Improved resilience of CIs against large scale transnational and systemic risks

The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909
ATLANTIS IDENTITY CARD

**WHO:** 37 PARTNERS FROM 10 COUNTRIES (+ 8 INDIRECTLY ASSOCIATED)

**WHAT:** EC HE GRANT UNDER THE CALL CL3-2021-INFRA-01

**WHEN:** 1 October 2022 → 30 September 2025 (36 MONTHS)

**WHY:** IN RESPONSE TO TOPIC: CL3-2021-INFRA-01-01 “EUROPEAN INFRASTRUCTURES AND THEIR AUTONOMY SAFEGUARDED AGAINST SYSTEMIC RISKS”

**MISSION:** IMPROVE THE RESILIENCE AND THE PROTECTION CAPABILITIES OF INTERCONNECTED ECI EXPOSED TO EVOLVING SYSTEMIC RISKS DUE TO EXISTING AND EMERGING LARGE-SCALE, COMBINED, CYBER-PHYSICAL THREATS AND HAZARDS, GUARANTEE THE CONTINUITY OF OPERATIONS, WHILE MINIMIZING CASCADING EFFECTS BY ADOPTING SUSTAINABLE SECURITY SOLUTIONS.

**HOW:** HORIZON INNOVATION ACTION (BUDGET: € 12,728,564.50, FUNDING: € 9,998,535)
The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909

ATLANTIS COVERAGE #1

GEOGRAPHICAL COVERAGE

- **Central:** Italy, France, Belgium, Germany, Luxembourg, Austria, Netherlands
- **Southern-East:** Greece, Cyprus, Romania, Slovenia, Croatia, Albania, Slovakia, Hungary,
- **Southern-West:** Spain
ATLANTIS COVERAGE #2

VALUE-CHAIN COVERAGE

• CI OPERATORS AND CI END-USERS IN VARIOUS SECTORS (12): LUK (PORT), LUR (PORT), DARS (HIGHWAY), SITAF (HIGHWAY), SZ (RAILWAY), FST (RAILWAY), TS (TELCO), PET (ENERGY), HYG (HEALTHCARE), CXB (FINANCE), JRC (FINANCE SERVICE), SDIS73 (FIRE SERVICE)

• CIP/CIR SOLUTION/TECHNOLOGY PROVIDERS (6): ENG, CS GROUP, INTRA, SLG, SIEM, RES

• RESEARCH INSTITUTES (9): KEMEA, ICS, SAT, JSI, PRFI, CEA, CERTH, LINKS, VICOM

• INNOVATIVE HIGH-TECH SME WITH SECURITY EXPERTISE (6): SYN, NETU, BYTE, ATC, CRI, SNEP.

• SECURITY GOVERNMENT ENTITIES (4): MZI (SLOVENIAN MINISTRY FOR INFRASTRUCTURE), UIV (SLOVENIAN MINISTRY OF INFORMATION SECURITY), MDI (ROAD, RAIL AND COMMUNICATIONS SECURITY), HPL (HELLENIC POLICE)
The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909

ATLANTIS LANDSCAPE #1

- **EU Security Union Strategy for the period 2020-2025** identifies the protection of CI as one of the main priorities for the EU and its Member States.

- **Digital and interconnected CIs** are based on novel and sophisticated technologies which generate potential **new vulnerabilities**, either accidental or intentional.

- **Networked CIs** might cause **long-lasting cascading effects** in other multi-sector and cross-border CIs.

- **CIs** increasingly appear as potential **new targets** for new threats and attacks, especially the hybrid ones (e.g. cyber-physical), operating in a **rapidly evolving societal, technological and business environment**.

- **Limited research** on large scale, transnational and cross-domain coordinated attacks, especially at a **systemic level**.
ATLANTIS LANDSCAPE #2

- **Attack surface and the impact of attacks** can escalate rapidly and negatively affect other CIs and wider parts of vital societal functions.

  - **Cyber-physical and coordinated** (among different actors, even in different countries), **mixed** (using different tactics), **disruptive** (leading to the collapse of entire systems, sectors or regions), **unexpected, subversive, and difficult to identify** early.

  - **Major natural hazards** (e.g. floods, wildfires, often unexpected and unpredictable) are also big concerns that can create disruption to ECI, thus affecting wider functions of our society.

