ATLANTIS

In collaboration with

SUNRISE

Operationalizing Earth Observation for Critical Infrastructure Resilience: Interoperability and standardization insights from ATLANTIS

Policy Brief - August 2025

Co-funded by
the European Union

Executive Summary

This policy brief aims to enhance the resilience of European critical infrastructure (CI) through Earth observations (EO) and other space-based solutions, while addressing areas for potential improvement. It responds to the urgent need to protect CI against escalating climate-driven hazards and hybrid threats, ensuring operational continuity across Europe's interconnected infrastructure. CI across Europe is increasingly using EO from satellites, aircrafts, drones, and other space-based technologies. Note that EO systems like Copernicus Sentinel satellites provide high-resolution data to monitor structural vulnerabilities and potential impacts/disruptions in energy grids and transport networks. and EO can technically offer CI operators the capability to track changes in a timely manner over large, potentially remote, areas and, possibly, risky conditions. In turn, this tracking capability potentially leads potentially to early warning systems.

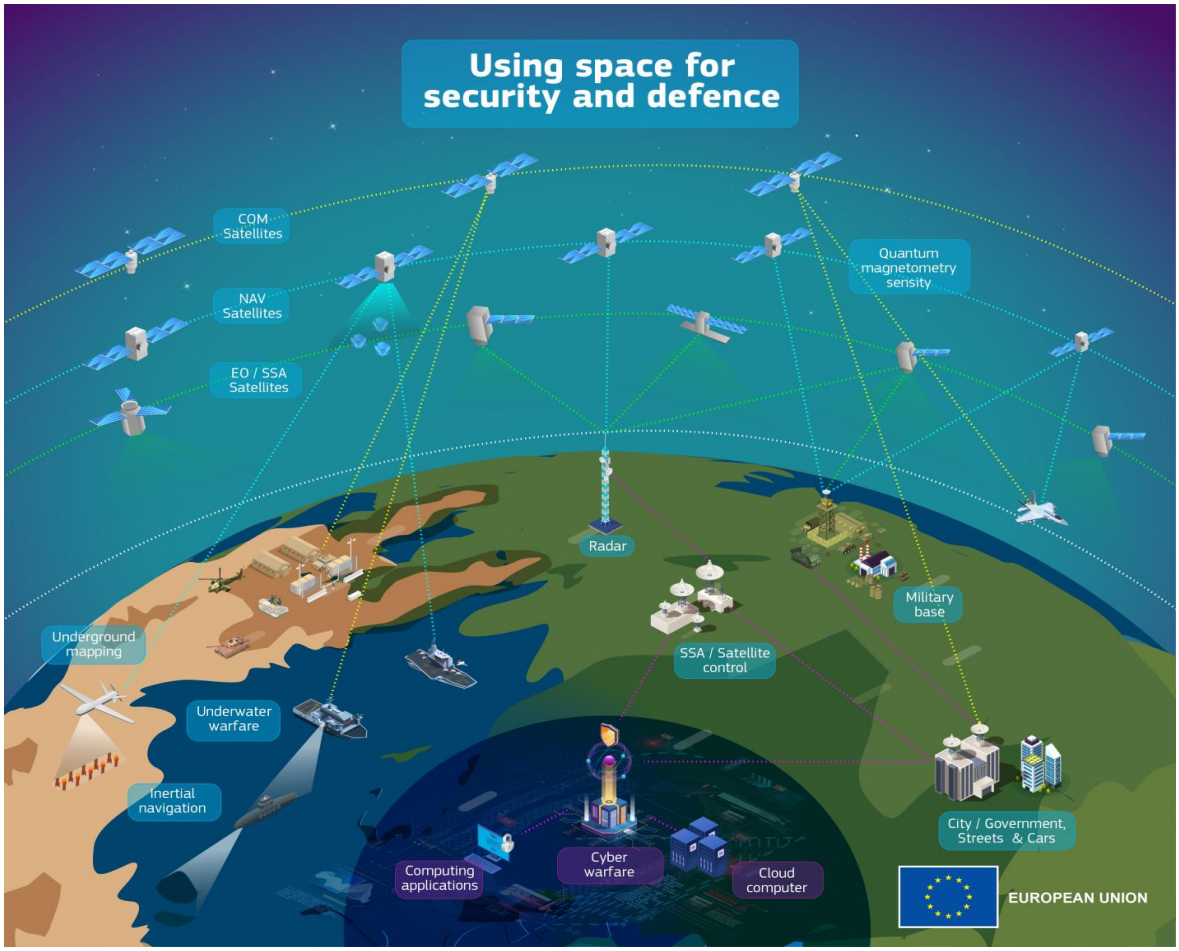


Figure 1: *European Commission, EU Space Strategy for Security and Defence, 2023. © European Union, 2023*

