear: resilience must become a cornerstone of infrastructure policy and standardization to ensure the safeguarding of CI and civilians against current and emerging complex disruptions.

Disclaimer:

The views and recommendations expressed in this policy brief are those of ATLANTIS project and contributors and do not necessarily reflect the official position, mandate, or institutional agendas of any participating organization.

The work presented in this policy brief has been partially funded by the ATLANTIS project, which has received funding from the European Union's Horizon Europe framework programme under grant agreement No. 101073909.

The work presented in this document represent the views of the authors only. The European Research Executive Agency and the European Commission are not responsible for any use of the included information.

Context: The need for resilient CI in Europe

There is a need to establish a unified and secure operational environment across the EU to protect all critical assets from an all-hazard perspective. A wider "resilience" perspective will improve their protection, and at the same time, enhance their adaptability and recovery capabilities. This is exactly the strategy of the CER and NIS2 Directives: shifting the focus on resilience will enforce new activities and pro-activities in the involved (public, private) entities, thus enhancing preparedness and overall security.

Across the EU, the functioning of society increasingly depends on a complex web of CIs, ranging from energy and transport to telecommunications, water, healthcare, and digital systems. These infrastructures and systems are becoming ever more interconnected and interdependent, while the threats they face are growing in intensity, complexity, and transnational scope.

Cyberattacks, natural disasters, and physical threats are no longer isolated events. Instead, they trigger cascading effects that can rapidly compromise the delivery of essential services and the safety of populations across borders. Climate change, geopolitical instability, and technological vulnerabilities further amplify these risks. They place unprecedented pressure on both national and EU-wide infrastructure governance.

Despite this evolving risk landscape, the current frameworks for CI protection across the EU remain fragmented. Many MSs operate under divergent security standards, varying RM practices and limited interoperability, preventing coordinated response and increasing systemic vulnerabilities. While the NIS2 and CER Directives mark progress toward resilience-focused governance, Europe still lacks an integrated framework aligning cyber, physical, and natural hazard protections.

Furthermore, the integration of public-private cooperation in infrastructure governance remains inconsistent. Many CI operators still require access to shared threat intelligence, interoperable tools, and guidance on best practices. According to the Confederation of European Security Services (CoESS) White Paper on PPPs (2023) [2], issues of trust, fragmented legal frameworks, and liability concerns continue to hamper the full potential of PPPs [3] in the security domain. This fragmentation risks undermining both national preparedness as well as the EU's strategic autonomy in the face of evolving threats.

This policy brief responds to these challenges by identifying the key vulnerabilities in the current security and resilience landscape for CI in Europe. It advocates for a more integrated, interoperable and forward-looking approach to security standards, risk governance, and PPPs.

The brief is structured around three (3) strategic dimensions:

- The harmonization of cross-sectoral and cross-border standards focuses mainly on the development and adoption of EU-wide interoperability standards and best practices, which integrate protections against physical, cyber, and natural threats.
- The integration of AI-enabled RM tools such as predictive analytics, earth observation images, stress-testing tools, and shared intelligence platforms, which would be valuable in supporting the anticipation of cascading threats and the management of systemic vulnerabilities across CI networks.

» The institutionalization of trusted PP coordination mechanisms by building a resilient backbone for crisis management that relies on a national 'Point of Contact', shared protocols, and joint investment in security and emergency response innovations.

The brief concludes with a roadmap outlining short, medium, and long-term policy actions to embed resilience-by-design into Europe's infrastructure governance.

Overview of comprehensive standards and frameworks for European critical infrastructure Resilience

Nowadays, societies are more reliant than ever on the seamless functioning of CI systems. These systems are foundational to daily life and economic stability, public safety, and sustainable development. As climate change and other evolving threats increase the frequency and severity of disruptions, ensuring that infrastructure is designed, built and maintained to withstand a wide range of hazards has become a strategic imperative for resilience across Europe.

Yet, current infrastructure planning, financing, design, operations, and decommissioning practices often remain siloed and reactive. The deeply interdependent nature of infrastructure networks and the increasingly systemic, cascading impacts that disasters can trigger across sectors are frequently overlooked. Without integrated RM and resilience embedded in CI policy and investment decisions, countries face heightened vulnerability, economic losses, and prolonged shock recovery.

