ATLANTIS

D6.5 Dissemination & Standardisation & Communities Liaison (initial version)

Work Package:	WP6		
Lead partner:	Institute for Corporative Security Studies (ICS)		
Author(s):	Jolanda Modic (ICS), Theodoros Semertzidis (CERTH)		
Due date:	M6		
Version number:	0.7	**Status:**	Draft

Project Number:	**101073909**	**Project Acronym:**	ATLANTIS
Project Title:	Improved resilience of Critical Infratsructures AgainsT LArge scale transNational and sysTemic rISks		
Start date:	October 1st, 2022		
Duration:	36 months		
Call identifier:	HORIZON-CL3-2021-INFRA-01		
Topic:	HORIZON-CL3-2021-INFRA-01-01 European infrastructures and their autonomy safeguarded against systemic risks		
Instrument:	IA		

Dissemination Level	
PU: Public	✓
SEN: Sensitive	

Funded by the European Union

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

Revision History

Revision	Date	Who	Description
0.1	30/01/2023	ICS	Release of the document template and initial drafts of all sections.
0.2	09/03/2023	ICS	Updated introduction (Section 1) and executive summary.
0.3	13/03/2023	ICS	Updated Section 2 on collaboration activities.
0.4	19/03/2023	ICS	Updated Section 6 on standardisation and policy making, and conclusions (Section 7).
0.5	20/03/2023	CERTH	Updated Sections 3, 4, 5 on communication, dissemination, and training.
0.6	20/03/2023	ICS	Final edits and preparation of the document for the initial peer review and SAB check.
0.7	28/3/2023	ICS	Revision after peer review.
0.8	30/3/2023	RESA	Updated Section 6 on standardisation and policy making.
0.9	30/3/2023	ICS	Added AB feedback. Final edits.

Quality Control

Role	Date	Who	Approved/Comment
Internal review	23/03/2023	HYG	Otilia Kocsis
Internal review	29/03/2023	SZ	Aleš Hohnjec
Security Review	21/03/2023	ICS	Denis Čaleta

Disclaimer

This document has been produced in the context of the ATLANTIS Project. This project is part of the European Union's Horizon Europe research and innovation programme and is as such funded by the European Commission. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. All information in this document is provided 'as is' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Executive Summary

The first ATLANTIS report on impact generation activities provides a deeper insight into the refined strategy for promoting project activities and results, transferring newly generated knowledge, and shaping the future standards and policies at local and European level.

Specifically, for each of these activities, we elaborate on the goals we want to achieve and the targeted audience we want to reach. Further, for each activity, we present the tools and the channels we are using, the specific actions we are taking on individual and consortium level to realize our goals, and the performance indicators that will help us continuously monitor the progress and adjust the strategy, if needed.

The next iteration of this report will be released in a year, at M18 (as D6.6).

Table of Contents

List of figures

List of Tables

Definitions and acronyms

AB	Advisory Board
AI	Artificial Intelligence
CA	Consortium Agreement
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
C/P	Cyber/Physical
CPH	Cyber – Physical – Human
DoA	Description of Action
EC	European Commission
EU	European Union
GA	Grant Agreement
PC	Project Coordinator
R&D	Research & Development
SAB	Security Advisory Board
SDO	Standards Development Organisation
SIPS	Sensitive Industrial Plants and Sites
SC	Scientific Coordinator
TM	Technical Manager
WP	Work Package

1. Introduction

In the recent years, the European Union has been faced with numerous crises, ranging from pandemic to escalating conflicts and the growing threat of climate change. These crises have highlighted the paramount importance of resilient Critical Infrastructures (CIs) that can withstand complex, large-scale, transnational, cross-domain, systemic risks, and are thereby able to ensure stability, security, and prosperity in the region.

The mission of ATLANTIS is to improve resilience of the interconnected European CIs exposed to evolving systemic risks due to existing and emerging large-scale, combined, cyber-physical-human threats, and thereby guarantee continuity of vital operations, while minimizing cascading effects in the infrastructure itself, the environment, other CIs, and the involved population. To this end, ATLANTIS has defined concrete and ambitious strategic goals that include generating new knowledge, developing and deploying sustainable organisational measures and technological solutions, and enhancing collaboration among various CI stakeholders across Europe.

To ensure that the obtained insights, know-how, and innovations generate direct, tangible, and long-lasting impacts, the project defines several complementary activities described in the remainder of this report, including collaboration, communication, dissemination, training, standardisation, and policy making.

These activities have different goals and target audiences, use different tools and channels, and comprise different activities based on the different phases of the project and maturity of project results, as illustrated in Figure 1 and discussed below.

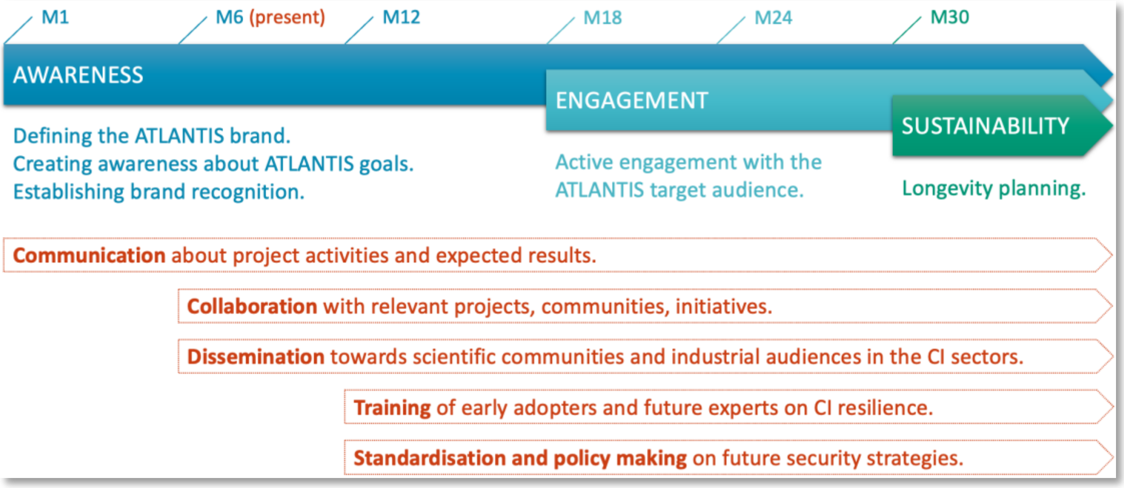

M1
M6 (present)
M12
M18
M24
M30
AWARENESS
ENGAGEMENT
SUSTAINABILITY
Defining the ATLANTIS brand.
Creating awareness about ATLANTIS goals.
Establishing brand recognition.
Active engagement with the ATLANTIS target audience.
Longevity planning.
Communication about project activities and expected results.
Collaboration with relevant projects, communities, initiatives.
Dissemination towards scientific communities and industrial audiences in the CI sectors.
Training of early adopters and future experts on CI resilience.
Standardisation and policy making on future security strategies.

Figure 1. Timeline of the ATLANTIS collaboration, communication, dissemination, training, standardisation, and policy making activities.

In the first, the so-called **AWARENESS** phase (M01 – M18, October 2022 – March 2024), the focus is on increasing visibility of the project and creating awareness about its mission, goals, and results to be produced by (i) establishing the ATLANTIS brand and defining key messages to be conveyed to various target audiences, (ii) identifying opportunities for collaboration with relevant networks, (iii) selecting, establishing, and utilising appropriate communication and dissemination channels, and (iv) shaping the material and actions to be taken to ensure that the generated know-how is effectively transferred to the next generation of researchers, software developers and integrators, CI operators and authorities, relevant standardisation bodies, and policy makers.

In the next, the so-called **ENGAGEMENT** phase (M19 – M30, April 2024 – March 2025), the project will focus on result-oriented activities through which the consortium will actively engage with relevant scientific and industrial communities, various CI stakeholders, and decision makers to (i) disseminate knowledge, promote results, and thus create exploitation opportunities, (ii) train new experts and skilled individuals, and (iii) potentially influence emerging standards and future policies.

In the final, the so-called **SUSTAINABILITY** phase (M31 – M36, April 2025 – September 2025), the efforts will be concentrated on ensuring that the outcomes and impact of the project are maintained beyond its completion. The consortium will work on disseminating final project results, promoting their adoption and replication, ensuring their long-term impacts, and advocating for changes on existing standards, policies, and practices that may impede their realization.

All above-mentioned activities are aligned with well-established **open science practices**. ATLANTIS is promoting openness and reproducibility of research, and therefore adopts best practices to increase the findability, transparency, and accessibility of scientific results. Due to the sensitivity of the topics addressed by ATLANTIS, the project **Security Advisory Board** (**SAB**) is engaged for checks and authorisations for the sharing of potentially security-sensitive information.

In the remainder of the document, we provide further details on each of the assumed impact generation activities. Namely, Section 2 presents the ATLANTIS **collaboration** strategy (coordinated by ICS), highlighting the currently identified opportunities for connecting and networking, and plans on how to seize these opportunities in the future. The **communication** plan (coordinated by CERTH) is presented in Section 3, where we elaborate on ongoing awareness raising. Section 4 is dedicated to the scientific and industrial **dissemination** strategy (coordinated by CERTH), whereas the planned **training** activities (coordinated by CERTH), as a subset of the dissemination task, is described in Section 5. Finally, a set of activities enabling **standardisation and policy making** (coordinated by DMIA) is presented in Section 6.

For each activity, we elaborate on the goals we want to achieve and the targeted audience we want to reach. Further, for each activity, we present the tools and the channels we are using, the specific actions we are taking on individual and consortium level to realize our goals, and the performance indicators that will help us continuously monitor the progress and adjust the strategy, if needed.

This report is a continuation of the work presented in deliverable D6.1 "Project Web Site & Social Channels" submitted at M2 and is closely related with the exploitation report D6.2 "Market Study and Exploitation Plans" submitted at M6. The next iteration of this document is expected at M18, in which we will present an updated strategy for impact generation and impacts achieved in the first half of the project.

2. Collaboration and Outreach Strategy

2.1. Goals

As the complexity and interdependence of the European Critical Infrastructures (CIs) grow, it becomes increasingly challenging for individual organizations to identify, analyse, and manage systemic risks on their own. Effective collaboration among CI operators, authorities, and other stakeholders can lead to a better, shared understanding of the evolving risks and their impacts, as well as the identification and joint development of technological solutions and response plans, and the sharing of best practices for a coordinated mitigation of (i) the negative impacts on individual CIs and (ii) the propagation of cascading effects between the physical and the cyber world, and among the interconnected and interdependent CIs across domains and borders.

Collaboration among the European CIs can result in improved resilience and faster response times in the event of a crisis. Additionally, cooperation and collaboration can facilitate the development of new technologies and approaches, helping critical infrastructures to stay ahead of emerging threats and challenges while maintaining autonomy and sovereignty. Ultimately, by working together, CIs can create a more secure, prosperous, trustworthy, and sustainable environment for everyone.

Collaboration is one of the four strategic goals of ATLANTIS. On the one hand, it will be fostered through **joint R&D activities of the consortium CI stakeholders** throughout the project duration. Namely, each ATLANTIS large-scale pilot includes representatives of different critical sectors and European countries, who will share practices and experience while addressing specific security challenges. On the other hand, ATLANTIS will establish a **scientific, technological, and policy-based collaboration** with other relevant experts and communities with the following goals:

- To **achieve consensus on the current and emerging security issues** relevant for CIs on a cross-domain and cross-border level, and propose new approaches, best practices, strategies, policies, and future projects tackling these issues.
- To **increase awareness of the research gaps** for joint optimisation and/or development of innovative technologies for effective identification, understanding, and management of evolving, systemic risks for European interconnected CIs.
- To **improve the shared situational picture** across the European CIs and realise **joint coordinated procedures** to effectively manage systemic risks on a cross-domain and cross-border level.

To this end, in Section 2.2, we first identify the relevant target groups to achieve these goals, and then we briefly present the tools and channels to be used for establishing, maintaining, and promoting collaboration in Sections 2.3 and 2.4, respectively. The concrete activities done so far, by M6 (March 2023), and the future planned activities along with their expected outcomes, are presented in Section 2.5.

2.2. Target Audience

Engaging with the appropriate target audiences is crucial to the success of the project, as it helps to ensure that the project results are relevant and impactful, and that the project achieves its goals. By identifying and involving the right stakeholders, the project can benefit from a diversity of perspectives, knowledge, and experience.

To make joint advancements in relevant scientific, technological, and policy-making areas, the ATLANTIS consortium has established / will establish links with other funded **research and innovation projects** (and relevant **clusters** of such projects) addressing topics such as risk management, cybersecurity, security, and data science.

The initial list of such Horizon 2020 (H2020) and Horizon Europe (HE) projects, which will be continuously updated, is presented in the set of tables under Table 1. In Table 2, we list relevant national projects, whereas in Table 3 we list complementary EDA funded projects. For each included project, we provide some **basic information** about the project itself (acronym, name, type, duration, website), their **scope** and **intersections** with ATLANTIS that reflect potential areas for technical and/or strategic collaboration (that may change as project results mature), **links** with ATLANTIS partners, and the following two aspects:

- The **type** of collaboration:
    - Technical (reuse of data or technical results).
    - Promotional (participation in joint events and/or publications).
    - Commercial (joint exploitation).
- The **degree** of collaboration:
    - Continuous.
    - Frequent (from time to time but without a scheduled plan).
    - Isolated (one time collaboration).

