AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework

Angeliki Tsanta, AI4CYBER Dissemination & Communication Leader

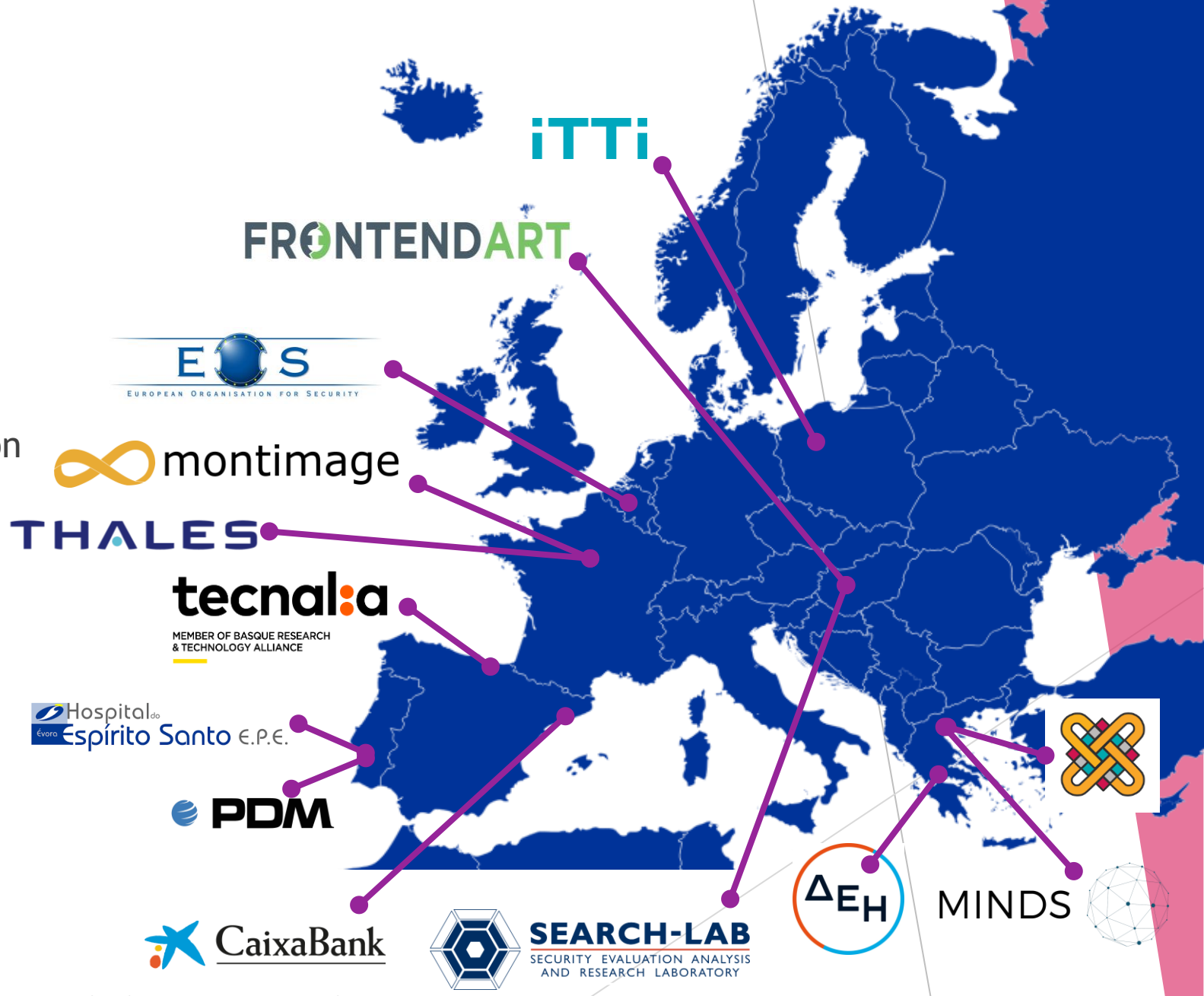
EUROPEAN ORGANISATION FOR SECURITY

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 101070450.

AI4CYBER Project

- **Coordinator:** TECNALIA
- **Consortium:** 13 partners; 7 EU MS
- **Project Type:** Research and Innovation



- **GA ID:** 101070450
- **Start Date:** 1 September 2022
- **End Date:** 31 August 2025

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 101070450.

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 101070450.

Introduction - Motivation

- Artificial Intelligence (AI)
  - Revolutionary technology
  - Countless improvements in multiple domains
  - EC Artificial Intelligence Act → development of trustworthy and ethical AI
- **AI + Cybersecurity**
  - Double-edged sword
  - Malicious use of AI technology
  - AI as target of adversarial attacks

Need of innovative cybersecurity methods and tools that are **more intelligent** than their offensive counterparts

Funded by the European Union

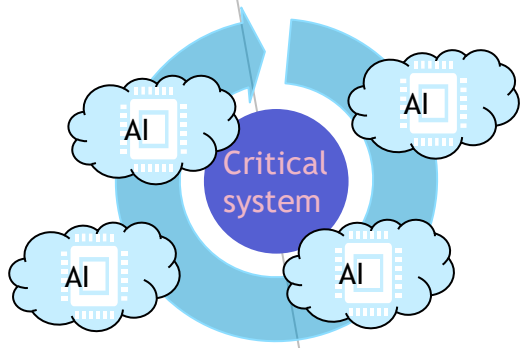
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

Key objectives

To establish an **Ecosystem Framework of next generation AI-based services** for supporting critical system developers and operators to **efficiently manage** system **robustness**, **resilience**, and appropriate **response** in the face of **advanced and AI-powered cyberattacks**.

Continuum of care



O1

Provide an **Ecosystem Framework of next-generation trustworthy cybersecurity services** that leverage AI and Big Data technologies to support system developers and operators in effectively managing **robustness**, **resilience**, and dynamic **response** against **advanced** and **AI-powered cyberattacks**.

O2

Deliver a new breed of **AI-driven software robustness** and **security testing services** that significantly facilitates the testing experts work, through smarter **flaw identification** and **code fixing automation**.

O3

Provide cybersecurity services for **comprehension**, **detection** and **analysis** of **AI-powered attacks** to prepare the critical systems to be resilient against them.

O4

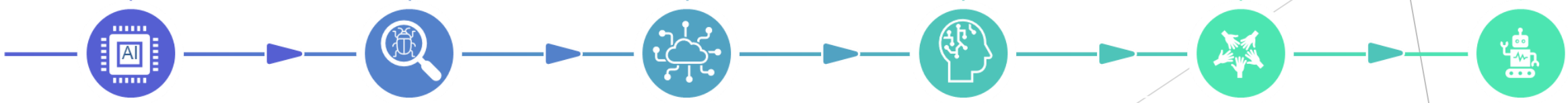
Offload security operators from complex and tedious tasks offering them mechanisms to **optimize the orchestration** of the most appropriate combination **of security protections**, and continuously learn from system status and defences' efficiency.

O5

Ensure European **fundamental rights and values-based AI technology** for the AI4CYBER framework through the integration of demonstrable **explainability, fairness** and **technology robustness (security)** capabilities **in the AI4CYBER components**.

O6

Foster open innovation and **business opportunities** through **demonstration of AI4CYBER services** integrated into **critical services** use cases relevant for Europe.



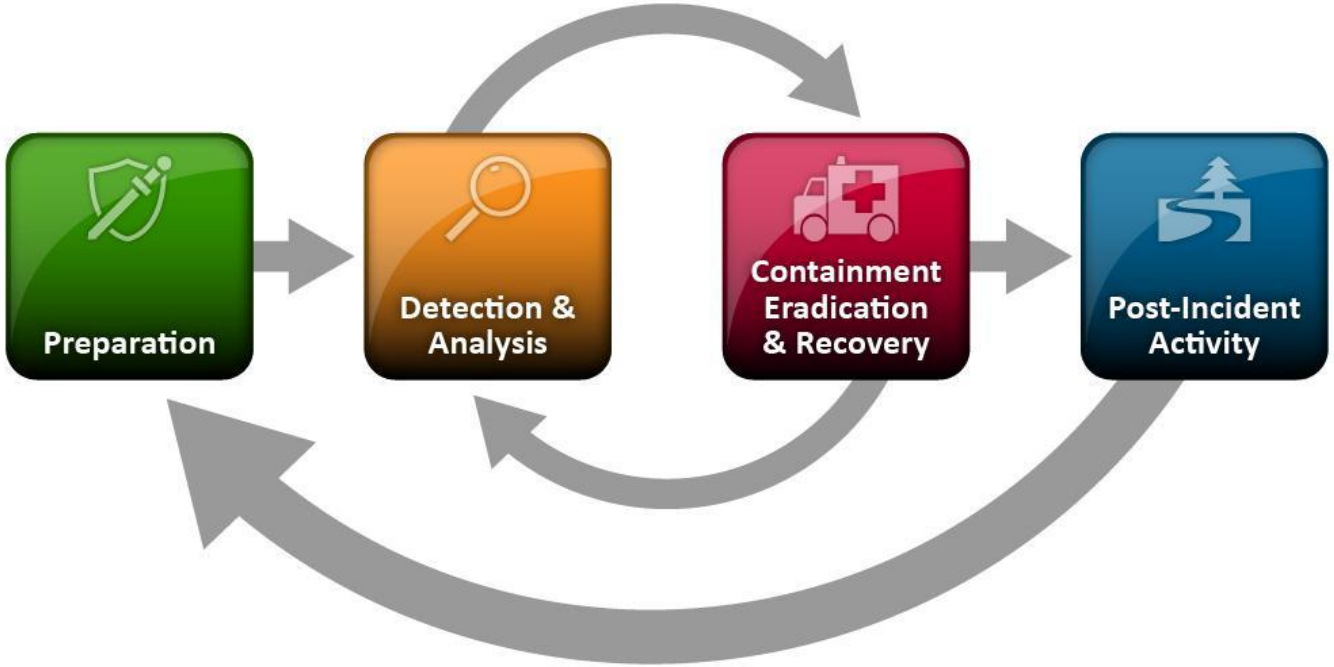
Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

The AI4CYBER Framework

- A framework of AI-driven cybersecurity tools to ensure a continuum of system protection against advanced cyberattacks, including AI-powered attacks
- AI4CYBER solution addresses the cybersecurity incident response process
  - Alignment with NIST 800-61



