

ATLANTIS

improved resilience of critical infrastructures against large-scale, transnational and systemic risks

Our Mission

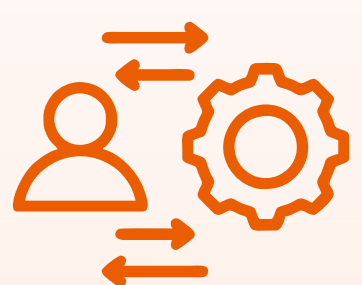


The mission of ATLANTIS is to improve the resilience and protection capabilities of interconnected Critical Infrastructures in Europe. We aim to guarantee the continuity of operations while minimizing cascading effects from evolving large-scale, combined, cyber-physical threats and hazards.



The Challenge: A New Generation of Threats

Critical Infrastructures (CIs) are increasingly facing complex challenges that are not adequately addressed by traditional security solutions. The growing interdependence of cyber-physical systems requires a holistic approach to security that can predict and anticipate systemic risks.



Our Approach: The Preventive Security as a Service (PSaaS) Model

ATLANTIS is developing a comprehensive security solution that pre-emptively security risks and protects against potential attacks. Our strategy is built on:

- **Continuous Risk Assessment:** Constantly monitoring the security state across all CI levels and cyber-physical domains.
- **Proactive Measures:** Developing new secure measures to reduce systemic risks and incorporating a defence "by innovation" and "by design" philosophy.
- **Integrated Solutions:** Addressing cyber-physical-human protection for cross-border and cross-domain systems.
- **Stakeholder Collaboration:** Fostering a collaborative approach to security among industry leaders, academic institutions, and government agencies.



Key Innovations & Technologies

ATLANTIS is composed of several Key Exploitable Results (KERs). Here is a selection of our core technologies:

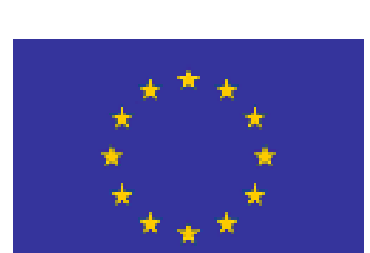
- **KER01: AI-based Anomaly Detection System** An AI-powered security module designed to detect unknown attacks (zero-day or variants) that cannot be caught by traditional signature-based systems. It analyzes network traces and data to provide a trustworthiness score.
- **KER03: Social Channels & Crowd-sources Disinformation Support** A software solution for threat detection via social media channels. It helps mitigate systemic risks using XAI tools based on social media feeds for CI and cross-CI customers.
- **KER11: GreenTwin Platform (3D Digital Twin)** A 3D Digital Twin that works as a situational awareness interface, enabling the analysis of the environment to detect abnormal events and predict long-term systemic risks. It combines a 4D display with a Decision Support System and Work Order Management.
- **KER13: Copernicus-based EO for Surveillance of Critical Infrastructures** A tool that uses Synthetic Aperture Radar (SAR) imagery to monitor large infrastructures for slow and continuous terrain subsidence that could cause damage over time.
- **KER19: Application to Exchange Sensitive Data** A blockchain-based platform using the Cosmos SDK and IBC protocol to solve the lack of interoperability and secure data sharing across different blockchain networks for entities managing critical infrastructure.

Joint Exploitation: Stronger Together

To maximize impact, partners have joined forces to build Joint Exploitation Plans covering complementary KERs. Key schemes include:

- **ACF Situational Awareness Framework** • **Risk Management & Risk Reduction Framework** • **Emergency Response Management**
- **Privacy Preserving Framework** • **Copernicus based EO for Surveillance** • **Dynamic Security Governance**

See these innovations in action at our joint Final Event with the EU-CIP and SUNRISE projects in Brussels on September 29, 2025. Visit our website for more details.



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073909

