ATLANTIS

Newsletter #2 **November 2023**

In our first newsletter, we outlined the ATLANTIS project's commitment to securing Europe's critical infrastructures—those essential services that underpin our society's well-being and economic health. As these infrastructures become more interconnected through digital advancements, they also become more exposed to complex threats. ATLANTIS is actively engaged in identifying and addressing these emerging vulnerabilities.

ATLANTIS is pioneering a novel, AI-based security solution designed to be adaptive, flexible, and customizable to the needs of European CIs while promoting the collaboration necessary for managing systemic threats.

Progress within the ATLANTIS project is demonstrated through the advancements in its three large-scale pilots (LSPs), each targeting key areas of the European CI:

- **LSP#1** focuses on the Transport, Energy, and Telecoms sectors, involving key stakeholders like the Port of Koper and Telekom Slovenia. This pilot highlights the strategic importance of cross-border cooperation and the need for a collective risk management approach to protect the intricate network of interdependent infrastructures.

- **LSP#2** targets the Health, Logistics/Supply Chain, and Border Control sectors, validating ATLANTIS' cyber-physical-human security framework. The pilot is a testament to the project's efforts to counter cyber threats, enhance situational awareness, and ensure the safety of interconnected infrastructures, with the Hygeia Group and Schengen II Information System playing pivotal roles.

- **LSP#3**, led by CaixaBank, turns the spotlight on the FinTech/Financial sector, seeking to bolster cyber-human security and operational resilience. This pilot underscores the critical nature of information sharing and the robust defenses required to protect Europe's financial stability from systemic cyber threats.

Through these pilots, ATLANTIS is not just addressing the current security challenges but also setting a precedent for the future of European CI protection. The project continues to drive forward, aiming to elevate the systemic resilience of Europe's critical infrastructures and safeguard European security, well-being, and economic prosperity against the risks of the modern era.

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

After this brief introduction, the second ATLANTIS newsletter will offer updates on the progress made by each partner organization within the Large-Scale Pilots (LSPs), highlighting their roles and contributions to the project.

LSP1: Cross-Border/-Sector Large Scale Pilot in Transport, Energy, and Telecommunications

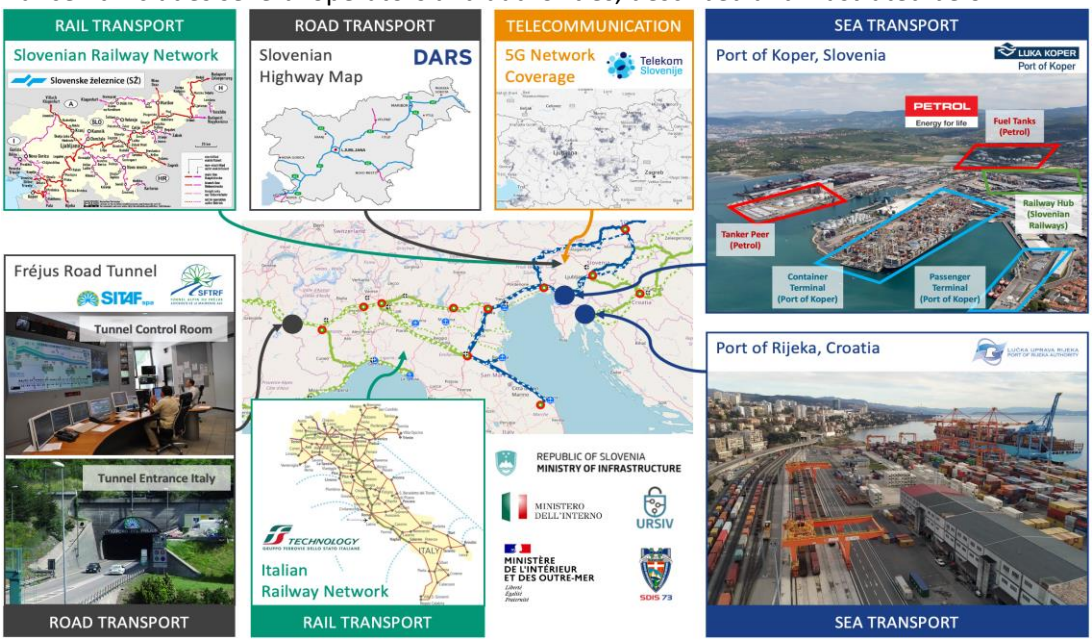
Lead Partner: Institute of Corporate Security studies