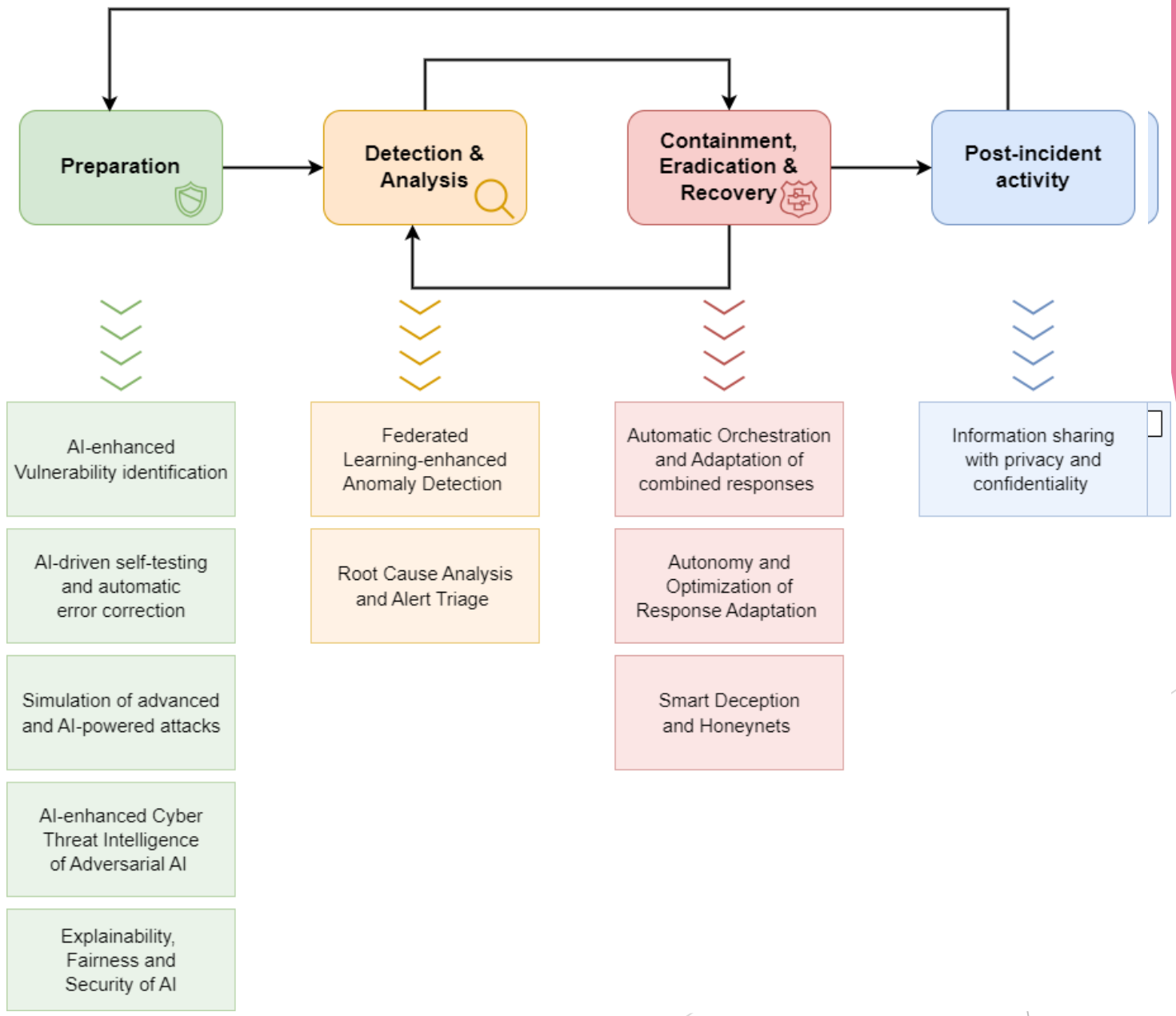
The incident response lifecycle defined in NIST SP 800-61

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 101070450.

The AI4CYBER Framework

- A framework of AI-driven cybersecurity tools to ensure a continuum of system protection against advanced cyberattacks, including AI-powered attacks
- AI4CYBER solution addresses the cybersecurity incident response process
  - Alignment with NIST 800-61

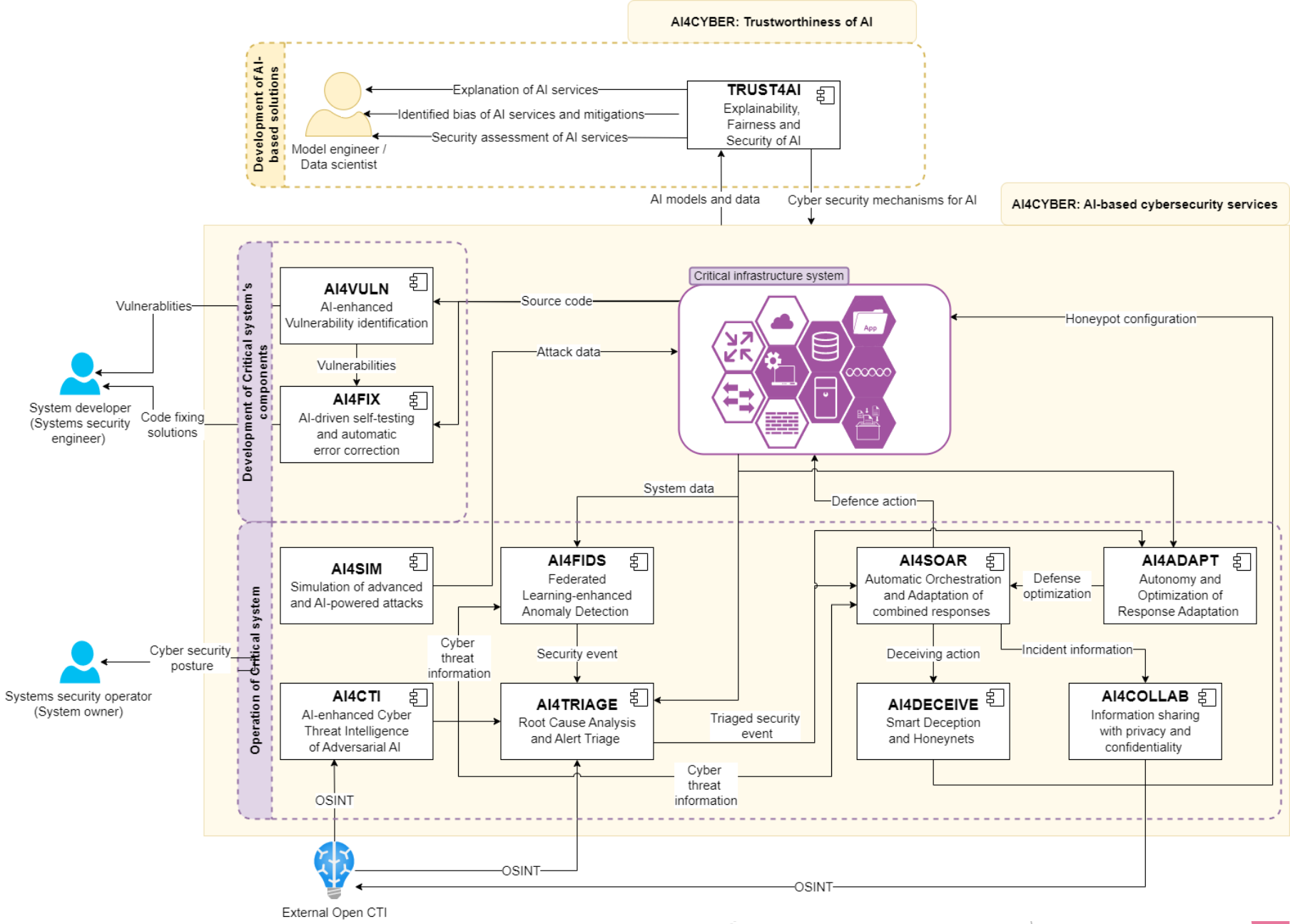


Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

The AI4CYBER Framework

- High-level architecture



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 101070450.

Implementation and demonstration

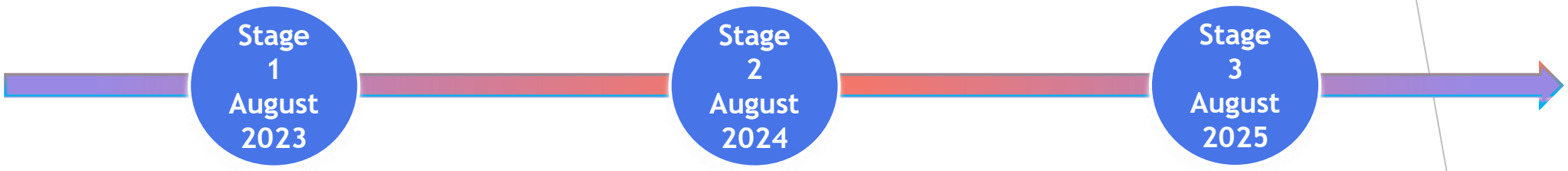
- Implementation of standalone innovative services that cover the different stages of cybersecurity
- Challenge on obtaining or generating datasets that include emerging advanced attacks.
- Realistic industrial use cases
  - Energy, banking and healthcare
- Datasets containing signatures and behaviours of advanced and AI-based attacks will be generated and released

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 101070450.

AI4CYBER Timeline

Project implementation
September 2022 – August 2025



Stage 1 - Design
Initial architecture of the AI4CYBER Framework

Stage 2 - First release
First release of the AI4CYBER Framework services and tools

Stage 3 - Final release
Final release of the AI4CYBER Framework services and tools

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 101070450.

Conclusions

- Achieving trustworthy AI systems has become one of the priorities at the European level
- AI4CYBER framework,
  - an ecosystem of cybersecurity services that use the potentiality of AI to support critical infrastructure owners on the management of the entire lifecycle of the response incident process
  - Ensure trustworthy AI (i.e. explainability, fairness and security of AI) is achieved within the AI systems
- Generation of cybersecurity-related datasets to promote the improvement of cybersecurity knowledge in the community

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 101070450.

AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

https://ai4cyber.eu

https://twitter.com/Ai4Cyber

https://www.linkedin.com/company/ai4cyber/

Angeliki Tsanta

EOS

angeliki.tsanta@eos-eu.com

Thank you for your attention!

