SUNRISE

ATLANTIS

Enhancing Resilience of Critical Infrastructures in Europe

Insights and Recommendations from ATLANTIS and SUNRISE Projects

Policy Brief – December 2024

Co-funded by
the European Union

Executive Summary

Resilient Critical Infrastructure (CI) is the backbone of a stable and prosperous Europe, yet it faces mounting challenges stemming from systemic risks such as pandemics, cyber threats, climate-induced disasters, geopolitical developments, and continuous hybrid warfare that takes place not only in traditional urban and industrial hubs but also in remote areas such as underwater and in space. The EU-funded projects SUNRISE and ATLANTIS have combined their expertise to address these threats, offering a comprehensive perspective on enhancing CI resilience across the EU. Key insights from the projects highlight the critical need for proactive collaboration among organizations, sectors, and nations to address vulnerabilities effectively. They emphasize the importance of aligning with EU policies such as the CER and NIS2 Directives, integrating scenario-based planning to prepare for cascading risks, and adopting data-augmented Decision Support Systems (DSS) to enhance situational awareness and informed decision-making.

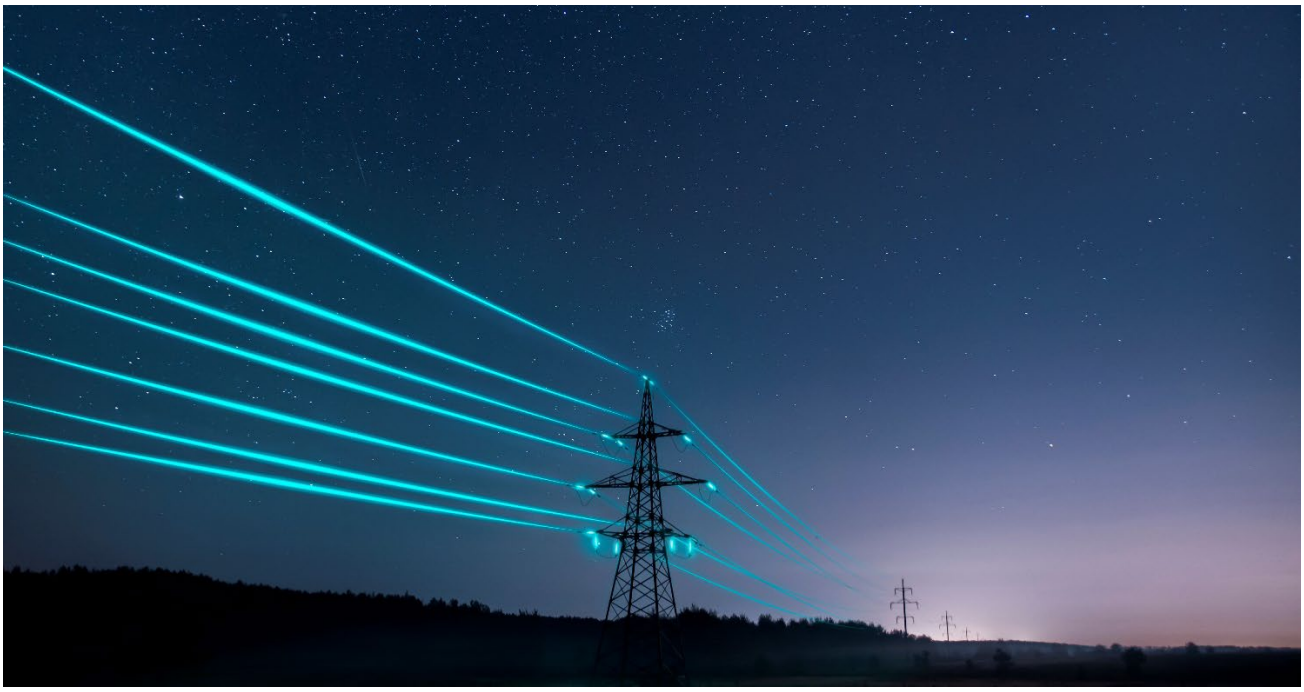
To secure the CI in Europe, the projects recommend immediate actions that focus on harmonizing standards across sectors, fostering real-time data sharing, and encouraging joint scenario-based exercises to build preparedness for crises. They also stress the adoption of AI-enabled DSS to manage complex risks and optimize resources in real-time. Strengthening these frameworks will not only address current vulnerabilities but also equip the EU to handle emerging challenges, ensuring societal stability and economic continuity.