LSP1 Overview:

The ATLANTIS LSP#1 is a collaborative initiative led by ICS, designed to enhance the resilience and continuity of critical infrastructures in the domains of transport, energy, and telecommunications across borders and sectors in Slovenia, Croatia, Italy, and France. The project involves a consortium of operators and authorities, each bringing unique contributions to ensure the safeguarding of vital services against a spectrum of risks. Key stakeholders include Port of Koper, Petrol, Slovenian Railways, DARS, Telekom Slovenia, Port of Rijeka Authority, Italian Railways, and the Fréjus Road Tunnel operators, all supported by pertinent CI authorities. By focusing on cross-border and cross-sector interdependencies, LSP#1 aims to fortify these infrastructures against disruptions, ensuring the seamless operation of the integrated European network. The partnerships forged in this endeavor underpin the strategic approach towards a collective risk management, highlighting the essential nature of cooperation in safeguarding the critical infrastructure ecosystem.

Partner Contributions:

The ATLANTIS LSP#1 focuses on safeguarding the autonomy, continuity, and resilience of the critical infrastructures within and across the transport (sea, rail, road), energy (oil), and telecommunication domains, within and across the national borders of neighbouring EU countries Slovenia, Croatia, Italy, and France. It includes several operators and authorities, described and illustrated below.



Port of Koper (**LUK**) operates a multi-purpose freight port located in the northern part of the Adriatic Sea, in Slovenia, connecting markets of Central Europe and Far East. The total maritime throughput in the port in 2021 topped over 23 million tonnes, making it the first port for the Austrian market in terms of total cargo throughput, the first port for the Hungarian and Slovak markets in terms of

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

container throughput, one of the largest ports in the Mediterranean for vehicle throughput, and the most important container port in the Northern Adriatic.

Petrol (PET) is the largest Slovenian energy company. Its main business activity is trading in oil derivatives, gas, and other energy products. PET controls over 300 petrol stations in the country and almost 200 of them in other countries in Southeast Europe. Additionally, in Slovenia, PET is the largest importer, the largest company in terms of revenues, and one of the largest retail companies. A complex logistic hub of PET is operating in the Port of Koper.

Slovenian Railways (SZ) is the Slovenian national train operating company. It operates 1,229 km of standard gauge tracks and 331 km as double track. It reaches all Slovenian regions and directly connects them by rail to all surrounding countries. SZ has one of the main railway hubs for transport of goods in the Port of Koper.

DARS is the Slovenian national operator of (600 km of) motorways, expressways, and the related infrastructure. It guarantees traffic safety, free traffic flow, and comfort for the highway network users. DARS builds, manages, and maintains one of the most important transport corridors in the region, connecting the Port of Koper with Central and Southeast Europe.

Telekom Slovenia (**TS**) is the main communications service provider in Slovenia. It is recognized as the leader in mobile and fixed communication services (including a 5G network), system integration and cloud services and multimedia content. It operates the most reliable and high-quality telecommunications network in Slovenia, as well as one of the most complex backbone networks in the region of Southeast Europe. TS ensures the security and uninterrupted operation of its network and services 24/7/365, and the company guarantees uninterrupted operation of its own systems and those of its users in its modern data centres at several locations, including the above-mentioned CIs.

Port of Rijeka Authority (LUR) is an institution founded by the Government of the Republic of Croatia to manage, plan and develop the port of Rijeka area. The area consists of five port basins with twelve specialized terminals. Its core responsibilities are to grant concessions, develop strategy plans, harmonize and supervise concessionaires according to the Croatian and European laws and regulate order, safety and security in the port. This large port area was declared a port of special (international) economic interest to the Republic of Croatia and became the most important national port for international transport. Ports of Koper and Rijeka are located only 100 km apart.

Italian Railways (FST) manage the infrastructure (over 16.800 km of railway lines, almost 2.000 tunnels, and 23.000 bridges and viaducts), transport (10.000 trains per day), and real estate services in Italy as well as in other European countries. In the northern part of the country, the Italian railways offer direct connections for passenger and cargo transport between Slovenia and France.

Fréjus Road Tunnel (SITAF/SINA on the Italian and SDIS73 on the French side) is an integral part of the European road transport network, supporting one of the major trans-Alpine transport routes between France and Italy that is being used for 80% of the commercial road traffic. The tunnel is 12,87 km long and is located at an altitude of 1.300 m, thus being subject to significant climatic hazards (snow, landslides, etc.). It is the only tunnel connecting France and Italy that allows for the transport of hazardous goods.