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 101070450.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 101021981

APPRAISE

Facilitating public & private security operators to mitigate terrorism scenarios against soft targets

Anastasios (Tassos) Dimou - *CERTH*

Website | Twitter | Coordinator Contact Email

About us

Yana Lazarova

Project Coordinator
CS GROUP

Defense & Homeland Security
business unit
yana.lazarova@csgroup.eu

Helen Grantham

Communication and
Dissemination Lead

CENTRIC
Sheffield Hallam University
h.grantham@shu.ac.uk

Marco San Biagio

Technical Manager

Engineering Ingegneria
Informatica

Marco.SanBiagio@eng.it

Tassos Dimou

Scientific Manager

Visual Computing Lab
CERTH/ITI

dimou@iti.gr

ABOUT APPRAISE

APPRAISE aims to build on the latest advances in big data analysis, artificial intelligence, and advanced visualisation by creating a robust security framework that will improve both the cyber and physical security and safety of public spaces.

Why APPRAISE?

To create a framework improving the security and safety of public spaces while preserving the freedom of citizens, a challenge that faces all of society.

To protect soft targets from an evolving range of cyber and physical terrorist threats.

To provide an integrated security approach bringing together public and private security operators, before, during, and after an incident occurs.

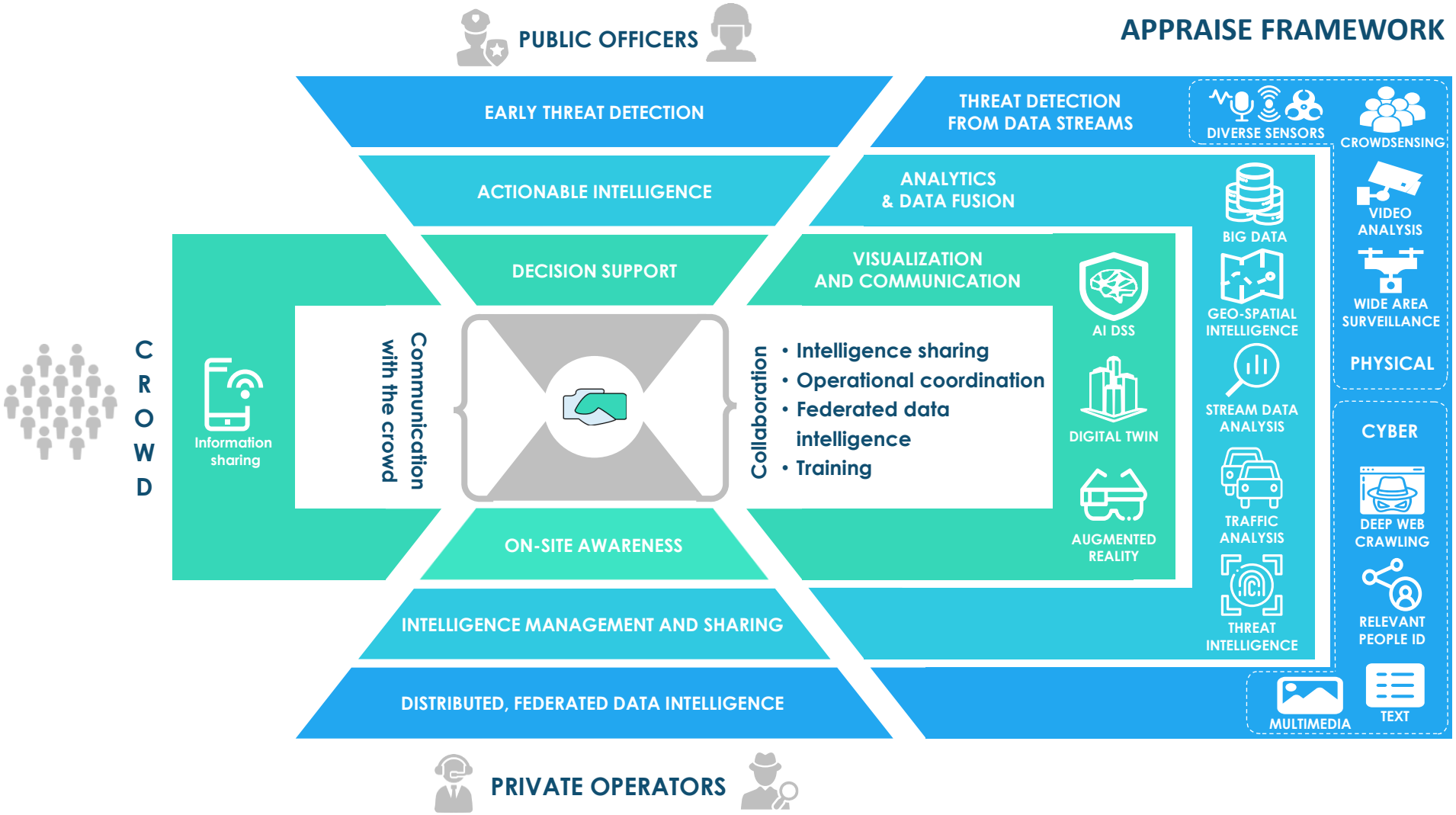
APPRAISE - key facts

- **Coordinator:** CS Group, France
- **Partners:** 27 organisations from 10 EU countries (5 LEAs)
- **Type:** Innovation Action
- **Budget:** €9.4million
- **SU-FCT03-2018-2019-2020:** Information and data stream management to fight against (cyber)crime and terrorism

Strategic goals

- Improve capacity to detect current and emerging cyber, physical threats in soft targets
- Improve active cooperation among public and private operators for the protection of soft targets
- Improve awareness, decision-making and operational performance of security practitioners
- Deliver a modular framework to integrate feeds and decision-support services
- Co-design socially accepted technologies with LEAs, technology and SELP experts

Overall concept



List of Tools (1)

Internet contents analysis
Monitoring of criminal intent through online textual content analysis
Detection of terrorist activity indications in multimedia content
Identification of relevant people and criminal groups from online contents
Context-based risk assessment of soft targets

Tools for real-time threats detection
Detection of threat-related objects and people from visual data
Video-based event and anomaly detection
Drone-based wide area mapping & surveillance
Relevant sound detection
CBRN & hostile UAV threat detection
Crowd sensing and human sensors
Real-time crowd dynamics analysis
Detection of cyber-attacks on surveillance system

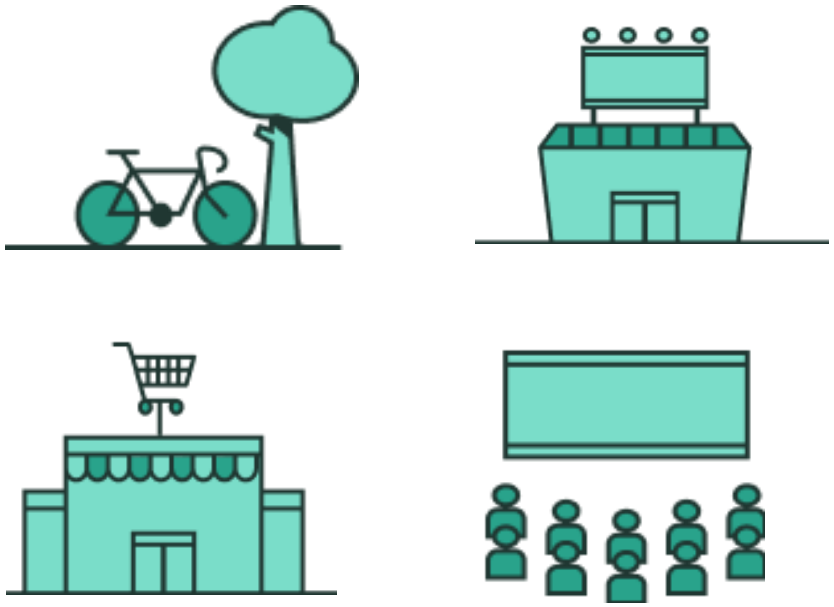
List of Tools (2)

Actionable intelligence for proactive security
Advanced stream data analytics for early warning
Mobility for situational awareness
Threat intelligence & real-time risk analysis
Event evolution prediction
Geo-spatial intelligence
Risk-based surveillance attention

Public-Private interoperability and collaboration services
Context information integration and harmonization
Cyber-secure context information and intelligence management and sharing
Tools for communication with the crowd
AR tools for on-site situational awareness and collaborative training
Distributed collaborative improvement of situational awareness tools