The growing reliance of CI on space-based solutions, such as observations, navigation, and communications (figure 1), implies that common issues, such as the need for standardization and interoperability amongst EO, ought to be addressed. We reiterate that fragmented data usage across Member States (MSs) delays coordinated responses, exacerbating risks to CI security. However, leveraging space-related knowledge, experience, and capabilities of MSs and EU institutions, can bolster the resilience of CI from hybrid threats. Emerging technologies, such as AI and quantum encryption, can further strengthen EO security by enhancing data integrity and predictive hazard modelling through inputs like surface information (surface temperatures, surface and soil humidity,

land cover, etc.), underscoring the need to prioritize governance frameworks that support their integration. We focus on these strategic aspects, aiming to provide actionable recommendations for policymakers and industry leaders, including a strategic roadmap with short, medium-term steps.

The brief's objectives are to describe the barriers encountered when using EO data to protect CI, and to propose measures that will inform policy, support standardization, and raise awareness of CI resilience. The brief further enhances its connection to broader frameworks from the ATLANTIS and SUNRISE projects with the EU strategies on space (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2023) and internal security (European Commission, 2025), ensuring alignment of project outcomes with EU priorities. Key findings highlight the critical need for standardizing EO-based information and services to protect CI against hybrid threats, as demonstrated by the ATLANTIS large-scale pilot (www.atlantis-horizon.eu), which addressed the impact of floods and wildfires.

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.

Introduction

The role of Earth Observation space-based technology in critical infrastructure resilience

European CI (transport, energy, water, and digital communication systems) faces growing risks from climate change, extreme weather, and hybrid threats, including GNSS (e.g. GALILEO/EGNOS) jamming incidents that disrupt satellite-based navigation. Space-based EO sensors, such as Synthetic Aperture Radar (SAR) and multispectral imaging, are recognized as valuable tools to enhance CI resilience (Der Sarkissian et al. 2023). These systems deliver reliable imagery and radiofrequency data to detect and monitor impacts affecting CI, e.g. coastal erosion threatening port facilities (Pranzini et al. 2015). By enabling timely detection and response, EO helps estimate disruptions that could cascade across interconnected CI sectors, aiming at reducing potential significant economic and societal impacts.

EU initiatives, such as the CER Directive and the EU Space Programme, highlight EO's value in enhancing the resilience of CI. Horizon Europe projects like ATLANTIS demonstrate practical applications, such as mapping floods, landslides and wildfire risks in transboundary regions to support coordinated response. However, EO data is often underutilized in operational risk management due to uneven integration and a lack of standardized data formats across systems and sectors. This gap can delay responses to fast-evolving crises, such as wildfires or cyber threats. By leveraging AI-driven analytics, EO can monitor hazards like floods, landslides and earthquakes, and forecast their impacts on CI, enabling proactive mitigation and reducing economic losses.

This policy brief advocates for the standardized use of space-based EO technologies to strengthen CI resilience (Figure 2). It emphasizes EO contribution to the monitoring and protection of EU-wide CI, as well as cooperation with third countries to protect CI beyond the EU. EO integration with frameworks like the EU Space Program and the UN Committee on the Peaceful Uses of Outer Space (COPUOS), as well as the combination of EO data with ground-based sensors, can enhance decision-making and safeguard CI. This approach could support cost-effective hazard mitigation and ensure the continuity of Europe's space capability.

Figure 2: ESA ground station network / CC BY-SA 3.0 IGO

Need for standardization in Earth Observation for critical infrastructure protection

The protection of EU and Member States (MSs) CI increasingly relies on the seamless integration of space-based services. However, fragmented data usage and inconsistent practices across involved stakeholders hinder the capability to leverage these technologies effectively, exposing CI to systemic risks. Standardizing the use of space-based services is essential to ensure interoperability, enhance data sharing, and strengthen resilience. By drawing on lessons from the ATLANTIS project, in particular for EO-based services and emerging technologies like AI and quantum encryption (EuroHPC), more cohesive frameworks to safeguard critical services can be developed.