Table 1. H2020 and HE projects relevant for ATLANTIS collaboration activities.

Project	**EU-CIP**: European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection. Coordination and Support Action October 2022 – September 2025 https://www.eucip.eu/		
Scope and intersections	EU-CIP aims to establish a novel pan-European knowledge network for resilient infrastructures to enable policy makers to shape and produce data-driven evidence-based policies while boosting the innovation capacity of CI operators, authorities, and innovators (including SMEs). ATLANTIS can utilize the audience in EU-CIP to further discuss systemic risks in CIs in other domains and countries not addressed with the ATLANTIS pilots, and can jointly promote developed solutions, best practices, and recommendations for future standards and policies.		
Links	**ENG** is the coordinator of EU-CIP and **FST** is a project partner.		
Type	Promotional	**Degree**	Continuous

Project	**CyberSEAS**: Cyber securing energy data services Innovation Action October 2021 – September 2024 https://cyberseas.eu/
Scope and intersections	CyberSEAS aims to improve the resilience of energy supply chains against cyber-attacks, protecting consumers and the Energy Common Data Space through an ecosystem of 30 customizable security solutions. The project delivers real-time security monitoring, risk assessment, and skills improvement, among other

	features, and is validated through experimental campaigns and piloting infrastructures in 6 European countries. Exchanging ideas, sharing insights on systemic risks to CIs, and potentially reusing developed technology could be beneficial for both projects. Links and common topics of both projects also offer opportunities for strategic collaboration in terms of shared standardisation and policy making efforts.		
Links	**ENG** is the coordinator of CyberSEAS. **ICS**, **SYN**, and **PET** are project partners. ATLANTIS and CyberSEAS are both members of the project cluster **ECSCI**.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**SUNRISE**: Strategies and technologies for united and resilient critical infrastructures and vital services in pandemic-stricken Europe. Innovation Action October 2022 – September 2025 https://sunrise-europe.eu/		
Scope and intersections	SUNRISE facilitates collaboration among CI operators in Europe to jointly tackle future pandemics and build back better with a focus on sustainability and green recovery. The project is identifying pandemic-specific vital services and CIs, developing innovative tools and strategies to ensure their availability, reliability, security, and continuity, and piloting them in operational environments of the CIs while considering legal, ethical, societal, economic, and climate aspects. Sharing insights on interconnected CIs, systemic risks to them, and potential cascading effects could be beneficial for both projects. Exploring opportunities for joint development and promotion of innovations could strengthen both projects. Strategic collaboration in terms of shared standardisation and policy making efforts will be explored.		
Links	**ICS**, **TS**, **SZ**, **MZI**, and **NCI** are project partners. ATLANTIS and SUNRISE are both members of the project cluster **ECSCI**.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**PRAETORIAN**: Protection of critical infrastructures from advanced combined cyber and physical threats. Innovation Action June 2021 – September 2023 https://praetorian-h2020.eu/		
Scope and intersections	PRAETORIAN aims to increase the security and resilience of European CIs against combined physical and cyber threats. It is providing a multidimensional toolset, including physical, cyber, and hybrid situation awareness systems, as well as a coordinated response system, to assist CI security managers in decision-making to prevent and resist potential security threats. The project is demonstrating its results in 3 international pilot clusters, involving 9 outstanding CIs such as international airports, ports, hospitals, and power plants. Know-how and lessons learnt from the PRAETORIAN R&D work, pilots, and impact generation activities will be transferred to the ATLANTIS consortium through activities coordinated by the ECSCI cluster and the EU-CIP action.		
Links	ATLANTIS and PRAETORIAN are both members of the project cluster **ECSCI**.		
Type	Promotional	**Degree**	Frequent

Project	**PRECINCT**: Preparedness and resilience enforcement for critical infrastructure cascading cyber-physical threats and effects with focus on district or regional protection. Innovation Action October 2021 – September 2023 https://www.precinct.info/		
Scope and intersections	PRECINCT aims to develop a systematic approach to security and resilience management for CIs, which will connect private and public stakeholders in a geographical area to a common cyber-physical security management method. The project is delivering a framework specification, a cross-facility collaborative management infrastructure, a vulnerability assessment tool, digital twins, and smart ecosystems in 4 large-scale living labs and transferability validation demonstrators to provide measurement-based evidence of the targeted advantages. The project aims to produce a protected territory for citizens and CIs, which can be replicated efficiently for a safer Europe. Know-how and lessons learnt from the PRECINCT R&D work, pilots, and impact generation activities will be transferred to the ATLANTIS consortium, especially the LSP#1, through piloting activities coordinated by ICS in PRECINCT and through collaboration coordinated by the ECSCI cluster and the EU-CIP action.		
Links	**ENG**, **ICS**, **SZ**, **TS**, and **FST** are project partners. ATLANTIS and PRECINCT are both members of the project cluster **ECSCI**.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**FeatureCloud**: Privacy preserving federated machine learning and block-chaining for reduced cyber risks in a world of distributed healthcare. Research and Innovation Action January 2019 – December 2023 https://featurecloud.eu/		
Scope and intersections	The FeatureCloud project aims to improve healthcare through big data and AI while reducing the risks to sensitive clinical data stored in critical healthcare ICT infrastructure. It proposes a transformative security-by-design concept that integrates federated machine learning with blockchain technology to safely apply next-generation AI technology in medical innovations. The project is employing the world's first privacy-by-architecture method, with no sharing of sensitive data via communication channels and no data storage in one central point. Know-how and lessons learnt from the FeatureCloud R&D work, pilots, and impact generation activities will be transferred to the ATLANTIS consortium through activities coordinated by the ECSCI cluster and the EU-CIP action.		
Links	ATLANTIS and FeatureCloud are both members of the project cluster **ECSCI**.		
Type	Promotional	**Degree**	Frequent

Project	**EU-HYBNET**: Empowering a pan-European network of counter hybrid threats. Coordination and Support Action May 2020 – April 2025 https://euhybnet.eu/
Scope and intersections	EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academics, industry players, and SME actors aimed at preparing for and defending against hybrid threats, incidents that put our safety and security at risk. The project is identifying urgent needs for countering hybrid threats by bringing

	together practitioners and stakeholders, undertaking an in-depth analysis of gaps and needs, and testing the most promising innovations (technical and social) to create a roadmap for success and solid recommendations for uptake, industrialization, and standardization across the European Union. ATLANTIS can utilize the audience in the EU-HYBNET ecosystem to further discuss systemic risks in CIs in other domains and countries not addressed with the ATLANTIS pilots, and can jointly promote developed solutions, best practices, and recommendations for future standards and policies.		
Links	**KEMEA** and **JRC** are project partners.		
Type	Promotional	**Degree**	Continuous

Project	**eFORT**: Establishment of a framework for transforming current EPES into a more resilient, reliable, and secure system all over its value chain. Innovation Action September 2022 – August 2026 https://efort-project.eu/		
Scope and intersections	eFORT aims to upgrade electrical power and energy systems to make them more reliable, resilient, and secure, while also complying with environmental and societal concerns. The project is implementing solutions such as an interoperable intelligent platform, asset management developments, and digital technologies, all validated in relevant environments through 4 demo cases covering the whole grid value chain. Additionally, eFORT will establish a common regulatory and standardisation framework, perform technical and cost-benefit analysis, and evaluate new related business models and replication potential. The insights about relevant risks and associated countermeasures identified and proposed by eFORT may support the work being done in ATLANTIS, especially in parts of LSP#1 comprising, among others, CIs from the energy sector. Both projects can jointly promote the developed approaches, solutions, best practices, and strategies to influence and improve future standards and policies.		
Links	**LINKS** and **CERTH** are project partners.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**MobiSpaces**: New data spaces for green mobility. Research and Innovation Action September 2022 – August 2025 https://mobispaces.eu/
Scope and intersections	The MobiSpaces project aims to develop an end-to-end mobility-aware and mobility-optimized data governance platform that extracts actionable insights from ubiquitous mobile sensor data and IoT devices in a decentralized way. The project will demonstrate the impact of the platform in real-life scenarios with 5 mobility use cases, from smart public transport services to vessel tracking. The platform will offer intelligent transportation services, enforce privacy constraints, and apply XAI techniques to create interpretable prediction models. Both projects, ATLANTIS and MobiSpaces, deal with data governance and data management. Both use cutting-edge technologies such as artificial intelligence (AI). For this reason, insights and techniques developed in one could be applied in the other. Potentially identified gaps in existing standards and policies surrounding this topic could be jointly promoted to relevant standardisation bodies and policy makers.

Links	**SIEM**, **NetU**, and **NCI** are project partners.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**APPRAISE**: Facilitating public & private security operators to mitigate terrorism scenarios against soft targets Innovation Action September 2021 – February 2024 https://appraise-h2020.eu/		
Scope and intersections	APPRAISE aims to develop an integrated threat intelligence solution to protect public spaces from evolving cyber and physical threats while preserving citizens' freedom. Using big data analysis, AI, and advanced visualization, the project is offering unprecedented capabilities to predict and identify criminal and terrorist acts, improve strategies for protection of soft targets, and enhance private-public collaboration among security actors. The project is demonstrating its solutions in 4 pilot sites, including a tennis tournament, a transnational cycling tour, an international fair, and a mall. Both projects, ATLANTIS and APPRAISE, deal with issues related to safety and security, so we will explore opportunities for collaboration or knowledge sharing in areas such as risk assessment, crisis management, and technology solutions. Potentially identified gaps in existing markets, standards, and policies surrounding these topics could also be jointly promoted to relevant audiences.		
Links	**CS** is the coordinator of APPRAISE. **ENG**, **CERTH**, **LINKS**, **VICOM**, and **ICS** are project partners.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**STARLIGHT**: Sustainable autonomy and resilience for LEAs using AI against high priority threats Innovation Action October 2021 – September 2025 https://www.starlight-h2020.eu/		
Scope and intersections	STARLIGHT aims to increase the awareness, adoption, and long-term impact of AI in European Law Enforcement Agencies (LEAs) while reinforcing legal, ethical, and societal values. The project is providing opportunities for LEAs to exploit AI tools and solutions in their operational work, protect their own AI systems, and combat the misuse of AI-supported crime and terrorism. STARLIGHT is also raising high-quality datasets and an interoperable and standardized framework and is creating an AI hub for LEAs to enhance the EU's strategic autonomy in AI. Since both, ATLANTIS and STARLIGHT, focus on enhancing security through the use of advanced technologies, we will explore collaboration opportunities in areas such as developing AI-based security solutions, sharing expertise and knowledge in the use of AI for security purposes, and exploring the use of advanced technologies to combat emerging security threats. Potentially identified gaps in existing markets, standards, and policies surrounding these topics could also be jointly promoted to relevant audiences.		
Links	**ENG**, **CERTH**, **LINKS**, and **VICOM** are project partners.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**5G-LOGINNOV**: 5G creating opportunities for logistics supply chain innovation.

	Innovation Action September 2020 – August 2023 https://5g-loginnov.eu/		
Scope and intersections	5G-LOGINNOV comprises a range of port-driven technological and societal innovations, tailored to realise the objectives including automation for ports; generation of data on floating trucks and emission; automated truck platooning and involvement of high-tech SMEs. The innovations of 5G-LOGINNOV are being implemented and tested in real operating conditions in three Living Lab environments, associated with the three 5G-LOGINNOV ports, namely Athens (Greece), Hamburg (Germany), and Koper (Slovenia). Lessons learnt from the Slovenian Living Lab set up in the Port of Koper (LUK) will be transferred to the ATLANTIS LSP#1. Additionally, joint exploitation opportunities may be explored.		
Links	**LUK**, **TS**, and **VICOM** are project partners.		
Type	Commercial	**Degree**	Continuous

Project	**NEMO**: Next generation meta operating system. Research and Innovation Action September 2022 – August 2025 https://meta-os.eu/		
Scope and intersections	NEMO aims at creating an open-source, flexible, adaptable, and cyber-secure meta-operating system to establish itself as a game-changer for the IoT-Edge-Cloud Continuum. It is introducing innovations at different layers of the protocol stack, enabling on-device cyber-secure federated machine learning, and is validating solutions in 5 industrial sectors. NEMO's sustainability and engagement with SMEs will be achieved via open-source ecosystems, standardization initiatives, and two open calls. Both projects, ATLANTIS and NEMO, focus on developing innovative solutions related to, among others, cybersecurity. Specifically, NEMO's focus on cybersecure federated machine learning could potentially complement ATLANTIS' efforts to develop secure, trustworthy, and scalable AI-powered solutions for increasing resilience of European CIs. Furthermore, both projects aim to leverage existing technologies and open standards, indicating potential for collaboration and knowledge-sharing.		
Links	**ENG**, **NCI**, and **SYN** are project partners.		
Type	Technical, Promotional	**Degree**	Frequent

Project	**KINAITICS**: Cyber-kinetic attacks using artificial intelligence. Research and Innovation Action October 2022 – September 2025 https://kinaitics.eu/
Scope and intersections	KINAITICS aims to explore new attack opportunities and defense capabilities in the interconnected cyber-physical world with the introduction of AI-based control and perceptive systems, and behavioral understanding of physical systems and cyber-attacks. The project is providing innovative tools and methodologies to protect against new threats, incorporate human factors and uncertainties, and assess the regulation of big data uses to counter AI attacks. Both projects, ATLANTIS and KINAITICS, address cybersecurity challenges and the interconnection between information and operational technologies. Know-

	how and lessons learnt from the research, development, and impact generation activities will be transferred among both projects through joint events and R&D partners participating in both projects.		
Links	**CEA** is the project coordinator. **CERTH**, **VICOM**, and **ENG** are project partners.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**EITHOS**: European identity theft observatory system. Research and Innovation Action October 2022 – September 2025 https://www.eithos-project.eu/		
Scope and intersections	EITHOS aims to develop a new system to prevent and investigate identity theft related crimes in Europe. It will educate citizens and provide tools for law enforcement agencies to address challenges and enhance investigations, offering access to information about identity theft trends and utilizing cutting-edge AI-based technology. EITHOS could provide valuable insights and tools to ATLANTIS to help address the cybersecurity challenges that critical infrastructure operators face. This could be complementary to ATLANTIS' focus on systemic resilience. In turn, EITHOS could benefit from the knowledge and expertise that ATLANTIS partners will develop through large-scale, cross-border pilots. This would help inform the development and implementation of the EITHOS observatory system.		
Links	**CERTH** is the project coordinator. **ENG**, **KEMEA**, and **VICOM** are project partners.		
Type	Technical, Promotional	**Degree**	Continuous

Project	**PROMENADE**: Improved maritime awareness by means of AI and BD methods. Innovation Action October 2021 – March 2023 https://www.promenade-project.eu/		
Scope and intersections	PROMENADE is a joint R&D action involving technology developers, users, and research institutions to develop advanced maritime surveillance services exploiting Artificial Intelligence algorithms and different data sources (e.g., AIS, EO, data from practitioners). This project could present synergies for monitoring of CI as ports.		
Links	**SATCEN** is a partner of the consortium and will keep a communication link with the coordinator of PROMENADE after finalization.		
Type	Technical / Promotional	**Degree**	Frequent

Table 2. Ongoing national projects relevant for ATLANTIS collaboration activities.

