# ATLANTIS

## Improved Resilience of Critical Infrastructures Against Large Scale Transnational and Systemic Risks

Reliable operation of Critical Infrastructures (CIs) is a pre-requisite for the integrity and resilience of vital elements in our society that help to ensure the security, well-being, and economic prosperity of Europe, its citizens, and businesses. However, CIs have become very complex, operating in a rapidly evolving societal, technological, and business environments. Growing digitalisation generates new vulnerabilities, including those carried through people and employees, either intentionally through insider threats or through human errors and social engineering. Moreover, since CIs are becoming more interconnected and reliant upon one another, disruptions in one CI can have severe and long-lasting cascading effects in other CIs that are essential for the continuity of critical societal and economic activities, even in multiple sectors and countries. This increases the attack surface as well as the scale and significance of the impacts of attacks.

In this emerging safety-security landscape, European Critical Infrastructure (ECI) are increasingly becoming the targets of new categories of hybrid threats and attacks powered by technological innovations. However, limited research has been conducted on large scale, transnational, and cross-domain coordinated attacks. More importantly, large-scale vulnerability assessment and systemic risks analysis of ECI, considering the risks derived by major man-made or natural hazards and complex Cyber-Physical-Human (CPH) threats as well as consequences of the entire system collapse, have never been addressed before. A fundamental challenge to governing systemic risks is to understand the system as a complex network of individual and institutional actors with different and often conflicting interests, values, and worldviews.

**ATLANTIS** evaluates and addresses systemic risks against major natural hazards and complex attacks that could potentially disrupt vital functions of the European society. The mission of ATLANTIS is to improve the resilience of the interconnected ECI exposed to ever evolving, existing and emerging, large-scale, combined, CPH threats and hazards. By providing future-proof, sustainable security solutions, ATLANTIS supports public and private actors in guaranteeing continuity of vital operations while minimizing cascading effects in the infrastructure itself, the environment, other CIs, and the involved population.

**Innovation Action**

Start Date
**October 2022**

End Date
**September 2025**

**38**
Partners

**11**
CI Operators

**6**
CI Authorities

**10**
Countries

**12.7** MEUR
Total Cost

## MISSION #1

Improving knowledge on large-scale vulnerability assessment and long-term systemic risks management in ECIs.

## MISSION #2

Improving the systemic resilience of ECI through novel, adaptive, flexible, and customizable security solutions based on AI.

## MISSION #3

Facilitating effective cooperation among CI operators and authorities while preserving CI autonomy and sovereignty.

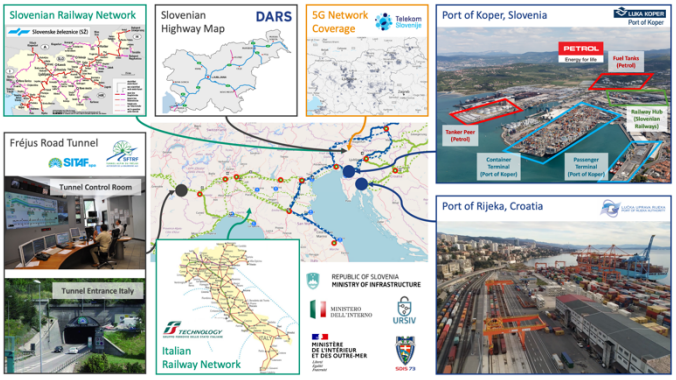
## MISSION #4

Delivering AI-based solutions (TRL7) for increased awareness, capability, and cooperation in managing systemic threats.

ATLANTIS will be validated and demonstrated in 3 large-scale cross-border and cross-sector pilots (LSPs), with a focus on improving the security of the information exchange at different levels of operation: inside individual CIs, across CIs in a national security environment, and across borders between CI operators.