The urgency is clear. As systemic threats grow in scale and complexity, the European Commission should act decisively. By leveraging the findings and recommendations from SUNRISE and ATLANTIS, the EU can spearhead a unified, innovative, and sustainable approach to CI resilience, securing a future that is safe, stable, and adaptive to unforeseen challenges.

The work presented in this policy brief has been partially funded by two projects, namely ATLANTIS and SUNRISE, which have received funding from the European Union's Horizon Europe framework programme under grant agreements No.101073909 and No.101073821, respectively.

Introduction

In recent years, Europe's reliance on resilient Critical Infrastructure (CI) has become increasingly evident, especially in the face of global shifts driven by growing interconnectivity of essential systems, geopolitical instability, and other human- or nature-induced hazards. The COVID-19 pandemic underscored the profound interdependencies between the CI and societal stability, as disruptions extended beyond healthcare into essential services like transport and energy. Furthermore, Europe's interconnected CIs are increasingly vulnerable to large-scale, cascading and compounding hazards - both natural and human-induced - that can ripple across sectors, across the entire supply chains, causing widespread societal and economic disruptions. Strengthening the resilience of the CI is now more urgent than ever, as Europe strives to ensure continuity, mitigate risks, and advance sustainably in a climate-conscious world.



Two Horizon Europe projects, namely SUNRISE (grant agreement ID 101073821) and ATLANTIS (grant agreement ID 101073909), have been funded to address these challenges through different but complementary approaches. SUNRISE focuses on the resilience of interconnected CIs specifically in the context of pandemics, promoting collaboration among the CI operators and authorities across Europe to identify vital services, understand their direct and indirect interdependencies, establish effective risk management strategies, and deliver adaptable tools that support their implementation. Meanwhile, ATLANTIS takes a similar but broader approach by addressing cross-organisational/-sectorial/-border CI resilience against large-scale, systemic risks associated with various cyber, physical, and hybrid threats through innovative security measures and advanced AI-based solutions.

Apart from delivering future-proof strategies and innovative data-driven tools, both projects also aim to understand existing policies designed to enhance the resilience of the CI in Europe, identify their weaknesses, and provide evidence-based recommendations for improvement.

This policy brief aims to inform the European Commission of key findings and recommendations derived from both projects. By integrating the pandemic-specific insights of SUNRISE with the broader, systemic resilience strategies of ATLANTIS, it offers a comprehensive perspective on enhancing CI resilience. The recommendations are designed to guide future policy development, presenting evidence-based strategies to ensure the continuity, security, and adaptability of the CI in Europe in the face of both anticipated and unforeseen hazards and risks.

Methodology

One of the main expected outcomes of the two projects is to contribute to shaping the ongoing EC-wide efforts on identifying key challenges and improvements required in the EU Policy Space, informing key actors about the needs of private and public CI stakeholders towards EU policy level, and enabling a technological leap forward to support greater CI resilience. In view of that, from a methodological point of view, the policy and standard assessment in SUNRISE and ATLANTIS was approached at strategic, technological, and operational levels, as described below.

The strategy for CI resilience has been addressed with a focus on (1) the multi-dimensional effects of systemic risks and threats to the CI, as a special case of temporary conditions, and (2) ways to increase the resilience of CI and continuity of vital services. The process of implementing the strategy started with an overview on the current situation and the context, including organizational, structural, and regulatory aspects. After the identification of general conditions, we have assessed possible scenarios, potential consequences, and available countermeasures that include special economic policies to tackle the effect of CI's systemic risks and threats to the economy.