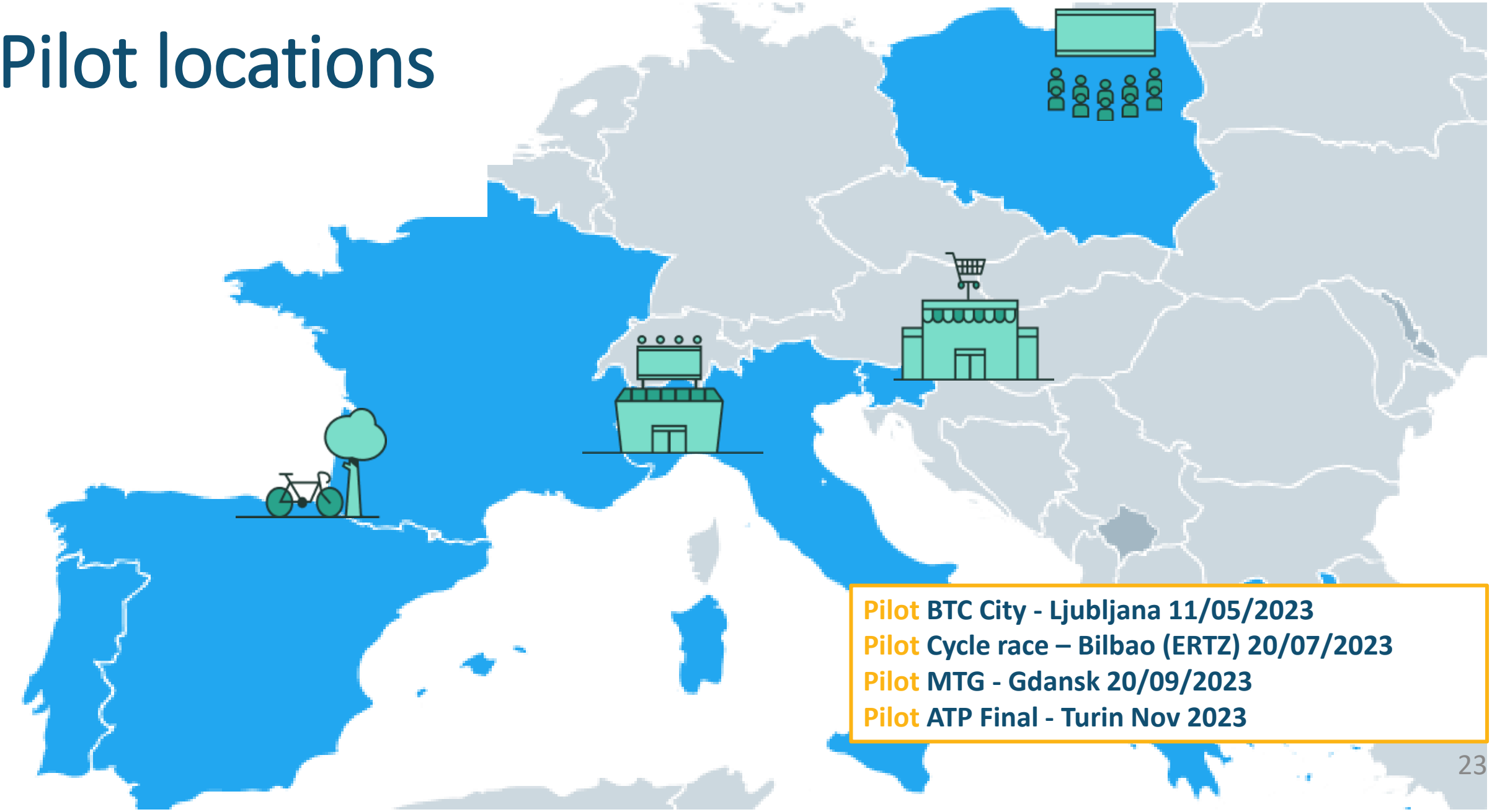
Visualization and DSS services
Intelligent Digital Twin-based Hypervision and Operation Management System (DITHO)
AI augmented decision support

APPRAISE pilots



- **No. of use cases:** 4
- **Lead partner:** ICSS
- **Accessibility:** from large scale outdoor to small scale indoor
- **Security measures:** mix of several public and private practitioners
- **Existing infrastructures:** information, surveillance systems, networks
- **Density:** from hundreds to thousands of people

Pilot locations



Pilot BTC City - Ljubljana 11/05/2023
Pilot Cycle race – Bilbao (ERTZ) 20/07/2023
Pilot MTG - Gdansk 20/09/2023
Pilot ATP Final - Turin Nov 2023

Shopping mall Ljubljana

End-user involvement

Pilot Ljubljana : APPRAISE Tools

USE CASE: ***A visitor takes out a handgun and starts shooting randomly, injuring people and causing panic. Due to the loud environment, visitors cannot recognize the sound of gunshot.***

Key Tools:

- **Dark web & Social media analysis**
- **Cyber-attack detection**
- **Crowd density**
- **Sound detection and localisation**
- **Communication and coordination (HoloLens)**

>35 Tools involved

Cross border cycling event Basque Country

End-user involvement

APPRAISE

START LINE

02

Lapurdi

afaorra

arrival

Zuberc

Gipuzkoa

departure

ra ba

Na

ONLINE

01

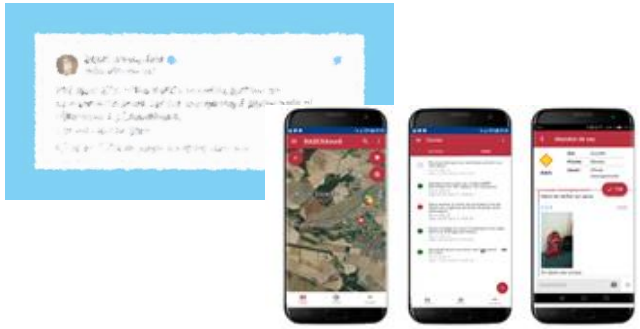
#threat tweets

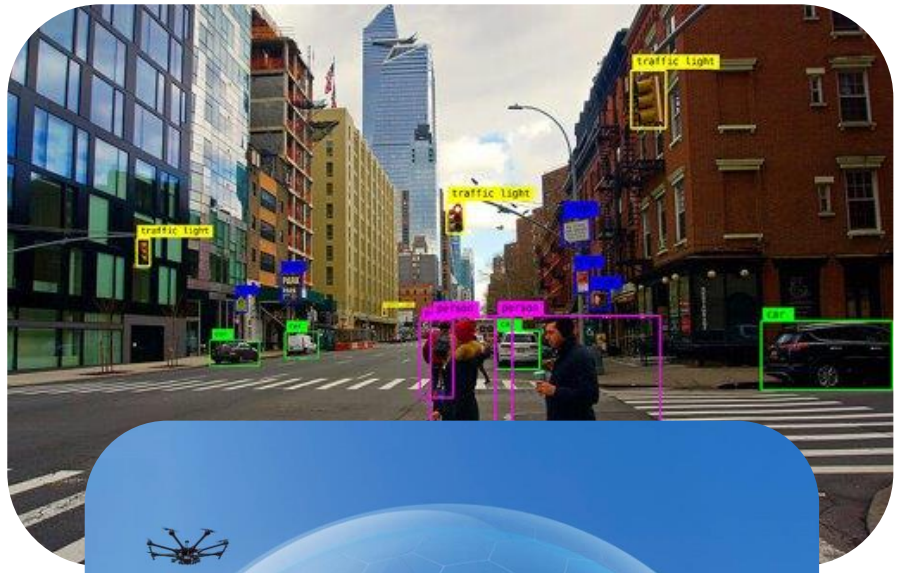
Pilot Bilbao: APPRAISE Tools

USE CASE: ***Online threat and terrorist attack with the intention of harming or killing those attending the event. Cross-border event with neutralization of the terrorist in France***

Key Tools:

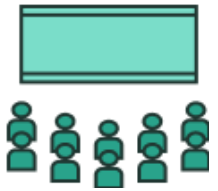
- Social network analysis
- Video analysis
- UAV Area surveillance
- UAV Detection
- UAV Neutralisation
- Unified GUI for all actions and sensors (DITHO)





>40 Tools involved

International fair Gdansk



End-user involvement

POLICJA

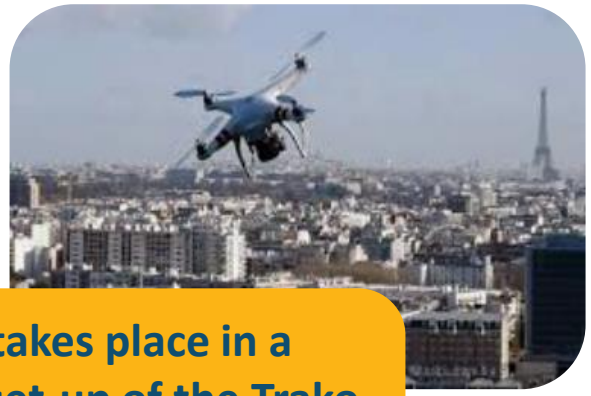
MTG

Pilot Gdansk: APPRAISE Tools

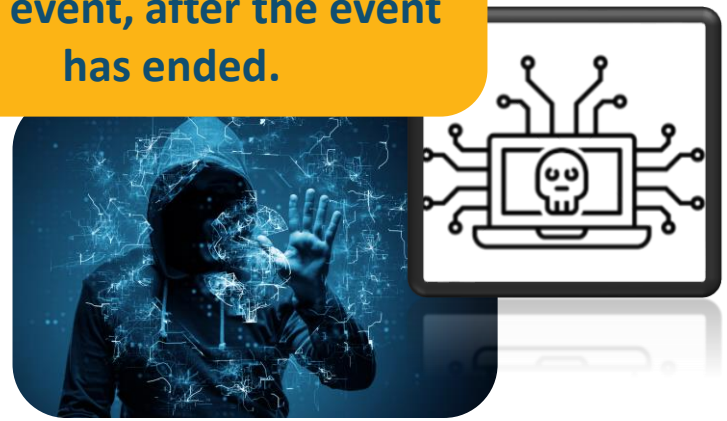
USE CASE: ***A person entering the AmberExpo with a cold weapon and attacking the fair attendants. The attack causes panic, which resulting in people getting crushed by the escaping fair participants.***

Key Tools:

- Cyber-security monitoring
- Area monitoring by drone
- Dangerous object detection
- Controlled evacuation (Crowd APP)



Pilot takes place in a realistic set-up of the Trako 2023 event, after the event has ended.



>35 Tools involved

APPRAISE

Kappa Futur Festival

Torino

End-user involvement

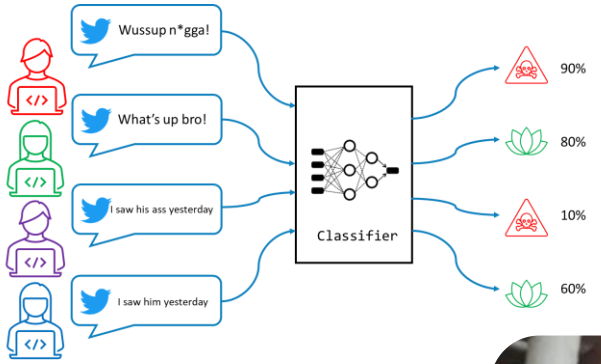
LOCAL POLICE OF TURIN

Pilot Turin: APPRAISE Tools

USE CASE: ***Online threat and vehicle-based terrorist attack with the intention of harming or killing those attending the event.***

Key Tools:

- **Social network analysis**
- **CCTV analysis**
- **Crowd sensing**
- **Investigative tool**
- **Communication and coordination**



>30 **Tools involved**

Partners


ES
GROUP


ICS
INSTITUTE FOR
CORPORATIVE
SECURITY STUDIES


ENGINEERING


inov
inesc • inovação


ALSE


MTG


ASTRIAL
REDEFINING COMMAND, CONTROL & INTELLIGENCE


POLISH PLATFORM
FOR HOMELAND SECURITY


alchera
TECHNOLOGIES


HOLO-LIGHT


POLICE
NATIONALE


Organizaciones ciclistas
euskadi


REPUBLIKA SLOVENIJA
POLICIJA


CERTH
CENTRE FOR
RESEARCH & TECHNOLOGY
HELLAS
iti
Information
Technologies
Institute


POLICJA


BTC


ERTZAINTZA


CENTRIC
Centre of Excellence in Terrorism,
Resilience, Intelligence and
Organised Crime Research


vicomtech
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE


iTTi


LINKS
ISMB


list
ceatech


ΕΛΙΑΜΕΠ
ELIAMEP
ΕΛΛΗΝΙΚΟ ΙΔΡΥΜΑ ΕΥΡΩΠΑΪΚΗΣ & ΕΞΩΤΕΡΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
HELLENIC FOUNDATION FOR EUROPEAN & FOREIGN POLICY


ethics


aitek


POLÍCIA
SEGURANÇA PÚBLICA


LOCAL POLICE OF TURIN

Join the APPRAISE community.

