Empowering a Pan-European Network to Counter Hybrid Threats

Hybrid threats and Critical Infrastructure Protection

Dr. Päivi Mattila/ Laurea, EU-HYBNET Coordinator

20/9/2023

EU-CIP Project & ECSCI Cluster 1st Annual Conference on CI Resilience

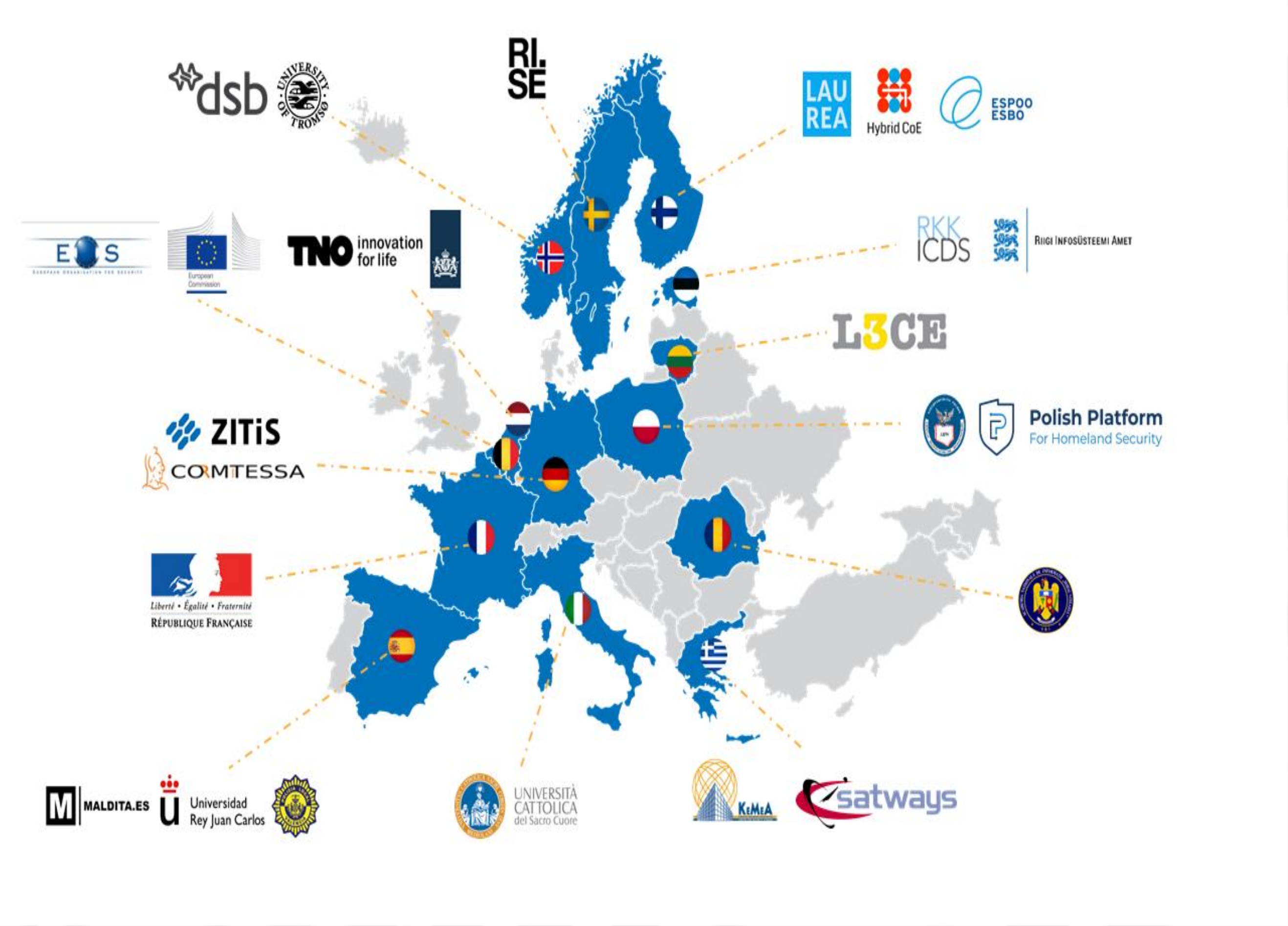
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Project in Nutshell

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

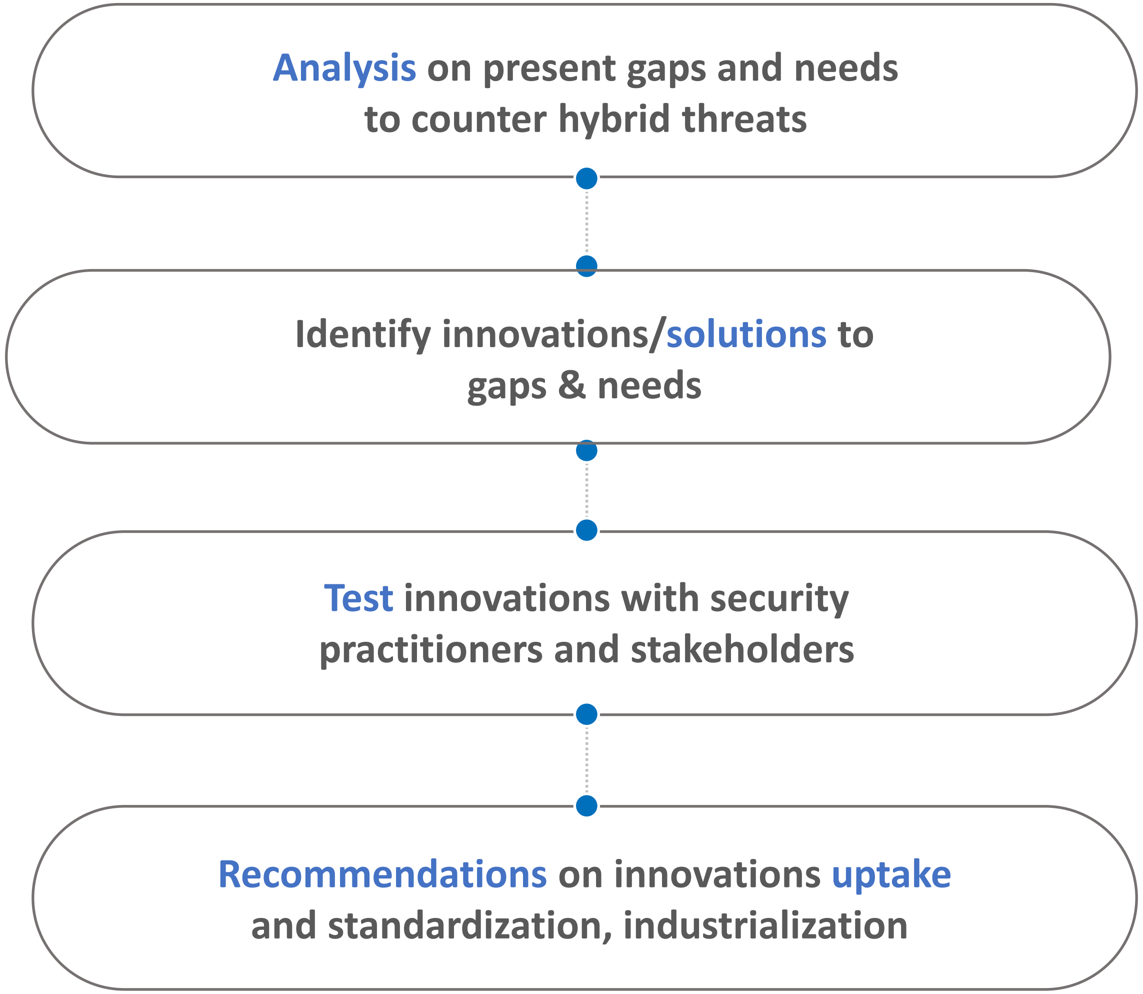
General information

- Consortium 25 partners/ 13 EU MS & Norway
- c.120 pan-European Network members
- Duration 2020-2025
- Network of Security Practitioners –Project, CSA
- 3.500.000 €



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Core Activities of EU-HYBNET