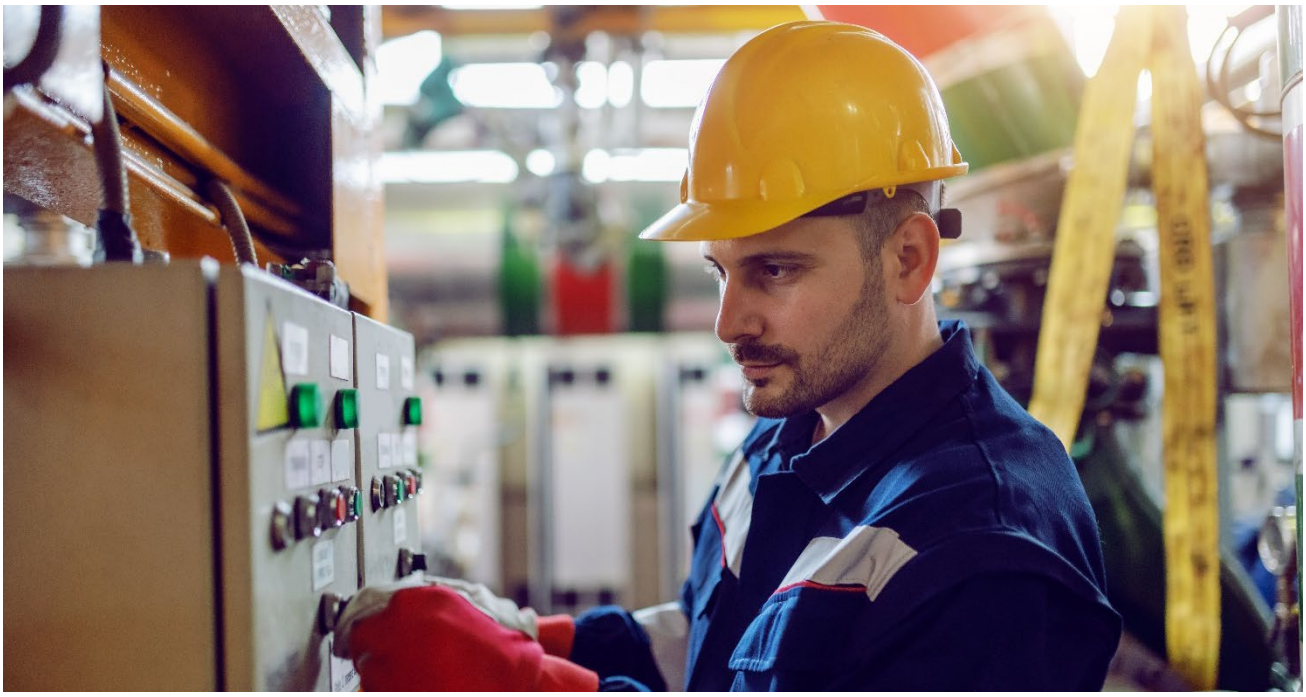
By encouraging the use of innovative technologies for cyber-physical-human threat detection to enhance CI resilience, both projects are fully in line with relevant directives and the EU Security Strategy. However, policies are based on assumptions about normal or emergency operations, with a limited number of in-between situations or scenarios where collaboration and adaptivity depend on workforce and supply chain availability. Several workshops with the involvement of CI operators were organised to discuss lessons learned from previous crises (including the COVID-19 pandemic) and technology adoption, assessing what worked well and what not, allowing policymakers to revise or update policies for better alignment with real-world capabilities and limitations.

Finally, several policy and standardisation Task Forces (TFs) were set up to gather and handle all the key findings derived from the previous two steps. The TFs gather representatives, on a voluntary basis, from the ATLANTIS and SUNRISE consortia and from external organisations, with relevant background and expertise. A fruitful collaboration and cooperation among the two projects, with other related EU-funded projects (e.g., EU-CIP and EU-HYBNET), and with other relevant stakeholders (e.g., CI operators, authorities, academics, external expert groups, etc.) was activated with the aim to gather, prioritize, and focus on policy-related information as well as to draft policy recommendations. In parallel, conferences, workshops, and other policy-focused events have been attended and organized to further emphasize the relevance of the EU Policy Space, assuring all the achieved outcomes from the two projects are developed consistently with the latest EU strategies, technologies, policies, and regulations, taking into account ongoing changes and initiatives for improvements.