The CI operators are supported by several CI authorities:

- **Ministry for Infrastructure**, Slovenia
- **Government Information Security Office**, Slovenia

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

- **Ministry of Interior, State Police**, Italy

The interconnections and interdependencies among all these critical infrastructures reflect the need for a common approach for identifying and analysing cross-sectorial and cross-border vulnerabilities, threats, hazards, and risks, as well as for defining optimal countermeasures. By adopting such a holistic approach, we can increase the resilience of CIs against evolving systemic risks, and thus minimize the probability and the negative impacts of the cascading effects of attacks and incidents affecting either or many of them.

A disruption to an essential service operated by one of these organisations can significantly affect the availability, reliability, security, and safety of vital services provided by other organisations in their physical ecosystem or supply chain. For example, any major disruption to telecommunication services in the Port of Koper could cause significant delays in the sea, rail, and road transport of vital goods within Slovenia, also affecting many other countries in the region, including Croatia and Italy. On the other hand, a major fire in the Fréjus tunnel would not only put in danger dozens of citizens crossing the tunnel at that moment but would also cause severe cascading effects to the Italian-French supply chain, also indirectly affecting supply chains in a wider geographic area.

To identify and address the most important risks that these CIs are subject to, the LSP#1 considers several use cases in different parts of the pilot ecosystem, including cyberattacks, physical/terrorist attacks, natural disasters, systemic threats, and large-scale supply chain disruptions.

Challenges and Technological Solutions:

LSP#1 faces a myriad of challenges in safeguarding the resilience of the involved CIs. These challenges encompass a wide range of both natural and human-made threats, which have the potential to disrupt essential services and supply chains. Here, we outline the major problems or gaps identified within LSP#1 and the technological innovations employed to address these issues.

Cross-Border and Cross-Sector Interdependencies

A key challenge within LSP#1 is the complex network of interdependencies among CI operators across different sectors and countries, and the fact that potential large-scale disruptions cannot be isolated to a single organisation, sector, region, or even country. To this end, LSP#1 CIs will use the ATLANTIS risk management solution, underpinned by the concept of digital twins, that enables a comprehensive and joint identification, assessment, visualisation, and management of multi-dimensional systemic risks, as well as a real-time cross-sector/-border communication and coordination.

The utilization of digital twins in risk management provides a dynamic and real-time situational awareness. By creating digital replicas of physical assets and systems, LSP#1 CIs gain an invaluable tool for monitoring, modelling, and simulating various scenarios, and thereby a holistic view of the interconnected ecosystem and potential vulnerabilities.

Furthermore, the system leverages cutting-edge technologies to monitor the status and performance of different CI assets and services across sectors and borders. It provides immediate alerts and (secure) information sharing capabilities to ensure that all relevant stakeholders are well informed and can take timely, joint, and coordinated actions in response to disruptions, reinforcing the robustness and continuity of the interconnected European vital services.

Cybersecurity Threats

The growing reliance on digital technologies presents a significant challenge, particularly when considering that the data landscape is expanding at an unprecedented pace. Additionally, CI operators typically rely on multiple technology providers, making the situation even more intricate. The exponential growth of data and the multifaceted technology landscape further heightens the

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

vulnerability of CIs to cyberattacks. These evolving threats have the potential to not only disrupt vital services but also compromise the security of extensive and sensitive datasets.
In response to this pressing challenge, LSP#1 CIs will use the ATLANTIS state-of-the-art cybersecurity solutions, including AI-driven threat detection and mitigation systems. These technologies continuously monitor network traffic, identify anomalies, and take automated actions to safeguard CIs' systems from cyber threats. Moreover, the LSP#1 CIs will also employ intelligence gathering technology that allows for the swift gathering of information on potential vulnerabilities, threats, and attacks, enabling them to stay ahead of emerging risks. The CIs will also use an advanced technology to combat disinformation on potential threats by verifying the authenticity of information to counteract the spread of false or misleading data.