Analysis on present gaps and needs to counter hybrid threats

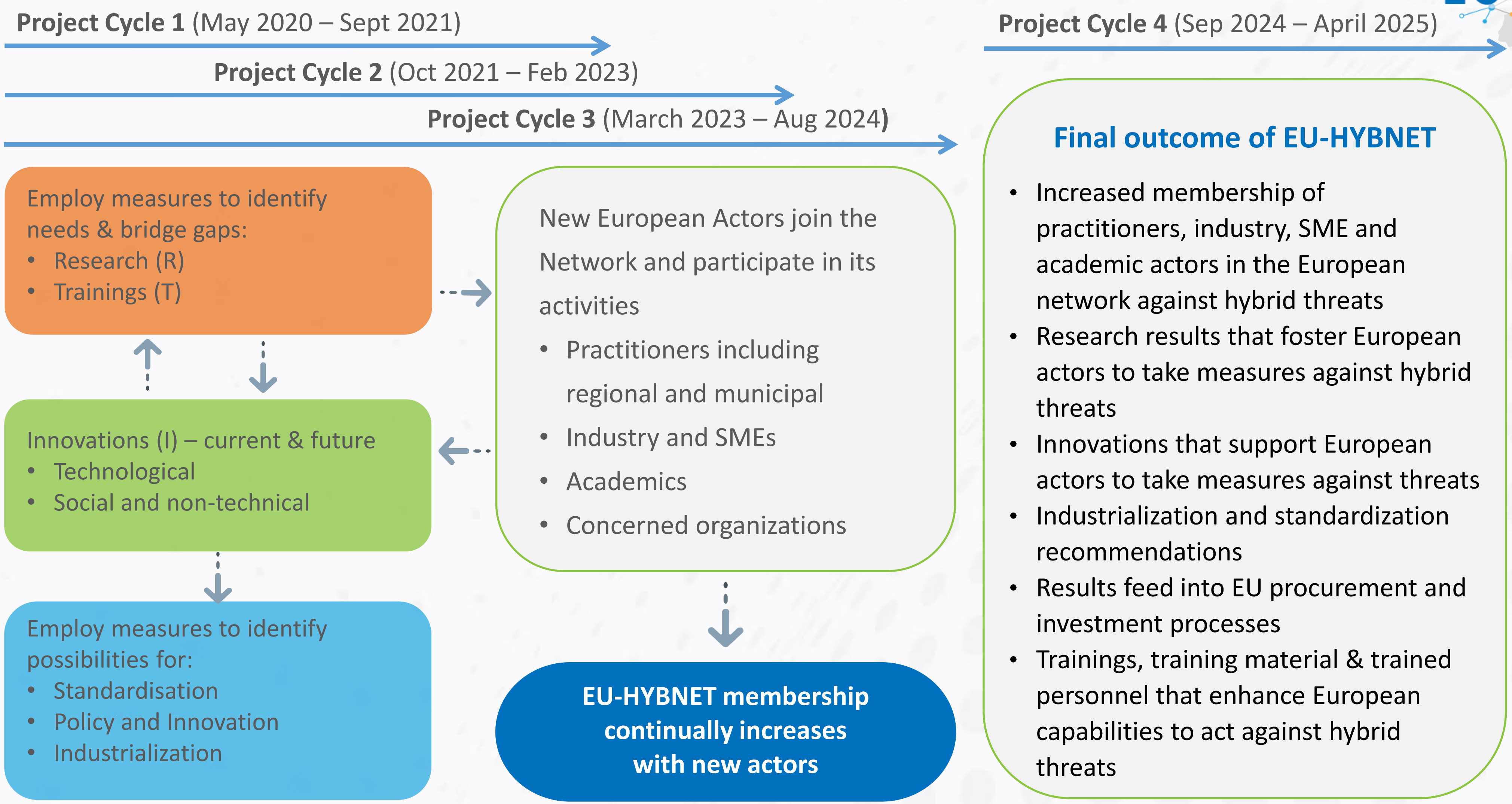
Identify innovations/**solutions** to gaps & needs

Test innovations with security practitioners and stakeholders

Recommendations on innovations **uptake** and standardization, industrialization

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET structure – process and content



Project Cycle 1 (May 2020 – Sept 2021)

Project Cycle 2 (Oct 2021 – Feb 2023)

Project Cycle 3 (March 2023 – Aug 2024**)**

Project Cycle 4 (Sep 2024 – April 2025)

Employ measures to identify needs & bridge gaps:

- Research (R)
- Trainings (T)

Innovations (I) – current & future

- Technological
- Social and non-technical

Employ measures to identify possibilities for:

- Standardisation
- Policy and Innovation
- Industrialization

New European Actors join the Network and participate in its activities

- Practitioners including regional and municipal
- Industry and SMEs
- Academics
- Concerned organizations

EU-HYBNET membership continually increases with new actors

Final outcome of EU-HYBNET

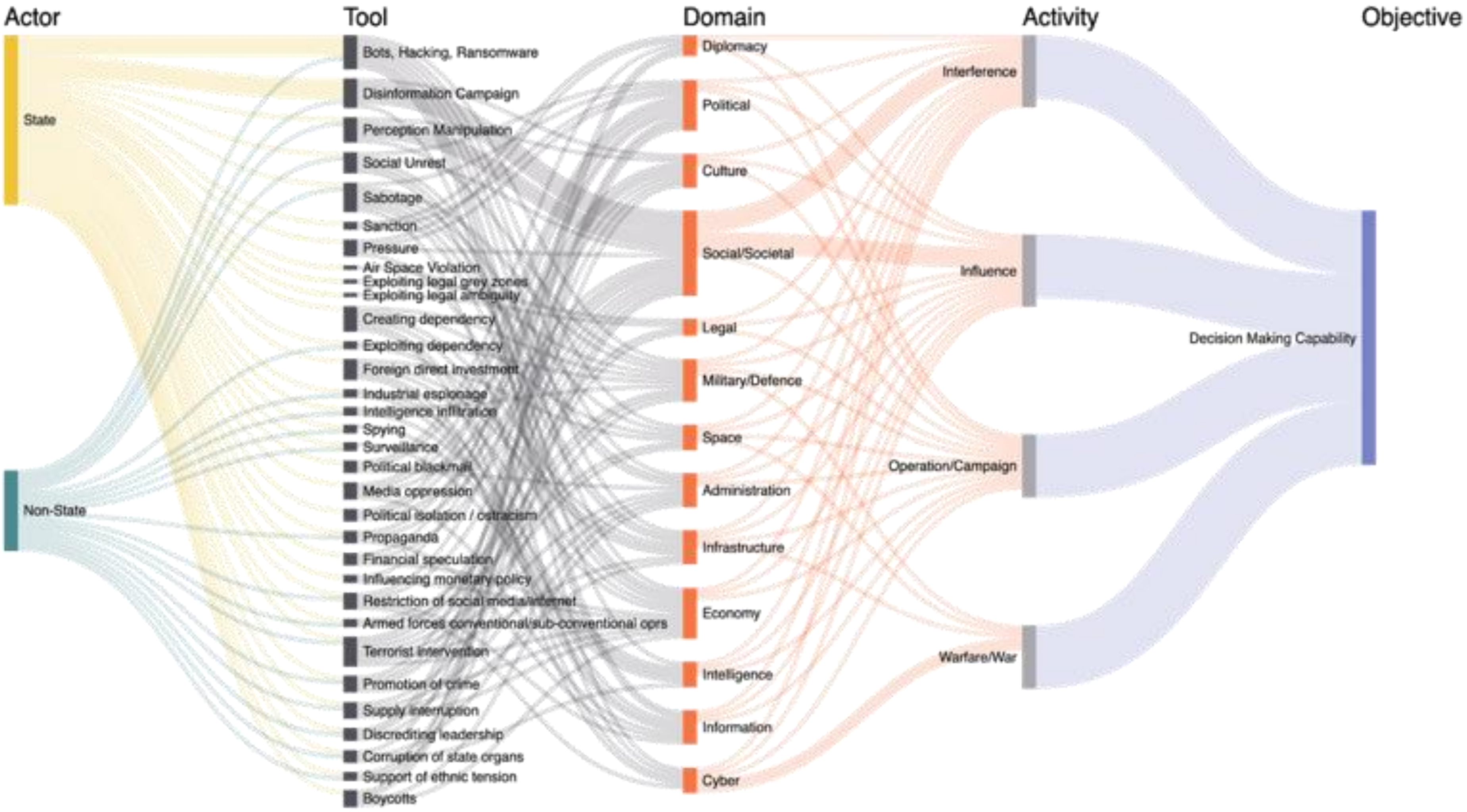
- Increased membership of practitioners, industry, SME and academic actors in the European network against hybrid threats
- Research results that foster European actors to take measures against hybrid threats
- Innovations that support European actors to take measures against threats
- Industrialization and standardization recommendations
- Results feed into EU procurement and investment processes
- Trainings, training material & trained personnel that enhance European capabilities to act against hybrid threats