- **Understand the system as a complex network of individual and institutional actors** with different and often conflicting interests.
ATLANTIS STRATEGIC CHALLENGE AND MISSION

ATLANTIS AIMS AT ENHANCING RESILIENCE AND CYBER-PHYSICAL-HUMAN (CPH) SECURITY OF THE KEY ECI, GOING BEYOND THE SCOPE OF DISTINCT ASSETS, SYSTEMS, AND SINGLE CI, BY ADDRESSING RESILIENCE AT THE SYSTEMIC LEVEL AGAINST MAJOR NATURAL HAZARDS AND COMPLEX ATTACKS THAT COULD POTENTIALLY DISRUPT VITAL FUNCTIONS OF THE SOCIETY.

THE MISSION OF ATLANTIS IS TO IMPROVE THE RESILIENCE AND THE PROTECTION CAPABILITIES OF INTERCONNECTED ECI EXPOSED TO EVOLVING SYSTEMIC RISKS DUE TO EXISTING AND EMERGING LARGE-SCALE, COMBINED, CYBER-PHYSICAL THREATS AND HAZARDS, GUARANTEE THE CONTINUITY OF OPERATIONS, WHILE MINIMIZING CASCADING EFFECTS IN THE INFRASTRUCTURE ITSELF, THE ENVIRONMENT, OTHER CIs, AND THE INVOLVED POPULATION, ENABLING PUBLIC AND PRIVATE ACTORS TO MEET CURRENT AND EMERGING CHALLENGES BY ADOPTING SUSTAINABLE SECURITY SOLUTIONS.
ATLANTIS SECURITY STRATEGIC GOALS

1. **AWARENESS.** Improve knowledge on large-scale, vulnerability assessment and long-term systemic risks.

2. **CAPABILITY.** Improve the systemic resilience of ECI, through novel, adaptive, flexible, and customizable security measures (“by design”) and tools (“by innovation”).

3. **COOPERATION.** Effective cooperation among CI operators and government security stakeholders, while preserving CI autonomy and sovereignty.

4. **TECHNOLOGY.** Deliver an open technological framework that will provide the ECIs with AI-based solutions for increased awareness, capability, and cooperation in managing systemic threats.

The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909.
ATLANTIS OBJECTIVES

1. **Continuous and collaborative** Large-scale Hybrid Vulnerability Assessment support
2. **Long-term intra-domain, cross-domain, and cross-border** Systemic Risk Analysis
3. **Confidentiality preserving** Federated Machine Learning (FML) and Explainable AI (XAI)
4. **Trusted collaborative** Cross-Domain/Cross-Border Knowledge Sharing and Mitigation
5. **5G and multi-constellation satellite systems** to complement GNSS in PNT services
6. **Improved use of Threat Intelligence** for the anticipation of systemic risks
7. **Systemic, large-scale, CPH** situation awareness for resilient ECI
8. **Real-time cooperative cyber/physical security monitoring** and mitigation facility
9. **Real-world demonstration of ATLANTIS** methodology and framework
10. **Skills improvement and capability maturity**
11. **Cooperation support and ethical, legal, and societal acceptance of the ATLANTIS solutions**

ATLANTIS
The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909
The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909
The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909.
VALIDATION IN LARGE SCALE PILOTS – LSP #1

Cross-Border/Cross Domain Large Scale Pilot in Transport, Energy and Telecoms (Slovenia, Croatia, Italy and France)
VALIDATION IN LARGE SCALE PILOTS – LSP #2

Cross Domain Large Scale Pilot in Health, Logistics/Supply Chain and Border control (Greece, Cyprus, Croatia, Albania)
VALIDATION IN LARGE SCALE PILOTS – LSP #3

Cross Domain Large Scale Pilot in Health, Logistics/Supply Chain and Border control (Spain, Germany and Cyprus)
### VALIDATION IN LARGE SCALE PILOTS – OVERVIEW

<table>
<thead>
<tr>
<th>Countries</th>
<th>Security</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Directly Involved</td>
<td>Indirectly Involved</td>
</tr>
<tr>
<td>LSP1</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>LSP2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>LSP3</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENT

The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909
The project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073909