ATLANTIS

Newsletter #4 **November 2024**

In our previous newsletters, we introduced the ATLANTIS project's mission to enhance the resilience of Critical Infrastructures in Europe. These essential systems support the well-being and economic security of societies across Europe and safeguarding them from emerging threats is paramount.

This edition continues our journey by showcasing the progress made in the project's three Large-Scale Pilots (LSPs), which focus on **cross-border** and **cross-sector** collaboration to protect critical infrastructure across transport, energy, telecommunication, border control, supply chains, and finance. By defining and modelling **multiple hazards, threats, risks and CIs/assets interdependencies** and by developing and deploying **cutting-edge technologies**, these LSPs are paving the way for a more resilient and secure European infrastructure.

This newsletter demonstrates the progress of the LSPs that are being developed for the needs of ATLANTIS project.

LSP#1 focuses on securing **cross-border transport, energy, and telecommunication networks**, specifically along the **Mediterranean Corridor**, which connects key ports, railways, and highways across Slovenia, Croatia, Italy, and France.

By deploying technologies like **Digital Twins** and **AI-driven protection tools**, LSP#1 enhances the resilience of these critical infrastructures, minimizing the risks of cascading failures due to interconnected threats.

LSP#2 strengthens **border control, healthcare, and supply chain** resilience through **advanced data exchange, cybersecurity tools**, and **real-time monitoring systems**. By addressing both physical and digital threats, this LSP ensures the continuity of essential services in the face of cyberattacks and disinformation.

LSP#3 applies **AI and advanced risk management** to the **financial sector**, protecting critical financial infrastructures across Spain and Germany. The LSP focuses on detecting cyber threats, preventing network intrusions, and safeguarding operations in volatile areas like cryptocurrency trading, ensuring financial systems remain secure and resilient.

Throughout this newsletter, we highlight key advancements and demonstrate how each LSP is tackling the complex risks of today's highly interconnected world. From AI-powered risk mitigation to real-time threat detection and cross-sector collaboration, the ATLANTIS project continues to drive efforts in securing Europe's critical infrastructures for the future.

After this brief introduction to the current situation of the project, the fourth ATLANTIS newsletter will offer updates on the progress made by each LSP partner, highlighting the developed technologies and their impact on the project.

ATLANTIS The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

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

A Collaborative Approach to Secure Transport, Energy, and Telecommunications

LSP#1: Overview

The LSP#1 focuses on increasing resilience of the critical infrastructures that enable smooth, secure, and safe running of essential services within and across the transport (sea, rail, road), energy (oil), and telecommunication domains, within and across the national borders of neighboring EU countries Slovenia, Croatia, Italy, and France (Figure 1).
This pilot involves CI operators and authorities along the **Mediterranean Corridor**, one of the main priority axes of the Trans-European Transport Network (TEN-T), connecting the Mediterranean Basin with Central Europe and Ukraine. The corridor primarily consists of road and rail, but it also provides a multimodal link for the ports of the Western Mediterranean with the center of the EU.
The Corridor is an important trade route for the following CI operators participating in LSP#1:

- Sea ports in Rijeka, Croatia, and Koper, Slovenia.
- National rail operators in Slovenia and Italy.
- National highway operator in Slovenia.
- Cross-border Frejús tunnel operators on the Italian side, fire and rescue service providers on the French side of the tunnel.
- Slovenian oil derivatives distributer.
- Slovenian telecommunication service provider.

These CI operators are supported by the following CI authorities:

- Ministry for Infrastructure, Slovenia.
- Government Information Security Office, Slovenia.
- Ministry of Interior, Railway State Police, Italy.