Project	**EGIDA**: Information privacy technologies. Cervera excellence network. Research project funded by the Spanish Ministry of Science and Innovation and the Center for Industrial Technological Development (CDTI) January 2020 – December 2022 [**FINISHED**] https://egidacybersecurity.com/en

Scope and intersections	EGIDA was the first and only Spanish network of security and privacy technologies formed by technology centers of excellence. The project addressed research in security and privacy technologies with a clear objective, namely the protection of information privacy. The centers that formed the network, namely Vicomtech, Gradiant, Fidesol, and Ikerlan, worked on four technical objectives focused on applied cryptography technologies, digital identity and privacy, security in distributed systems, and development of secure information systems. The technologies, best practices, and lessons learnt by **VICOM** are being brought to ATLANTIS.		
Links	**VICOM** was a project partner.		
Type	Technical, Promotional	**Degree**	Isolated

Table 3. Past EDA-funded projects relevant for the ATLANTIS work.

Project	**PYTHIA**: Predictive methodology for technology intelligence analysis. Coordination and Support Action funded under the EU's Preparatory Action for Defence Research programme. February 2018 – August 2019 [**FINISHED**] https://www.pythia-padr.eu/		
Scope and intersections	PYTHIA's created an innovative methodology to improve strategic civil and defence technology foresight. Using big data analytics, the project analysed large volumes of technology information to identify future disruptive technologies and recommend themes for European defence research. The best practices and lessons learnt in data management, machine learning, and security market trends were brought to ATLANTIS through the coordination teams at ENG that are involved in both projects.		
Links	**ENG** was the project coordinator for PYTHIA.		
Type	Technical	**Degree**	Isolated

Project	**SOLOMON**: Strategy-oriented analysis of the market forces in EU defence Coordination and Support Action funded under the EU's Preparatory Action for Defence Research programme. June 2019 – May 2021 [**FINISHED**] https://www.solomon-padr.eu/		
Scope and intersections	SOLOMON delivered methodologies and tools to ensure that the industries responsible for EU armament systems could rely on a trusted supply and to tackle supply risk in a world of changing strategies and emerging technologies. The best practices and lessons learnt in terms of improving resilience and protection capabilities of interconnected large infrastructures and complex supply chains were brought to ATLANTIS through the coordination teams at ENG that are involved in both projects.		
Links	**ENG** was the project coordinator for SOLOMON.		
Type	Technical	**Degree**	Isolated

Project	**ECYSAP**: European cyber situational awareness platform Research project funded under the European DID programme. February 2021 – May 2021 https://www.ecysap.eu/

Scope and intersections	ECYSAP seeks to strengthen European capabilities in the defence of cyberspace. The project is incorporating capabilities for visualisation, detection, and response to cyber threats and offers support for decision-making at the mission level, as well as an autonomous response capability. To this end, recent advances in cyber defence technologies and emerging areas of expertise as well as innovative research prototypes will converge. Mutually sharing best practices know-how in terms of assessing cyber risks, estimating propagation effects, as well as possible impacts on targets will benefit both projects, ATLANTIS and ECYSAP.		
Links	Projects have no participating partners in common. Nevertheless, links will be sought directly as well as through events (co-)organised by ATLANTIS.		
Type	Technical	**Degree**	Frequent

Apart from seeking synergies with individual projects, ATLANTIS has joined the European Cluster for Securing Critical Infrastructure (**ECSCI**; https://www.finsec-project.eu/ecsci), which currently gathers 30 past and ongoing EU-funded projects, as illustrated in Figure 2.

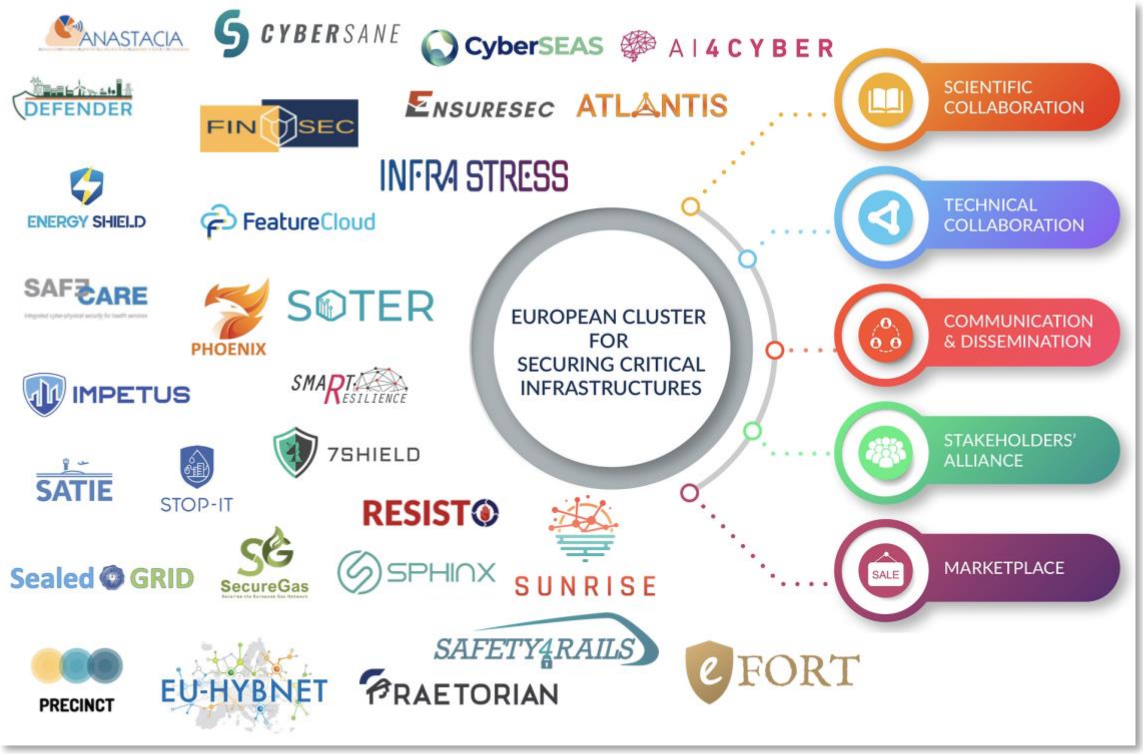


Figure 2. Members of the ECSCI project cluster.

The main objective of the ECSCI cluster is to create synergies among the complementary EU-funded projects and thus foster synchronised development of emerging disruptive solutions for evolving security issues via collaborative innovation. ATLANTIS will take the opportunity of this membership to seek potential joint R&D activities, knowledge sharing, promotion, standardisation, and policy making.

2.3. Tools

Collaboration with target projects and clusters will be based on sharing the following tools that will be prepared by the ATLANTIS consortium partners, presenting project ambitions, results, lessons learnt, and recommendations for shaping relevant future R&D programmes, standards, and policies:

- Scientific papers and whitepapers.
- Conference and workshop presentations.
- Posters and leaflets.
- Open datasets and research outcomes, open-source technologies.

2.4. Channels

Collaboration with target audiences will be pursued through the following channels:

- Conferences and workshops, mainly organised in the scope of the ECSCI cluster and two ongoing Coordination and Support Actions, namely EU-CIP and EU-HYBNET.
- Joint publications to disseminate the work done in respective collaborative projects and/or to showcase their joint findings to wider audiences.

2.5. Activities and Impacts

Collaboration will mainly be sought through conferences and workshops organised by the ECSCI cluster and the ongoing Coordination and Support Actions, namely EU-CIP and EU-HYBNET. To monitor the success of these activities and, most importantly, their benefits and impacts, we define specific KPIs presented in Table 4. For each defined KPI, we also elaborate on its status at M6 (March 2023) in terms of collaborations already formed and joint events already planned.

Table 4. Collaboration activities and impacts (defined KPIs and their status in M6).

Activity (input KPI)	**Impact (output KPI)**	**Status in M6**
Collaboration with at least 2 EDA projects.	≥1 jointly organised or attended events and/or publications on topics relevant for ATLANTIS.	Collaboration with **2 (finished) EDA-funded projects** (PYTHIA, SOLOMON) has been established and the relevant know-how and lessons learnt have already been transferred to the ATLANTIS consortium. With this, the input KPI has been achieved. Collaboration with **at least 1 ongoing EDA-funded project** (at least ECYSAP) will be sought over the next 12 months to define common interests and (as much as possible) jointly pursue common goals. Concrete plans for participation in / organisation of joint events and/or joint publications will be established within the next 12 months. With this, the output KPI shall be achieved.
Collaboration with at least 4 H2020 security project.	≥6 jointly organised events and/or publications on topics relevant for ATLANTIS.	Collaboration with **14 ongoing EU-funded and national projects** has already been established. With this, the input KPI has already been achieved. The first **2 joint events** are already being organised under the scope of the ECSCI cluster and EU-CIP project. More details about these planned events are provided below. With this, we will make great progress towards achieving the output KPI.

Over the next year (by M18 – March 2024), ATLANTIS aims to co-organise and participate (at least) in the following events:

- **EU-CIP – ECSCI joint workshop** in September 2023 for which **ICS** will be one of the main co-organisers. The detailed scope of the workshop has yet to be defined.
- Online **ECSCI workshop** in early December 2023 to discuss research gaps, market needs, and joint roadmaps for future technologies, standards, and policies needed for securing European critical infrastructures. **ICS** is the workshop initiator and will be one of the main event organisers.

The outcomes of the formed synergies and organised events will be reported in the next iteration of this report at M18 (March 2024).

3. Communication Strategy

3.1. Goals

In addition to increasing awareness of systemic risks and the role of ATLANTIS in improving resilience, communication activities aim to achieve several goals in order to create a more resilient and sustainable society. One of the main goals is to make sure that the industrial community and significant stakeholders are directly involved in developing a cooperative strategy for tackling the problems presented by systemic risks. Making sure that non-specialized audiences are reached and that everyone is aware of the value of resilience in society and how they can contribute is another important objective.

3.2. Target Audience

The goal of the communication initiatives in ATLANTIS is to reach a wide range of audiences, including citizens, academics, lifelong learning communities, and stakeholders of critical infrastructure. The main objectives are raising systemic risk awareness and enhancing critical infrastructure's resilience. In order to better serve stakeholders, we aim to develop novel methods for addressing systemic risks, conduct focused research in their areas of interest, and pinpoint the solutions that matter to them.

Stakeholders for critical infrastructure in industries like energy, telecommunications, transportation, and others include operators, authorities, and service and technology providers. Stakeholders in these industries may play a variety of roles, including those of IT departments, Chief Information Security Officers (CISOs), and other important decision-makers. The objective is to guarantee that all interested parties are knowledgeable and equipped to manage systemic risks in critical infrastructure.

In addition to the above, the citizens and academics are also key target audiences for improved transparency and better understanding of the complexities of systemic risks as well as the building of trust to guidelines and procedures that are proposed by the CI operators.

The full list of target audiences and key messages to be conveyed are shown in Table 5.

Table 5. Target audience for communication activities.

Target audience	Key messages
Citizens in general	• Understand the complexity of systemic risks. • Trust the procedures enforced by policy makers and operators. • Follow the guidelines to reduce risks.
Citizens and lifelong learning community	• Be informed about novel solutions related to critical infrastructure safety and security. • Understand the stakeholders' roles and the interconnection of multiple systems in our societies. • Appreciate and improve acceptance of the evolving security procedures that may be posed due to the complexity and the dependency of our societies to critical infrastructures.
Stakeholders' groups	• Be informed on the novel approaches for addressing CI systemic risks. • Learn about specific research performed on your field of interest. • Identify solutions that may be important for you.