Fragmentation in EO data usage poses a significant barrier to CI protection. Different MSs, and even practitioners within the same MS, often employ diverse EO data formats and processing tools, leading to inconsistent information that delay coordinated responses. The ATLANTIS project has demonstrated these gaps, showing how non-standardized EO data delayed risk assessments for gas pipelines exposed to landslides (Deliverable 4.5 of ATLANTIS – https://www.atlantis-horizon.eu/deliverables/). Without common metadata, standards and interoperable interfaces, overlaying EO data with CI asset maps or combining it with Positioning, Navigation and Timing (PNT) for precise geolocation remains inefficient, undermining the EU's ability to protect CI.

Standardization of data collection, usage and data-sharing systems are vital to unlocking the full potential of space-based services for CI resilience. The ATLANTIS project illustrates how standardized EO solutions enable faster integration of hazard maps with CI assets, improving coordination across stakeholders. For example, harmonized EO data formats allowed ATLANTIS to map flood risks in transboundary river basins, supporting timely responses for transport and energy infrastructure (Belenguer-Plomer et al. 2025). Similarly, integrating EO with satellite communications (e.g. GOVSATCOM for secure data relay) and PNT (e.g. Galileo for precise geolocation) enhances real-time monitoring and response capabilities. The Copernicus program and the International Charter on Space and Major Disasters (https://disasterscharter.org/fr) provide models for standardized data sharing, enabling seamless information flow across borders. However, broader adoption of such frameworks is needed to ensure space-based services work cohesively, aligning with technical standards like those in the EU Space Program and COPUOS guidelines (UNOOSA, 2025).

AI and quantum encryption enable standardization and security for space-based services. AI processes Earth Observation data to estimate potential infrastructure impacts, while quantum encryption secures data transmission. Standardized frameworks integrating these technologies ensure information consistency and secure data, enhancing CI resilience.

Need for interoperability in Earth Observation for critical infrastructure protection

Interoperability, the seamless connection of the space-based services across platforms and borders, is also key to transforming EO data into actionable insights for CI protection. While standardization ensures consistent data formats, interoperability enables systems to work together, supporting rapid crisis response and long-term planning. The ATLANTIS project underscores the urgency of addressing gaps in cross-system functionality, skills shortages and regulatory alignment to safeguard CI against evolving threats.

Fragmented tools and isolated datasets across MSs hinder the effective use of EO for CI protection. For instance, monitoring cyberattacks on digital infrastructure, such as telecom networks, is