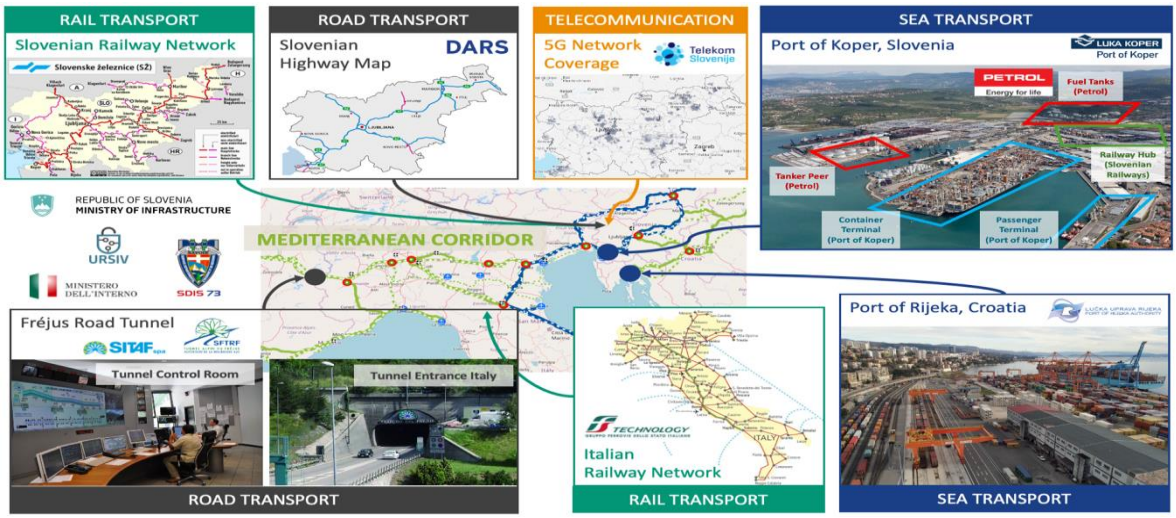

Figure 1. Mediterranean Corridor's integrated critical infrastructure network connecting Slovenia, Croatia, and Italy.

ATLANTIS The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

Each of these organizations is facing their **own unique challenges**, depending on their own internal processes, capabilities, and overall preparedness, as well as on the threats and hazards arising from their physical environment (e.g., floods due to specific geographical location), cultural specifics (e.g., large protests), political setting (e.g., cyber terrorism), supply chain disruptions, and more.

However, it is crucial to recognize that the challenges faced by each organization are **not isolated**; the CI operators often share vulnerabilities, environmental hazards, geopolitical threats, and other interdependencies.

The complex interconnections among all these organizations, the infrastructures they operate, and the essential services they provide on the Mediterranean Corridor, reflect the need for a **common approach** towards identifying, analyzing, and addressing **cross-sector and cross-border risks**. With this holistic and coordinated approach, we can increase their resilience against evolving systemic risks, and thus minimize the cascading effects and negative impacts on either or many of them.

Key Contributions

Based on a detailed analysis of the existing and most relevant cyber-physical-human (CPH) security threats, we have defined and elaborated an initial set of **pilot scenarios**.

For each scenario, we then identified **interdependencies** from the MACRO and MICRO perspective. MACRO (Figure 2) here relates to looking at the **essential services** provided by the different CI operators and on how **disruptions** in each of these services can affect others when different hybrid threats and systemic risks materialize. MICRO level relates to a more granular view of the interdependencies among the **key assets** of each CI operator, separately in the context of the specific scenario.

Figure 2. Macro-level interdependencies between critical transport hubs on the Mediterranean Corridor

Based on the identified key assets and their interdependencies, we have run the initial exercise of testing several ATLANTIS technologies:

- **Digital Twin** for visualizations of critical assets, information about their status, shared alerts, and cross-organizational communication.
- Situational awareness and decision support tool (**SAFER**) which includes the visualization of cross-organizational/sectorial interdependencies).

ATLANTIS The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

Improved resilience of critical infrastructures against large scale transnational and systemic risks ATLANTIS Newsletter #4

- AI-based technology for network monitoring and detection of unknown cyber-attacks (**SIGMO-IDS**).
- Environmental sensor for air quality assessment, measuring pollutants and CO2 levels (**SNIFFER**).
- Operational Picture of the current situation and by a mobile application for on-field users (**Hypervision**).
- Mobile app for capturing and reporting information about an incident, fostering a collaborative human-centric approach by incorporating technology, processes, and humans (**HiVIC**).
- Indicator of Compromise (**IoC**) that identifies potentially malicious activity on a system or network.
- **Earth Observation** technology for modelling natural hazards, and for preparing risk assessment and damage delineation maps.
- **Risk Reduction and Incident Management (RRIM)** technologies to provide post-crisis recommendations.