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Definitions and Approaches

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

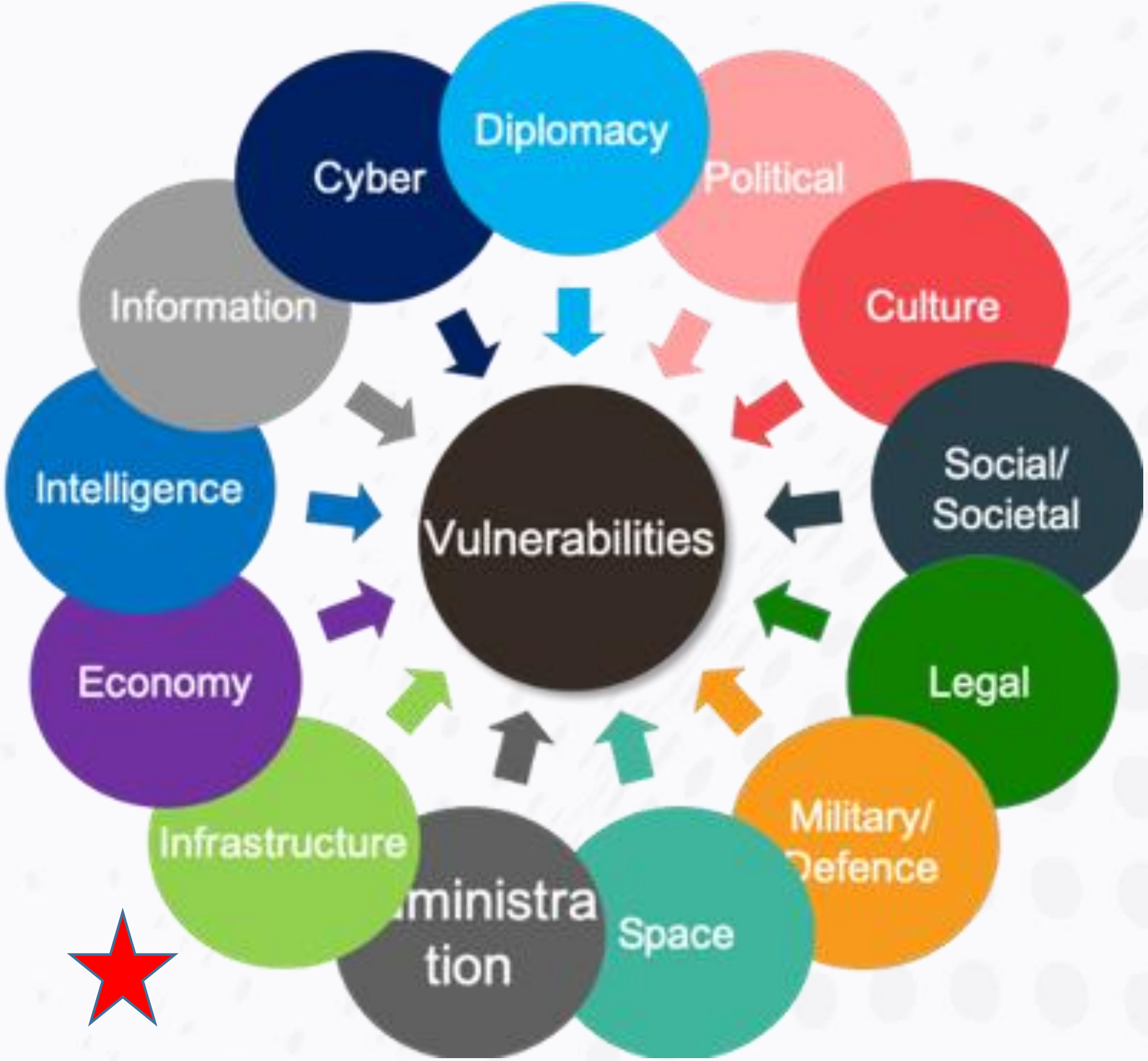
The Conceptual Model to Characterise Hybrid Threats



Conceptual Model: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

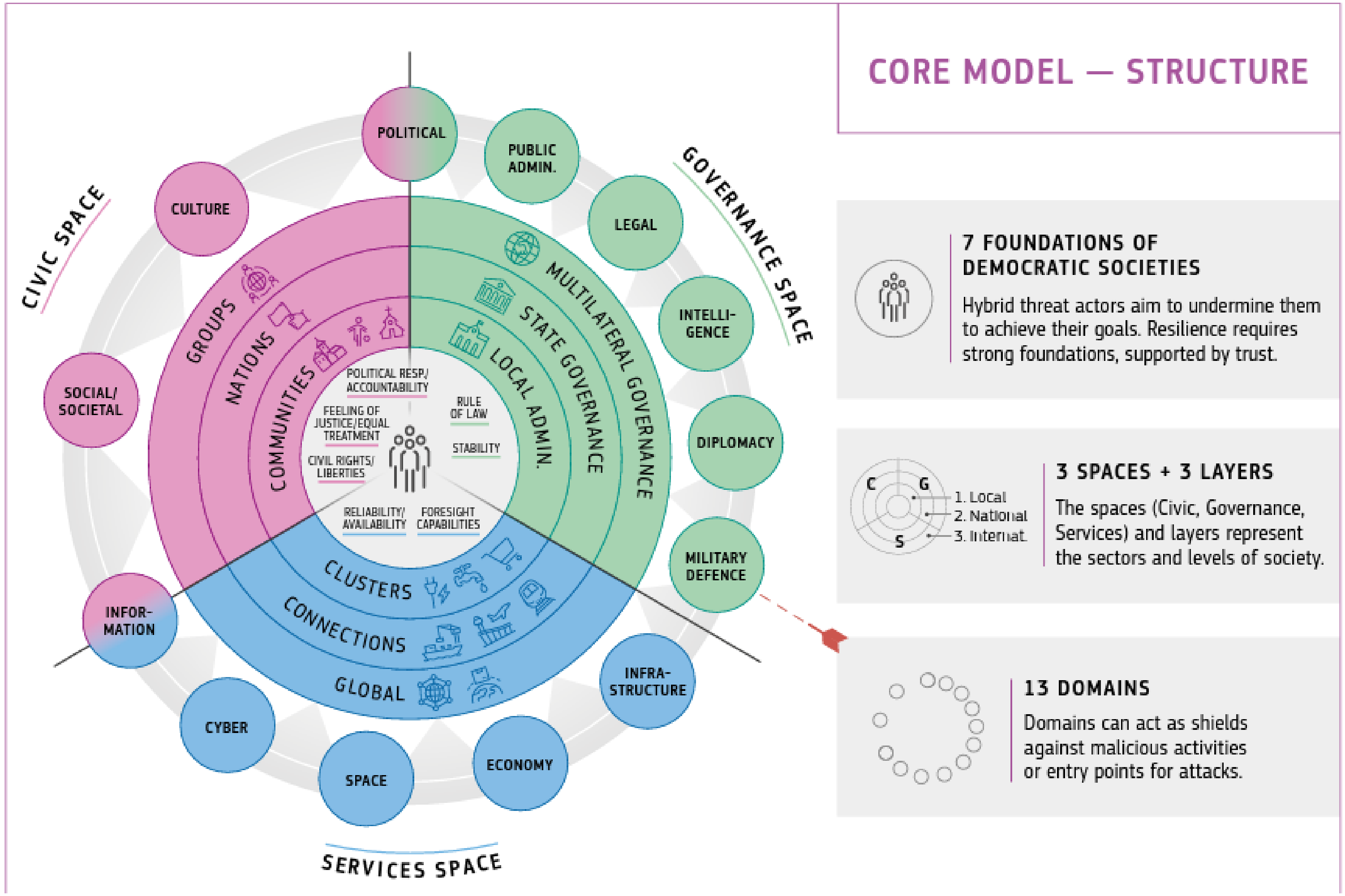
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Conceptual Model - domains of Hybrid Threats



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

The CORE Model to Characterise Hybrid Threats



CORE MODEL — STRUCTURE

7 FOUNDATIONS OF DEMOCRATIC SOCIETIES

Hybrid threat actors aim to undermine them to achieve their goals. Resilience requires strong foundations, supported by trust.

3 SPACES + 3 LAYERS

The spaces (Civic, Governance, Services) and layers represent the sectors and levels of society.

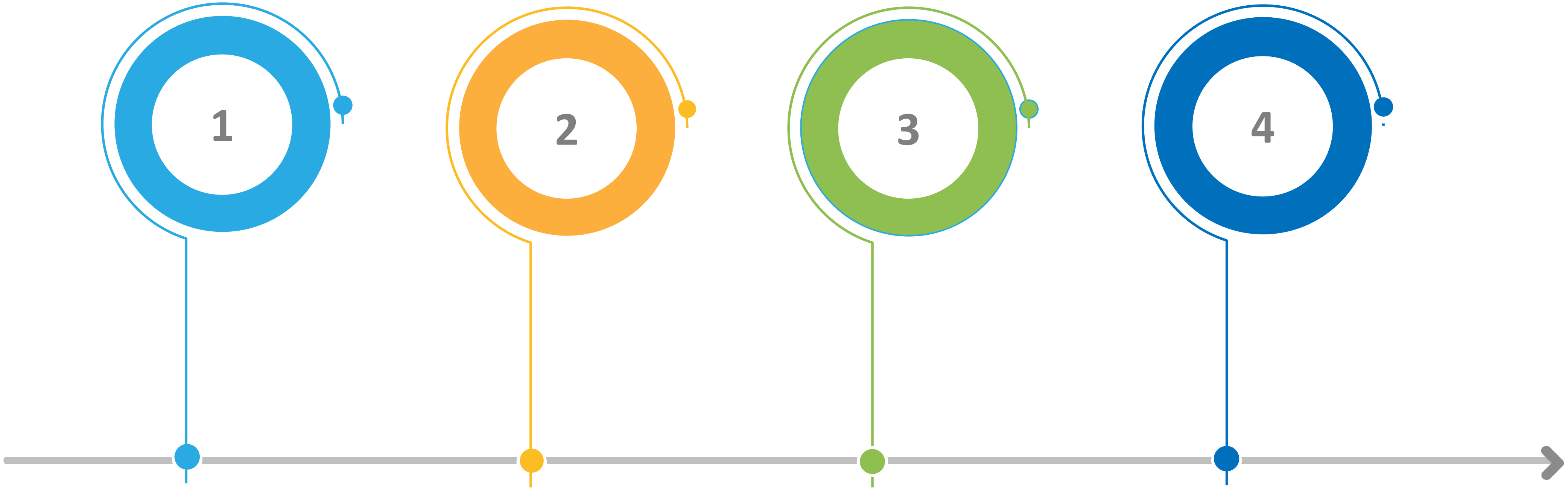
13 DOMAINS

Domains can act as shields against malicious activities or entry points for attacks.

https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en
https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Project Core Themes



Future Trends of Hybrid Threats

Cyber& Future **Technologies**

Resilient Civilians Local Level & National Administration

Information & Strategic Communication

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Gaps and needs
&
Innovations