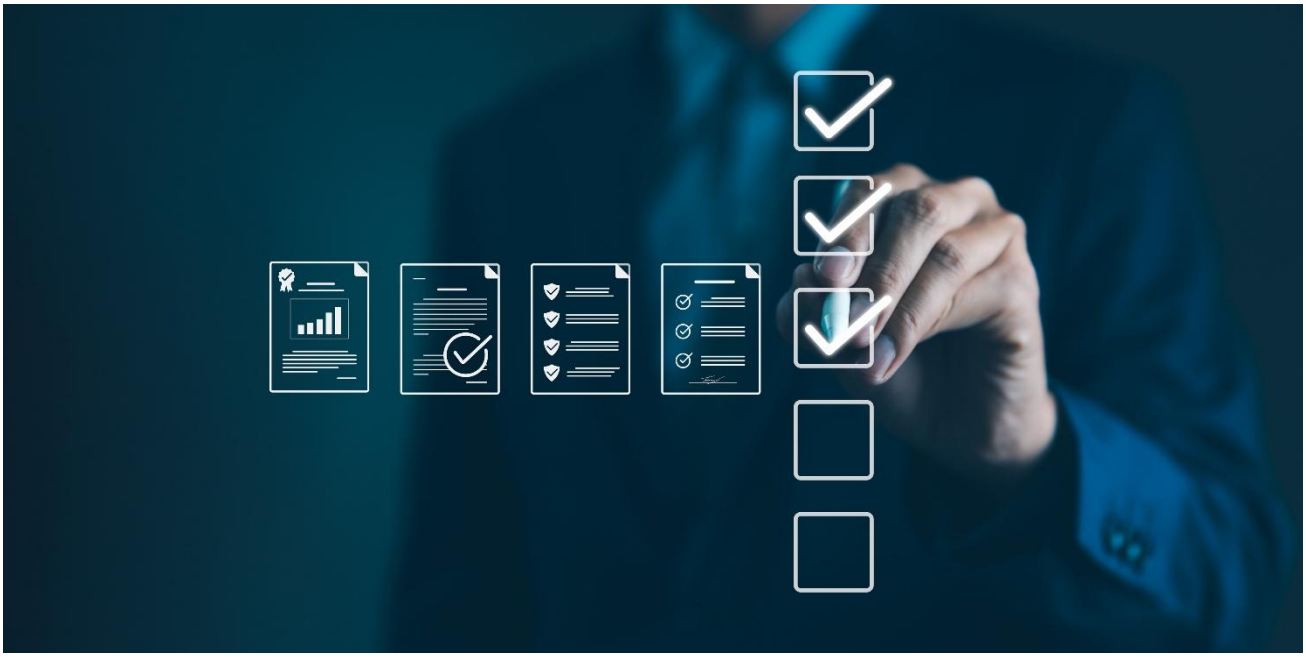
complicated when EO platforms produce incompatible outputs, delaying threat detection. The ATLANTIS project has shown that interoperable EO systems can overcome these barriers, as demonstrated in its pilots, which integrated EO with geographic information systems (GIS) to map wildfire risks for energy infrastructure (Belenguer-Plomer et al. 2025). The absence of harmonized interfaces also restricts the ability to combine EO with satellite communication for secure space data relay, exposing CI to risks. The Copernicus Space programme (https://www.copernicus.eu/en) offers a model for interoperability, providing open-access EO data through Sentinel satellites to support emergency response and climate adaptation. By integrating EO with different systems, authorities can enhance real-time monitoring, as seen in ATLANTIS's cyber threat detection pilots for financial infrastructure. The International Charter on Space and Major Disasters further demonstrates how interoperable data sharing enables cross-border crisis response, such as coordinating flood recovery for transport networks. The EU CER Directive (EU, 2022/2557) emphasizes space as a critical sector, calling for risk assessments of ground-based infrastructure. Aligning with technical frameworks, like the EU Space Program, ensures scalable integration, but gaps in cross-regional collaboration and regulatory implementation persist, limiting cohesive action.

Policies Recommendations & Strategic Roadmap

Aligned with the Horizon Europe programme, ATLANTIS project outcomes and the EU CER Directive (EU, 2022/2557), the following roadmap outlines short- and medium-term actions to enhance coordination, security and collaboration, ensuring space-based services safeguard CI infrastructure effectively. EO, satellite communications, positioning, and navigation should be integrated into CI resiliency frameworks.

Yet, it is important to mitigate the impact of potential risks affecting EO-based services and systems that could trigger cascading effects across CI, such as disrupted data flows or undetected impacts.

The following recommendations address immediate, intermediate, and future priorities to strengthen CI resilience through EO.



Short-Term (0–1 year): building technical capacity and standardizing responses to mitigate urgent risks

- **Foster a collaborative environment** for sharing technical expertise, drawing on ATLANTIS's success in mapping wildfire risks to inform best practices for EO integration (Belenguer-Plomer et al. 2025)
- **Perform regular climate and cybersecurity risk assessments** across ground-based space infrastructure, such as EO data centers, to identify vulnerabilities like flood-prone areas or data breaches, guided by models like the UK Space Agency's Climate Change Adaptation Report (UK Space Agency, 2025).

Medium-Term (1–3 years): Advance interoperability and regulatory frameworks to ensure cohesive EO-based service integration

- **Developing standards (e.g. leveraging ATLANTIS outcomes) at national level**. Without national buy-in, cross-border compatibility could falter, as MSs have varying technical capacities and regulatory priorities. National agencies must integrate these standards into their CI protection protocols, which may require capacity-building and funding support from the EU.
- **Including space-based infrastructure in the national transposition of the EU Critical Entities Resilience (CER) Directive.** MSs will need to adapt their regulatory frameworks to embed EO-driven monitoring, which could face resistance due to differing national priorities or resource constraints. EU guidance and incentives (e.g. funding via Horizon Europe) could bridge this gap.
- **The push for AI factories and public-private partnerships (PPPs) relies on MSs, aligning their innovation ecosystems with EU goals**. National policies must encourage local industries to participate in these partnerships, ensuring that EO applications are tailored to local CI needs while meeting EU standards.