Pilots

ATLANTIS includes three Large-Scale Pilots (LSPs) that aim to strengthen the resilience of CIs while focusing on selected critical sectors and considering different sector-specific systemic risks. LSP#1 is dedicated to increasing resilience in CI operators essential for the secure and efficient transport of goods along the Mediterranean Corridor - a critical route connecting Southern and Central Europe. It spans across different countries (Slovenia, Croatia, Italy, and France) and includes representatives of other sectors that heavily rely on the functioning of the transport services (and vice versa), namely telecommunications and energy. LSP#2 is focused on protecting mainly the health sector against complex cyber-physical threats, which can disrupt continuity of several essential services - including logistics and border control - across the borders of Greece and Cyprus. Finally, LSP#3 is aiming to bolster the cybersecurity of critical financial infrastructures and prevent major disruptions in banking and trading operations in Spain and Germany.

In contrast, SUNRISE defines four pilots that are based on the selected specific challenges that are common to different critical sectors. One is related to providing tools for risk-based access control to protect the essential workers and societies at large by better controlling physical access to critical infrastructure and facilities in pandemics to reduce the exposure of workforce to infectious diseases, while maintaining the continuity of operation of essential services. The technology is tested in a hospital in Slovenia and in factories in the Czech Republic. Second pilot provides solutions for remote infrastructure inspection to address the possible lack of personnel due to lockdowns and quarantines and maintain the critical physical assets functioning. This pilot is set in Slovenia and Italy in the energy sector, and in Spain in the water distribution domain. The third pilot is set in the digital and transport sectors in Slovenia, Italy, and Spain and addresses the growing cyber threats related to the convergence of information technology and operational technology systems, and specifically to the new challenges stemming from the increasing trend of remote working. The final, largest pilot is related to predicting resource demands to address changes in the needs of key resources such as skilled workers, hospital beds, energy, drinking water, and transport.



In both projects, each pilot serves not only as a testbed for new approaches and new technologies but also as a collaborative forum that engages diverse private and public stakeholders. By simulating real-world scenarios, these pilots offer critical insights into operational and strategic challenges, supporting the development of more cohesive and responsive frameworks for CI resilience across Europe. By (1) addressing a wide range of concrete challenges, (2) considering specifics of different critical sectors, (3) engaging public and private stakeholders from across Europe, and (4) facilitating cross-organisational, cross-sectorial, and cross-border collaboration, the projects have a great foundation to deliver sustainable and scalable solutions that address different geographical areas, sectorial specifics, physical environments, cultures, legal frameworks, and political contexts.

Existing Policies

The EU has implemented a wide range of policies and regulations that can significantly affect the strategy, tactical, and operational levels of CI operators across member states. These policies aim to enhance the security and resilience, but also efficiency of essential services and the underlying critical infrastructures. At a

strategic level, policies can impact long-term planning, resource allocation, and the overall investment. The NIS2 directive, for example, mandates CI operators to enhance cybersecurity measures, which implies that the CI operators must allocate resources towards investments in related technology, partnerships, and workforce development. Another type of policy, the CER Directive, targets cross-border collaboration, required to meet EU objectives for interconnected infrastructure systems and supply chain security, and requires CI operators to undertake (and share the results of) regular risk assessments considering both cyber and physical threats across the entire supply chains. Furthermore, the Cyber Resilience Act focuses on the security and resilience of (not necessarily critical) cyber systems; the AI Act regulates how algorithms and tools using AI concepts can be used in the EU to protect peoples' fundamental rights. In this way, both acts will also influence the daily business of CI operators.

In addition, in June 2024, the Critical Infrastructure Blueprint was adopted to strengthen the EU's capacity to respond to cross-border incidents disrupting essential services. It provides a roadmap for coordinated measures across key sectors, enhancing situational awareness and coordination at the EU level. Alongside the NIS2 and CER Directives, it is a crucial step in bolstering the resilience of the CI across Europe against evolving threats.