APPRAISE encourages a wide range of stakeholders to join its community, email us at appraise-h2020@csgroup.eu and get involved!

APPRAISE

APPRAISE

Facilitating public & private security operators to mitigate terrorism scenarios against soft targets

Questions?

appraise-h2020.eu

@appraise_h2020

appraise-project

website| twitter| email

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 101021981

ATLANTIS

Improved resilience of Critical Infrastructures
Against large scale transnational and systemic risks

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

EU-CIP Annual Conference – *20th September 2023*

ATLANTIS Identity Card

- **WHO**: **37 partners** from **10 countries (+ 8 indirectly associated)**
- **WHAT: EC HE Grant** under the call CL3-2021-INFRA-01
- **WHEN:** 1 October 2022 → 30 September 2025 (36 months)
- **WHY:** In response to topic: CL3-2021-INFRA-01-01 *"European infrastructures and their autonomy safeguarded against systemic risks"*

Mission: improve the resilience and the protection capabilities of interconnected ECI exposed to **evolving systemic risks due to existing and emerging large-scale, combined, cyber-physical threats and hazards**, guarantee the continuity of operations, while minimizing cascading effects by adopting sustainable security solutions.

HOW: HORIZON Innovation Action

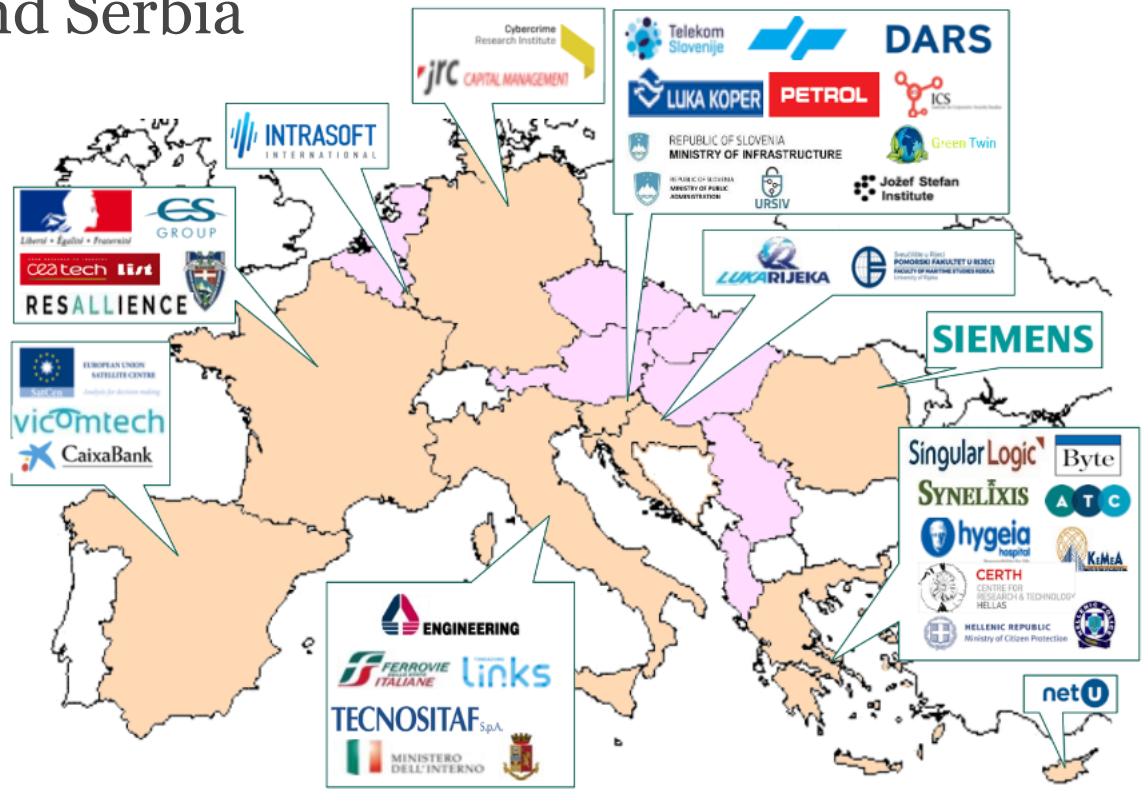
- Budget: **€ 12,728,564.50**
- Funding: **€ 9,998,535**

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

ATLANTIS Coverage #1

Geographical Coverage

- **Central:** Italy, France, Belgium, Germany, Luxemburg, Austria, Netherlands
- **Southern-East:** Greece, Cyprus, Romania, Slovenia, Croatia, Albania, Slovakia, Hungary, Czech and Serbia
- **Southern-West:** Spain



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

ATLANTIS Coverage #2

Value Chain Coverage

- **CI operators and CI end-users** in various sectors (**12**): Luka Koper (International Port), Luka Rijeka (International Port), DARS (Slovenia Highways Operator), Slovenske Zeleznice (Slovenian National Railways), Petrol (Slovenian Energy Company), Ferrovie dello Stato Technology (Italian Railways IT company), JRC Capital Management (Brokerage & Investment House), CAIXA Bank, Hygeia (Group of Hospitals in Greece and links with Albania), TECNOSITAF S.p.A. (Tunnel Operator/Italian side), Service Départemental d'Incendie et de Secours de la Savoie (Tunnel Rescue), Telecom Slovenia.
- **CIP/CIR solution/technology providers (6):** ENGINEERING, CS Group, NetCompany, SingularLogic, Siemens, Resallience Climatique
- **Research institutes (9):** KEMEA, ICS, SatCen, JSI, University of Rijeka, CEA, CERTH, LINKS Foundation, VICOMTECH
- **Innovative high-tech SME** with security expertise (**6**): Synelixis, NetU, BYTE Computers, Athens Technology Center, Cybercrime Research Institute, SNEP.
- **Security government entities (4):** MZI (Slovenian Ministry for Infrastructure), UIV (Slovenian Ministry of Information Security), Italian Ministry of Interior (Road, Rail and Communications Security), HPL (Hellenic Police).

research and innovation programme under the grant agreement No 101073909.

ATLANTIS Motivations

- EU Security Union Strategy for the period 2020-2025 identifies the protection of CI as one of the main **priorities** for the EU and its Member States.
  - Digital and interconnected CIs are based on novel and sophisticated technologies which generate potential **new vulnerabilities**, either accidental or intentional.
  - Networked CIs might cause **long-lasting cascading effects** in other **multi-sector and cross-border** CIs
  - CIs increasingly appear as potential new targets for **new threats and attacks**, especially the hybrid ones (e.g. cyber-physical), operating in a **rapidly evolving** societal, technological and business environment
  - Limited research on **large scale, transnational and cross-domain coordinated attacks**, especially at a **systemic level**

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

ATLANTIS Threat Landscape

- Attack surface and the impact of attacks can escalate rapidly and negatively affect other CIs and wider parts of vital societal functions
  - **Cyber-physical** and **coordinated** (among different actors, even in different countries), **mixed** (using different tactics), **disruptive** (leading to the collapse of entire systems, sectors or regions), **unexpected**, **subversive**, and **difficult to identify** early
  - Major **natural hazards** (e.g. floods, wildfires, often unexpected and unpredictable) are also big concerns that can create disruption to ECI, thus affecting wider functions of our society.
- Understand and analyse the system as a **complex network of individual and institutional actors** with different and often conflicting interests

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

ATLANTIS Strategic Challenge and Mission

ATLANTIS aims at ***enhancing resilience and Cyber-Physical-Human (CPH) security of the key ECI***, 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 functions of the society.

The mission of ATLANTIS is to ***improve the resilience*** and the protection capabilities of ***interconnected ECI exposed to evolving systemic risks*** due to existing and emerging large-scale, combined, cyber-physical threats and hazards, ***guarantee the continuity of operations***, while ***minimizing cascading effects*** in the infrastructure itself, the environment, other CIs, and the involved population, enabling public and private actors to meet current and emerging challenges by adopting sustainable security solutions.

