An innovative Greek start-up specialised in cyberspace security requires Eurostars partners for cyber-resilient satellite and critical infrastructure protection with explainable AI and Zero Trust (Eurostars Call 9)

Summary

Profile type	Company's country	POD reference
Research & Development Request	**Greece**	**RDRGR20250626006**
Profile status	**Type of partnership**	**Targeted countries**
PUBLISHED	**Research and development cooperation agreement**	**• World**
Contact Person	**Term of validity**	**Last update**
Enrico FRANZIN	**29 Jun 2025** **29 Jun 2026**	**29 Jun 2025**

General Information

Short summary

A Greek start-up is forming a Eurostars consortium to develop a cyber-resilient security architecture for space and critical infrastructures. The project combines the implementation of Zero Trust principles, explainable AI, and privacy-enhancing identity management to protect interconnected ground and satellite systems. Research and SME partners with expertise in cybersecurity, AI/ML, and secure embedded environments are sought.

Full description

As critical infrastructure becomes increasingly interconnected-linking operational technology (OT), SCADA, IoT, and satellite systems-it also becomes more vulnerable to sophisticated cyber threats. This project addresses exactly that growing risk by designing and developing an advanced lightweight cybersecurity architecture that integrates Zero Trust principles, privacy-preserving access controls, and explainable AI-based threat detection across both space and ground infrastructure. The initiative is led by a Greek deep-tech start-up specialised in building next-generation cybersecurity solutions for critical infrastructure and space systems.

The company combines expertise in Zero Trust architecture, privacy-enhancing identity management, decentralized

architectures and AI-based intrusion detection. It has been actively developing modular, scalable cyber defense technologies that support secure digital transformation in aerospace, and defense sectors. Its solutions are tailored for high-assurance environments and often involve integration with ground and space segment systems and satellites, OT systems, and decentralized infrastructure.

The core objectives of the project are: (1) to define and implement a Zero Trust Architecture using frameworks such as MITRE ATT&CK and SPARTA across satellite, ground station, and OT environments; (2) to develop a privacy-enhancing and access management system using technologies such as decentralized identities (DiDs), Zero Knowledge Proofs, and selective disclosure; (3) to integrate hardware-based security measures such as secure boot, Trusted Platform Modules (TPMs), and Hardware Security Modules (HSMs); (4) to build a lightweight and explainable AI-powered Collaborative Intrusion Detection System (CIDS) capable of operating locally in resource-constrained environments like satellites; and (5) to establish a cross-domain threat monitoring and incident response framework that enables real-time threat visibility and response.

The project applies to multiple critical infrastructure sectors- such as energy, telecommunications, and transport- as well as to satellite platforms and ground stations. It is expected to significantly reduce the attack surface, enable early detection of threats, and enhance system resilience. By delivering actionable and explainable insights, the solution will also support operator and mission stakeholder trust and accountability. Moreover, by introducing security-by-design access management and fine-grained segmentation, it will set a new standard in cybersecurity for distributed ecosystems.

The consortium currently includes the aforementioned Greek SME as project lead and a prospective academic partner from Norway specializing in Cybersecurity, Risk and Governance. The consortium is now looking to complement its expertise with additional partners- particularly research institutions and SMEs with strong backgrounds in Zero Trust implementation, design and implementation of embedded AI/ML algorithms for cyber threat detection, privacy-enhancing techniques and cryptographic protocols, and secure system design for OT and space systems.

The partners shall be SMEs based in Eurostars countries and be funding beneficiaries according to the requirements of the call for proposals in their own country.

With the estimated call deadline of 4 September 2025 and a project duration yet to be defined (less than 36 months), the team invites expressions of interest from potential partners ready to contribute to and benefit from this innovative endeavour.

Advantages and innovations

Unlike most Zero Trust implementations focused on enterprise IT, this project extends Zero Trust principles to hybrid infrastructures, including OT, SCADA, and satellite networks. This allows for micro-segmentation, continuous authentication, and dynamic access control even in highly distributed and heterogeneous systems.