Long-term recommendation (3 years +): EO should be embedded as a cornerstone of CI protection and align with global frameworks to ensure scalable resilience

- **Embedding EO into CI governance** requires MSs to integrate EO data into national planning processes. This demands national legislation or policies that prioritize EO, which may be challenging for MSs with limited space technology expertise. EU support, such as technical assistance or shared infrastructure, could facilitate this.
- **Aligning with global frameworks like the Outer Space Treaty or International Charter** requires MSs to harmonize their national space policies with international obligations. This could involve updating national laws to enable cross-border EO data sharing, which may face hurdles due to sovereignty concerns or data security policies.
- **A potential EU Space Law, such as the EU Space Act (EU Space Act - European Commission)**, would need MSs to align national regulations with EU standards. This could be complex, as MSs have diverse legal systems and economic priorities. A phased approach with pilot projects could help test and refine this alignment.
- **Requiring private EO companies to conduct regular risk assessments aligned with EU guidelines** would necessitate MSs to enforce these standards locally. National regulators would need to develop oversight mechanisms, which could strain resources in smaller MSs.
- **Adopting quantum encryption for EO data transmission** requires MSs to invest in compatible infrastructure. National cybersecurity agencies must align with EuroQCI standards, which could involve significant costs and technical upgrades.

Implementing these actions will enable the creation of a scalable, secure EO ecosystem aligned with the Space Programme and COPUOS guidelines. This roadmap strengthens CI resilience, mitigates cascading risks, and positions Europe as a global leader in space-based services for CI protection, ensuring critical services remain robust and future-proof.