Besides that, the EU has adopted a variety of non-binding strategic frameworks related to civil security, which are connected to the protection and resilience of the CI in Europe. Several of these frameworks are essential points of reference for articulating joint action within the ATLANTIS and SUNRISE projects. Among them, the EU Cybersecurity Strategy represents the framework that NIS2 (and formerly NIS) implement. A particular part of that are hybrid threats that are on the rise given the fast-changing geopolitical situation and have already been discussed in the Joint Framework on Countering Hybrid Threats and the Joint Communication on Increasing the Resilience and Bolstering Capabilities to Address Hybrid Threats. In recent years, the European Commission also developed a wide range of policies to address climate change and natural hazards-related risks, such as the 2021 EU Adaptation Strategy, the European Climate Risk Assessment (EUCRA), or the European Disaster Resilience Goals. All of them focus on potential impacts from climate change across Europe on an environmental, economic, and societal scale and how to improve the preparedness against them.

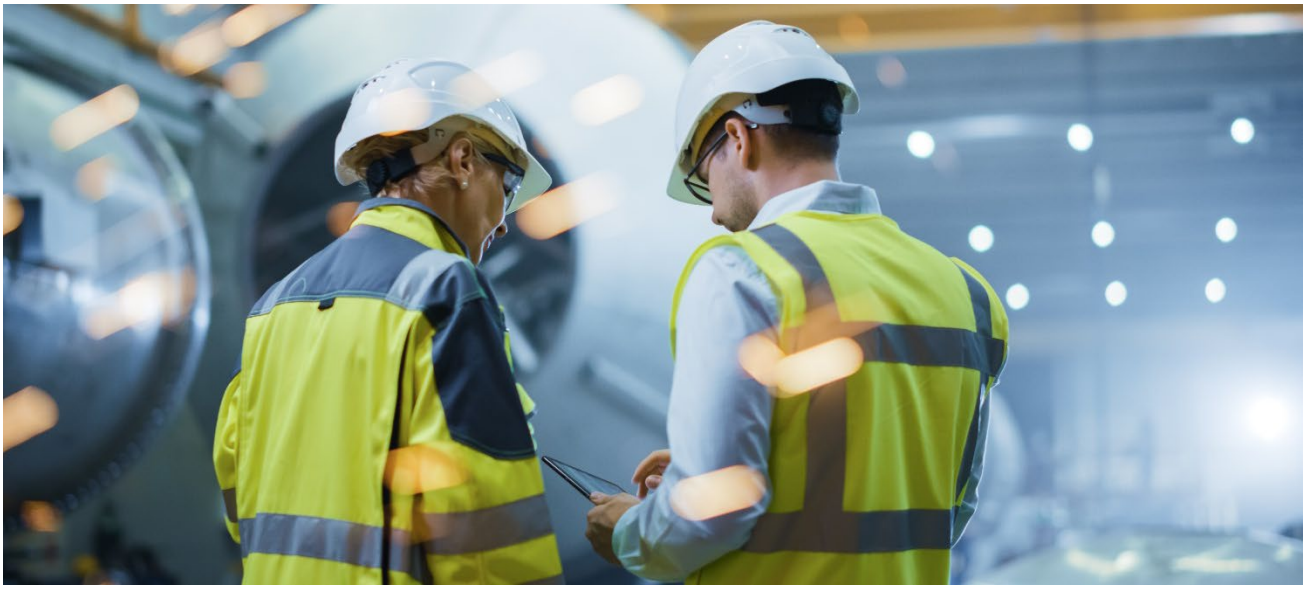
With their general focus on improving the resilience of CI, both ATLANTIS and SUNRISE are fully aligned with NIS2 and CER Directives. In ATLANTIS, a core focus lies on identifying and countering hybrid threats in a cross-organisational and cross-border setting, thus ATLANTIS is oriented towards the respective EU hybrid threat framework; in SUNRISE, the emphasis lies on preparing for the next pandemic, also considering the impact the climate change might have on the spreading of pandemics in the future, hence rather following the EUCRA and disaster resilience goals.

Key Findings

The policy-making endeavours in ATLANTIS and SUNRISE have resulted in a total of five main findings presented below.