3.3. Tools

The ATLANTIS project meticulously selected the communication channels that should be developed in order to reach the target audiences while taking into account the sensitivity of the information to be shared. As such, the consortium decided to focus on a small but effective set of communication tools that will be closely monitored to give a positive impact to the community of stakeholders that are engaged to ATLANTIS channels.

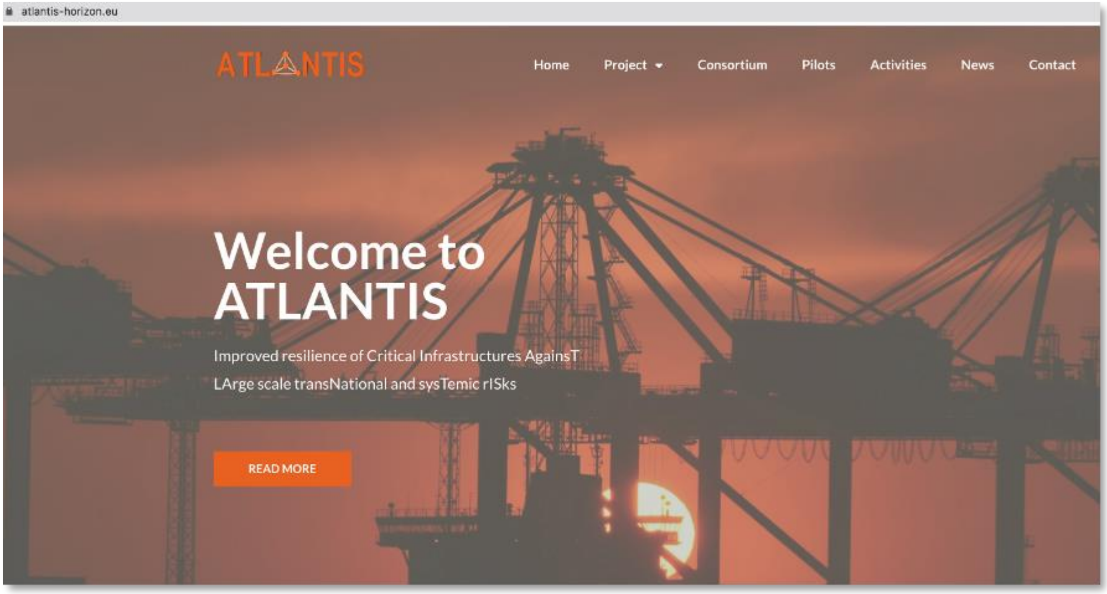
The communication tools that will be used in the ATLANTIS project are:

- **Website**: The project's main information source will be the ATLANTIS website, where all newly discovered information that is authorised for dissemination will be posted.
- **LinkedIn**: A LinkedIn channel will be used as a communication tool that focuses on the stakeholders of critical infrastructures and is primarily oriented towards business-related information and communication.
- **News items**: To keep the general audience up to date, regular news on project developments will be posted through the website news area.
- **Press releases**: To announce significant project accomplishments and milestones, press releases will be distributed to targeted media outlets.
- **Leaflets and brochure**: Material will be produced in ad hoc fashion targeting different audiences in events that ATLANTIS partners participate in.
- **Posters and roll-ups**: To promote the project, posters and roll-ups will be created and displayed at conferences and events.
- **Videos**: To raise awareness about securing critical infrastructures and the ATLANTIS offerings, 1 short video per partner will be produced to present each partner through the communication channels.

The focal point of our communication is the ATLANTIS website (as shown in Figure 3, presented in detail in deliverable D6.1, and accessible through the following web address: https://www.atlantis-horizon.eu/), where all new information that has the clearance to be shared, is posted. Through the website, the target audience is informed about the project in general, the members of the consortium, the pilots that will be performed throughout the project's duration and all activities organised by the project. A news part of the website will be used to communicate activities performed by the project and the members of the consortium on a regular basis. It is important to note that all clearance procedures will be followed for any publication of news or any other publication form.

In addition to the website, a LinkedIn channel was created and is used as a communication channel that focuses on the stakeholders of critical infrastructures and is oriented mainly towards business related information and communication.

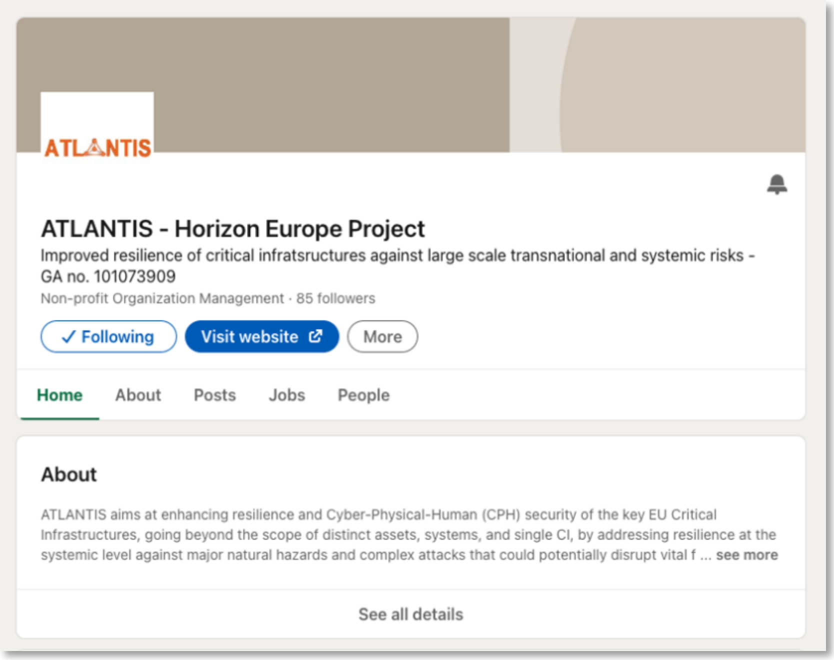
The ATLANTIS LinkedIn profile page is shown in Figure 4, and is available at the following address: https://www.linkedin.com/company/atlantis-horizon-europe-project/.



Welcome to ATLANTIS

Improved resilience of Critical Infrastructures AgainsT LArge scale transNational and sysTemic rISks

Figure 3. ATLANTIS website.



ATLANTIS - Horizon Europe Project

Improved resilience of critical infratsructures against large scale transnational and systemic risks - GA no. 101073909

Non-profit Organization Management · 85 followers

About

ATLANTIS aims at enhancing resilience and Cyber-Physical-Human (CPH) security of the key EU Critical Infrastructures, 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 f ... see more

Figure 4. ATLANTIS LinkedIn profile page.

3.4. Channels

The primary communication channel for the project will be its website, where all updates and information pertaining to it will be posted. This covers articles, occasions, publications, and other pertinent data. Additionally, to share project updates and interact with the target audiences, the project will use the social media platform LinkedIn. There was a thorough discussion about the social media channel or channels to use for communicating ATLANTIS results due to the confidentiality constraints and the criticality of the information and knowledge produced within the project. The decision was to focus on the LinkedIn profile and create effective campaigns there to have a deeper and more engaged communication with the target audience while safeguarding the important information and avoiding multiple channels and different speeds of interaction (e.g., Twitter's average communication frequency is way faster than LinkedIn or Facebook).

A further goal of the project is to publish articles in pertinent magazines to reach a larger audience. The communication strategy will target and identify particular instances of pertinent magazines. These will be both industry specific as well as magazines with high popularity and high penetration in the societies, to reach to wider audiences. Each partner of the ATLANTIS consortium will be responsible for publishing an article in a local/national newspaper of magazine in their local language and address local issues or local structures that need to be safeguarded. Examples of such magazines, to name a few, are:

- https://www.professionalsecurity.co.uk/
- https://industryeurope.com/
- https://europeanbusinessmagazine.com/
- https://www.cecimo.eu/newsroom/magazine/

Campaigns and innovation events will also be organised by the project to present significant results and gather feedback. These events may take place offline or online and, if necessary, concurrently with other events or in collaboration with other projects from the ECSCI cluster and other consortia. Presentations, workshops, and demonstrations could be included in the format of these events, depending on the specific objectives and target audiences. These events will have policymakers, operators, service providers, technology providers, academics, and citizens as their target audience according to the focus of each event. Some of the identified industrial events are:

- The **Emergency Services Show**, 19-20 September 2023, Birmingham, UK.
- **CIPRE** – Critical Infrastructure Protection & Resilience Europe. Organised every year in Europe.
- **CIPRNA** – Critical Infrastructure Protection and Resilience Americas. Organised every year in USA.
- International Conference on Sustainable and Resilient Critical Infrastructure Systems **ICSRCIS**, 05-06August 2023, Amsterdam, Netherlands.
- International Conference on Critical Infrastructure Resilience and Protection **ICCIRP**, 20-21 September 2023, Toronto, Canada.
- International Conference on Resilient Critical Infrastructure Systems **ICRCIS**, 22-23 July 2023, Berlin, Germany.
- **AI4Copernicus**, 25 May 2023, Luxembourg, Luxembourg.
- **CERIS** events, organized regularly and addressing Cluster 3 priorities and projects.

Finally, all project partners will promote ATLANTIS through their organisations' websites and social media channels to improve outreach to the local societies. News and events attended by ATLANTIS partners, that will be posted in the organisations' web sites and social media, will be re-posted and published also through the web site and LinkedIn page of ATLANTIS.

3.5. Activities and Impacts

To monitor the success of the ATLANTIS communication activities and, most importantly, their benefits and impacts, we define specific KPIs presented in Table 6. For each defined KPI, we also elaborate on its status at M6 (March 2023). Specifically, we elaborate on the actions we have made up to M6 (input KPIs) in the context of project communication, and the impacts these actions have had so far (output KPIs).

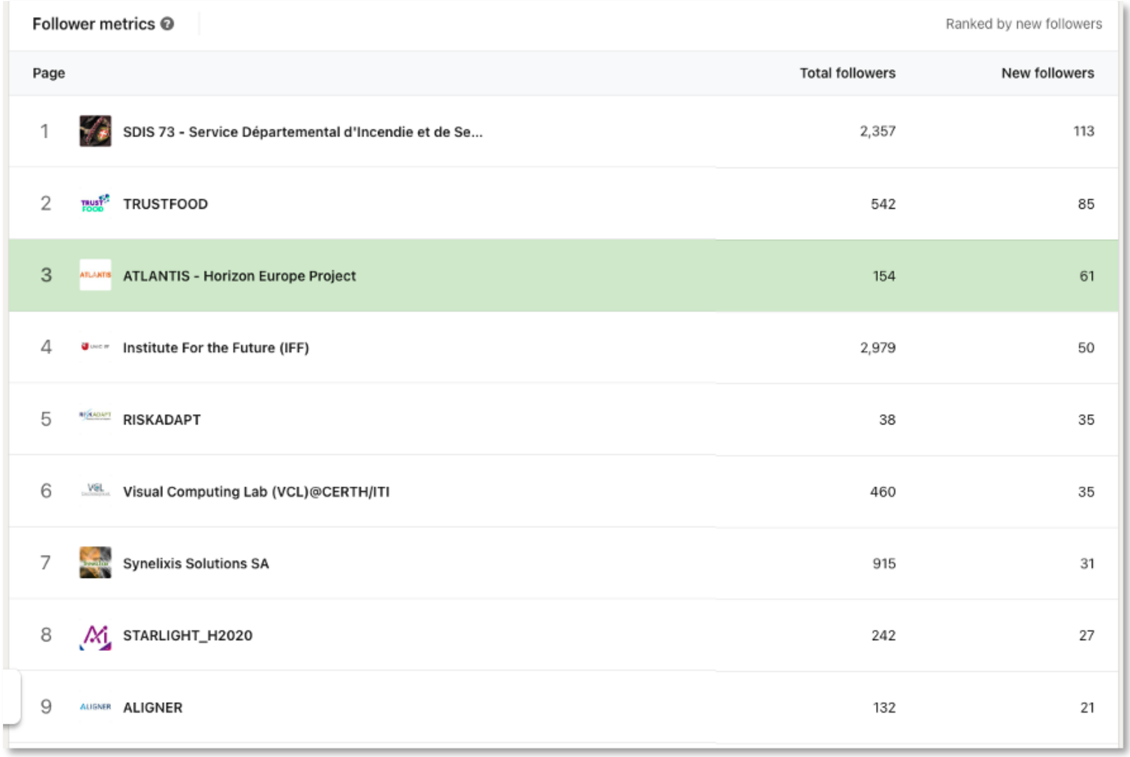
Table 6. Communication activities and impacts (status in M6).

Activity (input KPI)	**Impact (output KPI)**	**Status in M6**
Branding material		
2 newsletters / year	≥ 200 subscribers each	Newsletters will be produced in the next period with focus on the Use Cases and the role of partners in the project. Every information in the upcoming newsletter will be first screened by the Security Advisory Board.
2 leaflets, flyers, or brochures / year (mainly soft copies)	≥ 1 event each ≥ 200 downloads	The first set of leaflets will be shared in the Projects to Policy Seminar (PPS) organised by DG HOME (unit F2) and REA (unit C2) in Brussels (June 2023).
2 posters or rollups / year	≥ 1 event each	No events to be reported yet.
≥2 videos or podcasts	≥ 200 reads	The Q&A scenarios are under development to start producing short videos after M6, sharing the ATLANTIS goals and objectives as well as the partners' profiles.
≥2 whitepapers published	≥ 200 reads	None yet.
>50 news posts throughout the project duration	≥ 5000 reads	3 news posts, with a total of 445 reads so far
Project website		
Project website set up with relevant landing pages (>1 page per topic (events, labs, etc.))	Visibility / popularity (<5 results Google page (SERP))	The project web site appears in the first 5 results (actually, 1st) using as keywords: Atlantis Critical Infrastructure
	Number of visitors (>500 visits per year)	620 visitors in the first 6 months.
	Web page reads (≥3000)	1400 web page reads in the first 6 months.
Social media channels		
LinkedIn account set up.	≥300 followers	154 followers in less than 6 months of operation.
	≥300 visitors / year	268 visitors in the first 6 months.
> 10 video posts	> 1000 views	No videos produced yet.
Campaigns and Innovation events		
2 large-scale exhibition events	≥ 100 attendees	Nothing to report yet.