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Identified main Hybrid Threats to counter/ 2nd project working cycle (2022-2023)

EU-HYBNET

Core Theme: Resilient Civilians, Local Level and National Administration

Threats	Domains
Exploitation of existing political cleavages	*Political,* *Public administration,* *Social/societal*
🔴 **Exploitation of critical infrastructure weaknesses & economic dependencies**	*Infrastructure, Economy, Cyber*
🔴 **Exploitation or investment in companies by foreign actors**	*Political,* *Economy*

Core Theme: Cyber and Future Technologies

Threats	Domains
🟠 Space interference and counter-space weapons	*Space,* *Cyber,* *Military/defence*
🟠 Offensive cyber capabilities	*Cyber,* *Infrastructure*
🟠 Disruptive innovation (5G, AI)	*Political, Social/societal, Military/defence*

Core Theme: Information and Strategic Communication

Threats	Domains
🟠 Information manipulation with the aim of destabilization	*Information, Cyber*
Foreign interference in key information institutions	*Political, Culture*
Promoted ideological extremism and violence	*Information, intelligence, Legal*

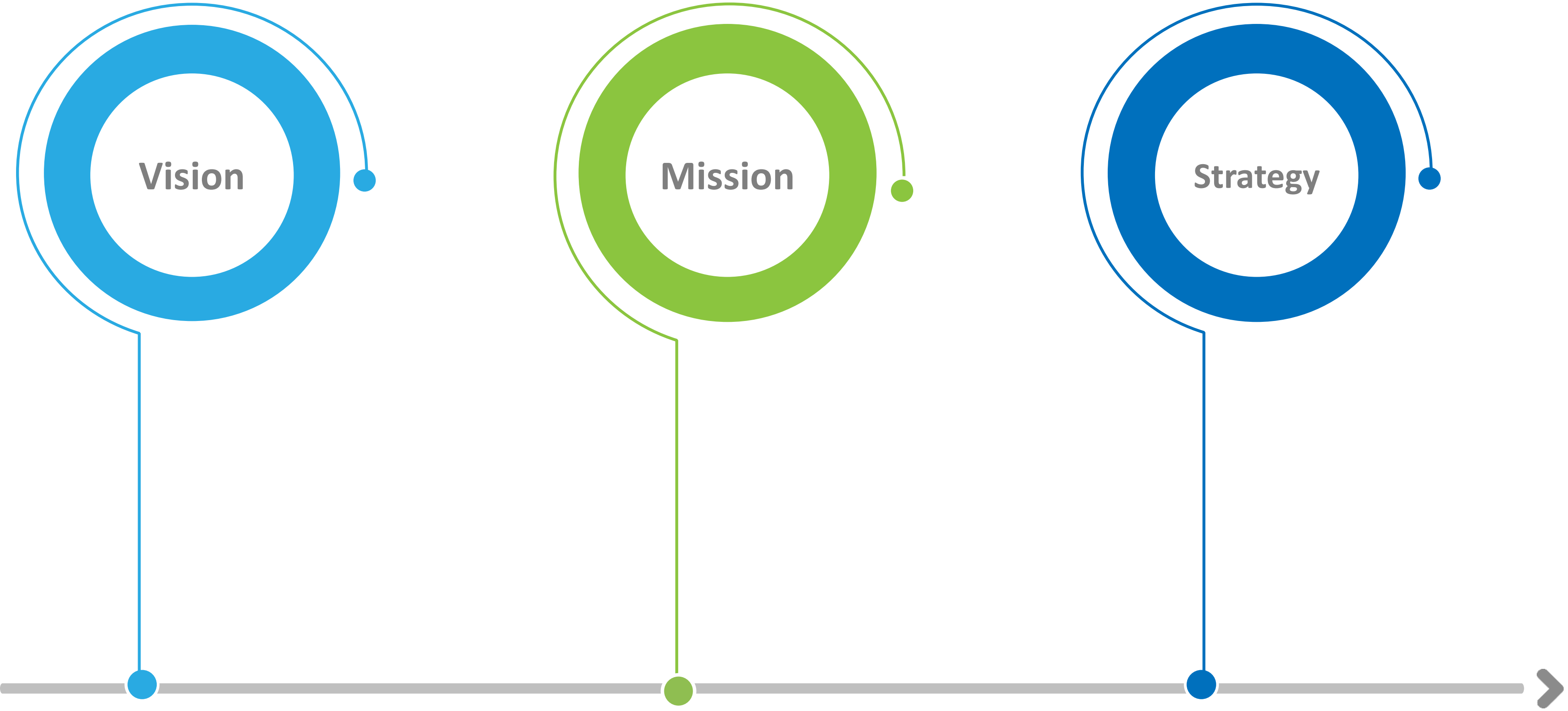
Core Theme: Future Trends of Hybrid Threats

Threats	Domains
Geopolitical heavyweight of domestic policy	*Political, Economy, Infrastructure*
🟠 Digital escalation and AI-based exploitation	*Cyber,* *Military/defence, Political*
Rise of populism	*Political, Social/societal, Information*

Based on EU-HYBNET Report/D2.10 (JRC) and Conceptual Model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Every innovation need vision, mission and strategy. Innovations in 2022-2023



Vision

Mission

Strategy

Innovations:

- ✓WINS
- ✓EESCM
- ✓MIMI
- ✓GECHO

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Results 2023: Promising Innovations to Counter Hybrid Threats

WINS

EESCM

MIMI

GECHO

- ✓ **What Information Needs to be Shared between CI entities to detect hybrid threats – methodology**
- ✓ **Enhanced and Extended Supply Chain Management – methodology**
- ✓ **A Market place for Information Manipulation and Interference Information –technological solution**
- ✓ **Gatekeeping ECHO chambers. A solution that monitors the online environment, identifies where and how interventions are needed, thereafter launching the appropriate actions to build resilience in vulnerable young people against possible entrapment in violent extremism and terrorism**

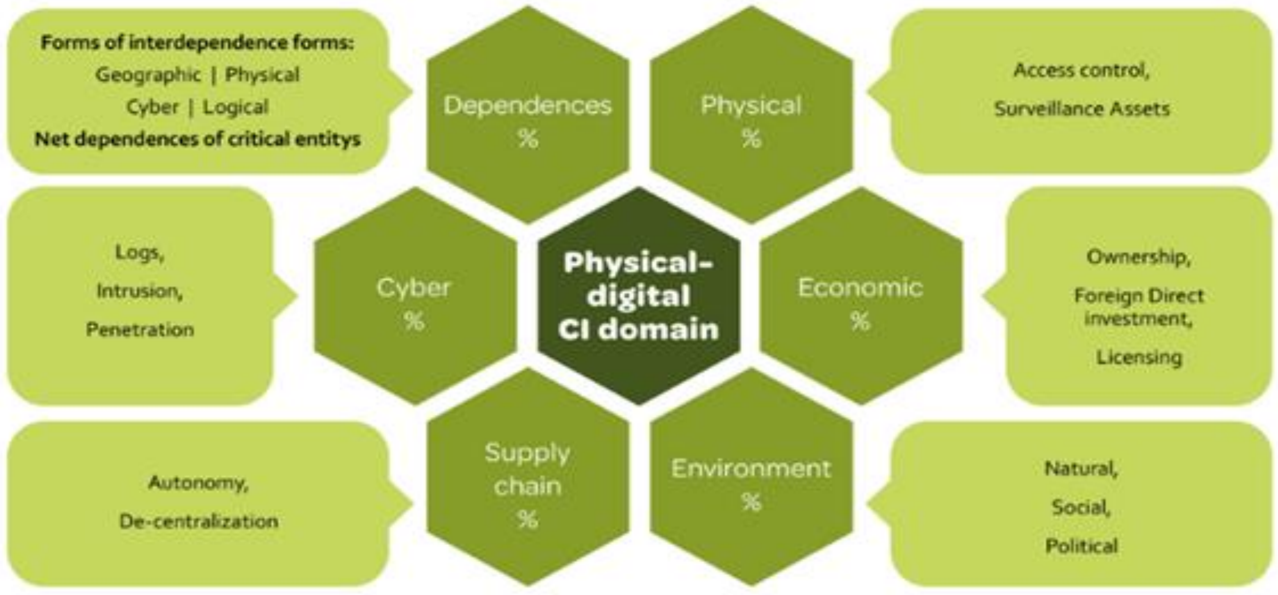
More information about 2023 results you can find under this link

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

WINS Innovation

- ***WINS*** is a ***methodological approach*** **to discover what information needs to be shared in order to enhance Critical Infrastructure (CI) entities resilience to counter hybrid threats & to be prepare for them**
- ***WINS*** builds on **CISAE** innovation; CISAE was identified as promising innovation and solution during the 1st EU-HYBNET project working cycle to support CI entities to counter hybrid threats
- ***CISAE*** (A common Information Sharing and Analysis environment) is answering to the question of **how to share CI information between CI stakeholders**.

CISAE - CRITICAL INFRASTRUCTURE INFORMATION BUILDING BLOCKS



Forms of interdependence forms:
Geographic | Physical
Cyber | Logical
Net dependences of critical entitys

Dependences
%

Physical
%

Access control,
Surveillance Assets

Logs,
Intrusion,
Penetration

Cyber
%

Physical-digital CI domain

Economic
%

Ownership,
Foreign Direct investment,
Licensing

Autonomy,
De-centralization

Supply chain
%

Environment
%

Natural,
Social,
Political

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

WINS Innovation

- In the core: **detection of anomalies** gives **early indicators of compromise/attack**.