With regards to ATLANTIS, the first key finding is the importance of the European Cybersecurity Strategy and its implementation by the CI operators. This strategy underscores a comprehensive security approach that advocates multilateral collaboration, the safeguarding of human rights, and democratic principles aiming to prevent conflicts, manage crises, and foster partnerships within and outside the EU. The second key finding focuses on enhancing cross-sector (and cross-border) security strategy effectiveness. This involves ensuring the relevance, applicability, interoperability, and adoption of solutions proposed by the project, aligning with current standards and policy trends, and contributing to the evolution of EU-level policies through foresight, engagement in policy and standards TFs, and dissemination activities. A core focus lies on collaborative risk management, space technology integration for Decision Support Systems (DSS), and harmonization of security standards across traditional, cyber, and natural hazards domains.

From the perspective of SUNRISE, the first key finding revolves around the specific operational context of critical entities. This relates to the strong focus of the CER Directive that these entities implement risk assessments, business continuity plans, and incident response protocols that assess threats to the continuity of service. The second key finding is the necessity of a multi-entity perspective on resilience. Since the CER Directive mandates risk assessments that consider interdependencies among critical entities, a multi-entity approach needs to be established through coordinated risk management and joint threat assessments, as well as contingency plans that consider dependencies on other sectors entities and supply chain vulnerabilities. The third key finding considers the importance of a coordinated emergency provision and response. Particularly the Integrated Political Crisis Response framework allows Member States to coordinate responses to major crises and facilitates information-sharing on a real-time basis. For example, cross-border coordination, rapid procurement and distribution of medical countermeasures are already emphasized by the EU Health Emergency Preparedness and Response Authority (HERA), and would also help critical entities to maintain operations when facing natural hazards, cyber-attacks, or other threats.



The key findings presented above in summary highlight the need for collaboration across organisations, sectors, and countries to address cascading risks and improve the overall CI resilience. This has been considered as essential in ATLANTIS and SUNRISE as well as in many previous EU policy documents. However, there are several challenges that still to this day persist to achieve optimal collaborations.

First and foremost, collaborating to enhance CI resilience often requires sharing sensitive (historical and, more importantly, real-time) data but organizations hesitate to share this information due to concerns over privacy, different levels of responsibility or accountability. Means to reduce barriers should be complemented by an assessment of incentives and motivational factors. Furthermore, CI operators are also highly interdependent and disruption in one system can cascade into others, complicating efforts to coordinate resilience strategies. Simulation tools and scenarios should address complex, adaptive systems with entities that often have differing capacities in terms of resources, urgency or expertise (that could be further affected by events such as pandemics).

Moreover, different organizations, sectors, or countries may have varying standards and practices for security, risk assessment, and resilience measures. Additionally, many CIs are managed by a combination of public and private entities, each with different goals, priorities, and constraints. Harmonizing these aspects is challenging, but necessary, especially when some industries are highly regulated while others are less so. Finally, the unpredictability of new and emerging threats makes it hard for stakeholders to agree on long-term resilience strategies. This is also linked to uncertainty in risk assessment, with divergent views on which resilience measures should be prioritized.

From a technological perspective, CI operators often rely on legacy systems that are outdated, making it difficult to integrate new technologies or resilience measures. On the other hand, the threat landscape is constantly evolving, so tools and technologies require continuous adaptation, and connection to real-time data sources about novel threats. Further, technology is often focused on short-term objectives, such as restoring service or securing systems against immediate threats. Plus, temporary operational conditions can significantly impact the effectiveness, dynamics, and decision-making processes. Hence, this can create tension between addressing urgent operational issues and pursuing long-term resilience goals. Technologies and tools should be adaptive enough to accommodate easily to temporary operational conditions.

Finally, despite the introduction of CER and NIS2 Directives, significant delays in their (national) implementation persist. As of November 2024, 23 out of 27 Member States have been notified of being too slow in transposing the NIS2 Directive into national law. There is an urgent need for capacity building to address knowledge gaps and ensure compliance. Not only to help the Member States with the transposition and enforcement, but also to ensure that the Member States are at similar preparedness levels and can effectively collaborate.

Policy Recommendations

Based on the discussions from the previous sections, we define two areas of priority for policy recommendations out of the ATLANTIS and SUNRISE projects: (R1) the application of scenario-based planning and (R2) the utilization of data-augmented Decision Support Systems.