Physical and Natural Hazards
The management of physical and natural hazards is further compounded by the diverse geographical and climatic characteristics of the countries involved, spanning Slovenia, Croatia, Italy, and France. These nations encompass a broad spectrum of landscapes, ranging from the Adriatic coastline to Alpine regions, and from Mediterranean to continental climates. Moreover, the increasing frequency and severity of weather events in recent years add an additional layer of complexity to this challenge. With more frequent and severe weather events, including snowstorms, floods, landslides, and other natural disasters, the CIs in the region face heightened risk.
To address these challenges, ATLANTIS offers a cutting-edge Earth observation technology that enables continuous monitoring and forecasting of disasters, facilitates the observation of land-use changes, and provides valuable insights into the evolving environmental conditions. By harnessing Earth observation technology, LSP#1 CIs will be better equipped to anticipate, respond to, and mitigate the impacts of natural hazards.

Pilots and Use Cases:
A set of hybrid and time-dependent cascading threat scenarios were defined based on an in-depth exercise aimed at understanding the challenges and concerns of the stakeholders within LSP#1 following several hands-on workshops and site visits to:

- The Fréjus tunnel.
- The operational and command centers of other key local actors (including a highway operator on the French side and the firefighters of the Savoie Region (SIDS73)).
- The Port of Koper logistics hub (encompassing the infrastructure of the port (LUK), railways (SZ), oil terminal (PET), and telecommunications infrastructure (TS)).
- The regional control center for the Slovenian highway operator.

During the site visits, workshops, and desk research, the teams have defined several use cases to be carefully analysed and scenarios to be simulated covering the following:

- Cyber-attacks and cross-organisational communication blackouts.
- Drone attacks and bomb threats.
- Explosions and large fires.
- Natural hazards including earthquakes, heavy rainfalls, snow melts, floods, and landslides.
- Protests, riots, and demonstrations.

The defined scenarios are built, among others, on some of the events that have recently severely affected the functioning of the CIs. For example, in August 2023, a major landslide occurred next to the French highway leading to the Fréjus tunnel, severely impacting the operations of the tunnel and the cross-border multi-modal transport system. In the same month, Slovenia was hit by extreme

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

rainfall, leading to devastating floods and landslides across the country damaging, among others, also parts of the critical infrastructure.

These scenarios provide interesting insights into what challenges CI systems do face and might face again in the future, and into how the ATLANTIS technologies can efficiently and effectively help to address them.

Upcoming Steps and Expected Outcomes:

As we move forward from the scenario definition exercise, pilot studies are now being designed to leverage this intelligence and define concrete development, integration, training, and validation plans to be implemented for a successful initial trial. This phase includes identification of all the digital and physical components that need to be available for the pilot, and the logistics of the trials (what to test where, when, and by whom). It also covers the engagement of the end users to gather their views and requirements to optimize its potential uptake down the line.

Subsequently, we will transition to the execution phase, during which the initial integrations will occur within relevant environments. This critical step will facilitate the preparation and testing (or simulation) of fundamental features of the ATLANTIS solutions. Equally crucial is the training of the CI employees, the end users, in the utilization of the ATLANTIS technologies. Based on the results obtained, we will refine our trial plans in readiness for the subsequent piloting cycle.

In the subsequent reporting phase, the outcomes of the pilot trials will undergo thorough analysis and verification, aligning them with our initial requirements and KPIs. The results will be documented and presented in the dedicated deliverable D5.2, marking an essential milestone in our progress.

LSP2: Cross Domain Large Scale Pilot in Health, Logistics/Supply Chain and Border control

Lead Partner: Byte Computer S.A.

LSP2 Overview:

ATLANTIS LSP#2 is an ambitious pilot targeting three critical infrastructure (CI) domains: health, logistics/supply chain, and border control. Its primary aim is to validate the ATLANTIS cyber-physical-human security framework, ensuring resilience against systemic risks across interconnected infrastructures.

In the health domain, the project focuses on safeguarding hospitals and Electronic Health Records by collaborating with Greece's Hygeia Group. The supply chain and border control aspect incorporate ERP solutions in Cyprus and the Schengen II Information System.

Central to the pilot's strategy is addressing a range of cyber threats, enhancing situational awareness, and fostering efficient decision-making through a network of interlinked critical infrastructures. The overarching goals encompass countering cyber-physical threats, elevating hospital safety standards, and amplifying situational awareness in logistics and border control operations.

Partner Contributions:

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

BYTE is the leading IT SME in cybersecurity, E.H.R. and digital signatures and has implemented the Greek Electronic Prescription System. BYTE is the leader of LSP#2, coordinates meetings and contributes to the first LSP#2 scenario involving a terrorist attack on the Hygeia Hospital.