A cross-sectoral, multi-hazard approach that brings together policymakers, regulators, CI operators, asset owners, and communities is thus crucial for effectively identifying vulnerabilities, understanding interdependencies, and managing systemic risks. This inclusive engagement supports better risk identification, decision-making, and preparedness by capturing the full economic, social and environmental impacts of disruptions.

The EU developed and put into force two (2) directives, the second versions of the NIS2 and CER Directives, and mainly focused on strengthening CIs in Europe. Standardized security protocols, implemented through these directives, are essential to ensure operational coherence and interoperability across MSs, especially in managing transboundary and systemic risks. The main objective of both directives is to improve the protection and resilience of CIs, or, more precisely, Critical Entities (CEs), as they are defined therein, i.e. emphasizing the importance of relations among critical entities, particularly their supply chains.

The table below provides an overview of the national entities designated by each EU MS to implement the CER Directive, illustrating the institutional landscape underpinning resilience governance across the Union.

MS	Institution
AT	**Protection of Critical infrastructure in Directorate for State Security and Intelligence (DSN), Ministry of Interior**
BE	**Directorate Critical Infrastructure Protection & Risk Analysis of the Belgian National Crisis Center, Ministry of Interior**
BG	**Ministry of Interior**
CY	**Cyprus Civil Defense**
CZ	**Ministry of Interior – Directorate General of Fire Rescue Service of the Czech Republic**
DE	**Federal Ministry of the Interior and Community, Referat KM 4- Schutz kritischer Infrastrukturen**

MS	Institution
DK	**Danish Emergency Management Agency**
EE	**Government Office of Estonia**
EL	**Secretary General for the Coordination of the Government**
ES	**National Center for Critical Infrastructure Protection, Ministry of Interior**
FI	**National Security Unit, Ministry of Interior of Finland**
FR	**Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Direction de la protection et de la sécurité de l'Etat/ Sécurité des activités d'importance vitale**
HR	**Civil Protection Directorate, Ministry of Interior**
HU	**Department for the Critical Infrastructure Coordination National Directorate General for Disaster Management, Ministry of Interior**
IE	**Office of Emergency Planning, Department of Defence**
IT	**Presidency of the Council of Ministers, Office of the Military Advisor**
LT	**Planning Bureau of the National Crisis Management Centre, Office of the Government of Lithuania**
LU	**Haut-Commissariat à la Protection Nationale**
LV	**Ministry of Interior**
MT	**Critical Infrastructure Protection Directorate, Ministry for Home Affairs, Security, Reforms and Equality**
NL	**Ministry of Justice and Security**
PL	**Critical Infrastructure Protection Unit, Government Centre for Security**
PT	**Internal Security Bureau**
RO	**Ministry of Administration and Interior – Centre for Coordination of Critical Infrastructure Protection**
SE	**Swedish Civil Contingencies Agency (MSB) and Ministry of Defense**
SI	**Critical Infrastructure Department, Civil Defense Division, Defense Affairs Directorate, Ministry of Defense**
SK	**Ministry of Interior of the Slovak Republic**

Table 1: *Overview of agencies that oversee CI aspects at the national level; compilation based on research by Prof. Vittorio Rosato.*

The application area of the NIS2 is the digital and cyber domain, whereas the CER focuses more on the physical aspects of CIs. With most CIs obliged to implement both, a comprehensive and effective cross-sectoral approach can be realized.

Below are a few examples from outside of Europe that illustrate the awareness and importance of defining policies to improve CI's resilience.

- The United States Federal Government published the National Resilience Strategy in 2025 [4], setting up the core vision of how resilience should be tackled and dealt with in America. It mainly evolves around a whole community approach, ranging across sectors and promoting RM and strong collaborations. For the cyber domain, the second version of the Cybersecurity Framework (CSF 2.0) published by National Institute of Standards and Technology (NIST) in

2024 [5] provides detailed and structured guidance to manage cybersecurity risks. The framework highlights best practices and controls to achieve a higher resilience not only for CIs but also for industry, government and other organizations in general.

- The UN General Assembly's Political Declaration on the Midterm Review of the Sendai Framework (A/RES/77/289) already calls for aligning infrastructure planning with disaster risk reduction strategies through multi-sectoral risk governance. It underscores the need for legal and regulatory frameworks that clearly define roles, foster accountability, and promote investment in resilience. It also stresses the importance of conducting multi-hazard risk assessments (RA) and stress testing before infrastructure investments are made. Similar calls are also reflected in EU policies, including the above-mentioned CER Directive and Council Recommendation on strengthening the resilience of CI (2023/C 20/01).

