Engagement	SHIELD: Water Utilities Protection with the Involvement of UxV Technologies and Cyber Security Modules						
Countries	**Project value (€)**	**% by EPSILON**	**€ by EPSILON**	**Engagement**	**Funding by**	**Date**	**Partners**
CH, DE, EL, GR, UK, PT, EL,AT, CY	6.226.762,50	10%	620.000	HORIZON	EU	07.03.2018	NKUA, CSEM, AVIONTEK, HES-SO, MND-GR, UNIWA, UoG, UTH, OCEANSCAN, MOBICS, TUV AUSTRIA,ATLANTIS CY, EYDAP, MB

Description

Critical Infrastructures (CIs), including water, energy, transport, communications, health, and financial services, are essential for countries' stability. Attacks on CIs, whether accidental or deliberate, can cause severe impacts, including cascading effects across sectors. Water systems are particularly vulnerable, with past incidents including biological, chemical, and cyber threats. Terrorists may target water infrastructure using drones or explosives, while natural disasters like floods or earthquakes can also cause damage.

Effective Early-Warning Systems (EWS) are crucial for water management, enabling real-time monitoring and rapid responses.

EPSILON and the consortium, proposed to offer a generic framework applied in water systems management. Water systems would be monitored by a set of sensors (IoT devices) placed in pipelines, dikes, polders and dams. SHIELD will offer a dense IoT network that will cover any critical part of the CI. SHIELD will adopt sensors related to water management. It should be noted that the adoption of sensors monitoring the water quality has already implemented in the project STOP-IT4 funded in the previous call for CIP. The adopted sensors would record data related to water temperature, pressure and flow that are to identify abnormality in the smooth distribution of water.

SHIELD was aimed to enhance water infrastructure protection by monitoring for unauthorized access, using ground infrastructure and UAVs/USVs for intrusion detection and neutralization. Unlike STOP-IT, which detects human presence in restricted areas, SHIELD also would defend against moving threats like drones and vehicles. It employs progressive electronic countermeasures, making it scalable and eco-friendly. Additionally, UAVs/USVs would perform inspections before or after emergencies and conduct water quality sampling in open areas like lakes and dams.

Outcome

- SHIELD offers a multi-tier platform that covers all the aspects of the CIP lifecycle. It aims to aggregate data observed by IoT devices or CaaS and cover multiple threats identification - response. Threats can be identified either locally or in the core system firing mitigation and response actions.
- SHIELD offers a set of components for each phase of a crisis management process while being compatible with the requirements of the CIP lifecycle
- Identify and analyze possible threats (physical, cyber, cascading) in water management systems
- Design and implement specific mechanisms for threats (physical or cyber) prevention and detection.
- Design and implement specific response mechanisms
- Design and implement specific mitigation strategies