Scenario-based planning is a method of preparing for diverse and unpredictable threats by simulating potential incidents and their cascading and compounding effects on critical infrastructure. It facilitates the identification of vulnerabilities, interdependencies, and effective response strategies, even during temporary operational conditions, such as those examied in SUNRISE in the context of pandemics. Scenario-based planning relies on diverse data inputs to construct plausible future scenarios, aligning closely with the principles of strategic foresight proposed by EC and OECD, which emphasizes exploring alternative futures to anticipate risks. This data must be provided from an operational level, for example, showing how operational conditions change in a temporary context (e.g., pandemics) or in response to geopolitical developments and hybrid warfare. It helps critical entities to plan resource needs under different conditions (e.g., staffing, equipment, financial resources).

As emphasized in both projects, the application of scenario-based planning for organizations to better prepare for various crises, such as natural disasters, cyberattacks, and economic disruptions, is critical. This approach reflects the foresight-driven policy-making supported by both the EC and OECD, which seeks to embed anticipatory and evidence-based planning into resilience strategies. By fostering collaboration and shared understanding across Member States and across sectors, scenario-based planning aligns with the CER and NIS2 Directives, which mandate risk assessments that consider various scenarios, including cross-border and cross-sector impacts. Furthermore, it helps policy makers and critical entities envision and prepare for non-linear consequences, ultimately improving operational readiness through the testing, validation, and refinement of resilience measures.

Data-augmented Decision Support Systems provide evidence-based situational awareness and enable real-time responses to incidents and, therefore, could help to provide actionable insights for managing risks, planning responses, and ensuring resilience. With the application of AI-based tools, the quality of DSS can be further improved, allowing for an extensive risk evaluation and resource optimization, and thus for quick and informed decision-making. In this context, ATLANTIS plans to leverage Space Technologies and Global Navigation Satellite Systems (GNSS) to improve the precision and effectiveness of DSS in managing CI in Europe, addressing specific aspects, i.e. data precision, resilience, and cybersecurity.

While the CER and NIS2 Directives require identifying risks and assessing vulnerabilities, data-augmented and AI-based DSS would enable this risk identification to happen in real-time, semi automatically, and continuously. In both ATLANTIS and SUNRISE, the significance of (real-time, heterogeneous) data-driven systems to create predictive analytics and to foresee disruptions or forthcoming demand for resources has been underlined. Such systems would help CI operators to fulfil and improve the requirement of a timely and accurate incident reporting as required by the CER and NIS2 Directives, e.g., by establishing a risk-based quantification that serves both obligatory reporting and voluntary threat sharing, and support joint risk assessments using harmonized datasets.

To translate the key findings from ATLANTIS and SUNRISE into actionable recommendations, we suggest the following short-, medium-, and long-term actions for the two priority areas.

R1. Develop and Deploy Scenario-Based Planning

Short-Term Actions

- R1.1. Conduct *regular stress tests and tabletop exercises* involving CI operators simulating a variety of temporary operational conditions (e.g., cyberattacks, natural disasters, pandemics, etc.).
- R1.2. Establish a *specific collaboration and communication framework* among the different public and private organisations from within and across borders to share real-time data and insights during temporary disruptions or service degradations aiming to enhance situational awareness and contingency planning.
- R1.3. Raise *awareness of CI operators and decision makers* on the importance of novel scenario-based exercises related to changes in operational context.

Medium-term Actions

- R1.4. Establish a *dedicated EU-level organization* building on existing EU-wide endeavours like the European Network for Cyber Security and Critical Entities Resilience Group to spearhead cross-sector and cross-border scenario development and implementation, foster knowledge exchange, and fortify resilience and emergency response strategies across the EU.
- R1.5. Strengthen *regional initiatives* to develop cross-border scenarios tailored to specific regional risks and interdependencies.
- R1.6. Incorporate *mandatory scenario-based risk assessments* from different sectors and countries into the regulatory framework for CI operators and establish information sharing protocols.

Long-Term Actions:

R1.7. Set up mechanisms for regular review and refinement of scenario-based planning approaches based on lessons learned from real-world incidents and operational exercises.

R1.8. Consider *scenario-related threats* within risk assessment and management as well as BCM methodologies on inter- and intra-organizational, sectorial, and national level.