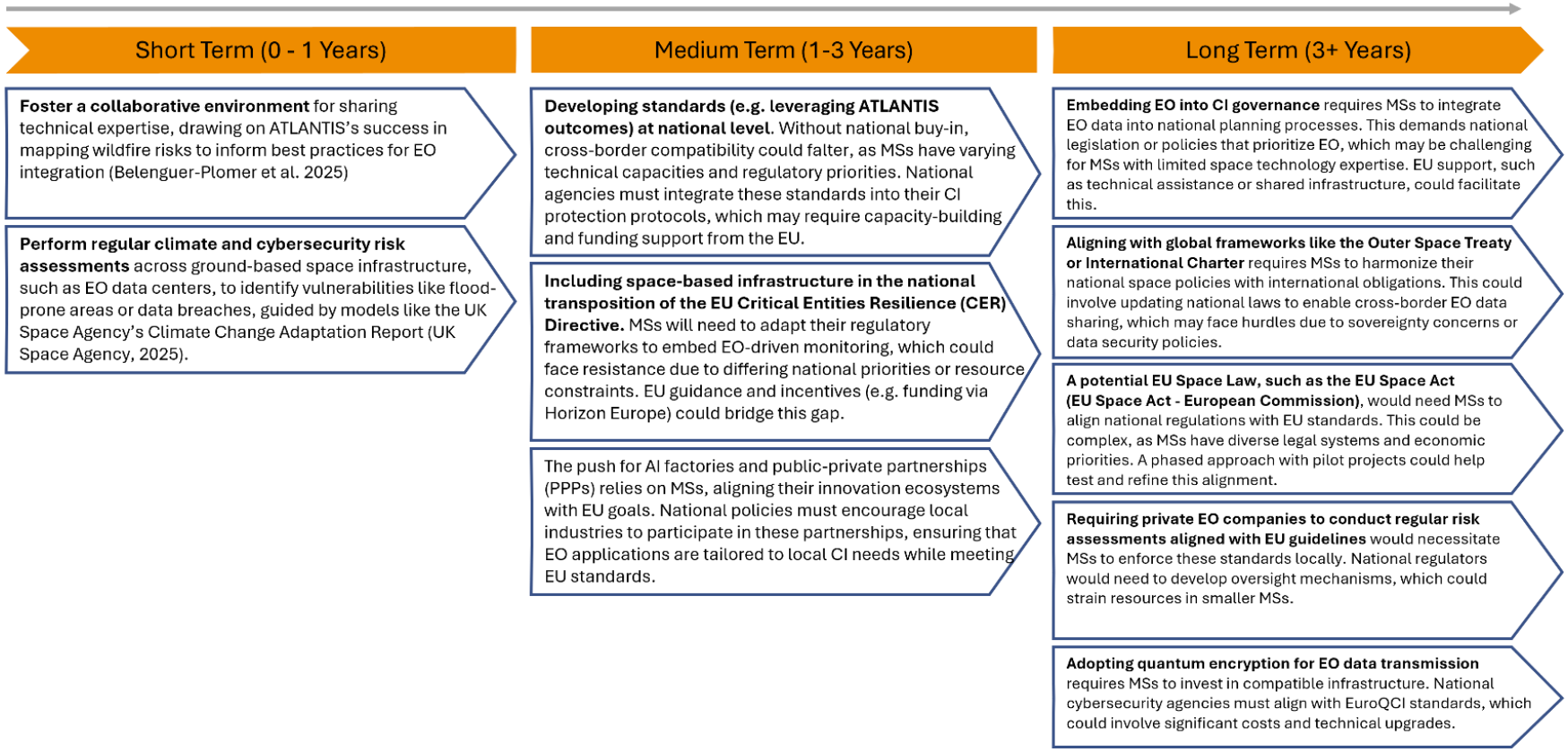


Figure 3: *Strategic roadmap for policy recommendations*

Conclusions

The ATLANTIS project highlighted how EO can enhance CI resilience, yet persistent gaps in data compatibility hinder progress. The evolving threat landscape demands immediate action to prevent disruptions that could cost billions annually. By fostering harmonized standards, investing in AI and quantum encryption, and encouraging public-private collaboration, these risks can be mitigated, as outlined in the strategic roadmap.

Policymakers and industry leaders must act now to perform EU-wide risk assessments, develop interoperable frameworks, and leverage existing expertise in the EU and across the MSs, in international organizations and third countries. Upcoming opportunities, such as Horizon Europe's innovation cycles, offer platforms to advance these priorities. Further analysis of emerging technologies and training programs is needed to ensure scalability. Protecting space-based infrastructure is urgent to secure CI, positioning Europe as a leader in resilient, future-proof systems.

Strategic Insights

The resilience of Europe's CI, from energy grids to transport networks, is increasingly relying on EO for its monitoring and protection of the systems providing these data and services. Space-based EO services and data rely not only on the protection of the space segment (i.e. satellites), but also on the protection of on-ground components (e.g. ground segment, user segment). These systems are exposed to an evolving array of man-made threats (sophisticated attacks blending cyber, physical, electronic, and informational tactics) that look for vulnerabilities and can disrupt critical services used for CI monitoring. Understanding these threats and their impact on infrastructure, especially EO infrastructure, underscores the urgent need for standardized, secure frameworks to protect EU space infrastructure.

Hybrid threats combine diverse tactics to disrupt systems without triggering open conflict, even beyond CI. For example, cyberattacks pose a significant threat to EO ground-based infrastructure, targeting the integrity and availability of data from systems like Copernicus Sentinel satellites, which are vital for monitoring impacts such as flood and fire spread or energy grid stability. A single breach could delay early warning systems, amplifying disruptions across interconnected sectors. Physical attacks on ground stations, as shown in the European Space Agency's Estrack network (figure 2), could sever satellite communication links, halting data relay for real-time oversight. Electronic warfare, like signal jamming or spoofing, further complicates matters by interfering with satellite navigation or data transmission, undermining important applications. Misinformation campaigns add another layer, exploiting EO imagery to spread false narratives, eroding public trust in disaster response systems. The EU's Space Strategy for Security and Defense highlights the dynamic nature of these threats, emphasizing the need for robust technical solutions to safeguard EO systems and their role in CI resilience (European commission, 2023).

The vulnerabilities of EO ground-based infrastructure stem from its global distribution and reliance on interconnected systems. Ground stations, often located in remote areas like French Guiana or Australia, face exposure to natural hazards such as tropical storms or earthquakes, which could disrupt satellite operations essential for infrastructure monitoring and/or operation. Cyber risks are equally pressing, with data centers vulnerable to hacking or ransomware that could corrupt data,

causing impacts such as delaying alerts for floods or wildfires and increasing economic costs for CI recovery.

The EU Space Program (EC, 2021) flagged cybersecurity as a primary concern, noting the risk of unauthorized access to sensitive data. Electronic vulnerabilities, such as jamming of satellite signals, can disrupt the precise timing needed for EO applications, while insufficient training among operators heightens risks of human error or social engineering attacks, as noted in the Digital Europe Programme (EU, 2021). A lack of standardized data formats across MSs further hinders secure data sharing, leaving EO systems fragmented and less effective in crisis response. These vulnerabilities, compounded by reliance on foreign technology, expose EO infrastructure to supply chain risks, which underscores the need for cohesive standards to protect CI and enhance the EU's economic security.