SingularLogic (SLG) member of the Space Hellas Group, is a leading software and digital integrated solutions provider for large enterprises and a supplier of the Model Hospital Management System (MHMS) at all hospitals in HYGEIA Group in both Greece and abroad. It has been involved in the development of the first LSP#2 scenario targeting the Hygeia hospital complex. As SLG is also involved in the development of ATLANTIS technologies, it is also supporting the group in decisions related to applying preventive technologies to reduce systemic risks as well as in the planning of countermeasures to fight disinformation campaigns in cooperation with ATC.

NetU is a leading IT SME in the Eastern Mediterranean that collaborates with the biggest banks and finance organisations in Cyprus and Greece and has implemented the Tax Administration System for the Tax Department of the Cyprus Ministry of Finance and the Schengen II Information System for border control in Cyprus, Greece and Croatia. NetU is responsible for the coordination of the second scenario in LSP#2, related to the cyberattack on the border control system.

CRI offers legal and ethical research and advisory services for strategy, policy, and legislation to SMEs in over 50 countries, including work with international bodies like ITU, UNODC, CTITF, and NATO.

Hygeia (HYG) is the largest group offering healthcare services in Greece. It owns three hospitals in Greece, with a total capacity of 1,261 beds and until recently the Hygeia General Hospital in Tirana. The Hygeia hospital is at the centre of the first scenario involving a cyber-physical attack on its infrastructure.

KEMEA, the Greek Centre for Security Studies, specialises in both theoretical and applied research with a focus on strategic-level studies, operating under the supervision of the Greek Ministry of Citizen Protection. In LSP#2, KEMEA plays a pivotal role, providing support for both scenarios through the implementation of risk mitigation technologies in a joint effort with Siemens.

The **Hellenic Police** (HPOL) is alerted to the situation to safeguard public safety, coordinate law enforcement actions, and offer additional security support. They also oversee the creation of emergency pathways for patient relocation, guaranteeing swift and secure transfers between facilities.

Challenges and Technological Solutions:

The main infrastructures associated with LSP#2 are found within the healthcare sector, border control, and the supply chain. Each has implemented and operates under adequate security measures. Common to all these infrastructures is the need for an integrated system that realizes cross-domain, cross-CI, cross-border knowledge sharing, risk assessment, threat analysis, and countermeasures mitigation.
For the first scenario, which involves a terrorist attack on the Hygeia Hospital, the following gaps and technological needs have been identified:

- Digital Twins (DT) can be utilized in the planning and preparation phase for training and simulation exercises, preparing for various emergency situations, including chemical attacks.
- Threat intelligence might provide information on an upcoming attack on the healthcare system.

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

- Systemic Risks Foresight and Incidents Detection DSS could identify a cyber-attack on the hospital's internal network, predict the imminent spread of the worm across the network, and the potential for credential theft.
- The Humans in Vicinity Sensing and Engagement tool (HiVIC) could enable Hygeia hospital staff to report suspicious incidents and receive instructions.
- A situational awareness and decision support tool can gather information from CI components and share it with other CIs.
- The Risk Reduction & Incident Mitigation DSS might help identify and coordinate appropriate countermeasures.
- Tools to combat disinformation could assist in identifying the source of information, determining its authenticity, and highlighting reliable information sources.
- A tool visualizing the operational status of CI is vital, supporting communication and coordination between relevant entities.

Regarding the second scenario, which concerns a cyber-attack on the Border Control System, including sensitive data breaches and supply chain disruption, the following technologies are deemed important:

- A digital twin of the Border Control System could act as a real-time replica of the physical system. If there's physical damage to the server infrastructure, the digital twin could replace the physical system, redirecting network traffic toward the digital twin.
- A Situation Awareness & Comprehension Framework can consolidate efforts to detect cyber-attacks and network intrusions. This component can integrate various data sources into the system. The Pattern Recognition system might pinpoint suspicious or anomalous patterns suggesting potential security threats, like forged documents.
- A Cross-CI Assessment and State Awareness System (CCIASAS) can act as an advanced security sentinel for border control systems. It continuously monitors and assesses infrastructural components to detect and alert on cyber threats while collaborating with other modules to analyze threats and recommend countermeasures.