The goals of ATLANTIS and its activities have been regularly promoted through partners' own websites and media channels. Some examples to consider are listed below:

- CERTH: https://vcl.iti.gr/project/atlantis-2/
- LUK: https://www.luka-kp.si/en/eu-projects/atlantis/
- LUR: https://www.portauthority.hr/novosti/horizon-europe-atlantis/
- PFRI: https://www.pfri.uniri.hr/web/en/projects.php
- SYN: https://synelixis.com/portfolios/atlantis/
- ICS: https://www.ics-institut.si/projekti/projekt-atlantis
- JRC: https://jrconline.com/atlantis-projekt/

The ATLANTIS LinkedIn profile is the 3rd trending, based on the number of new followers, among relevant profiles (Figure 5). The demographics of companies employing the followers of the ATLANTIS profile page are presented in Figure 6.



Follower metrics

Ranked by new followers

	Page	Total followers	New followers
1	SDIS 73 - Service Départemental d'Incendie et de Se...	2,357	113
2	TRUSTFOOD	542	85
3	ATLANTIS - Horizon Europe Project	154	61
4	Institute For the Future (IFF)	2,979	50
5	RISKADAPT	38	35
6	Visual Computing Lab (VCL)@CERTH/ITI	460	35
7	Synelixis Solutions SA	915	31
8	STARLIGHT_H2020	242	27
9	ALIGNER	132	21

Figure 5. LinkedIn profile trend in ATLANTIS related sector.

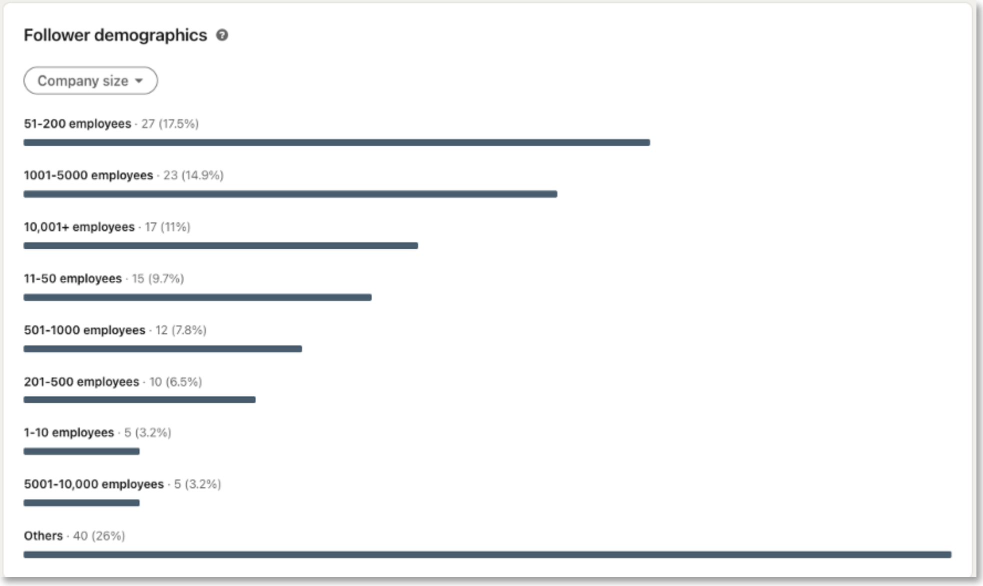


Figure 6. Company size demographic of ATLANTIS LinkedIn profile followers.

During the next year, the consortium partners will create a set of short video interviews, presenting their organisations and their contributions to the project. To that end, we have prepared a template questionnaire to be used as a scenario for the video production. There videos will be used as a material for reaching out to both experts in the field as well as citizens and locals through local/national channels.

Table 7. Video interview questionnaire template.

Presenter introduces the guest. Hello, I am XX from YY .... My background in on … and I am currently working on ....
Can you please present your organisation and your lab, particularly its overarching vision? YY is …
In your view, what are the most important challenges of critical infrastructure protection? The most …
How can the ATLANTIS project address these challenges, and what are its main exciting aspects to you? I believe …
Can you detail your specific role in ATLANTIS? Our role …
What are the Project's expected benefits for your organisation? The ATLANTIS project …
Questions specific to partner: …

4. Dissemination Strategy

4.1. Goals

Research that will be conducted in the scope of the ATLANTIS project will tackle some very interesting and important areas. The goal of the dissemination activities is to bring awareness on the importance of systemic risks as well as emerging C/P/H threats for the security of CIs. An additional goal is to increase awareness towards the research gaps that ATLANTIS aims to bridge such as on large scale, transnational and cross-domain coordinated attacks and countermeasure concepts. Furthermore, ATLANTIS will disseminate directions for guided research.

4.2. Target Audience

ATLANTIS will disseminate the research and countermeasure concepts and provide guided research directions, addressing related scientific audiences such as academia and researchers, as well as industries, SMEs, communication operators and policy making and regulatory stakeholders. Consortium partners will be actively engaged to enhance the quality and relevance of the publications so that the target audience is maximised, leading to a simultaneous maximisation of the impact.

Stakeholders for critical infrastructure in industries like energy, telecommunications, transportation, and others include operators, authorities, and service and technology providers. Stakeholders in these industries may play a variety of roles, including those of IT departments, Chief Information Security Officers (CISOs), and other important decision-makers. The objective is to guarantee that all interested parties are knowledgeable and equipped to manage systemic risks in critical infrastructure.

However, in addition to the above, the citizens and academics are also a key target audience for improved transparency and better understanding of the complexities of systemic risks as well as the building of trust to guidelines and procedures that are proposed by the CI.

The full list of target audiences for dissemination and knowledge to be transferred to them are shown in Table 8.

Table 8. Target audience for dissemination activities.

Target audience	**Specific areas, sectors, and/or profiles**	**Knowledge and results to be disseminated**
Academia and researchers	R&D centres, universities	Peer reviewed papers in journals and conferences from tasks in work packages WP1-WP4 will benefit research in the fields of Risk Management and Assessment, Cyber and C/P Security as well as Mobile Communication and 5G.
CI operators and stakeholders	CI operators in the energy, telecommunications, and transportation	CI operators and stakeholders can be alerted to emerging threats and systemic risks in their infrastructure through WP1 and mitigation measures through design and innovation by WP2 and WP3. Pilot results will also be disseminated to CI operators to study real-world situations and response guidelines.

Industries and SMEs in C/P security	IT engineers and SMEs operating in the security industry	Industries in security will be notified about protective technologies developed in WP3 of ATLANTIS as well as piloting results from WP5 for further development and implementation.
5G and Edge/Cloud operators	R&D departments of EU and national telecommunication operators	Communication needs for effective and secure CI protection detected in WP2.
CERTs, CSIRTs, ISACs, LEAs, Civil Protection Agencies	EU and national security authorities and LEAs	As the ATLANTIS offerings study both equally the cyber-attacks and threats of critical infrastructures, the identified stakeholders will be getting valuable information on the identified results of the Work packages WP5, WP6.
End users' stakeholders, policy, regulators	EU and national civil protection associations and general public	Cross-CI systemic risks and mitigation strategies identified and developed in WP1 will be communicated to the general public with targeted dissemination channels that will be carefully selected and evaluated with the help of the Security Advisory Board.

4.3. Tools

The main tools that will be employed for the ATLANTIS project dissemination activities will include peer-reviewed scientific papers in relevant journals and conferences in order to reach the academic and scientific community. Additionally, whitepapers and presentations in think tanks and European Commission events will disseminate the ATLANTIS results to industrial and SME stakeholders and policy and regulatory agencies across Europe.

Special consideration will be taken for the dissemination of the datasets produced by the project in open data repositories. Zenodo (https://zenodo.org/) and other open repositories will be used to disseminate generated data that are cleared by the ATLANTIS SAB.

4.4. Channels

One of the dissemination channels for the ATLANTIS results is participation in research and scientific conferences and industry events. A list of preliminarily identified relevant events and their relevance for the project is presented in Table 9.

Table 9. Research, scientific, and industry events relevant for ATLANTIS.

Event	Date, location	Relevance
Security / Privacy		
IEEE International Conference on System Reliability and Safety (ICSRS) http://www.icsrs.org/	22-24/11/2023, Bologna, Italy	WP1, WP3
Computers, Privacy and Data Protection (CPDP) https://www.cpdpconferences.org/	24-26/05/2023, Brussels, Belgium	WP1, WP3
IEEE Cybersecurity Development https://secdev.ieee.org/2023/home	18-20/10/2023, Atlanta, GA, USA	WP3, WP4
Communications		
International Conference for Internet Technology and Secured Transactions (ICITST)	13-15/11/2023, London, UK	WP1, WP3

IEEE European Symposium on Security and Privacy https://eurosp2023.ieee-security.org/	04-06/07/2023, Delft, Netherlands	WP1, WP3
IEEE Smart Grid https://sgc2023.ieee-smartgridcomm.org/	31/10-03/11/2023, Glasgow, Scotland	WP1-WP3
IEEE GLOBECOM https://globecom2023.ieee-globecom.org/	04-08/12/2023, Kuala Lumpur, Malaysia	WP1-WP4
IEEE Global IoT Summit https://globaliotsummit.org	19-20/06/2023, Berlin, Germany	WP2
IEEE Future Networks World Forum https://fnwf2023.ieee.org/	13-15/11/2023, Baltimore, USA	WP2

Additionally, publications in scientific journals and magazines with high impact in the research community will be considered, using open science practices when possible. A list of suitable journals and magazines, and their relevance for ATLANTIS, is shown in Table 10.

Table 10. Scientific journals and magazines relevant for ATLANTIS.

Event	Relevance
Security / Privacy	
Elsevier Computers & Security	WP1-WP4
IEEE Security and Privacy	WP1-WP4
Elsevier Journal of Information Security and Applications	WP1-WP4
Springer European Journal for Security	WP1-WP4
ACM Transactions on Privacy and Security	WP1-WP4
Journal of Telecommunications and Information Technology (JTIT)	WP2
Network (MDPI) Special Issue: Blockchain and Machine Learning for IoT: Security and Privacy Challenges https://www.mdpi.com/journal/network/special_issues/blockchain_ml_iot	WP4
Communications	
IEEE Communication Magazine	WP2, WP4
IEEE Sensors	WP2, WP4
MDPI Sensors	WP2, WP4
IEEE/ACM Transactions on Networking	WP2
IEEE Wireless Communications	WP2
ACM Computer Communications, Elsevier Computer Networks	WP2
Verticals	
MDPI Health Care	WP3, WP5
Wiley Transportation Security	WP1, WP3-WP5
MDPI Sustainable Transportation	WP1, WP3-WP5

Finally, all scientific project results and achievements will be published in a relevant section of the ATLANTIS webpage.

4.5. Activities and Impacts

The dissemination activities performed up to M6 are presented in the following table.

Table 11. Dissemination activities and impacts (status in M6).

Activity **(input KPI)**	**Impact** **(output KPI)**	**Status in M6**
≥10 publications in (open access) journals (≥5 publications in the ORE and EOSC platforms)	>80 citations (by M36) >150 citations (by +5 years)	No journal publications yet.
≥15 scientific conference presentations	>100 citations (by M36) >200 citations (by +5 years)	No conference publications yet.
≥3 exhibition stands in large events	More that 400 event visitors in total	**ICS** to organise an event addressing topics relevant to ATLANTIS at the 14th International Conference "Days of Corporate Security", organised by ICS / Slovenian Association for Corporate Security on May 22nd-23rd, 2023. **CERTH** will present ATLANTIS in its "OpenDay" event (May 12th, 2023), a big event in Thessaloniki region, where hundreds of researchers, academics and IT industry professionals participate.
≥2 large workshops organised	More than 80 participants in total	No workshops organised yet.
≥3 open days at trial sites with guided presentations	More than 30 of participants in total	1 open day presentation has been organised at JRC site in Berlin on February 28th, 2023. The event was open to 9 members of ATLANTIS with key roles in WP5, especially LSP#3, and the main topics of the event were **(i)** the overview of the current business processes of JRC and **(ii)** an open discussion on how ATLANTIS can best improve them. A snapshot from the event can be seen in Figure 7.
≥4 invited talks to workshops	More than 100 participants in total	No activity yet.
≥750 GB of anonymised datasets shared in FAIR repositories (e.g., EOSC, re3data.org, DataHub)	More than 10 reuse activities (downloads of data, citations in papers)	No data produced yet.

Figure 7. Snapshot from the JRC Open Day event (Berlin, February 2023).

5. Training Strategy

5.1. Goals

The training activities in ATLANTIS aim to create awareness of the systemic risks and potential threats to critical infrastructure systems, both physical and cyber, and to accelerate the adoption and uptake of concepts and results for maximising their availability.