- This **systemic anomaly detection** solution **allows CI providers** to ***early detect hybrid threats*** and *early prevent larger effects on the European CI.*

- Even though it is not part of CI entities duties to detect that something what occurs is in fact that part of a broader hybrid threat campaign, *still* **this information discovery** may now be reached and **support CI entities to be prepared for further challenges** and/or support **to reduce and cut the strength of the hybrid threat campaign.**

E.G.

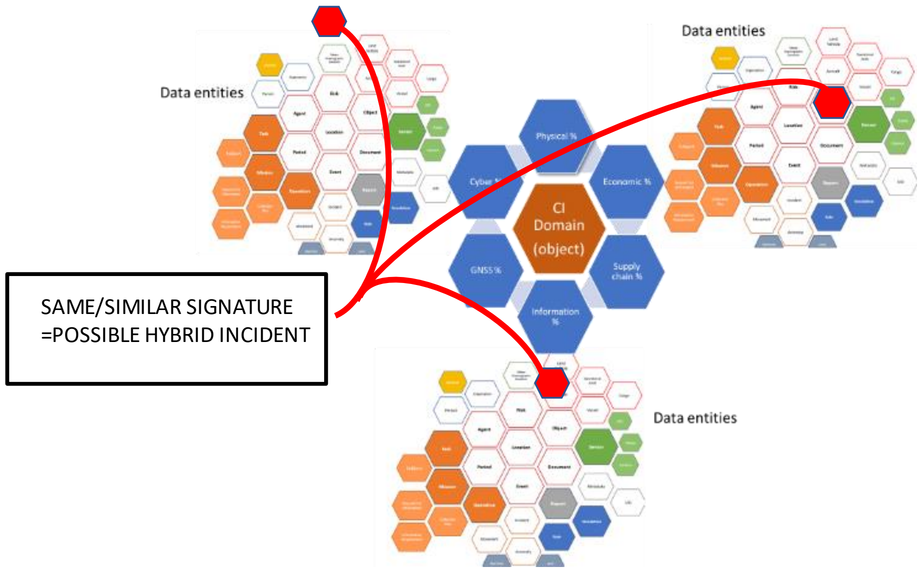
- *By knowing that certain foreign direct investments together with cyber espionage and riots have in other similar CI entities cases followed by exploiting thresholds, gaps and uncertainty in law and harming in this way CI entities functions and society* ***may provide situational awareness on emerging risk and hybrid threat campaign***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

WINS Innovation

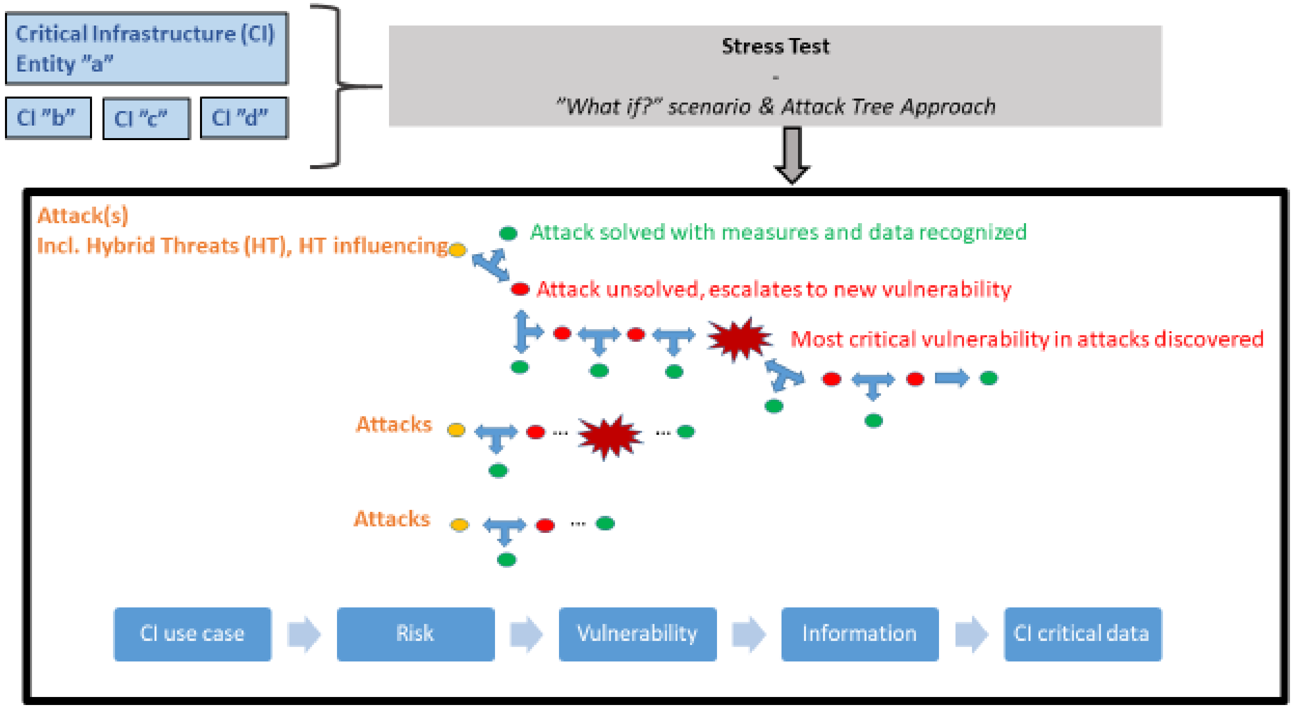
- *WINS (what to share?) builds on CISAE “Honey Comb” Approach (how to share?)*
- *WINS promotes use of: (i) Stress Tests, (ii) “What If?” Scenarios, (iii) Attack Tree Approach*

CISAE – Honey Comb Approach



SAME/SIMILAR SIGNATURE =POSSIBLE HYBRID INCIDENT

WINS – Stress Tests, ”What If?” Scenarios, Attack Tree Approach



Critical Infrastructure (CI) Entity ”a”

CI ”b” CI ”c” CI ”d”

Stress Test

-

”What if?” scenario & Attack Tree Approach

Attack(s)
Incl. Hybrid Threats (HT), HT influencing

Attack solved with measures and data recognized

Attack unsolved, escalates to new vulnerability

Most critical vulnerability in attacks discovered

Attacks

Attacks

CI use case → Risk → Vulnerability → Information → CI critical data

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

Identified main Hybrid Threats to counter/ 3rd project working cycle (2023-2024)

EU-HYBNET

Core Theme: Resilient Civilians, Local Level and National Administration

Threats	Domains
Spreading violence	*Intelligence, Social/societal, Culture*
Attack on social structures	*Social/societal, Culture Legal, Intelligence*
Undermining institutions' internal organisation	*Political, Social/societal, Legal, Administration*

Core Theme: Cyber and Future Technologies

Threats	Domains
Stealing data attacking individuals	*Cyber, Information, Cyber*
Online manipulation attacking democracy	*Cyber, Information, Political*
Attack on services	***Infrastructures, Cyber, Military/Defence, Social/societal, Administration***

Core Theme: Information and Strategic Communication

Threats	Domains
Media conundrum	*Information, Cyber, Social/societal*
Antagonizing victimization narratives in the informational space	*Information, Political, Culture*
Attack on information	*Information, Intelligence, Legal*

Core Theme: Future Trends of Hybrid Threats

Threats	Domains
Political deficiency	*Political, Information, Administration*
New agit-prop	*Cyber, Military/defence, Political , Legal*
Substitutive reality	*Social/societal, Information*

Based on EU-HYBNET Report/D2.11 (JRC) and Conceptula & CORE Model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Events – Join!

3rd Innovation and Knowledge Exchange Workshop

Valencia, 7th NOV 2023

- Goal: to present and have further analysis on promising innovations to the identified pan-European gaps and needs to counter Hybrid Threats
- Arranged by EOS & PLV, more information angeliki.tsanta@eos-eu.com

2nd Innovation Standardization Workshop

Valencia, 8th NOV 2023

- Goal: To develop recommendations for activities regarding the development & implementation of most promising EU-HYBNET's identified four innovations to counter hybrid threats
- Innovations representing (i) critical infrastructure & (ii) Information Manipulation and Interference
- JOIN & PRESENT your Case-Study!
- Arranged by PPHS & PLV, more informaiton malgorzata.wolbach@ppbw.pl