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

ATLANTIS Approach

- **Raise the level of complexity**:
  - Risks, attacks
  - Organisations
  - technologies (including misuse)
  - Cross-CI, cross-domain, cross-border, interdependencies
  - Large scale
  - Systemic-level
- **Leveraging on** previous experiences on CIP projects and solutions
- Cross-CI and cross-border require **sovereignty**

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

ATLANTIS Security Strategic Goals

1. **AWARENESS. Improve knowledge on large-scale**, vulnerability assessment and long-term systemic risks

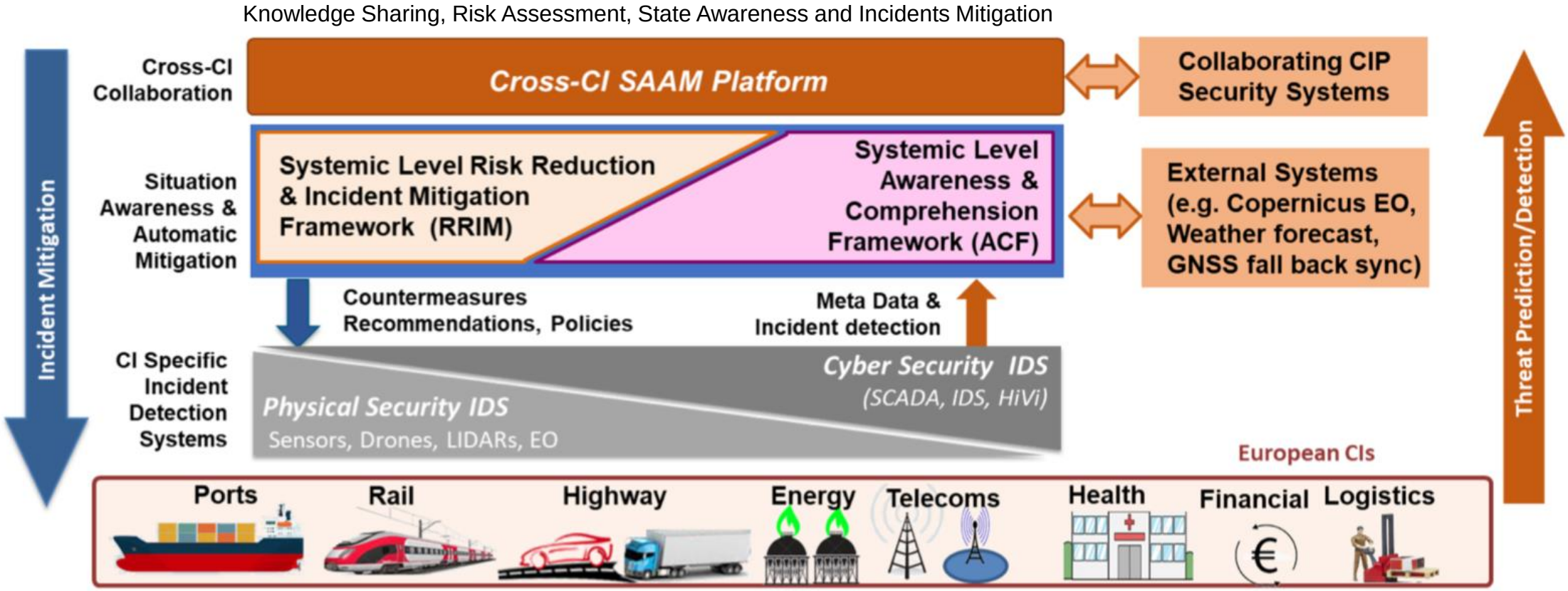
2. **CAPABILITY. Improve the systemic resilience of ECI**, through novel, adaptive, flexible, and customizable security measures ("by design") and tools ("by innovation")

3. **COOPERATION. Effective cooperation** among CI operators and government security stakeholders, while preserving CI autonomy and sovereignty

4. **TECHNOLOGY. Deliver an open technological framework** that will provide the ECIs with AI-based solutions for increased AWARENESS, CAPABILITY, and COOPERATION in managing systemic threats

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

ATLANTIS 3-Layer high-level architecture



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

VALIDATION in Large Scale Pilots – LPS#1

Cross-Border/Cross Domain Large Scale Pilot in Transport, Energy and Telecoms
(Slovenia, Croatia, Italy and France)

1. Luka Koper (LUK)
2. Petrol (PET)
3. Slovenian Railways (SZ)
4. Slovenian Motorways (DARS)
5. Telekom Slovenia (TS)
6. Port of Rijeka (LUR)
7. Italian Railways (FST)
8. Fréjus Road Tunnel (SITAF and SDIS73)
9. French Ministry of Interior
10. Italian Ministry of Interior
11. Slovenian Ministry of Infra
12. Slovenian National SO

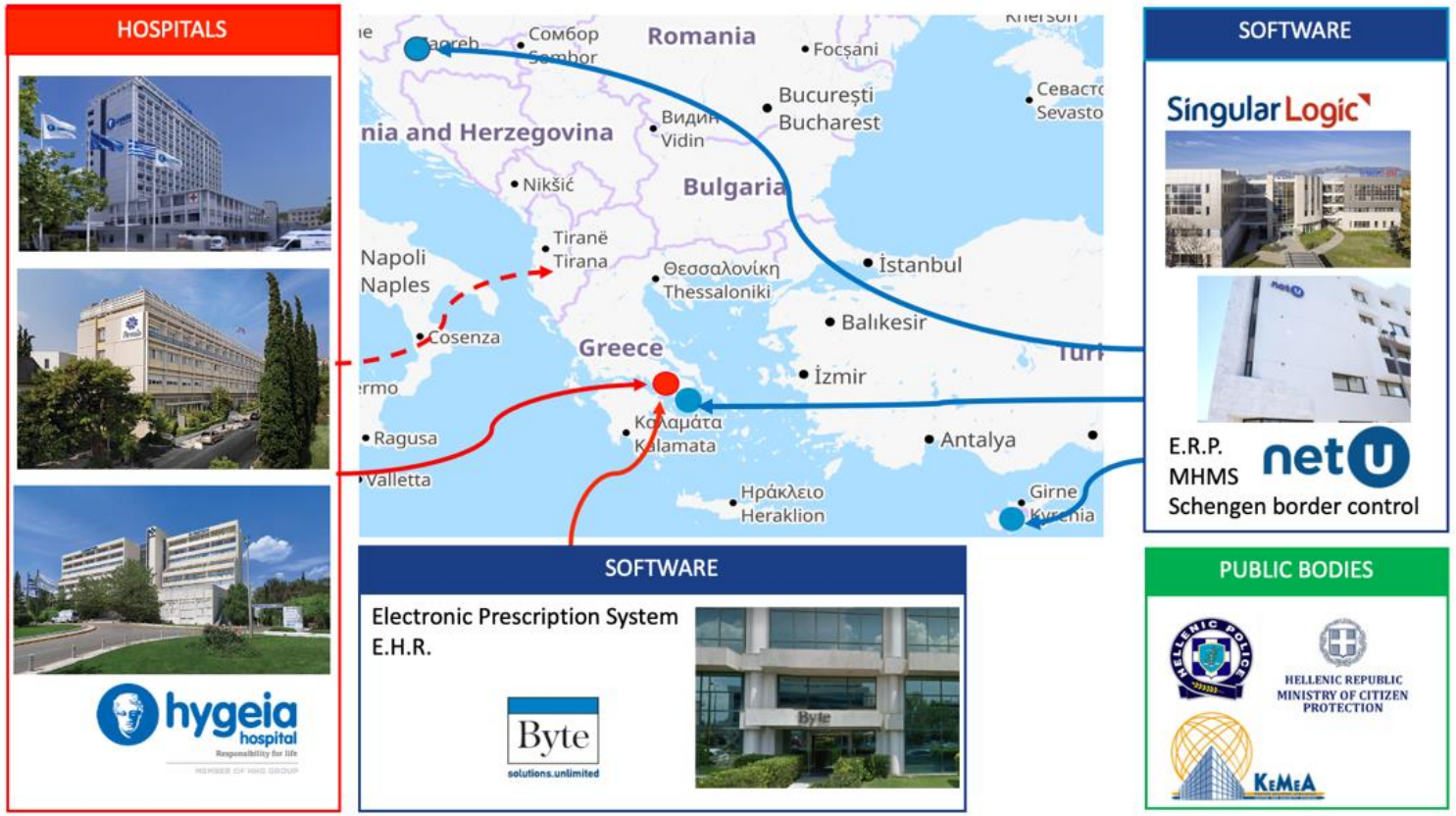
Threats: cyber-attack, terrorist attack (explosion, drones), fire (in the tunnel), natural hazards, aging, supply chain disruption

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

VALIDATION in Large Scale Pilots – LPS#2

Cross Domain Large Scale Pilot in Health, Logistics/Supply Chain and Border control
(Greece, Cyprus, Croatia, Albania)

1. **Hygeia Group (HYG)**
2. **Byte (E.H.R. in Greece)**
3. **Singular Logic (E.R.P. system provider in Greece)**
4. **NetU (Schengen II Information System for border control of Cyprus, Greece and Croatia)**



Threats: cyber-attack (including sensitive date breaches), terrorist attack (with chemical or virus spreading)

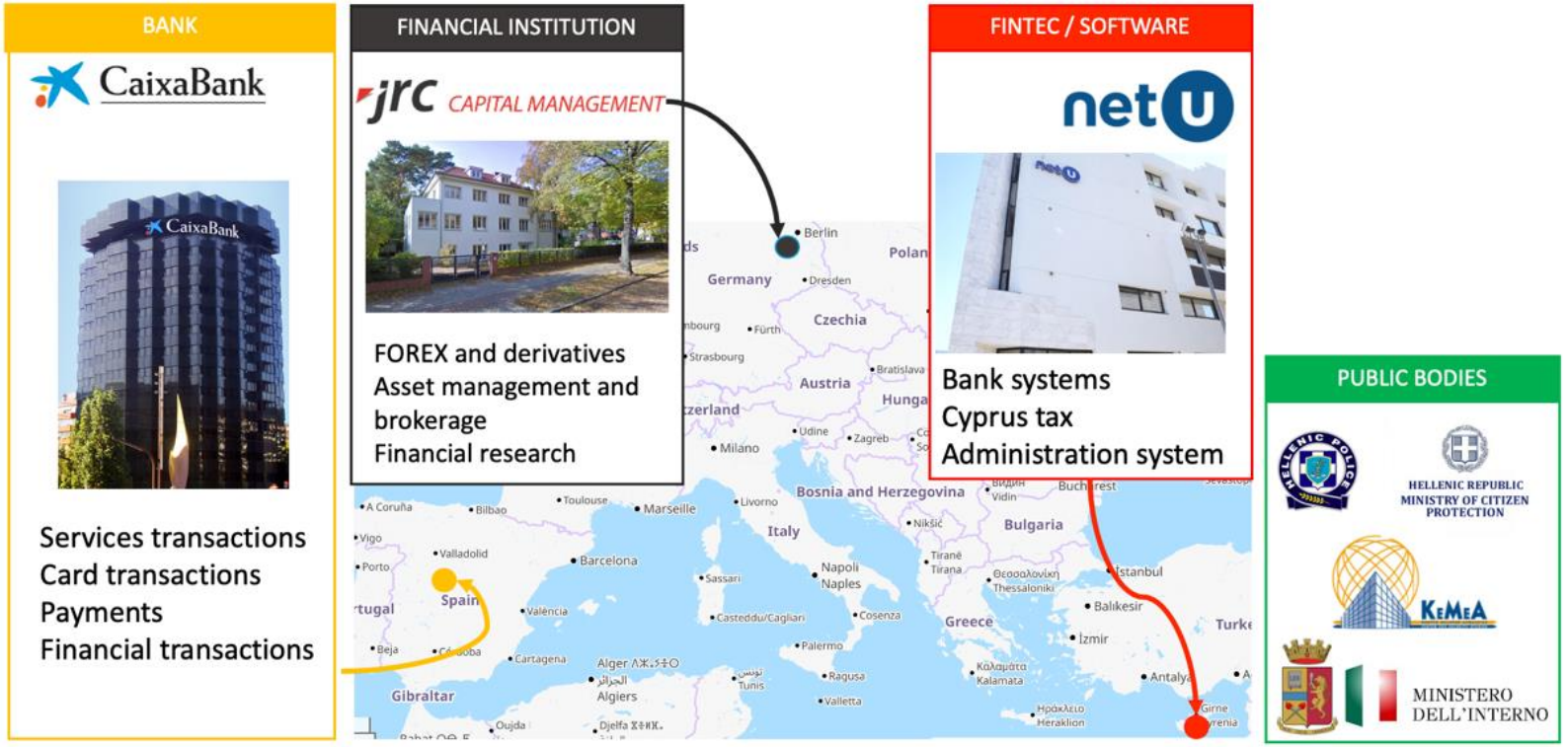
This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