LSP#2: Supply Chain/Border Control

Advanced Systems for Border Control, Healthcare, and Logistics

LSP#2: Overview

The main goals of LSP#2 (Figure 3) are to enhance security and resilience across critical infrastructure domains—health, logistics/supply chain, and border control—by developing and validating solutions that address CPH risks. The project seeks to ensure business continuity through robust security measures, effective information exchange, and resilience strategies. Specific goals include securing healthcare systems and Electronic Health Records, optimizing logistics and Enterprise Resource Planning (E.R.P.) platforms, and strengthening border control mechanisms. The initiative focuses on integrating and securing cross-domain and cross-border operations to improve overall system robustness and efficiency.

ATLANTIS LSP#2 involves critical infrastructure across health, logistics/supply chain, and border control, with the following CI operators participating:

- Hygeia Group, managing hospitals in Greece, including Hygeia Hospital, MITERA Maternity Hospital, and LETO Gynecological Hospital.
- Critical logistics operations across Greece and Cyprus, facilitated through ERP platforms integrated by SingularLogic.
- Border control systems operated by NetU, supporting the Schengen II Information System across Cyprus, Greece, and Croatia.

The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

Figure 3. Integrated healthcare logistics/supply chain and border control infrastructure network in the Eastern Mediterranean region.

Key Contributions

The Border Control Scenario under ATLANTIS LSP#2 focuses on several high-level areas of innovation. It addresses threat mitigation by tackling both cyber threats and misinformation to protect critical infrastructures, such as border control systems. Enhanced situational awareness is achieved through the use of advanced tools and technologies that improve real-time monitoring and response capabilities. The project aims to implement proactive security measures, enabling early detection and efficient decision-making processes to mitigate the effects of attacks. The "Tools to Fight Disinformation" monitors social media platforms to detect and counteract false information that could disrupt border operations. By collaborating with social media platforms, ATLANTIS ensures the dissemination of accurate information, preventing the spread of false alerts. These disinformation tools are tested in a simulated border control system provided by NetU, while the tool identifies and flags false alerts, maintaining public trust and operational integrity. This integration is underway, in an attempt to minimize border control cyber threats and disruptions and to maintain public confidence.
Additionally, it emphasizes resilience and recovery, strengthening the ability of border control systems to withstand and quickly recover from disruptions. Other technologies like HiVIC Dapps & Cosmos App for decentralized security, SAFER for malware and DDoS protection as well as Threat Intelligence (analysis and grouping of cyber threat intelligence data) are being considered for future integration.

LSP#3: Cross-Country Large-Scale Pilot in FinTech/Financial

Artificial Intelligence and Advanced Risk Management in Finance

LSP#3: Overview

LSP#3 focuses on increasing cybersecurity awareness and resilience among CIs within the financial sector across Spain and Germany. This LSP involves banking institutions that have very large and complex CIs, which should robust, constantly evolving and follow many regulatory guidelines and strict

The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

security frameworks. Also, the LSP counts on researchers that engage in economic and financial analysis to safeguard the assets in the marketplace and expose disinformation campaigns.
Each organization faces unique challenges based on their processes, capabilities, and the threats they encounter. LSP#3 goals involve identifying specific hazards and threats, analyzing operations to document interdependencies, and identifying and calculating risks based on detected alerts and trends in a real-time environment. Therefore, giving information to the end-users to better understand and make decisions based on real-time information and risk score.
To accomplish the hole objective, LSP#3 divides in 3 main use cases, each towards a specific aim:

- Use case 3.1, aims to test the resiliency of the JRC's CI by simulating a real-life scenario of threat vs opportunity detection of dis/mis/mal-information through the consumption of data and content from social media, news sources (e.g. sites, blogs, podcasts transcripts, video posts, etc.) that traders and customers of JRC are visiting -following on a daily basis not only to ensure the integrity of JRC's investment ecosystem but also to provide traders and clients with timely and accurate information for making investment decisions, especially in the cryptocurrency market, given the volatile cryptocurrency landscape.
- Use case 3.2, aims to establish a near real-time risk reporting solution in response to cyber-attacks targeting bank systems and operations (focusing mainly on the network intrusion threat and potential linked attacks or consequences derived from the attack). The solution will leverage Cyber Threat Intelligence (CTI) information and logs from CXB's Security Information and Event Management (SIEM) system to promptly identify, assess, and report risks and their criticality. By doing so, the developed tool will provide CXB with a comprehensive view of potential threats, vulnerabilities, and malicious activities, enabling proactive risk management and mitigation strategies that can be later implemented by Security Orchestration, Automation, and Response (SOAR) or recommended playbooks for the analysts.
- Use case 3.3, aims to detect spoofing and DoS attacks against PNT services, generally provided by GNSS. Considering the financial sector, the use case focuses on timing. Detecting this type of attack is essential to start mitigation actions promptly and reduce possible problems and complications that derive from time desynchronization such as data corruption and service denial, legal actions, and regulatory compliance.

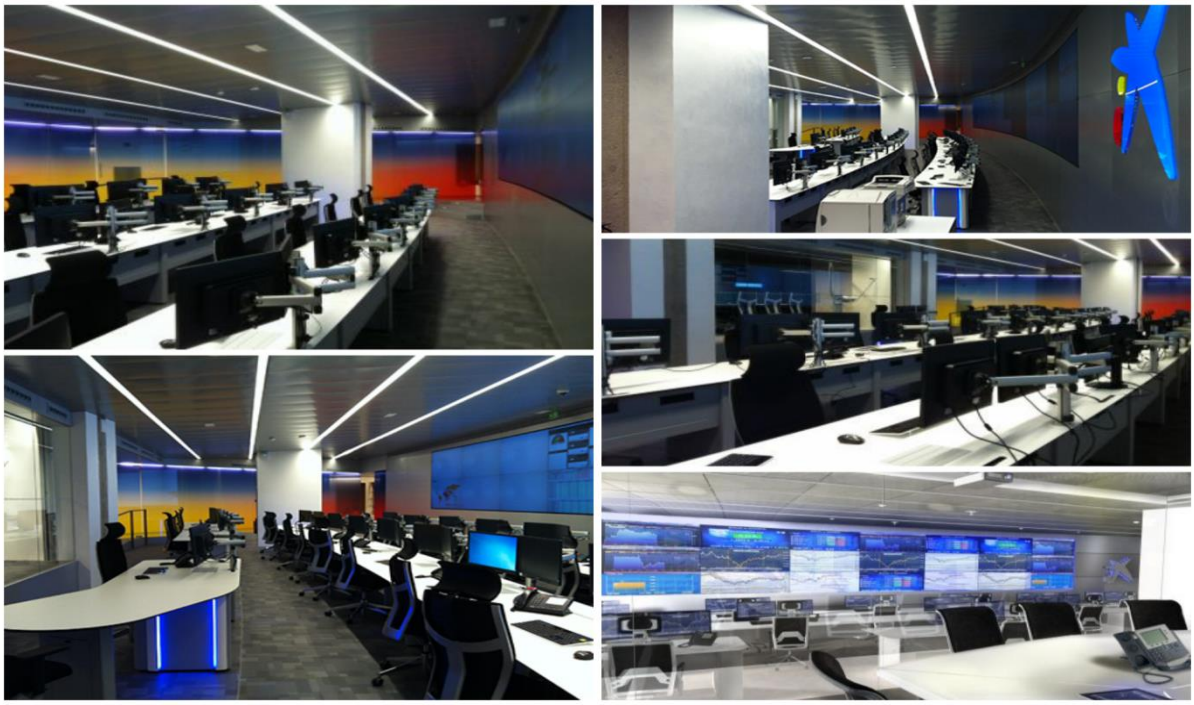

Figure 4. CXB Bank's Security Operations Center

ATLANTIS The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

Improved resilience of critical infrastructures against large scale transnational and systemic risks ATLANTIS Newsletter #4

LSP#3 includes critical infrastructure operators in the financial sector across Spain, Germany, and Cyprus, with the following CI operator participating:

- CXB Bank (Figure 4) in Spain, a major financial institution with extensive branch and ATM networks.