- Global standards, such as the Principles for Resilient Infrastructure [6] developed by UNDRR, in consultation with over 100 countries, businesses, academic institutions, and civil society organizations, provide a practical framework for building systemic resilience. These principles achieve a resilience gain across all lifecycle stages of infrastructure (design, build, operate, decommission), assuring the continuity of critical services through all phases of disruption management (preparation, absorption, recovery, and adaptation). To operationalize them, UNDRR, together with the Coalition for Disaster Resilient Infrastructure (CDRI), developed a global methodology for infrastructure resilience reviews, which was already implemented in countries across Africa, Asia, Latin America, and Europe (e.g. the Republic of Moldova). This approach helps to identify governance, coordination and policy gaps to enhance prevention, preparedness and response to CI disruptions at both sectoral and cross-sectoral levels, and to align government priorities and investments with the CER Directive and Council Recommendations on CI.

With climate change amplifying threats like extreme heat, floods and wildfires, in addition to emerging and fast-evolving hazards, integrated risk reduction and adaptation must become central to national and regional infrastructure planning. To advance this agenda, continued investment in research, development and innovation (R&D&I) is critical. Enhanced tools for simulation ("what if" reasoning) and stress testing can illuminate cascading risks and enable more effective resilience-building across systems and sectors.

Although such tools have been researched and developed in the past, most of them are tailored to domains and network types, e.g. the combination of energy and communication networks. They don't account for the required cross-sectoral, multi-hazard approach that is required for CIs on a regional or national scale. Increasingly, EU funding projects aim to bridge this gap by promoting multi-hazard approaches, among others. Thus, projects like ATLANTIS and SUNRISE follow a more general approach, developing simulation tools to address multi-hazard and cross-sectoral risks. For example, CCI-SAAM acts as a policy-based information broker of cyber, physical, and operational threat/risk intelligence across borders and CI sectors. Similarly, CASSANDRA, i.e. a simulation tool developed under the SUNRISE project, can model threats originating from multiple domains (e.g. cyber, physical, climate, hybrid) and estimate their cascading effects across interdependent infrastructures.

Strengthening Risk Management & Threat Intelligence for Critical Infrastructure Protection

Strategic decision makers could use RM concepts as a binding glue and a starting point to understand resilience (see the 2023 UK Government Resilience Framework), as well as a starting

point to address capabilities, investments and collaboration in times of uncertainties (e.g. pandemic temporary conditions or extreme climate phenomena). However, the RM process needs to be made more dynamic, proactive and adaptive, and ready to evolve rapidly and address interplay between acute and chronic risks, or combination of slow and fast onset adversary events that might be combined in a multi-hazard scenario. Sharing RA with partners and doing joint RA/RM exercises (e.g. pandemics should not be treated only as a health emergency but a systemic one) is also recommended. Joint RM exercises should include (a) simple versus complex assessments (nested RM), (b) dealing with predictable (Gaussian) distribution versus unpredictable (heavy tailed or fractal probability distributions), (c) different methods used for each risk category, (d) integration of strategic and operational issues (e.g. StratOps risk with feedback loop) and (e) integrating post-incident reviews, stress test outcomes, and continuous improvement protocols in order to anticipate a large panel of evolving possibilities and take uncertainties into account. In this area, as noted in ATLANTIS Policy Brief #1 on aligning AI innovation with risk governance for CI, the use of AI-based tools can help stakeholders to make informed decisions quickly, as predictive analytics can optimize the allocation of resources by forecasting where impacts are likely to be highest.

For scenario or threat-led stress testing that includes collaborative threat research and simulation activities, the inclusion of third-party risk management (TPRM) is also recommended. TPRM should align strategic goals and the use of third parties in emergency situations (e.g. private security services during pandemics), while considering tradeoffs and derived risks. Reviewing business impact and aligning with the resilience strategy should address issues such as contract renegotiation or alternative supply chains to ensure business continuity. Indeed, technological and operational processes are often focused on short-term objectives, such as restoring disrupted services or securing systems against immediate threats. However, the short-term focus can engender tension between addressing urgent operational issues and pursuing long-term resilience goals. There might be also ambiguity about the scope of the problem and the best course of action, thus hindering the strategic decision-making process. Moreover, temporary operational conditions marked by uncertainty can further complicate the use of technology due to incomplete or evolving information.