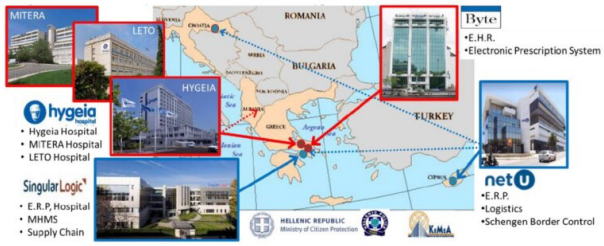
### LSP#1: Cross-Border/Cross-Domain LSP in Transport, Energy, and Telecoms

Validation in **(i)** multimodal cross-country transport encompassing sea transport with two international sea ports, rail transport with two national railway operators, and road transport with a national highway operator, **(ii)** energy (oil), and **(iii)** telecoms in four neighbouring countries: Slovenia, Croatia, Italy, and France.



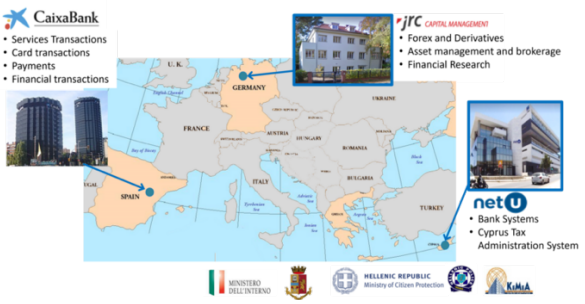

### LSP#2: Cross-Domain LSP in Health, Logistics/Supply Chain, and Border Control

Validation in **(i)** the health sector covering physical protection of hospitals and cybersecurity of Electronic Health Records with a group of 3 hospitals in Greece, **(ii)** logistics/supply chain covering logistics and Enterprise Resource Planning (ERP) platforms with one of the largest ERP tool providers in Greece and Cyprus, and **(iii)** border control with a focus on the Schengen II Information System for border control of Cyprus, Greece, and Croatia.




### LSP#3: Cross-Country LSP in FinTech/Financial

Validation in the financial sector covering cybersecurity incidents and systemic threats with an independent investment house, a bank, and technology providers specialised in developing technology, infrastructure, and business solutions for the financial sector.



**Project Coordinator**

**Mr. Gabriele Giunta**

Engineering, Italy

gabriele.giunta@eng.it

**Technical Manager**

**Mr. Artemis Voulkidis**

Synelix, Greece

voulkidis@synelix.com

Engineering
Ingegneria Informatica S.p.A.
[Italy]

CS Group
[France]

SIXENSE ENGINEERING
[France]

Netcompany-Intrasoft
[Luxembourg]

SingularLogic
[Greece]

Telekom Slovenije d.d.
[Slovenia]

SIEMENS AG
[Romania]

Synelix Solutions S.A.
[Greece]

NetU Consultants Ltd.
[Cyprus]

Byte computer S.A.
[Greece]

Snep Asset Management d.o.o.
[Slovenia]

Athens Technology Center S.A.
[Greece]

Cybercrime Research Institute GmbH
[Germany]

Luka Koper
[Slovenia]

Port of Rijeka Authority
[Croatia]

DARS
[Slovenia]

Slovenske Železnice
[Slovenia]

Petrol d.d.
[Slovenia]

Ferrovie dello Stato Technology S.A.
[Italy]

JRC Capital Management
[Germany]

CaixaBank S.A.
[Spain]

Hygeia
[Greece]

SITAF S.p.A.
[Italy]

Service Départemental d'Incendie
et de Secours de la Savoie
[France]

KEMEA – Centre for Security Studies
[Greece]

Institute for Corporative Security Studies, ICS
Ljubljana
[Slovenia]

European Union Satellite Centre
[Spain]

University of Rijeka,
Faculty of Maritime Studies
[Croatia]

Jozef Stefan Institute
[Slovenia]

CEA List Institute
[France]

Centre of Research & Technology Hellas
(CERTH)
[Greece]

Links Foundation
[Italy]

Vicomtech Foundation
[Spain]

Ministère de l'Intérieur, Securite-civile
[France]

Ministry of Infrastructure
of the Republic of Slovenia
[Slovenia]

Republic of Slovenia,
Government Information Security Office
[Slovenia]

Ministry of Citizen Protection,
Hellenic Police
[Greece]

Ministero Dell' Interno, Dipartimento di
Pubblica Sicurezza, Polizia di Stato
[Italy]