R2. Set-up and Operationalize Data-Augmented Decision Support Systems

Short-Term Actions

R2.1. Conduct a *comprehensive review of existing DSS* used by CI operators across the EU to identify gaps in functionality, data integration, and user adoption.

R2.2. Leverage the Data Act to *mandate and encourage voluntary (historical and real-time) data sharing*, enabling real-time situational awareness and support a more robust security posture across interconnected systems.

R2.3. Promote *best practices and available, effective measures* for CI operators not having situational awareness or DSS to quickly enhance decision-making capabilities.

R2.4. Establish *secure data-sharing protocols* between critical entities across sectors and borders to ensure DSS have access to relevant, high-quality, and real-time data, improving the accuracy and utility of risk assessments and predictions.

Medium-term Actions

R2.5. Develop a *modular DSS framework* for temporary operating conditions customizable to different CI sectors, scenarios, and multi-entity perspectives.

R2.6. Establish a *collection of countermeasures* to support decision makers in countering the multi-dimensional effects for different threat scenarios.

R2.7. Provide *training programs for CI operators* to effectively use DSS tools to improve the ability to forecast demand, allocate resources, and anticipate risks under various scenarios.

Long-Term Actions:

R2.8. Establish an increased *collaboration among CI operators* on collaborative DSS to share tactical- and strategic-level best practices as well as emergency response.

R2.9. *Standardize the application of DSS* across all critical sectors with the use of real-time and cross-sector data.

Overall, scenario-based planning and decision support systems mainly strengthen and drastically improve decision-making under uncertainty, which CI operators and governmental bodies are often facing when dealing with complex crisis situations. Scenario-based planning helps organizations to look into the future, consider complex – even unlikely – events as well as to anticipate how different conditions might impact their operations and plan accordingly. Data-augmented DSS help decision-makers to comprehend the current situation, analyze data, evaluate risks, and choose optimal courses of action based on the given data. Accordingly, both aspects can be used in training personnel to improve the collaboration under extreme operational conditions, including regular crisis simulations that involve multiple stakeholders, as well as the preparedness for rapid decision-making and coordination during real adversary events.

Conclusions

The SUNRISE and ATLANTIS projects highlight the critical importance of enhancing the resilience of the CI in Europe in order to safeguard societal stability and economic prosperity in the face of increasingly complex and systemic threats. Key findings underline the need for a proactive cross-organisational, cross-sectorial, and cross-border collaboration, the integration of scenario-based planning, and the adoption of data-augmented Decision Support Systems to address vulnerabilities effectively. The projects also emphasize the importance of aligning resilience strategies with evolving EU policies such as the CER and NIS2 Directives while addressing gaps in areas like hybrid threat mitigation, multi-entity coordination, and adaptive technological frameworks.

To ensure progress, the EU must act. The rapid pace of global change - spanning pandemics, cyber threats, and climate-related disasters - demands immediate policy adaptations and proactive investment in innovative resilience measures. Collaborative initiatives involving CI operators, public authorities, and other relevant private stakeholders should be prioritized, with a focus on harmonizing standards, enhancing real-time data sharing, and fostering a culture of unity and preparedness. By leveraging the insights and recommendations from SUNRISE and ATLANTIS, the European Commission can lead a coordinated effort to secure the CI in Europe, ensuring a resilient, sustainable, and future-proof foundation for its citizens and economy.

Contributors

Contributors are listed in alphabetical order:

Aljosa Pasic	Eviden
Gabriele Giunta	Engineering Ingegneria Informatica S.p.A.
Jolanda Modic	ICS Ljubljana
Judith Kieran	Carr Communications
Maria Carolan	Carr Communications
Milan Tarman	ICS Ljubljana
Oisin McQueirns	Carr Communications
Stefan Schauer	AIT Austrian Institute of Technology
Thomas Selegny	RESALLIENCE

As part of the review process, this brief has benefited from comments and suggestions from the following members of the ATLANTIS Advisory Board and SUNRISE External Expert Group:

Arthur van der Wees	Arthur's Legal
Denis Čaleta	ICS Ljubljana

For more information on this brief, contact:

Gabriele Giunta, gabriele.giunta@eng.it

Aljosa Pasic, aljosa.pasic@eviden.com