To effectively address hybrid risks, the EU Commission ought to promote **convergence** (and not competition), starting with the AI and cybersecurity communities, but ultimately bridging across all relevant actors involved in CI resilience. Siloed approaches across sectors and Member States often result in overlapping standards and fragmented responses, making coordination harder and creating uncertainty around roles and responsibilities. Establishing a shared governance culture, based on common taxonomies, aligned certification schemes, and interoperable standards is essential to ensure coherent RM across domains.

Rather than reinventing frameworks, the EU should align initiatives like the **Cyber Resilience Act**, the **AI Act**, and existing ISO/IEC cybersecurity norms (e.g., 27001, 62443) to foster mutual reinforcement. A joint expert group, from all the MSs and pertaining to various domains, which is hosted by the European Commission and ENISA, could facilitate dialogue, oversee harmonization efforts and ensure that emerging AI-enabled tools integrate cybersecurity-by-design principles. This convergence would foster trust, operational efficiency, and cross-sector coherence in CI protection.

During rapid-onset events, such as disasters or pandemics, one might witness the rapid introduction of new technologies (e.g. contact tracing technology). It is important to understand trade-offs and whether decision and policy makers have time to rely on assessments to understand the capabilities, limitations, risks, and potential impacts of these technologies. This implies involving users in the design and testing phases, ensuring tools are practical, intuitive, and tailored to real-world operational contexts, enabling rapid reconfiguration in response to evolving crisis scenarios and dynamic threat environments.

Regarding preparedness and stockpiling, recommendations provided in the 2020 UNDRR Handbook for Implementing the Principles for Resilient Infrastructure [6] mention flexibility and diversity of

scales to deal with redundancy in supplies, but also in alternative supply chains. Operators should operationalize redundancy for smaller-scale solutions.

CI might rely on legacy systems that are outdated, making it difficult to integrate new technologies, data sources or resilience measures. The threats facing CI are constantly evolving, so tools and technologies need to be up to date, requiring flexibility and adaptivity "by design" (e.g. use of scalable architectures that allow extension of functionality such as collection of data at the end nodes). Operational frontline teams should have adequate tools, training, and resources to effectively execute resilience measures.

Public-Private Partnerships (PPPs): A crucial pillar of critical infrastructure resilience

To enhance the implementation of the CER and NIS2 Directives, the EU should accelerate the creation of an EU-wide network of trusted national PoCs. These PoCs would function as 24/7 clearinghouses for physical and cyber alerts, responsible for collecting, analyzing, and disseminating threat intelligence across stakeholders, including Internet Service Providers (ISPs), satellite providers, vendors, and national authorities. As envisioned under both directives, this network would form the backbone of cross-border coordination, improving incident response and information sharing across MSs.

A critical pillar of this effort lies in revitalizing PPPs to address persistent gaps in collaboration, joint crisis management, and investment in security infrastructure. The EU's Preparedness Action Plan [7] already recognizes the need to "formulate emergency protocols with businesses to ensure rapid availability of essential goods and services, and to secure critical production lines." However, turning this principle into practice requires a more structured and trust-based approach.

Drawing on insights from the CoESS White Paper and Catherine Piana's presentation (2024), the argument is clear: PPPs must leverage the complementary strengths of public and private actors. Public authorities contribute on authority, access to classified information, and democratic accountability, while private security companies (PSCs) bring operational expertise, technological innovation, and a culture of efficiency.

To make this collaboration effective, six core success factors must guide all PPP initiatives:

Figure 1: *The six core success factors of PPPs.*

1. **Trust:** Built through transparency, shared goals, and in-person relationships.
2. **Competency and value recognition:** Acknowledging each party's unique contributions.
3. **Communication and collaboration:** Including common taxonomies and aligned training.
4. **Culture and flexibility:** Aiming to promote adaptive mindsets and institutional learning.
5. **Legal frameworks and institutional anchoring:** Clearly defining roles and responsibilities.
6. **Data and technology management:** Ensuring interoperability and responsible data sharing.

A recurring obstacle is the exchange of sensitive information between public and private stakeholders. Yet, the advantages are substantial: improved resource allocation, predictive policing, crime scripting, continuity in crisis response, and learning loops across sectors. To navigate legal and operational constraints, several practical tools are available, including ISO 22396 (on inter-organizational information sharing), security clearances, NDAs, the Traffic Light Protocol (TLP), and encrypted communication platforms. Moreover, clarifying the national application of GDPR and strengthening hybrid public-private teams would further reduce frictions.