The training sessions, both MSc and MOOC, will be run by academic partners, CI operators, technology providers, and will disseminate the results to graduate students. The goal is to build a culture of security among CI operators and stakeholders and to ensure that the results of the project are widely available and can be put into practice to enhance the resilience and security of critical infrastructure.

5.2. Target Audience

The produced training material will have 3 main target audiences. The first package of training material will target IT and security engineers and officers in order to advance knowledge in technical operations in the field of security related operations. The second package of training material targets managers and security related decision makers in CI and telecommunication operators, and protection agencies to advance knowledge in risk detection and mitigation strategies. Finally, the third package of training material targets university students of all levels to advance knowledge in the scientific fields related to ATLANTIS.

The full list of target audiences for training activities and the specific skills to be strengthened are shown in Table 12.

Table 12. Target audience for training activities.

Target audience	Specific stakeholders and profiles	Skills to be strengthened
Industries / SMEs in C/P security	EU and national IT operators and security officers, working or looking for employment in C/P security related industries.	Technical oriented training material regarding tools and modules produced from work packages WP2 and WP4.
Technology and utilities employees		
CI operators and stakeholders	CI operators, 5G and Edge/Cloud operators and LEAs / Civil Protection Agencies managers	Technical oriented training material regarding tools and modules produced from work packages WP1 and WP3.
5G and Edge/Cloud operators		
CERTs / ISACs / LEAs / Civil Protection Agencies		
MSc and graduate students	Graduate and MSc students in STEM	Scientific training material and courses regarding the advancements in work packages WP1-WP4.
Citizens and lifelong learning community		

5.3. Tools

The technical partners of the ATLANTIS project will produce presentations describing the tools and modules that are developed during the project. The presentations will be in the form of slideshows and cover a presentation duration of approximately 15 minutes. The content of the presentations will be approved by the Security Advisory Board before uploading them to a MOOC repository or adding them to an MSc program.

Video material will be also available where possible and will be focusing on less academic curricula but provide simplified and targeted information.

5.4. Channels

The material that will be produced by the partners will be focusing on the identified Key Exploitable Results (KERs) and Joint KERs and will be prepared either as a manual of the functionalities and the application of such tools in everyday CI operation or provide details and technical information or the science behind. The topics identified so far, from which the training material may be selected, are presented in Table 13.

Table 13. Training topics.

Tool/Module	Related Task
Terrestrial backup/alternative PNT to complement GNSS	T2.3
Social Channels & Crowd sources Disinformation support	T3.2
Awareness & Comprehension Framework	T3.3
Cyber- Physical-Human enriched DSS	T3.4
Risk Reduction & Incident Mitigation (RRIM) Framework	T3.5
Crowdsensing and human engagement	T3.6
Threat Intelligence solution for the anticipation of systemic risks	T4.1
Human Explainable AI and Intelligence Amplification	T4.2
Multi-CI/Cross-CI SAAM Framework	T4.3
Privacy preserving Federated Machine Learning framework	T4.4

5.5. Activities and Impacts

A set of specific KPIs for the training activities is presented in Table 14. For each defined KPI, we elaborate on its status at M6 (March 2023).

Table 14. Training activities and impacts (status in M6).

Activity (input KPI)	Impact (output KPI)	Status in M6
≥3 presentations for online training sessions	>100 attendees	No activity yet
≥2 training sessions in relevant events	>100 attendees	No activity yet
≥5 subjects in graduate, MSc and PhD level courses	>100 enrolled students	University of Rijeka, Faculty of Maritime Studies, will include ATLANTIS as part of a new elective Graduate Degree Programme in the next year. See details below.

At the **University of Rijeka, Faculty of Maritime Studies**, a new elective course at the Graduate Degree level will be created. The course will have the title "Critical Infrastructure" and will include the subjects:

- Definition and theoretical foundations of CI,
- Key resources and assets,
- Threat Actors and Agents in CI, Risk, threat, and vulnerability assessment,
- Cascading Effects from Interdependencies of CI,
- Coordination of CI Protection,
- Cyber-Physical Systems,
- Cyber security,
- Cyber Law and Regulation,
- Selected aspects of transportation CI.

Concrete examples from ATLANTIS, and any other information that can get SAB clearance, will be included in the curriculum as good practice examples.

6. Standardisation & Policy Making Strategy

6.1. Goals

Promotion of the ATLANTIS results within relevant Standards Development Organisations (SDOs), security networks and communities, and policy makers is one of the crucial project activities to maximise its impact and sustainability beyond the end of the project. In this context, the goal of ATLANTIS is to contribute to **(i)** the implementation of the EU Security Union Strategy and **(ii)** the development of a more coherent and effective cross-CI security strategy. By developing common standards and policies, ATLANTIS can help ensure that the solutions developed are interoperable and widely adopted across CI sectors, which will increase their effectiveness and impact.

As depicted in Figure 8, the ATLANTIS standardisation and policy making process involves the analysis of the landscape and opportunities for change (the "**planning**" phase) and the proactive contributions to the community (the "**development**" phase). Both phases rely on the participation of various stakeholders, including security researchers and experts, CI end users, and relevant standardisation bodies and policy makers, to ensure that the standards and policies developed reflect the needs and interests of all involved parties.

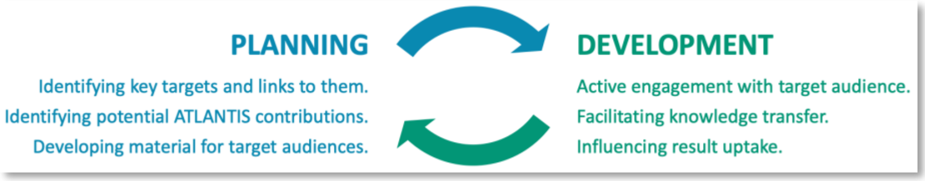

PLANNING
Identifying key targets and links to them.
Identifying potential ATLANTIS contributions.
Developing material for target audiences.
DEVELOPMENT
Active engagement with target audience.
Facilitating knowledge transfer.
Influencing result uptake.

Figure 8. The high-level ATLANTIS standardisation and policy making strategy.

The detailed process of standardisation and policy making is illustrated in Figure 9 and detailed below.

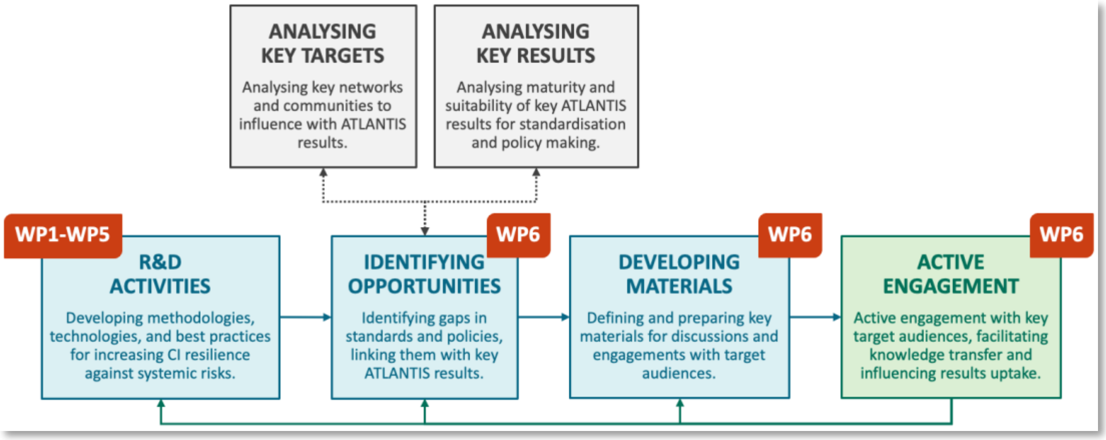

ANALYSING KEY TARGETS
Analysing key networks and communities to influence with ATLANTIS results.
ANALYSING KEY RESULTS
Analysing maturity and suitability of key ATLANTIS results for standardisation and policy making.
WP1-WP5
R&D ACTIVITIES
Developing methodologies, technologies, and best practices for increasing CI resilience against systemic risks.
WP6
IDENTIFYING OPPORTUNITIES
Identifying gaps in standards and policies, linking them with key ATLANTIS results.
WP6
DEVELOPING MATERIALS
Defining and preparing key materials for discussions and engagements with target audiences.
WP6
ACTIVE ENGAGEMENT
Active engagement with key target audiences, facilitating knowledge transfer and influencing results uptake.

Figure 9. The detailed ATLANTIS standardisation and policy making process.

All contributions to emerging standards and future policies will be based on the results of the R&D work done in the project. These results include innovative systemic multi-risk assessments (WP1) and tools and processes for increasing resilience of European interconnected CIs (WP2-WP5). Further details on the ATLANTIS Key Exploitable Results are described in the deliverable D6.2.

While the results are maturing, we will **(i)** analyse relevant networks and communities, their activities and strategies, to identify gaps and opportunities for change, and **(ii)** analyse maturity and suitability of the expected ATLANTIS key results to address these gaps. In this, we will use a range of criteria, for example:

- The **appropriateness** of the result from a technical and conceptual point of view.
- The **readiness** of the result from a technical point of view and IPR aspects.
- The **importance** of the result from a strategic and end user point of view.
- The **cost-benefit analysis** in terms of **(i)** the strength of our links with the relevant target audience are, **(ii)** the availability of engagement opportunities with the target audiences, and **(iii)** the efforts and time needed to make a change.

This task will result in a list of candidates for standardisation and policy making for which a set of tools (materials) will be prepared to ease the knowledge transfer and influence. Finally, active discussions will be pursued to maximise the chance of the project contributions being formally taken into account with the corresponding networks and communities. All feedback obtained from these interactions will be fed back to the consortium to optimise the R&D as well as the opportunities and activities for standardisation and policy making.

6.2. Target Audience

The consortium will primarily seek liaisons with communities and networks with already established links. This will shorten the time to generate impact and increase chances of the acceptance and uptake of results. The candidates for standardisation and policy making and the already established links with ATLANTIS are presented in Table 15. For each listed organisation, where relevant, we also propose a specific targeted Task Force (TF) or Working Group (WG). We note that as relationships and partnerships are constantly evolving and growing, this list is seen as a live document.

Specific contributions proposed and/or made to the listed organisations will be elaborated in the next version of this report, namely in D6.6 submitted at M18 (March 2024).

Table 15. Target audience for ATLANTIS standardisation & policy making activities.

Target audience	Specific TFs and WGs	Links with ATLANTIS
High-level Policy Institutions (EU Level)		
European Commission	N/A	**Project Officer**
EU Parliament	N/A	**DMIA / RESA**
DG Home	N/A	**DMIA / RESA**
High-level Policy Institutions (National Level)		
Countries engaged in LSPs	N/A	
European Association of State Territorial Representatives	N/A	**DMIA / RESA**
High-level Policy Institutions (International Level)		

ISO (International Organisation for Standardization) https://www.iso.org/home.html	• ISO/WD 22372 Security and resilience – Resilient Infrastructure – Guidelines	**RESA** is a contributor.
UNDRR (UN Office for Disaster Risk reduction) https://www.undrr.org/	• MCR2030 programme. • ARISE programme.	**RESA** is a member of both programmes.
Technical & Research Policy Institutions (Security)		
ECSO (European Cyber Security Organisation) https://ecs-org.eu/	• SWG 1.3 Standardisation, certification, labelling • WG6 Strategic Research and Innovation Agenda	**CEA** are members of the Board of Directors. **ENG**, **VICOM**, **SIEM**, **KEMEA**, and **URSIV** are active members.
EOS (European Organisation for Security) http://www.eos-eu.com/	• Artificial Intelligence TF. • Cyber and physical security TF.	**ENG** is a founding member. **ENG** and **KEMEA** are members of the Board of Directors. **VICOM** and **CEA** are members.
ENISA (European Union Agency for Cybersecurity) https://www.enisa.europa.eu/	• Stakeholder Cybersecurity Certification Group (SCCG).	**URSIV** is part of the Management Board. **INTRA**, **ENG**, **KEMEA**, and **CS** have direct links.
RENIC (National Excellence centre of research in Cybersecurity) https://www.renic.es/en	N/A	**VICOM** is a member.
Basque Cybersecurity Centre https://www.ciberseguridad.eu/	N/A	**VICOM** is a member of the Permanent Board and supports the preparation of the research agenda.
CERIS (Community for European Research and Innovation for Security) https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/about-ceris_en		Key staff of **VICOM** has been appointed as an expert in the group on an individual basis. **VICOM and SATCEN** actively participate in CERIS events (e.g., CERIS INFRA workshop).
Technical & Research Policy Institutions (Safety)		
PSCE (Public Safety Communication Europe Forum) https://www.psc-europe.eu/	N/A	**DMIA** is a PSCE User member.
Technical & Research Policy Institutions (R&D)		
One6G https://one6g.org/	• Security WG.	**VICOM** is a member and participates in the Security WG.