EU-HYBNET
INVITATION
3rd Innovation & Knowledge Exchange Workshop
&
2nd Innovation Standardisation Workshop

https://euhybnet.eu/events/

Role of LEAs in Combating Hybrid Threats

ON-LINE, 26th OCT, 13.00-15.00 CEST

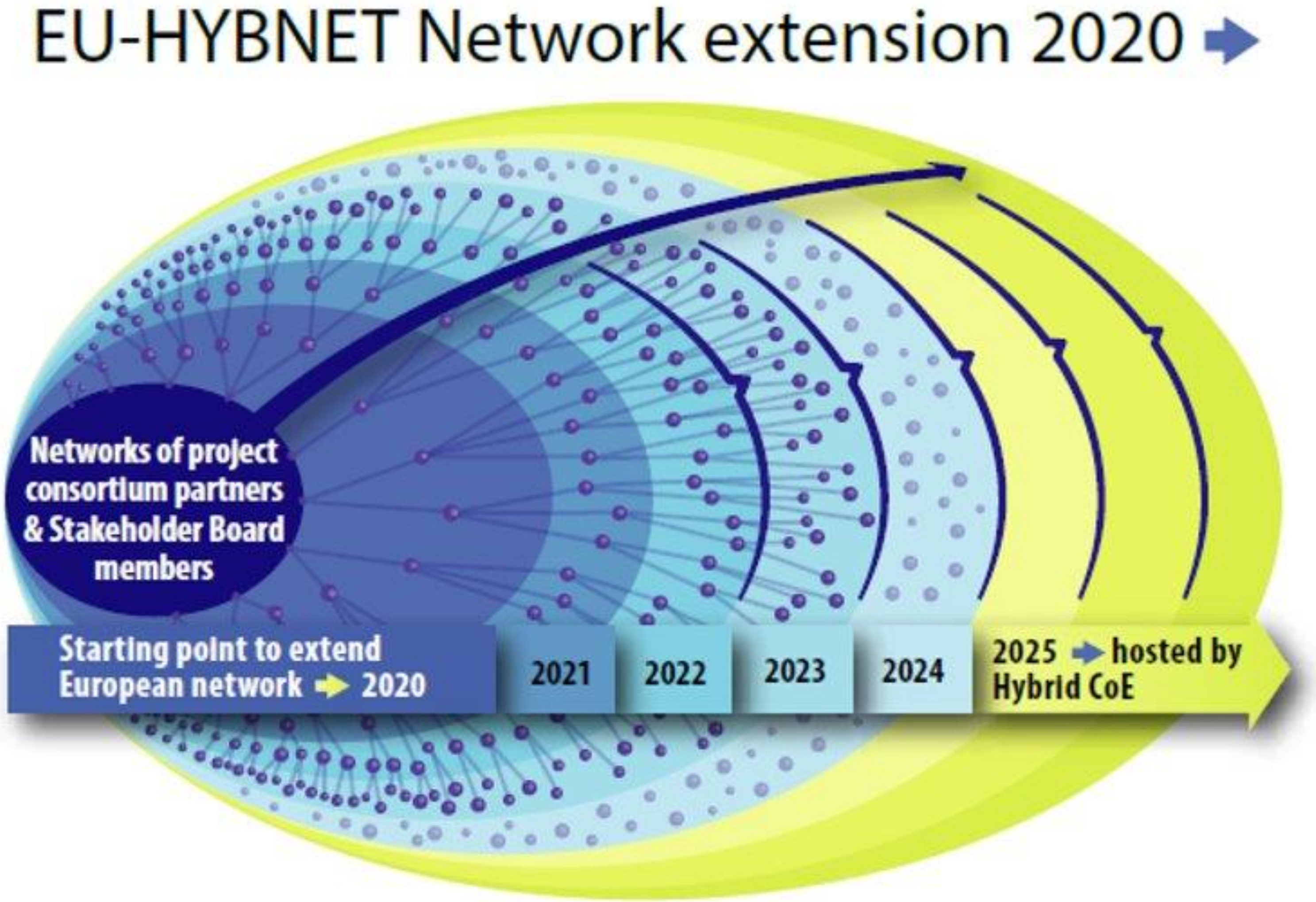
- Arranged by PPHS together with CyberSpace LEA Project Cluster
- Register https://euhybnet.eu/events/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Network

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Project Timeline and Network Extension


EU-HYBNET Network extension 2020 ➔
Networks of project consortium partners & Stakeholder Board members
Starting point to extend European network ➔ 2020
2021
2022
2023
2024
2025 ➔ hosted by Hybrid CoE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET Network Members in Spring 2023 – Welcome to join!

Practitioners

- 24 institutions
- 10 in consortium
- from 14 countries:

Italy, Germany, Slovakia, Poland, Sweden, Luxemburg, Georgia, France, Finland, Netherlands, Norway, Romania, Belgium

Academic & RTO

- 32 institutions
- 11 in consortium
- from 16 countries:

Italy, Germany, Austria, Poland, Georgia, France, Finland, Netherland, Norway, Romania, Belgium, Greece, Spain, Ukraine, Croatia, Bulgaria

Industry / SME

- 21 institutions
- 2 in consortium
- from 9 countries:

Sweden, Germany, Austria, Belgium, France, Netherlands, Romania, Finland, Spain

NGOs

- 16 institutions
- 2 in consortium
- from 12 countries:

Czech Republic, Slovakia, Latvia, Poland, Belgium, France, Lithuania, Italy, Finland, Portugal, Croatia, Romania

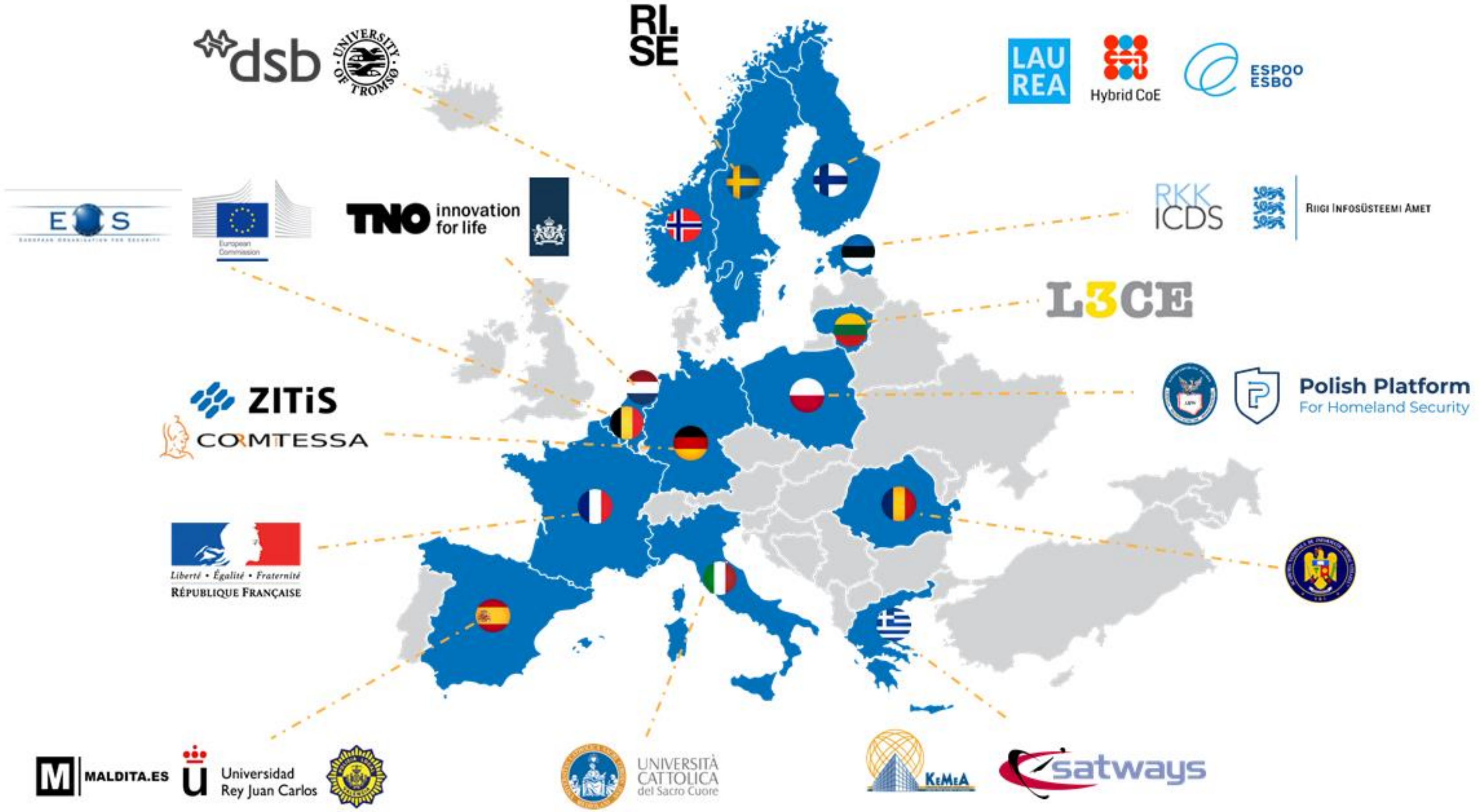
Welcome to join the Network!

More details about Members & how to join: here.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET

Thank you!