Legislators must support PPPs through targeted regulation, including public procurement rules, data governance frameworks, and standard-setting mandates. Law enforcement agencies (LEA) should institutionalize joint training and evaluation mechanisms with PSCs, while CI operators should engage in collaborative RA and maintain open communication channels with private actors. On their side, PSCs must prioritize staff training, regulatory compliance, and continuous innovation to be trusted partners in a dynamic security landscape.

Note that PPPs are not a side mechanism. They are integral to a broader security continuum. Trust, regulatory clarity, and a collaborative mindset are essential to unlock their full potential. With threats becoming increasingly complex and hybrid in nature, Europe must harness PPPs to deliver flexible, technology-enabled, and mission-driven protection for its CI.

With the right structures in place, PPPs can shift from reactive coordination to a lasting force for resilience, driving faster responses, smarter investments, and stronger protection for Europe's CI.

Policies Recommendations & Strategic Roadmap

To secure Europe's increasingly interdependent CI from systemic vulnerabilities, which are exacerbated by fragmented standards, hybrid threats and climate-induced disruptions, the EU must urgently pursue a **unified, interoperable, and forward-looking security framework**. Building on the outcomes of the ATLANTIS project, and aligned with the NIS2 and CER Directives, this roadmap outlines concrete short-, medium-, and long-term actions to embed resilience-by-design into European infrastructure governance.

The following recommendations reflect immediate operational needs, intermediate governance reforms, and long-term structural objectives to advance CI protection across the EU.

Short-Term (0–1 year): Focus on foundational resilience-building through harmonized RA, operational coordination, and capacity development

- **Mandate multi-hazard RA** covering physical, cyber and climate-related risks, within national CI protection strategies under the NIS2 and CER Directives, ensuring consistent threat baselines across MSs.
- **Establish a permanent coordination mechanism** for trusted national POCs to enable 24/7 cross-border information exchange on threats, based on common taxonomies and secure communication protocols.
- **Launch targeted capacity-building programs** for CI operators and regulators, emphasizing integrated RA, PP collaboration, and the operational use of stress-testing tools.
- **Introduce fiscal incentives for compliance with ISO/IEC 62443 and ISO 22396,** promoting early adoption of robust cybersecurity and crisis coordination standards across sectors.
- **Initiate cross-sector trust-building workshops.** Horizon Europe project consortia should organize structured dialogues between public and private CI actors to align expectations on

AI use, certification pathways and model oversight, filling a critical governance gap and promoting transparency.

Medium-Term (1–3 years): Advance regulatory coherence and operational readiness by scaling up institutional mechanisms and predictive capacities

- **Create a European Security Standards Hub** to align physical, cyber and climate security standards, bringing together ISA/IEC 62443, ENISA guidelines, and the UNDRR Principles for Resilient Infrastructure. As the UNDRR Principles are expected to become an ISO standard by the end of 2025, their adoption would reinforce international interoperability and policy alignment.
- **Deploy cross-border AI-powered threat forecasting platforms** building on the predictive analytics piloted in ATLANTIS and SUNRISE to detect cascading risks and hybrid threats across sectors such as transport, energy, and digital services.
- **Institutionalize regular collaborative crisis simulations,** drawing on the ATLANTIS Large-Scale Pilots (LSPs) and SUNRISE's operational models and stakeholder engagement strategies, to bring together CI operators, law enforcement, emergency services, and intelligence agencies for coordinated scenario-based stress-testing.

Long-term recommendation (3 years +): Institutionalize resilience-by-design through integrated governance, legislative convergence, and strategic foresight

- **Embed resilience-by-design as a foundational principle for all EU-level CI governance frameworks.** Legislative instruments such as the NIS2 and CER Directives could be progressively revised to foster convergence across domains, bridging cyber, physical and climate-related risk frameworks through interoperable implementation models and shared operational language
- **Establish a permanent inter-agency coordination mechanism** to connect intelligence services, regulators, and CI operators across MSs. This body, potentially under the umbrella of the EU Preparedness Union, should steer joint monitoring, information sharing, and hybrid threat response across critical sectors.
- **Operationalize a CI Infrastructure Resilience Data Observatory (CIR-DO)** as a central EU-wide platform for aggregating and curating heterogeneous datasets (from Earth Observation and cyber threat intelligence to climate models and supply chain analytics). The CIR-DO should support real-time situational awareness, feed predictive models, and reinforce evidence-based policymaking.
- **Ensure long-term policy continuity by transforming project-based outputs** from initiatives such as ATLANTIS, EU-CIP, and SUNRISE projects into durable strategic assets. This includes codifying validated practices, scenario exercises, and cross-border coordination protocols into EU-level guidance and future legislative proposals.
- **Leverage EU strategic foresight instruments** (e.g. via the Joint Research Center (JRC) and DG-HOME) to anticipate systemic disruptions and global shifts that could undermine CI resilience. Long-term horizon scanning, integrated with the CIR-DO, will inform preparedness strategies aligned with Europe's security, climate, and digital transitions.