VALIDATION in Large Scale Pilots – LPS#3

Cross Domain Large Scale Pilot in FinTech/Financial

(Spain, Germany and Cyprus)

1. CaixaBank (CXB)
2. JRC Capital Management (JRC)
3. NetU (Integrated Tax Administration System for Cyprus)



Threats: cyber-attack (to financial transactions, card transactions or payment system APIs, distributed denial of service (DDoS) and personal/sensitive data breaches); disinformation

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

Achievements after 12 months #1

- **List of vulnerabilities** and Cyber-Physical-Human Risk Assessment per LSP.
- **Use case definition and analysis** of CPH threats in critical infrastructures.
- **Design of inter-DLT** adapters to enable information sharing between different Blockchain technologies. Cosmos and Ethereum V2.0 are two Blockchain platforms that will be used in the project.
- **Systematic methodology** that combines remote sensing data (including satellite imagery), artificial intelligence, and geospatial analysis techniques to be integrated in the existing disaster risk management (DRM) systems and frameworks.
- **First specification of the comprehensive architecture** of the ATLANTIS secure and reliable framework

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

Achievements after 12 months #2

- **ATLANTIS Data Management Plan**, including Data Lifecycle and Procedures, Data Security and Protection, Legal and Ethical aspects
- **First meeting with Advisory Board members** to collect feedback on how to improve relevant markets, standards, policies.
- Participation at **Defence Exhibition Athens** (May 9-11), **Corporate Security Days** (May 22-23), **RISE-SD 2023 Conference** (May 29-31), **Project2Policy EC Seminar** (June 14-15). Other events are coming soon.

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

ATLANTIS

Thank You!

For info, please contact
Gabriele Giunta
ATLANTIS Project Coordinator
gabriele.giunta@eng.it

DYNABIC Project summary

EU-CIP/ECSCI 1st Annual Conference & PRAETORIAN Final Event, 20 September 2023.

Ioan Constantin, ORANGE Romania

DYNABIC

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 101070455.

DYNABIC

Dynamic Business Continuity and Response of Critical Systems against advanced cyber-physical threats

- **Project Coordinator:** Tecnalia
- **Consortium:** 16 partners
- **Budget:** € 4,999,695
- **Project Type:** RIA
- **Grant Agreement No.:** 101070455
- **Start Date:** 01/12/2022
- **Duration:** 3 years

DYNABIC

Overall Objective

> *"**Increase** the **resilience and business continuity** capabilities of European **critical services** in the face of **advanced cyber-physical threats**."*

The focus is on **cyber-physical threats** that may cause **business disruption** or underperformance **risks**, including the assessment of their **cascading effects** on **interconnected critical infrastructures**.

DYNABIC

Main contributions

- The **DYNABIC Framework** to predict, quantitatively assess and mitigate in real-time business continuity risks and their potential cascading effects.

- By enabling the **dynamic autonomous adaptation** of critical infrastructures to **meet Resilience goals** by the automatic optimization and orchestration of response strategies.

DYNABIC

Detailed objectives

Objective 1: Deliver the **DYNABIC Framework** for ensuring **increased resilience** of critical systems, while assuring the **continuity** of business and operations.

Objective 2: Enable Operators of Essential Services to Predict, Quantitatively Assess and Mitigate Real-time **Business Continuity Risks** and **cascading effects**.

Objective 3: Enable **Disaster Preparedness** in Critical Infrastructures and improve **the Prevention** of business continuity risks **cross-organisation** and **cross-domain**.

Objective 4: Enable the **Dynamic Autonomous Adaptation** of critical infrastructures to meet Resilience goals

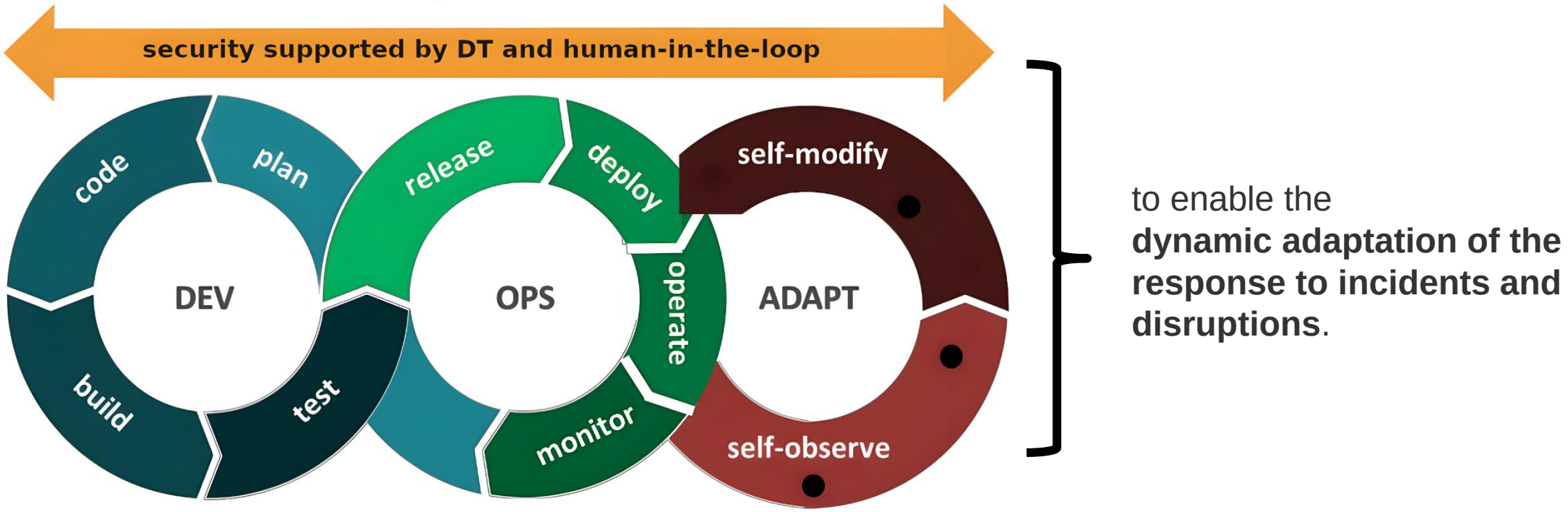
Objective 5: Facilitate the **Coordinated vulnerability and threat information sharing** across the EU and Enable CI operators meeting the EU NIS Directive 2.

Objective 6: **Demonstration** of the DYNABIC Framework integrated into critical services use cases relevant for Europe.

DYNABIC

DYNABIC Approach

- Business continuity risk management in critical infrastructures, based on **SecDevOpsAdapt cycle**.



to enable the
dynamic adaptation of the response to incidents and disruptions.