Päivi Mattila/ Laurea

paivi.mattila@laurea.fi

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

PRAETORIAN

Protection of Critical Infrastructures from advanced combined cyber and physical threats

EU-CIP

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection

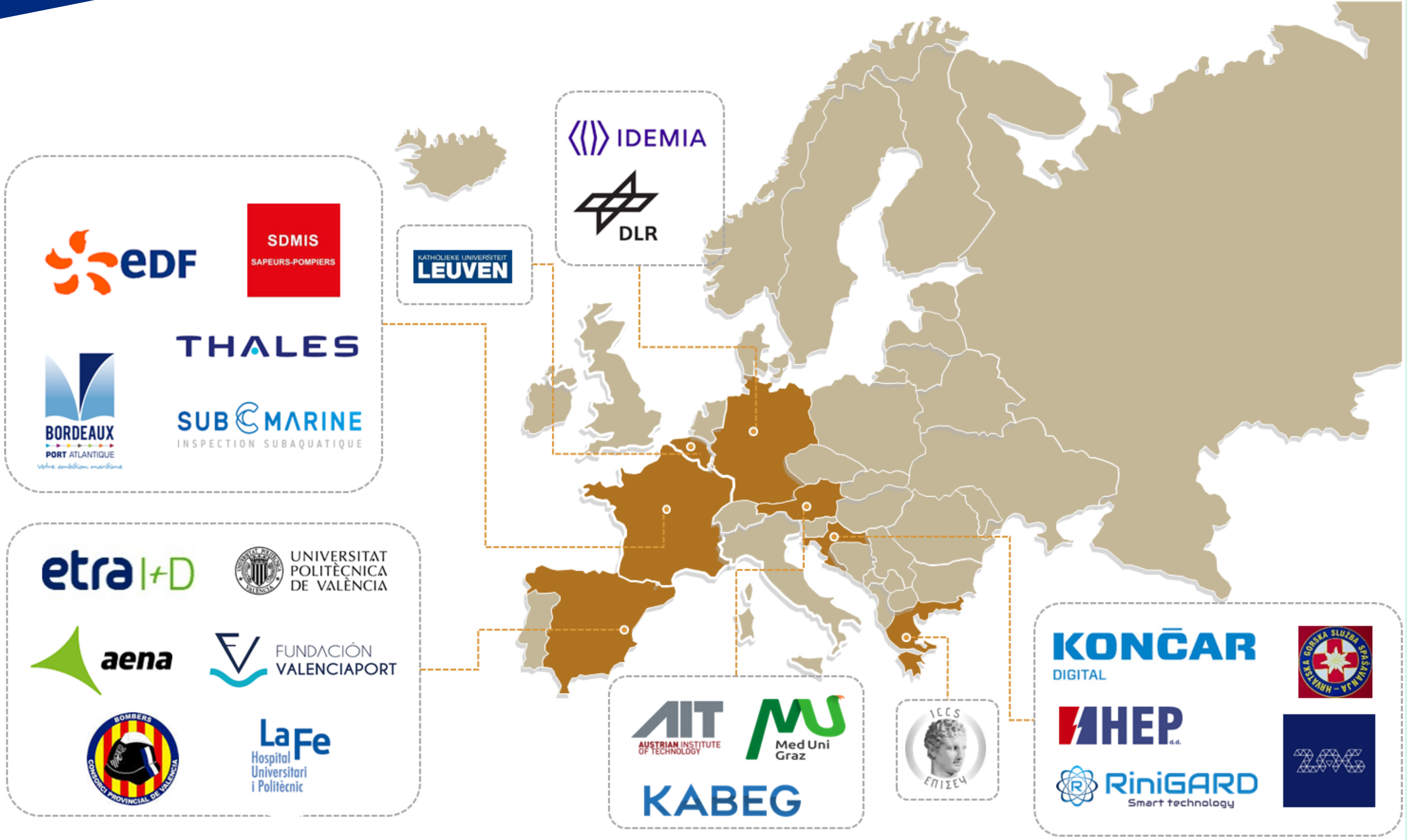
& ECSCI CLUSTER

1ST ANNUAL CONFERENCE ON
CRITICAL INFRASTRUCTURE PROTECTION
&
ECSCI WORKSHOP

PRAETORIAN Project Overview

Lazaros Papadopoulos – ICCS/NTUA

This project has received funding from the European Union’s Horizon 2020
Research and Innovation programme under Grant Agreement No 101021274


EDF
SDMIS SAPEURS-POMPIERS
THALES
BORDEAUX PORT ATLANTIQUE
SUBMARINE INSPECTION SUBAQUATIQUE
KATHOLIEKE UNIVERSITEIT LEUVEN
IDEMIA
DLR
etra I+D
UNIVERSITAT POLITÈCNICA DE VALÈNCIA
aena
FUNDACIÓN VALENCIAPORT
LaFe Hospital Universitari i Politècnic
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Med Uni Graz
KABEG
ICCS
KONČAR DIGITAL
HEP
RiniGARD Smart technology

PRAETORIAN AT A GLANCE

- Coordinator: EDF
- 23 partners from 7 EU countries
- 3 pilot sites in 4 EU Member States
- Total budget: 9,04 M€
- Total funding: 7,58 M€
- Start date: 01/06/2021
- End date: 30/09/2023

“

PRAETORIAN strategic goal is to increase the **security and resilience** of European CIs, facilitating the **coordinated protection** of **interrelated CIs** against **combined physical and cyber threats**.

PRAETORIAN OBJECTIVES

- **Technological objectives**

Evaluate hazards and minimize their level of risk

Improve the understanding of any physical or cyber threat

Improve the resilience of the CIs, enable coordinated response to attacks

Share with the public information on the risks

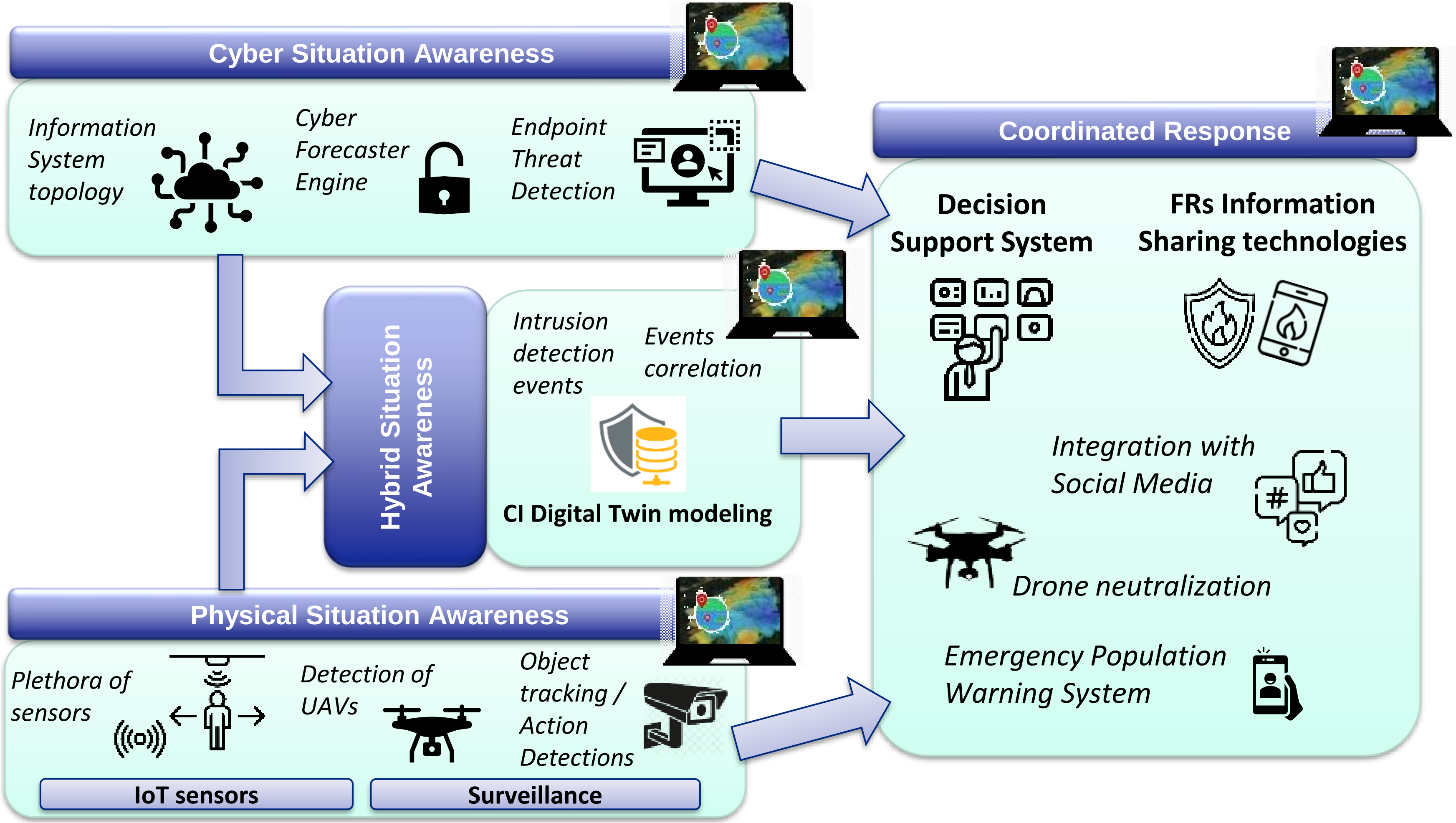
- **Impact and user-oriented objectives**