NESSI (Networked European Software and Service Initiative) https://nessi.eu/	N/A	**ENG** and **SYN** are members.
EARTO (European Association of Research and Technology Organisations) https://www.earto.eu/	• Security & Defence WG	**VICOM** is a member and participates in the Security & Defence WG.
ICIT (Institute for Critical Infrastructure Technology) https://icitech.org/	N/A	**RESA** has direct links.
CIRI (Critical Infrastructure Resilience Institute) https://ciri.illinois.edu/	N/A	**RESA** has direct links.
ERRAC (European Rail Research Advisory Council) https://errac.org/	N/A	**RESA** has direct links.
Industry Groups & Institutions (The Built Environment)		
GlobalABC (Global Alliance for Buildings and Construction) https://globalabc.org/	• WG on Climate Adaptation	**RESA**'s CEO is leading the WG.
Industry Groups & Institutions (Energy)		
World Energy Council https://www.worldenergy.org/	N/A	**RESA** has direct links.
Industry Groups & Institutions (Transport)		
T&E (The European Federation for Transport and the Environment) https://www.transportenvironment.org/	N/A	**RESA** has direct links.
UITP (The international association of Public Transport) https://www.uitp.org/	N/A	**RESA** has direct links.
CLECAT (European Association for Forwarding, Transport, Logistics and Custom Services) https://www.clecat.org/	N/A	**RESA** has direct links.
PIARC (World Road Association) https://www.piarc.org/en/	N/A	**RESA** has direct links.
PIANC (World Waterborne Transport Infrastructure Association) https://www.pianc.org/	N/A	**RESA** has direct links.

EIM (The European Rail Infrastructure Managers Association) https://eimrail.org/	N/A	**RESA** has direct links.
Industry Groups & Institutions (Data & Telecom)		
Networld Europe https://www.networldeurope.eu/	N/A	**SYN** is a member.
AIOTI (Alliance for Internet of Things) https://aioti.eu/	• Agriculture and Energy (Vertical WG) • Security and Privacy WG	**SYN** is a member and is monitoring activities of several WGs, especially the Agriculture and Energy ones. **VICOM** is a member and active in Security and Privacy WG. **ENG**, **SIEM**, **INTRA**, **LINKS** are members.
BDVA (Big Data Value Association) https://www.bdva.eu/	• TF6 Technical • TF7 Applications	**ENG** and **ATC** are board members. **INTRA** is leading SG7 within TF7 Applications. **VICOM** is a member and participates in the Security Work Group.
5G-PPP (5G Infrastructure Public Private Partnership) https://5g-ppp.eu/	• 5GTANGO - 5G-PPP Phase2 Innovation Action. • Security WG.	**SYN** is included as a party to the 5G-PPP collaboration agreement.[1] **VICOM** is a member and participates in the Security WG. **ENG**, **INTRA**, **SIEM**, **TS**, and **CS** have links.
Industry Groups & Institutions (Space)		
ESA (European Space Agency) https://www.esa.int/	• WG 12 Smart Energy • WG 10 Smart Water Management	**SatCen**, **RESA**, **CS**, and **LINKS** have direct links with ESA.
Connect by CNES https://www.connectbycnes.fr/	N/A	**RESA** is a member.
GEO (Group on Earth Observation) https://www.earthobservations.org/index.php	• General • SPACE-SECURITY	**SATCEN** is a Participating Organization and the leader of SPACE-SECURITY Pilot Initiative, promoting the use of EO for security-related scenarios.

6.3. Tools

The efforts towards standardisation and policy making will be based on a 360 approach where both top-down and bottom-up approaches will be deployed and integrated – thereby co-creating the content with key EU-related policy institutions but also seeking insights from citizen-led and end-beneficiary led groups so as to ensure policy relevance and traction.

[1] https://5g-ppp.eu/parties-to-the-5g-ppp-collaboration-agreement/

Standardisation and policy making will be based on custom material prepared for specific target audiences. In general, this material will be based on the project deliverables, scientific papers, event presentations, and open data and software. This will include:

- Findings from other WPs in ATLANTIS.
- Review of examples from international community for best practice in resilience-targeted security policy frameworks identification and lessons learnt from poor practice to identify challenges, gaps, and ways forward.
- Scientific papers and presentations on relevant topics.
- Policy whitepapers with key recommendations.
- Posters and leaflets.

6.4. Channels

Standardisation and policy making impact will be pursued through the following channels:

- Task forces, working groups, and other inclusive communication platforms (including with target organisations' WGs mentioned above and with industry-led and citizen-led groups) to provide bottom-up information on policy appetite and readiness for the study.
- Key policy events/conferences, including events organised by target organisations.
- Policy-focused general media (radio / TV, newspapers, magazines) and social media to inform the public and gain traction for advocated recommendations.
- ATLANTIS Advisory Board presented below.

We have formed an **Advisory Board (AB)** that comprises 6 experts in the security field (1 female, 5 male) that have direct links and affiliations with our target audience, and/or are highly active in the standardisation and policy making sphere. Their connections include EOS, ECSO, ISO/IEC, BDVA, AIOTI, ITU, ADRA, EFFRA, and EU Alliance for Industrial Data, Edge, and Cloud. To safeguard the privacy of the AB members, their names are not included in this report.

The AB will help us to navigate complex regulatory and policy environments and ensure that project outcomes are relevant and impactful for the wider industry. The value of having an AB can be expressed in several ways: Firstly, the AB can provide valuable **insights and guidance on standardization and policy-making issues** that may affect the project. This can help ensure that the project is aligned with existing and emerging standards and policies, reducing the risk of delays or rework caused by non-compliance issues. Secondly, the AB can help the consortium **identify additional potential stakeholders and build relationships** with key decision-makers in relevant standardization and policy-making organizations. This can provide the project with a more significant voice in shaping standards and policies that affect the project and the wider industry. Finally, the AB can help to **disseminate project results and recommendations** to a broader audience, including standardization and policy-making organizations. This can help to increase the impact and sustainability of the project results and may lead to their adoption as industry best practices.

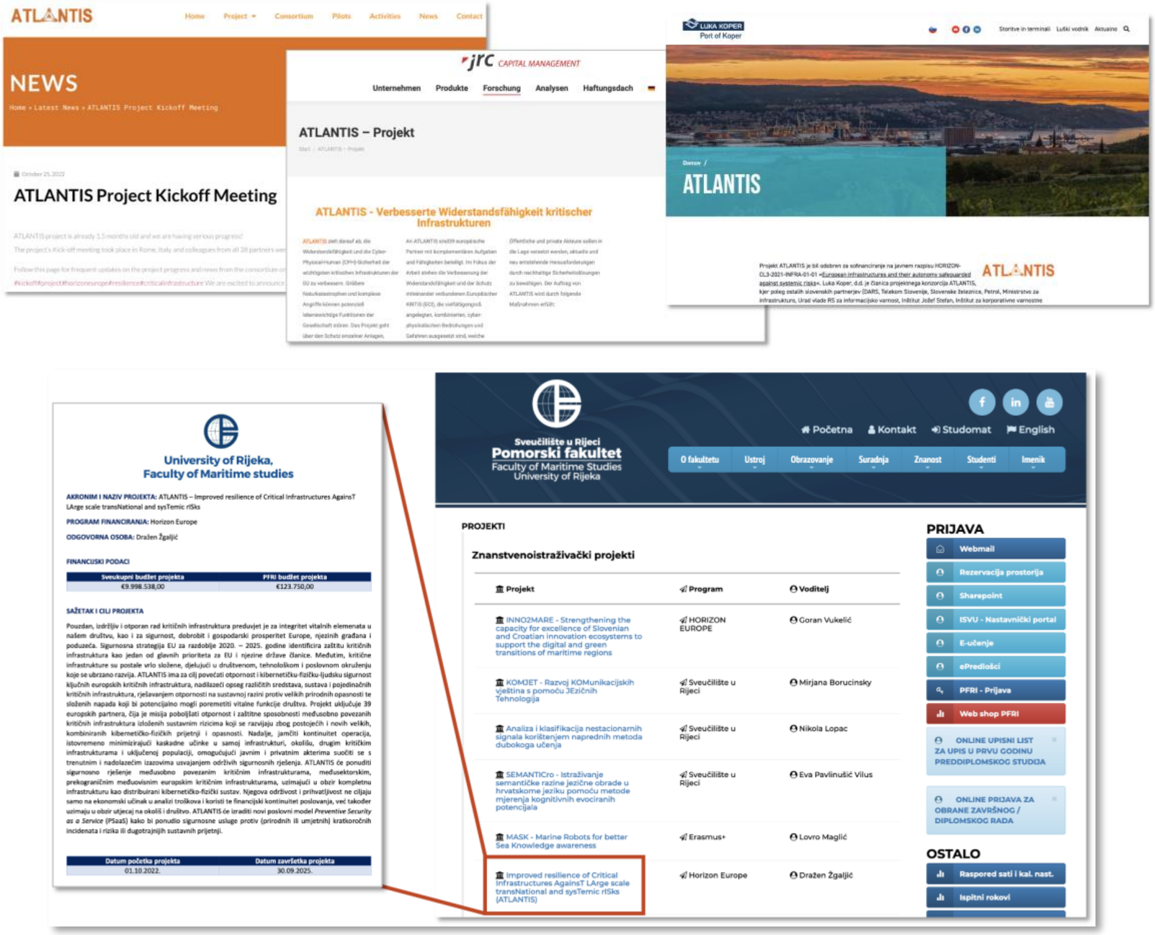
6.5. Activities and Impacts

The consortium will participate in events (e.g., meetings, workshops) organised by relevant task forces and working groups to influence future standards, policies, and strategies. To deepen the understanding of the importance of the project activities and the results it will produce, we will further promote ATLANTIS through press releases, publications, and other media outlets in local language to reach local authorities and decision makers.

To monitor the success and benefit of these activities, we define specific input and output KPIs presented in Table 16. Specifically, we elaborate on the actions we have made up to M6 (input KPIs) in the context of standardisation and policy making, and the impacts these actions have had so far (output KPIs).

Table 16. Standardisation & policy making activities and impacts (status in M6).

Activity (input KPI)	**Impact (output KPI)**	**Status in M6**
≥8 contributions to standards, policy recommendations, or future strategies	≥2 contributions accepted	We have started the R&D activities that will generate relevant contributions, and we have started identifying opportunities for standardisation and policy making.
≥4 press releases at 4 EU languages for local publicity and engagement of local authorities and policy makers	≥200 reads / impressions for each press release, on average	We have prepared the initial press release introducing the project in English and 3 other EU languages, namely German, Slovenian, and Croatian. For each of these, we show examples in Figure 10. On average, each of these has received ≥200 reads. Total impressions for all languages will be reported in the next iteration of this report.
≥2 publications in local newspapers, TV, radio for local publicity and engagement of local authorities and policy makers	≥500 reads / views / impressions for each publication, on average	We have published an article discussing the importance of the project in the Corporate Security Magazine (in Slovenian) that is read by C-suite executives and government representatives in Slovenia, as illustrated in Figure 11. The magazine was published in 1000 physical copies, was distributed in a digital form among 1000 organisations, and was shared through social media (to around 300 LinkedIn followers), where it gained 225 impressions, as shown in Figure 12.



NEWS

Home » Latest News » ATLANTIS Project Kickoff Meeting

October 25, 2022

ATLANTIS Project Kickoff Meeting

ATLANTIS project is already 1.5 months old and we are having serious progress!

The project's Kick-off meeting took place in Rome, Italy, and colleagues from all 38 partners wer

Follow this page for frequent updates on the project progress and news from the consortium or

#kickoff#project#horizoneurope#resilience#criticalinfrastructure We are excited to announce

ATLANTIS – Projekt

Start / ATLANTIS – Projekt

ATLANTIS - Verbesserte Widerstandsfähigkeit kritischer Infrastrukturen

ATLANTIS zielt darauf ab, die Widerstandsfähigkeit und die Cyber-Physical-Human (CPH)-Sicherheit der wichtigsten kritischen Infrastrukturen der EU zu verbessern. Größere Naturkatastrophen und komplexe Angriffe können potenziell lebenswichtige Funktionen der Gesellschaft stören. Das Projekt geht über den Schutz einzelner Anlagen,

An ATLANTIS sind 39 europäische Partner mit komplementären Aufgaben und Fähigkeiten beteiligt. Im Fokus der Arbeit stehen die Verbesserung der Widerstandsfähigkeit und der Schutz miteinander verbundener Europäischer KRITIS (ECI), die vielfältig angelegten, kombinierten, cyber-physikalischen Bedrohungen und Gefahren ausgesetzt sind, welche

Öffentliche und private Akteure sollen in die Lage versetzt werden, aktuelle und neu entstehende Herausforderungen durch nachhaltige Sicherheitslösungen zu bewältigen. Der Auftrag von ATLANTIS wird durch folgende Maßnahmen erfüllt:

Domov /

ATLANTIS

Projekt ATLANTIS je bil odobren za sofinanciranje na javnem razpisu HORIZON-CL3-2021-INFRA-01-01 »European infrastructures and their autonomy safeguarded against systemic risks«. Luka Koper, d.d. je članica projektnega konzorcija ATLANTIS, kjer poleg ostalih slovenskih partnerjev (DARS, Telekom Slovenije, Slovenske železnice, Petrol, Ministrstvo za infrastrukturo, Urad vlade RS za informacijsko varnost, Inštitut Jožef Stefan, Inštitut za korporativne varnostne

University of Rijeka,
Faculty of Maritime studies

AKRONIM I NAZIV PROJEKTA: ATLANTIS – Improved resilience of Critical Infrastructures AgainsT LArge scale transNational and sysTemic riSks