Additional support for financial infrastructure in this LSP is provided by:

- JRC Capital Management in Germany, specializing in Forex and derivatives.
- NetU in Cyprus, offering technology and business solutions for banks and finance organizations.

Key Contributions

LSP#3 aims to use AI tools to improve cybersecurity resilience by enhancing a better understanding of the risks involving a financial entity or sector. Furthermore, LSP#3 dives into the detection of spoofing attacks to PTN services via GNSS to mitigate possible consequences regarding time dyssynchronization.

LSP#3 will develop a new method of risk management involving interdependencies between assets to be aware of possible lateral movements and visibility from the point of view of a potential attacker and correlate risks and new vulnerabilities with the corporative SIEM logs to update the risk level and adapt it to reality.

The tools involved in this LSP (Figure 5) which use AI are:

- **Truly Media**, which uses AI engines to detect Deepfakes, Disinformation Campaigns and possible frauds.
- **SAFER**, which together with the Decision Support System (DSS) will catalogue and create the risk assessment of emerging threats and incidents.
- **RRIM**, the intelligent Risk Reduction Incident Mitigation system counter-measuring recommendations for the different risks.

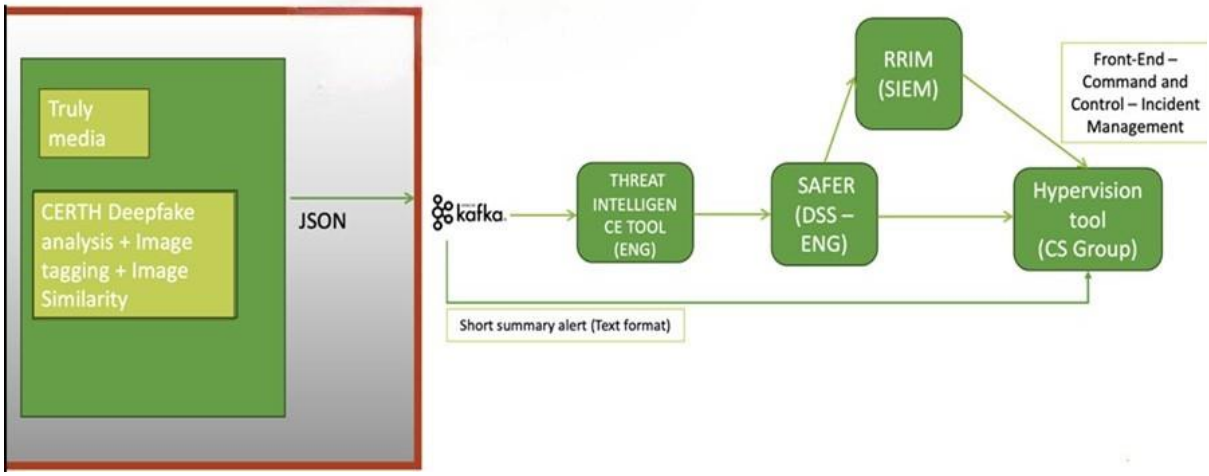

Figure 5. Data flow description regarding disinformation campaigns and deepfake analysis.

ATLANTIS The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

Project Coordinator
Mr. Gabriele Giunta
Engineering, Italy
gabriele.giunta@eng.it

Technical Manager
Dr. Artemis Voulkidis
Synelixis, Greece
voulkidis@synelix.com

Web

LinkedIn

https://www.atlantis-horizon.eu/

ATLANTIS The ATLANTIS project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909