Recent incidents illustrate the growing threat to EO infrastructure and the stakes for CI resilience. In 2022, a cyberattack on Viasat's KA-SAT network disrupted satellite communications across Europe, affecting ground terminals and delaying data flows critical for CI monitoring (Viasat, 2022). This incident revealed how cyberattacks can compromise EO data integrity, impacting sectors like telecommunications. Signal jamming in the Baltic region disrupted the Global Positioning System and EO satellite signals (France 24, 2024), threatening air travel and CI monitoring for transport and energy networks. Such electronic warfare tactics highlight the need for resilient communication systems. A 2021 anti-satellite test in Low Earth Orbit generated debris that endangered EO satellites (Nasa, 2021), posing a physical risk to Europe's space infrastructure. These cases, among others, emphasize the need to protect space systems, specifically ground segments, against various hazards and threats, minimizing economic and operational impacts.

References & Sources

[1] European Parliament & Council of the European Union. (2021, April 28). Regulation (EU) 2021/696 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing previous acts (OJ L 170, pp. 69–148). Official Journal of the European Union.

[2] European Commission. The Digital Europe Programme (DIGITAL). Accessed August 19, 2025. European Commission Digital Strategy. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[3] Rita Der Sarkissian, Youssef Diab, Marc Vuillet, The "Build-Back-Better" concept for reconstruction of critical Infrastructure: A review, Safety Science, Volume 157, 2023, 105932, ISSN 0925-7535,: https://doi.org/10.1016/j.ssci.2022.105932

[4] European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2023, March 10). Joint communication to the European Parliament and the Council: European Union Space Strategy for Security and Defence (JOIN(2023) 9 final). Brussels.

[5] European Commission. 2025. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ProtectEU—A European Internal Security Strategy (COM(2025) 148 final). Strasbourg, April 1.

[6] Belenguer-Plomer, M.A.; Barrilero, O.; Saameño, P.; Mendes, I.; Lazzarini, M.; Albani, S.; El Beyrouthy, N.; Al Sayah, M.; Rueche, N.; Edjossan-Sossou, A.M.; et al. Remote Sensing as a Sentinel for Safeguarding European Critical Infrastructure in the Face of Natural Disasters. Appl. Sci. 2025, 15, 8908. https://doi.org/10.3390/app15168908

[7] Pranzini, E., Wetzel, L. & Williams, A.T. Aspects of coastal erosion and protection in Europe. J Coast Conserv 19, 445–459 (2015). https://doi.org/10.1007/s11852-015-0399-3

Further reading

https://disasterscharter.org/fr

https://www.esa.int/Enabling_Support/Operations/ESA_Ground_Stations/Estrack_ESA_s_global_ground_station_network

https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

https://eur-lex.europa.eu/eli/reg/2021/696/oj/eng

https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/

https://www.france24.com/en/europe/20240501-russia-accused-of-meddling-in-the-gps-systems-of-baltic-sea-countries

https://ntrs.nasa.gov/citations/20220001918

https://www.euspa.europa.eu/eu-space-programme/secure-satcom/govsatcom

https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

https://www.eurohpc-ju.europa.eu/index_en

https://disasterscharter.org/

https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

Climate Change Adaptation Report - GOV.UK

https://www.unoosa.org/oosa/en/oosadoc/data/documents/2025/aac.105l/aac.105l.340add.12_0.html

How to cite this brief

ATLANTIS Consortium (2025). *Operationalizing Earth Observation for Critical Infrastructure Resilience: Interoperability and Standardization Insights from ATLANTIS. ATLANTIS Policy Brief No. 2 (PIA2). 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 strengthen the clarity and coherence of the brief. The final content remains the responsibility of the authors:

Mario AL SAYAH	RESALLIENCE
Gianfranco CAPUTO	LINKS Foundation
***Reviewed by an independent expert in critical infrastructure**	-
Abla EDJOSSAN-SOSSOU	RESALLIENCE
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:

Naji EL BEYROUTHY	RESALLIENCE
Nidhi NAGABHATLA	UNU-CRIS, University of Ghent
Expert team from the European Union Satellite Centre	SatCen
Christine NAM	Climate Service Center Germany
Josip RADMAN	Ministry of Infrastructure of Slovenia

For more information on this brief, contact:

Thomas SELEGNY, thomas.selegny@resallience.com