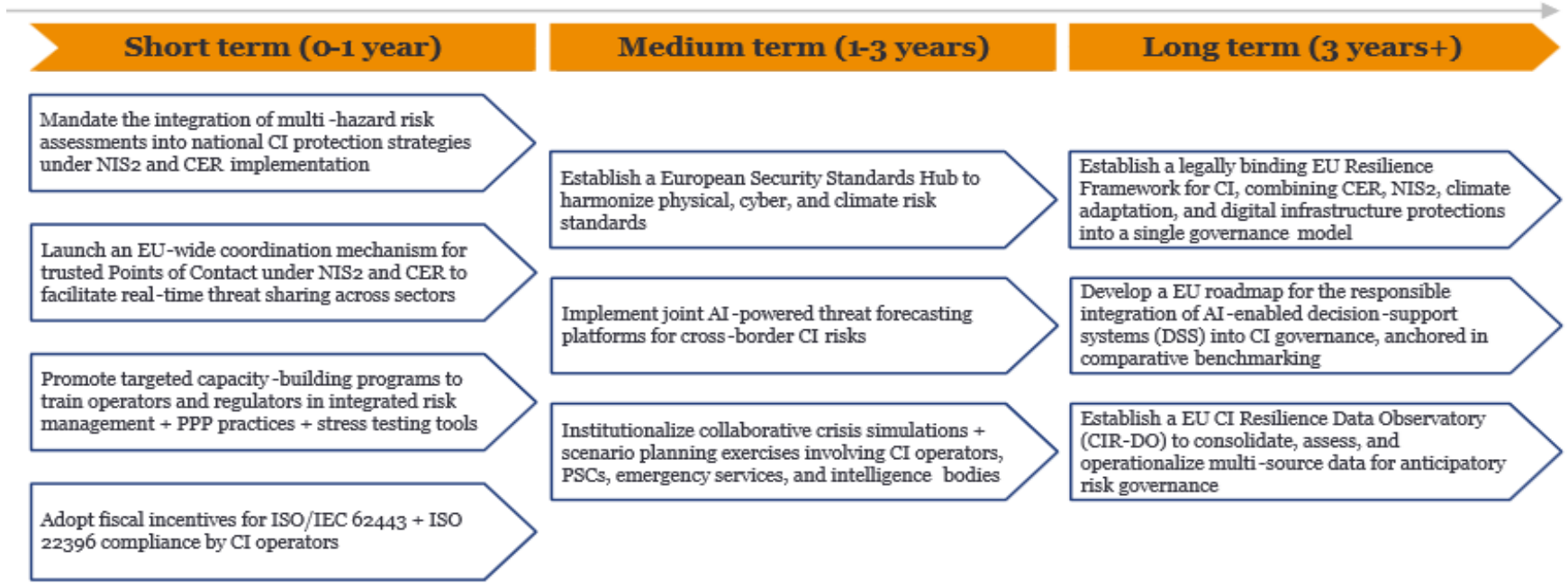

Figure 2: *Strategic roadmap for policy recommendations*

Looking Ahead

Europe's CIs are under mounting pressure from a rapidly evolving threat landscape, where cyber-attacks, climate-induced disasters, and hybrid risks increasingly intersect. This policy brief highlights the urgent need for a more integrated, interoperable, and forward-looking approach to CI protection. Fragmented standards, isolated RM practices, and inconsistent public-private collaboration continue to undermine the EU's collective resilience.