Pilots and Use Cases:

Hygeia Scenario:

In a meticulously planned cyber-physical attack, a threat actor breaches the security of Hygeia Hospital, gaining access to its ERP and EHR systems. After stealing sensitive patient data, the attacker corrupts patient records while simultaneously stealing medical personnel credentials, which are carelessly identical across both the hospital's EHR and Greece's nationwide EPS. Exploiting this, the malefactor accesses expansive patient treatment data. To intensify the chaos, a DDoS attack is initiated on IDIKA, the national healthcare system, causing substantial delays in patient care due to data corruption and system strain. Concurrently, a chemical attack in the hospital's waiting area causes widespread respiratory distress. The hospital's SOC, albeit responsive, can only manage a partial evacuation, inadvertently compromising patient care and tarnishing the institution's reputation. With medical records tampered and EPS access blocked, many patients face the peril of incorrect treatment. Amplifying the chaos, a parallel disinformation campaign paints a distorted picture of the healthcare sector on social media, blending fact with fiction and sowing seeds of distrust and confusion among the public.

The Hygeia scenario covers the following use cases:

- UC2.1 Cyber-attack to a vital CI's as a part of hybrid threats including the disinformation campaigns

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

- UC2.2 Cyber-attack to the E.H.R. and/or Electronic Prescription System portability, including modification that may put in risk the human life, distributed denial of service (DDoS) and sensitive data breaches
- UC2.3 Physical terrorist attack with chemical or virus spreading (e.g. COVID-19) to workforce or patients

Border Control Scenario:
Amidst geopolitical tensions, a nation-state actor aims to disrupt international travel by targeting the Border Control System. The onslaught starts with physical damage to server infrastructure, paired with cyberterrorism tactics, such as spreading fake alerts on social media, causing widespread panic. Capitalizing on the ensuing chaos, the attackers introduce malware, corrupting data from various border control authorities, and launch a DDoS attack, creating border operation halts. They exploit system flaws, corrupting more data and intercepting communications. Amid the crisis, an admin inadvertently erases crucial data, hindering recovery. The climax sees a successful phishing scheme, duping employees into yielding login details, granting the adversaries access to privileged data.
The Border Control scenario covers the following use case:

- UC2.4 Cyber-attack to Schengen II border control including sensitive data breaches and supply chain disruption

Upcoming Steps and Expected Outcomes:

- Organisation of multilateral and bilateral **meetings** with technology providers.
- Identification which ATLANTIS **components** can support the LSP#2 scenarios and how they will be "integrated" with the Critical Asset (i.e., border control system) towards the initial validation.
- Represent scenario **concepts** such as CI, actors, threats, data, security protocols etc. within the ATLANTIS framework.
- Preparations for **trial** execution plans, provision of datasets, security protocols and other assets.

LSP3: Cross-Country Large-Scale Pilot in FinTech / Financial

Lead Partner: CaixaBank S.A.

LSP3 Overview:

ATLANTIS LSP#3 will validate cyber-human security, protecting against systemic risks, and offering business continuity and resilience measures in the finance sector. It will focus on information sharing at several operational levels, including the internal CI and cross-border security environment.
Cyberattacks against financial CI operators in the form of hybrid threats would have a significant negative impact on Europe's business continuity. For instance, any cyberattack on CXB might have a significant impact on other financial institutions throughout Europe and beyond. Significant disruptions to banking and trading operations might have significant cascading repercussions that would affect many other European countries.
CaixaBank, the LSP#3 leader, and JRC are two end-user organizations that are involved in this finance sector-focused trial. The following are some of the advantages that ATLANTIS architecture might provide

- Improved defenses against physical and digital threats to important banking assets can help stop financial losses and reputational harm.

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

- Enhancements to consumer protection and data privacy can assist secure the confidentiality, integrity, and availability of sensitive financial information.

Improved detection and response to security incidents can help reduce the effect of disruptions to banking operations and services.

Use Cases: Over the above combination of CI, the main scenarios to be validated are:

- **UC3.1** Cyber-attack to a vital CI's as a part of hybrid threats including the disinformation campaigns
- **UC3.2** Cyber-attack to the financial transactions, bank systems and operations, card transactions or payment system APIs (with focus on the bank interfaces), including modification, distributed denial of service (DDoS) and personal/sensitive data breaches
- **UC3.3** Validate PTN services without using GNSS support (focus on timing)

Partner Contributions:

CXB CaixaBank S.A. is a financial institution in charge of payments, financial services and card transactions. CXB is the largest financial institution in Spain in terms of number of clients, currently the leading force in Spanish retail banking. Moreover, Caixa Bank has a network of more than 5000 branches, more than 9500 ATMs, and a workforce of over 32,400 employees and has the largest customer base in Spain (21 million people). CXB is leading the LSP3 and directly defining two Use Cases: 3.2 Cyber-attack to the financial transactions, bank systems and operations, card transactions or payment system APIs (with focus on the bank interfaces), including modification, distributed denial of service (DDoS) and personal/sensitive data breaches, defining how to prevent and detect malicious access to CXB systems as well as by using ATLANTIS tools to help the decision taking. UC3.3 - Validate PTN services without using GNSS support (focus on timing) identifying the disruption in the signal and automate the handover of the received signal to another precise time reference alternative, mitigating the effects of the attack and providing time to identify the attacker.

JRC Capital Management Consultancy & Research GmbH is a financial institution focusing on quantitative investment strategies for trading in the most liquid assets, for instance Forex markets. JRC is regulated by the BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) and stands under the supervision of the German Bundesbank. JRC is CI stakeholder, operator and end user. JRC will participate mainly by providing information associated with its CI, analyses use case *3.1- Cyber-attack to a vital CI's as a part of hybrid threats including the disinformation campaigns* and system risks, define countermeasures and contribute to the European CI security policy. The exploitation is directly associated with offering advanced CI security at tactical and strategic level.

Challenges and Technological Solutions:

UC3.1 – The challenge of this use case is to protect the decisions made by the trader based on the news feed and to filter the platform residing on the JRC infrastructure from cyber-attacks, which will cause losses to the JRC's business.

UC3.2 – Main challenge will be to identify any sensitive non-controlled information around the network and detect properly any malicious access to that information, in order to prevent an attack.

The other challenge would be to provide adequate mitigation and response actions when a specific KPI surpasses the maximum desired level of risk. The sensitivity of the information to be managed

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

implies that the use case should be deployed completely in CXB premises or provide adequate data privacy and security mechanisms.

UC3.3 – In case that the attacker can access a range distance in which it can generate signals that can disturb the GNSS signals received by the NTP servers in the data centre.

The main challenge is to provide efficient mechanisms to detect and prevent or mitigate in real-time any attack that affects the PTN signal and can derive disruptions in the time reference information of the data centre devices and applications.

Pilots and Use Cases:

UC 3.1 - Cyber-attack to a vital CI's as a part of hybrid threats including the disinformation campaigns (JRC)

JRC plans to use ATLANTIS tools to identify disinformation campaigns that can influence the decisions of their traders and brokers, deriving an impact on its business. Although most of the JRC business models on wealth management are based on historic quantitative data, those sets of internal and external workers from JRC also use several sources of information to guide their day-to-day activities. Any disinformation campaign can modify their vision towards the markets and their final decisions and timing. By identifying those disinformation campaigns, they want to select only those sources of information that are reliable and take them as a basis.

UC 3.2 - Bank network intrusion and sensitive information leak (CXB)

ATLANTIS tools will help to prevent network intrusion and potential disruption attacks, by monitoring the bank infrastructure and providing a better knowledge and control of the overall cybersecurity situational picture, matching them with the cybersecurity risks of the company (and offering the possibility to configure mitigation action playbooks), to correct any increasing risk KPIs.

UC 3.3 – Data center time (NTP) disruption (CXB)

This use case wants to assess the robustness and resiliency of the time synchronisation infrastructure and protocols on CXB applications. Evaluate and validate that those systems are well protected against time spoofing attacks and that those attacks do not have any impact on the security and business continuity of the entities.

Upcoming Steps and Expected Outcomes:

Goal of UC 3.1- Overcome individual and coordinated cyber threats, attacks based on orchestrated disinformation campaigns or isolated events that could breach trust and result to loss of equity and financial instability and to that extent cause operational disruption to FinTech CI as well as to the investors. Decision support system supporting situational awareness in financial transactions.
Goal of UC 3.2 - Provide tools that increase cybersecurity awareness and real-time cybersecurity risk assessment of the bank.

React earlier to cyberattacks, make efficient decisions, successfully mitigate effects of attacks, and better reduce cascading effects. Identify non-controlled sensitive information spread across Caixa Bank network and systems (e.g., password credentials or configuration information not properly protected).

Goal of UC 3.2 - Validate PTN services without using GNSS support (focus on timing).

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
Mr. Artemis Voulkidis
Synelix, 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