PROGRAM FINANCIRANJA: Horizon Europe

ODGOVORNA OSOBA: Dražen Žgaljić

FINANCIJSKI PODACI

Sveukupni budžet projekta	PFRI budžet projekta
€9.998.538,00	€123.750,00

SAŽETAK I CILJ PROJEKTA

Pouzdan, izdržljiv i otporan rad kritičnih infrastruktura preduvjet je za integritet vitalnih elemenata u našem društvu, kao i za sigurnost, dobrobit i gospodarski prosperitet Europe, njezinih građana i poduzeća. Sigurnosna strategija EU za razdoblje 2020. – 2025. godine identificira zaštitu kritičnih infrastruktura kao jedan od glavnih prioriteta za EU i njezine države članice. Međutim, kritične infrastrukture su postale vrlo složene, djelujući u društvenom, tehnološkom i poslovnom okruženju koje se ubrzano razvija. ATLANTIS ima za cilj povećati otpornost i kibernetičku-fizičku-ljudsku sigurnost ključnih europskih kritičnih infrastruktura, nadilazeći opseg različitih sredstava, sustava i pojedinačnih kritičnih infrastruktura, rješavanjem otpornosti na sustavnoj razini protiv velikih prirodnih opasnosti te složenih napada koji bi potencijalno mogli poremetiti vitalne funkcije društva. Projekt uključuje 39 europskih partnera, čija je misija poboljšati otpornost i zaštitne sposobnosti međusobno povezanih kritičnih infrastruktura izloženih sustavnim rizicima koji se razvijaju zbog postojećih i novih velikih, kombiniranih kibernetičko-fizičkih prijetnji i opasnosti. Nadalje, jamčiti kontinuitet operacija, istovremeno minimizirajući kaskadne učinke u samoj infrastrukturi, okolišu, drugim kritičkim infrastrukturama i uključenoj populaciji, omogućujući javnim i privatnim akterima suočiti se s trenutnim i nadolazećim izazovima usvajanjem održivih sigurnosnih rješenja. ATLANTIS će ponuditi sigurnosno rješenje međusobno povezanim kritičnim infrastrukturama, međusektorskim, prekograničnim međuovisnim europskim kritičnim infrastrukturama, uzimajući u obzir kompletnu infrastrukturu kao distribuirani kibernetičko-fizički sustav. Njegova održivost i prihvatljivost ne ciljaju samo na ekonomski učinak u analizi troškova i koristi te financijski kontinuitet poslovanja, već također uzimaju u obzir utjecaj na okoliš i društvo. ATLANTIS će izraditi novi poslovni model *Preventive Security as a Service* (PSaaS) kako bi ponudio sigurnosne usluge protiv (prirodnih ili umjetnih) kratkoročnih incidenata i rizika ili dugotrajnijih sustavnih prijetnji.

Datum početka projekta	Datum završetka projekta
01.10.2022.	30.09.2025.

PROJEKTI

Znanstvenoistraživački projekti

Projekt	Program	Voditelj
INNO2MARE - Strengthening the capacity for excellence of Slovenian and Croatian innovation ecosystems to support the digital and green transitions of maritime regions	HORIZON EUROPE	Goran Vukelić
KOMJET - Razvoj KOMunikacijskih vještina s pomoću JEzičnih Tehnologija	Sveučilište u Rijeci	Mirjana Borucinsky
Analiza i klasifikacija nestacionarnih signala korištenjem naprednih metoda dubokoga učenja	Sveučilište u Rijeci	Nikola Lopac
SEMANTICro - Istraživanje semantičke razine jezične obrade u hrvatskome jeziku pomoću metode mjerenja kognitivnih evociranih potencijala	Sveučilište u Rijeci	Eva Pavlinušić Vilus
MASK - Marine Robots for better Sea Knowledge awareness	Erasmus+	Lovro Maglić
Improved resilience of Critical Infrastructures AgainsT LArge scale transNational and sysTemic riSks (ATLANTIS)	Horizon Europe	Dražen Žgaljić

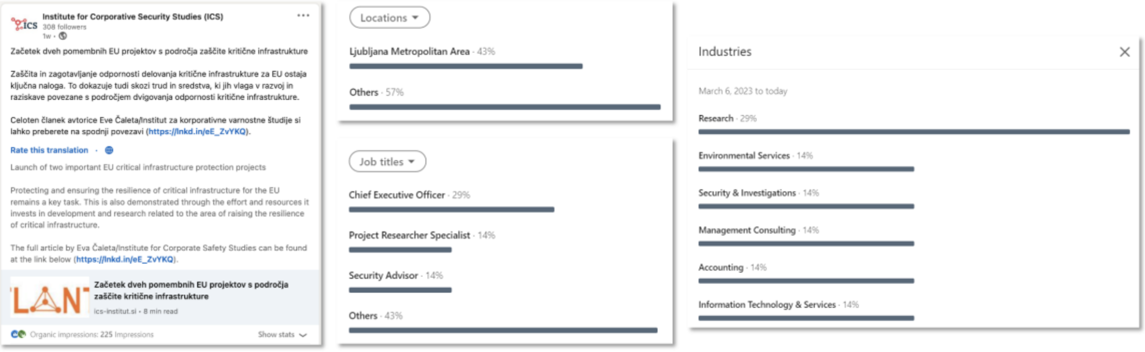
PRIJAVA
Webmail
Rezervacija prostorija
Sharepoint
ISVU - Nastavnički portal
E-učenje
ePredlošci
PFRI - Prijava
Web shop PFRI
ONLINE UPISNI LIST ZA UPIS U PRVU GODINU PREDDIPLOMSKOG STUDIJA
ONLINE PRIJAVA ZA OBRANE ZAVRŠNOG / DIPLOMSKOG RADA
OSTALO
Raspored sati i kal. nast.
Ispitni rokovi

Figure 10. Press releases introducing ATLANTIS in official EU languages, namely (from top to bottom, left to right) in English, German, Slovenian, and Croatian.

Korporativna varnost
ICS
Ustvarjamo vezi, ki bogatijo in tako gradimo pot do uspeha!
Letnik 2022, december • Š. 30
Tradicionalna 14. mednarodna konferenca »Dnevi korporativne varnosti 2023«
Brdo pri Kranju, 23-24. maj 2023
Slovensko združenje korporativne varnosti vključujoča varnostna platforma prihodnosti
ZAČETEK DVEH POMEMBNIH EU PROJEKTOV S PODROČJA ZAŠČITE KRITIČNE INFRASTRUKTURE
ATLANTIS
53
55

Zaščita in zagotavljanje odpornosti delovanja kritične infrastrukture za EU ostaja ključna naloga. To dokazuje tudi skozi trud in sredstva, ki jih vlaga v razvoj in raziskave povezane s področjem dvigovanja odpornosti kritične infrastrukture.

Figure 11. Publication discussing the importance of ATLANTIS in the Slovenian Corporate Security Magazine.



Institute for Corporative Security Studies (ICS)
308 followers
1w ·

Začetek dveh pomembnih EU projektov s področja zaščite kritične infrastrukture

Zaščita in zagotavljanje odpornosti delovanja kritične infrastrukture za EU ostaja ključna naloga. To dokazuje tudi skozi trud in sredstva, ki jih vlaga v razvoj in raziskave povezane s področjem dvigovanja odpornosti kritične infrastrukture.

Celoten članek avtorice Eve Čaleta/Institut za korporativne varnostne študije si lahko preberete na spodnji povezavi (https://lnkd.in/eE_ZvYKQ).

Rate this translation ·

Launch of two important EU critical infrastructure protection projects

Protecting and ensuring the resilience of critical infrastructure for the EU remains a key task. This is also demonstrated through the effort and resources it invests in development and research related to the area of raising the resilience of critical infrastructure.

The full article by Eva Čaleta/Institute for Corporate Safety Studies can be found at the link below (https://lnkd.in/eE_ZvYKQ).

Začetek dveh pomembnih EU projektov s področja zaščite kritične infrastrukture
ics-institut.si · 8 min read

Organic impressions: 225 Impressions
Show stats

Locations
Ljubljana Metropolitan Area · 43%
Others · 57%

Job titles
Chief Executive Officer · 29%
Project Researcher Specialist · 14%
Security Advisor · 14%
Others · 43%

Industries
March 6, 2023 to today
Research · 29%
Environmental Services · 14%
Security & Investigations · 14%
Management Consulting · 14%
Accounting · 14%
Information Technology & Services · 14%

Figure 12. Impacts of promoting ATLANTIS in Corporate Security Magazine on LinkedIn.

Further, we have organised the first (online) meeting with the ATLANTIS Advisory Board, that has taken place in March 2023. The goal of the meeting was to (i) present the goals of the project, the R&D activities undertaken, and the expected results, and (ii) gather feedback from the AB on further ideas on improving relevant, emerging standards and policies. Short notes from the meeting are available in Annex I.

As project results mature, more meetings with the AB will be organised and their outcomes reported in the future versions of this report (in D6.6 submitted at M18 – March 2024).

Furthermore, over the next year (by M18 – March 2024), ATLANTIS aims to organise roundtable discussions with relevant policy makers on a local as well as international level, to **(i)** help policy makers in the critical infrastructure security field to better understand the challenges and opportunities presented by the project, and how it fits within the wider policy landscape, and **(ii)** help the consortium to better understand the perspectives and priorities of policymakers. Ultimately, this engagement can help to ensure that the ATLANTIS outcomes are relevant, actionable, and impactful, can be successfully integrated into broader policy frameworks, and can contribute to positive change in the relevant fields.

7. Conclusions and Future Outlook

Collaboration, communication, dissemination, training, standardisation, and policy making activities are essential components of ATLANTIS that aims to address systemic risks in European CIs. Collaborative efforts enable the project to bring together a diverse range of stakeholders, including researchers, industry partners, and policymakers, to share expertise and knowledge and thus ensure that the project results are comprehensive and effective. Communication and dissemination are essential for ensuring that the project results and outcomes reach a wide audience, including the general public, scientific communities, industry stakeholders, and policymakers. Training activities help to build capacity among various stakeholders, enabling them to better respond to emerging risks and threats. Standardisation activities contribute to the development of common approaches and frameworks, which are critical to achieving systemic resilience in interconnected cross-domain and cross-border CIs. Finally, policy making efforts contribute to the development of policy recommendations and guidelines for the development of effective and sustainable security solutions. Together, these activities help to improve the resilience and protection capabilities of critical infrastructure, enhancing the security and wellbeing of the society.

This report has outlined specific goals and target audiences for each of these activities as well as the tools and channels that have been used so far and will be used in the future. To enable an agile approach to generating impact, we have defined specific input and output KPIs, and have elaborated on our current progress towards achieving the targets.

In the first 6 months of the project (October 2022 – March 2023), we have established the ATLANTIS brand and have started creating awareness about the project mission, goals, and results to be produced. We have refined our target audiences, identified suitable means to use to effectively reach them, and have started implementing various actions to reach the expected impacts.

Future activities will be oriented towards further expanding the ATLANTIS visibility across multiple channels and within various communities, and strengthening its recognition and reputation, ultimately paving the way for effective knowledge transfer and wide adoption of results. These will be elaborated in the next version of this report that is to be submitted at M18 (D6.6, March 2024).

Annex I – Notes from the 1st Advisory Board Meeting

Date and time: March 30th, 2023, 15:00 – 17:00

Agenda:

- [**ENG**] Welcome and introductions.
- [**ENG**] Overview of the project, our mission, our goals.
- [**SYN**] Overview of the R&D activities and use cases.
- [**ICS**] Advisory Board ideas on improving relevant standards and policies.
- [**ENG**] Summary of key takeaways and next steps.

Participants:

- Key representatives of the ATLANTIS consortium (ENG, SYN, ICS).
- 3 Advisory Board Members (*names provided upon request*) with relevant expertise on security, privacy, critical infrastructure, standardisation, and policy making.

Key notes:

- The Project Coordinator (**ENG**) presented the high-level overview of the project, the current activities, and results produced so far.
- The Technical Coordinator (**SYN**) further elaborated on the ongoing research and technical activities, the initial results, and the future roadmap.
- The Advisory Board (AB) provided support and inputs in terms of relevant emerging standards and regulations for ATLANTIS consider, namely:
    - The AB offered support to explore opportunities to help shape standards on the CER Directive.[2]
    - The AB suggested to explore relevance of the following standards, policies, and tools:
        - Cyber Resilience Act.[3]
        - ISO/IEC CD 9837-1 Software and systems engineering – Systems resilience – Part 1: Concepts and vocabulary[4]
        - MITRE CREF Navigator[5,6]
        - MITRE Cyber Infrastructure Protection Innovation Centre's (CIPIC's) work on technical capabilities to ensure resiliency of our nation's and our allies' cyber infrastructure and techniques to deter adversaries and mitigate risk.[7]

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN
[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en
[4] https://www.iso.org/standard/83604.html
[5] https://www.mitre.org/news-insights/news-release/mitre-launches-cyber-resiliency-engineering-framework-navigator
[6] https://crefnavigator.mitre.org/navigator
[7] https://www.mitre.org/our-impact/mitre-labs/cyber-infrastructure-protection-innovation-center

  - The AB commented on the general need to align the architectures proposed in the context of CI resilience and cyber resilience, which is a problem that extends the scope of the ATLANTIS project and creates issues in achieving interoperability. The AB offered to provide support in addressing this within ATLANTIS.
  - The AB congratulated the consortium on the presented risk assessment methodology and taxonomy and proposed to standardise the first and share the latter. Support is offered for this.

Next steps:

- The AB will provide further feedback and offer support (offline) on tasks listed above.
- The second AB meeting will be organised by the ATLANTIS consortium in the fall 2023. Afterwards, meetings will be organised with the AB twice per year.

Funded by the
European Union

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