Drawing on insights from the ATLANTIS and SUNRISE projects, the brief underscores three strategic imperatives:

1. Harmonizing security standards across domains and MSs
2. Advancing dynamic and AI-enabled RM
3. Institutionalizing trusted public-private partnerships

These pillars are not only technically feasible but politically timely, as the EU enters a critical window to implement the NIS2 and CER Directives and align them with broader resilience and digital sovereignty goals. Action is needed now. The convergence of systemic risks and institutional gaps presents both a challenge and an opportunity. Without decisive coordination, Europe risks falling behind in its ability to anticipate, absorb, and adapt to disruptions. However, with the right frameworks, tools and partnerships, the EU can lead globally in designing infrastructure that is resilient by default.

The overarching message is clear: resilience must be built into the DNA of European infrastructure governance. This means investing in shared standards, enabling real-time threat intelligence, and fostering a culture of trust and collaboration across sectors and borders. The recommendations outlined in this brief offer a concrete roadmap to get there, starting with short-term actions like establishing national PoC and culminating in a long-term vision for a unified EU Resilience Framework.

References & Sources

[1] European Commission (2023). 2023 Strategic Foresight Report – Sustainability and people's wellbeing at the heart of Europe's Open Strategic Autonomy. Available at: https://commission.europa.eu/system/files/2023-07/SFR-23-beautified-version_en_0.pdf

[2] Piana, C. (2025, January 31). PPPs: Unlocking the potential for enhanced security [Presentation]. ATLANTIS Project Policy Taskforce working group session, Brussels, Belgium. CoESS. Available at: https://coess.org/newsroom/publications/white-paper-on-ppps/

[3] CoESS (2025) Shaping the Future of Critical Infrastructure Protection in Europe. White Paper, June 2025. Available at: https://www.coess.org/newsroom.php?page=white-papers

[4] U.S. Federal Government (2025). National Resilience Strategy. Available at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/National-Resilience-Strategy.pdf

[5] NIST (2024). Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, U.S. Department of Commerce. Available at: https://www.nist.gov/cyberframework

[6] UNDRR (2023). Handbook for implementing the principles for resilient infrastructure. United Nations Office for Disaster Risk Reduction. Available at: https://www.undrr.org/media/87213/download?startDownload=20250805

[7] European Commission (2023). Preparedness for future crises – a Strategic Approach. Brussels. Available at: https://commission.europa.eu/system/files/2023-07/SFR-23-beautified-version_en_0.pdf

[8] ENISA Threat Landscape 2023: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[9] ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems: https://www.iso.org/standard/50275.html

[10] UK Government Resilience Framework (2023): https://www.gov.uk/government/publications/the-uk-government-resilience-framework

[11] EU Strategic Foresight Report 2023: https://commission.europa.eu/system/files/2023-07/SFR-23-beautified-version_en_0.pdf

[12] Directive (EU) 2022/2557 on the Resilience of Critical Entities (CER Directive): https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[13] Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2 Directive): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

How to cite this brief

ATLANTIS Consortium (2025). *Resilient by Design: Integrating Standards, Tools and Partnerships to Secure Critical Infrastructure in Europe. ATLANTIS Policy Brief No. 3 (PIA3). Horizon Europe Project ATLANTIS (Grant Agreement No. 101073909). Brussels.*

Acknowledgements & Contributors

We would like to thank the following reviewers for their valuable comments and feedback. Their input helped to strengthen the clarity and coherence of the brief. The final content remains the responsibility of the authors.

Gabriele GIUNTA	ENG and ATLANTIS project coordinator
Emilia GUGLIANDOLO	ENG
Nidhi NAGABHATLA	UNU-CRIS and University of Ghent
Catherine PIANA	CoESS
Sean TRAVERS	Carr Communications
Rory McGLYNN	Carr Communications

This policy brief was coordinated by **Thomas SELEGNY** (RESALLIENCE), Policy manager of the ATLANTIS project, with contributions of:

David BAKER	UNDRR
Nestor ALFONZO-SANTAMARIA	OECD
Domenico di FRANCESCO	EY
Abla EDJOSSAN-SOSSOU	RESALLIENCE
Antonio KUNG	TRIALOG
Aljosa PASIC	EVIDEN and SUNRISE project coordinator
Josip RADMAN	Ministry of Infrastructure of Slovenia
Stefan SCHAUER	ATI
Vittorio ROSATO	Faculty of Engineering, University Campus Biomedico, Roma
Daniel VLADUSIC	XLAB
Nidhi NAGABHATLA	UNU-CRIS and University of Ghent

For more information on this brief, contact:

Thomas SELEGNY, thomas.selegny@resallience.com