Figure 1: DYNABIC SecDevOpsAdapt cycle for Resilient systems

DYNABIC

The DYNABIC Framework

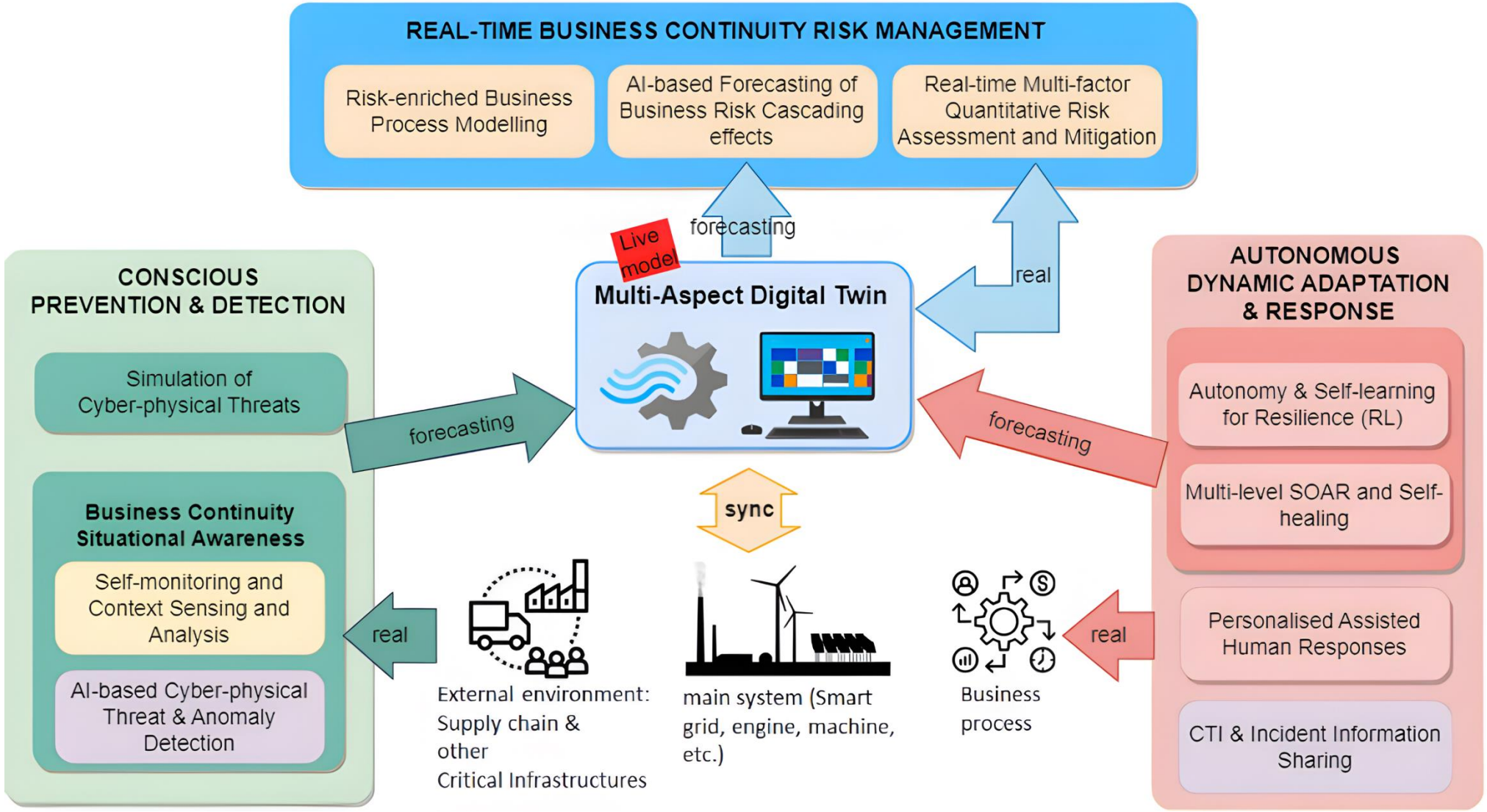


Figure 2: The DYNABIC Framework components

DYNABIC

The DYNABIC MADT

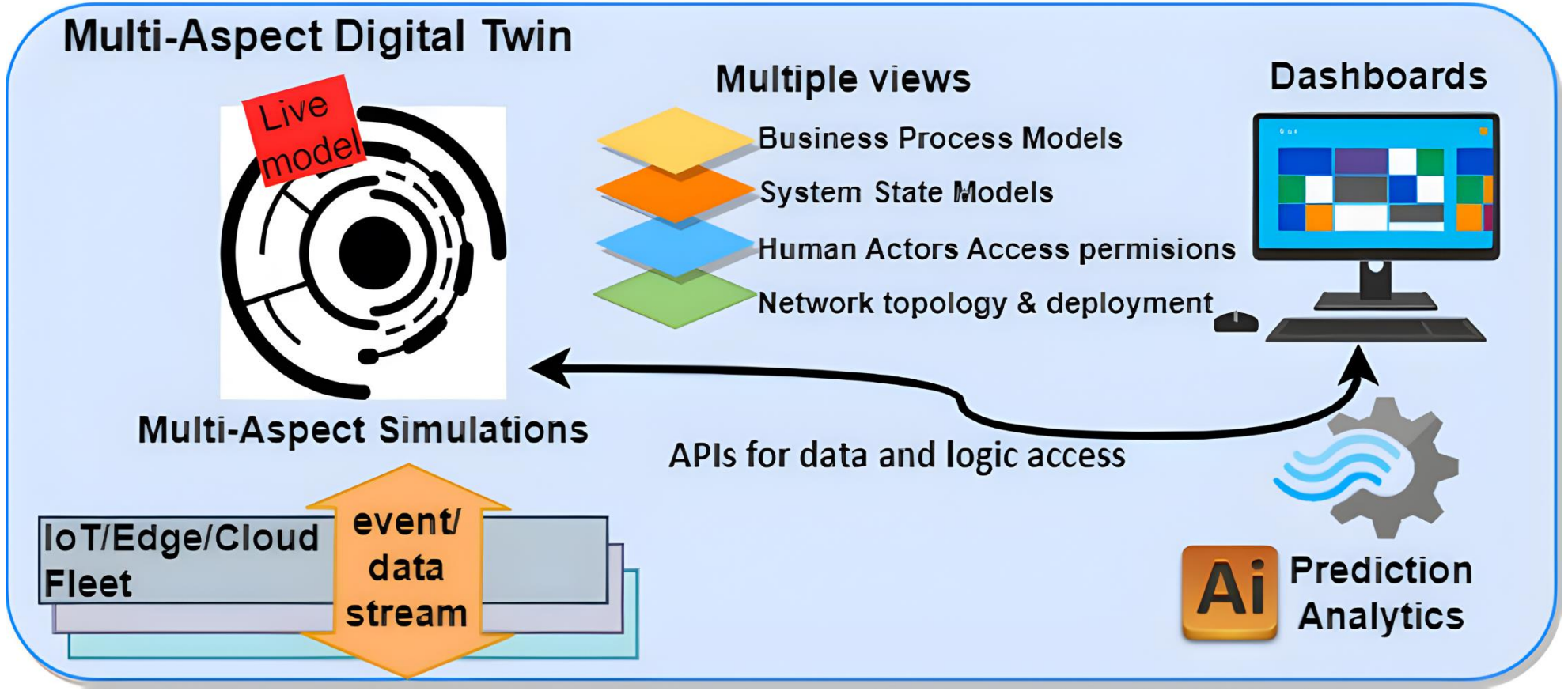
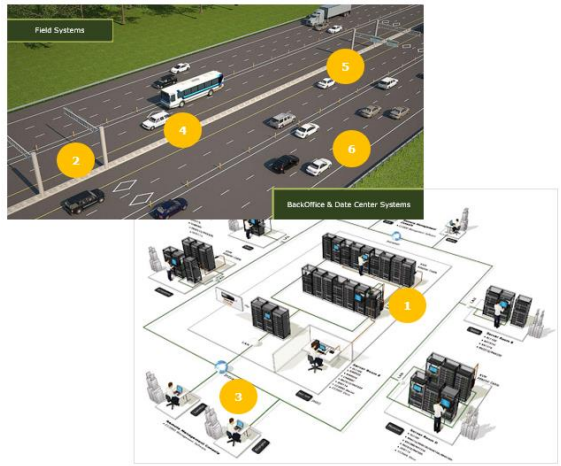


Figure 3: DYNABIC Multi-Aspect Digital Twin concept

DYNABIC

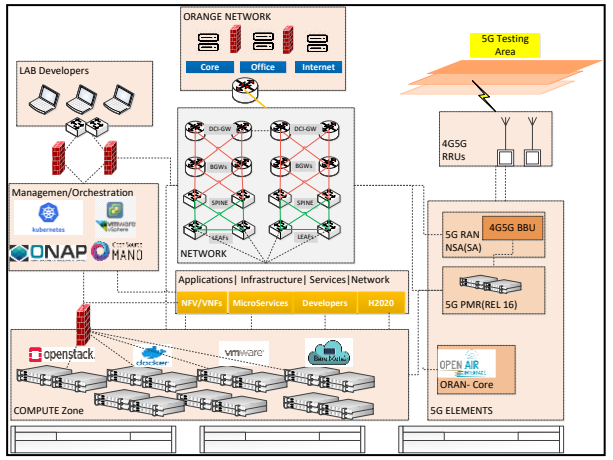
Use cases

- Smart **Preparedness**, **Prevention** and **Response** to Business disruption risks in 4 critical infrastructures and supply chains

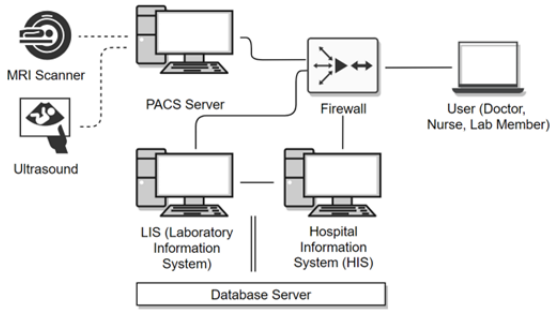


Transport services

EV charging station



5G Telcommunications

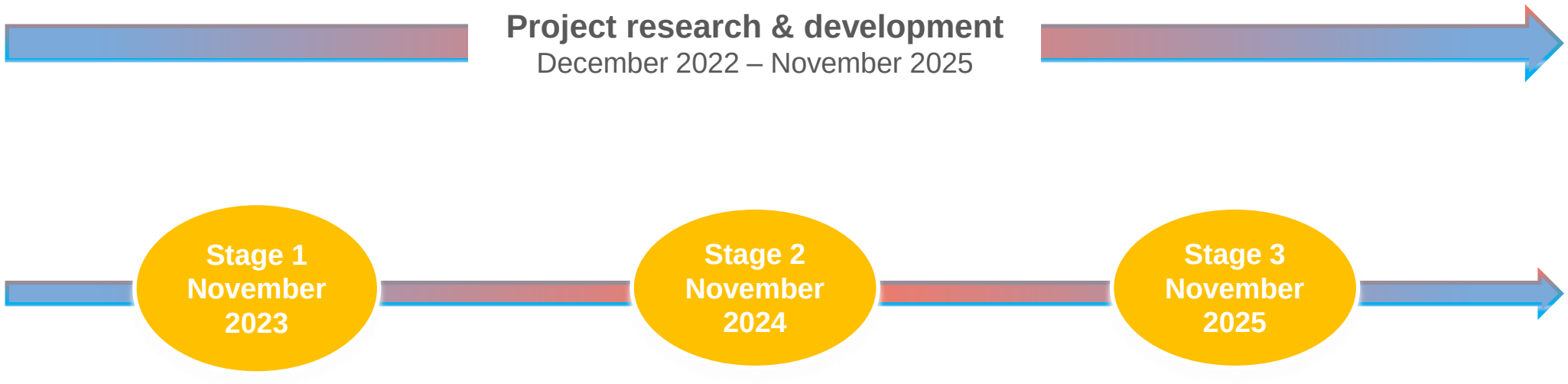


Healthcare

Cascading effects in Interconnected CI

DYNABIC

The DYNABIC Timeline



Stage 1 - Design
Initial architecture of the DYNABIC Framework solution

Stage 2 – First release
First release of the DYNABIC Framework services and tools

Stage 3 – Final release
Final release of the DYNABIC Framework services and tools

DYNABIC

Thank you for your attention!!

Website: https://dynabic.eu

Follow us on Twitter: @dynabic_eu

Contact: Erkuden.Rios@tecnalia.com & Eider.Iturbe@tecnalia.co

DYNABIC

EU-CIP

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection

& EUROPEAN CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES (ECSCI)

Coffee Break
We will return at 15.00

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.