The identity and access management component integrates cutting-edge cryptographic methods, such as, decentralized identities (DiDs), Zero Knowledge Proofs (ZKP), and selective disclosure. These methods enhance privacy while supporting secure, fine-grained control of access to resources across both ground and space nodes.

The project also delivers a collaborative AI-driven threat detection and response system designed specifically for constrained environments, such as, embedded systems, satellites, and remote OT devices. By focusing on explainable federated AI algorithms, the system can operate efficiently under limited computational resources while providing transparent, actionable insights to system operators and mission stakeholders. This ensures trust and usability in real-world deployment scenarios.

One of the key innovations is the creation of a Collaborative Intrusion Detection System (CIDS) that enables distributed detection, prioritization, and sharing of threat intelligence across space and ground domains. This

contributes to enhanced situational awareness and coordinated response without reliance on centralized infrastructure.

Collectively, these innovations will lead to a reduced risk of cyber disruption across mission-critical and highly distributed infrastructure. By integrating explainability, adaptability, and strong cryptographic primitives, the project provides a future-ready cybersecurity solution aligned with European priorities such as the AI Act, the EU Cybersecurity Strategy, EU Space Act and digital sovereignty goals.

Technical specification or expertise sought

The consortium is now looking to complement its expertise with additional partners based in Eurostars countries.

Specifically, they are looking to partner with a research institution or university with strong expertise in Zero Trust cybersecurity design and implementation, OT/SCADA threat modeling (e.g., MITRE ATT&CK, SPARTA), and applied cryptographic methods, such as, Zero Knowledge Proofs (ZKP) and decentralized identities (DiD). Experience with secure hardware architectures (TPM/HSM, secure boot) and micro-segmentation strategies is also of interest, but not mandatory.

In parallel, the consortium is seeking an SME with applied knowledge in artificial intelligence and machine learning for cybersecurity. Ideal partners will have experience with anomaly and intrusion detection, behavioral analytics, and explainable AI, particularly in environments where computing resources are limited (e.g., satellites, embedded systems).

Prior participation in collaborative R&D projects under Eurostars, Horizon Europe, or ESA would be considered a strong advantage.

Stage of development

Lab tested

IPR Status

IPR Notes

Sustainable Development goals

- **Goal 9: Industry, Innovation and Infrastructure**

Partner Sought

Expected role of the partner

The academic partner will contribute to threat modeling using MITRE ATT&CK and SPARTA for both space and critical infrastructure environments. They will advance cryptographic methods such as decentralized identifiers (DiD) and Zero Knowledge Proofs (ZKP) and support the design of the architecture with defining micro-segmentation and trust boundaries. Additionally, they will assist in designing and/or testing of hardware-based trust measures. Their role is to provide the scientific foundation and support the development of secure and privacy-enhancing frameworks.

The SME will focus on designing and implementing AI-driven threat detection and response for satellite and OT environments (resource-constrained environments). They will develop lightweight, explainable AI models suitable for constrained systems, and build the Collaborative Intrusion Detection System (CIDS). Their role includes integrating CIDS into the Zero Trust architecture, deployment of CIDS in target systems ensuring effective and efficient cybersecurity analytics across all infrastructure layers.

Type of partnership

Research and development cooperation agreement

Type and size of the partner

- **University**
- **SME 50 - 249**
- **R&D Institution**
- **SME <=10**
- **SME 11-49**

Call Details

Framework program

Eureka

Call title and identifier

Eurostars call for projects- September 2025

Submission and evaluation scheme

Anticipated project budget

Coordinator required

No

Deadline for EoI

Deadline of the call

5 Aug 2025

4 Sep 2025

Project duration in weeks

Web link to the call

https://eurekanetwork.org/opencalls/eurostars-september-2025/

Project title and acronym

Resilient Zero Trust Cyber Defense with Explainable AI for Satellite and Critical Infrastructure Ecosystems

Dissemination

Technology keywords

- **01003001 - Advanced Systems Architecture**
- **01003003 - Artificial Intelligence (AI)**
- **01003008 - Data Processing / Data Interchange, Middleware**

Market keywords

- **01006001 - Defence communications**
- **01004002 - Data communication components**
- **01004008 - Other data communications**

Targeted countries

- **World**

Sector groups involved