Validate in real contexts of interdependent CIs

Ensure compliance with legal, ethical, privacy, and societal principles

Disseminate results to relevant communities of users

PRAETORIAN SOLUTION



Cyber Situation Awareness

Information System topology

Cyber Forecaster Engine

Endpoint Threat Detection

Hybrid Situation Awareness

Intrusion detection events

Events correlation

CI Digital Twin modeling

Physical Situation Awareness

Plethora of sensors

Detection of UAVs

Object tracking / Action Detections

IoT sensors

Surveillance

Coordinated Response

Decision Support System

FRs Information Sharing technologies

Integration with Social Media

Drone neutralization

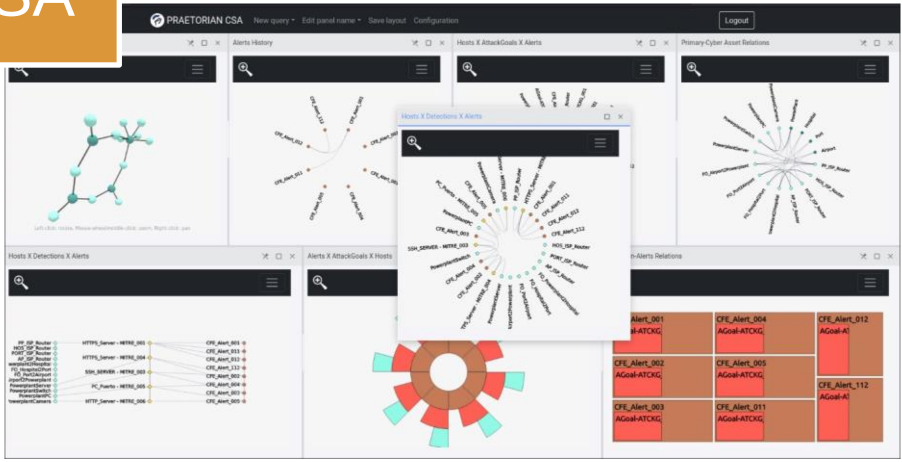
Emergency Population Warning System

End users of the tools:

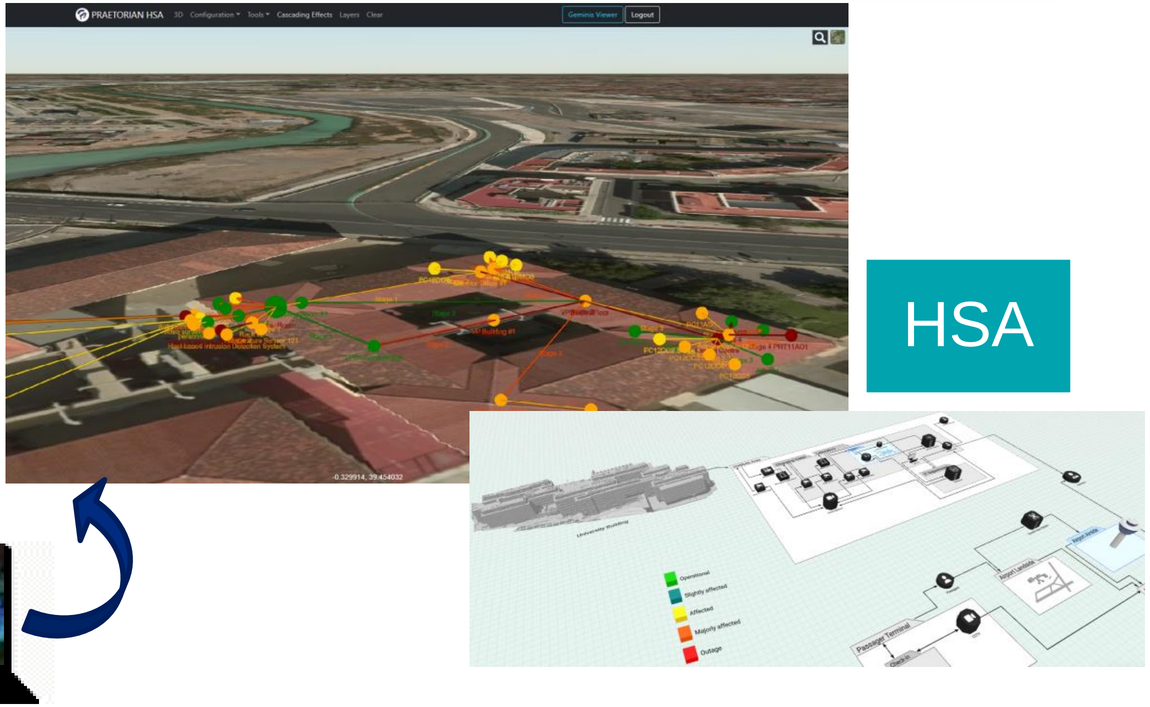
- Critical Infrastructure (CI) operators
- First Responders (FRs)

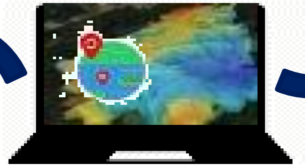
PRAETORIAN Dashboards

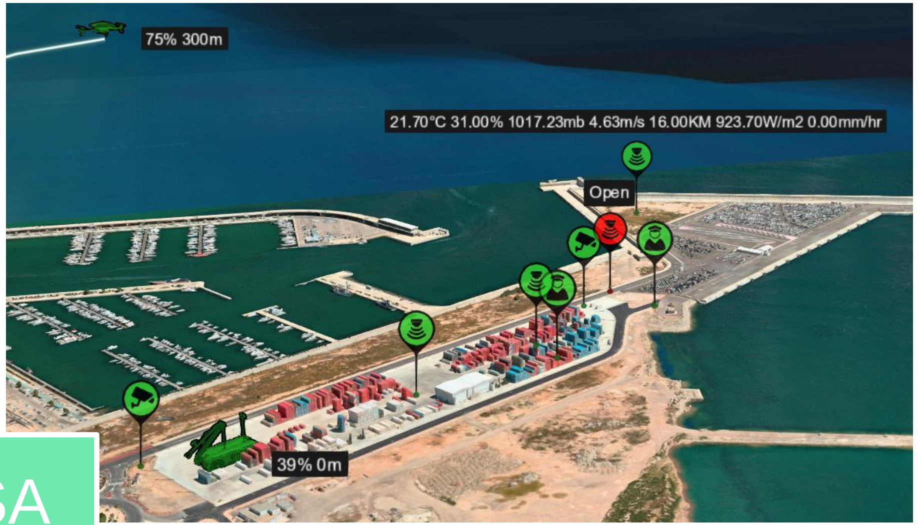
CSA


PRAETORIAN CSA
New query
Edit panel name
Save layout
Configuration
Logout
Alerts History
Hosts X AttackGoals X Alerts
Primary-Cyber Asset Relations
Hosts X Detections X Alerts
Alerts X AttackGoals X Hosts
Alerts Relations

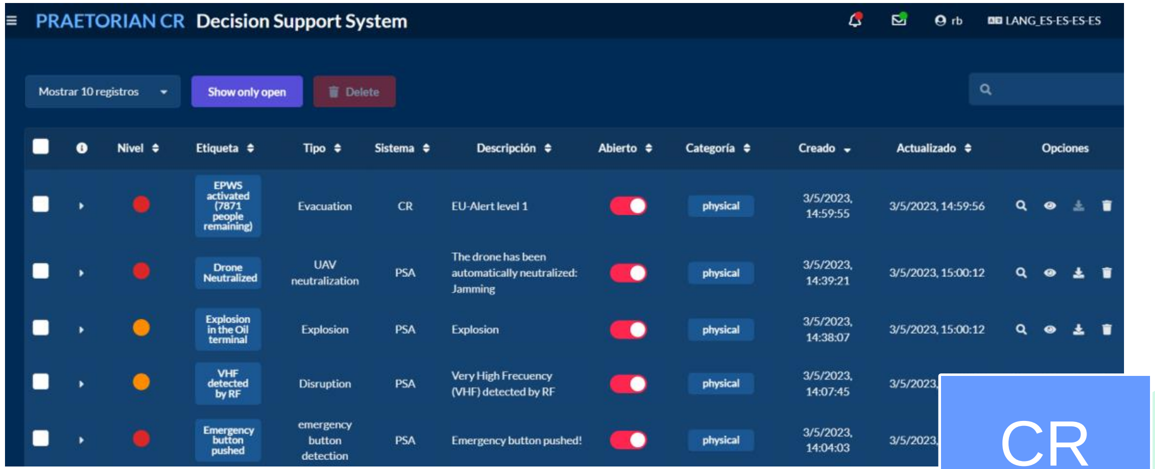
HSA






75% 300m
21.70°C 31.00% 1017.23mb 4.63m/s 16.00KM 923.70W/m2 0.00mm/hr
Open
39% 0m

PSA



PRAETORIAN CR Decision Support System

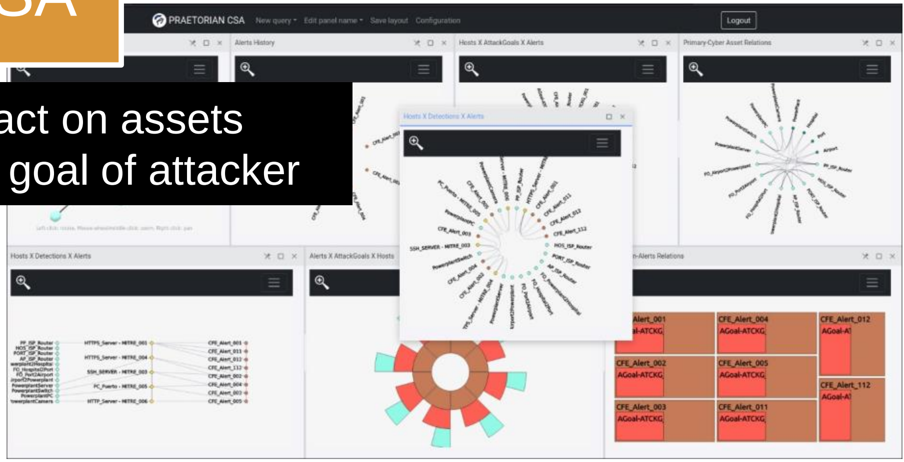
□		Nivel	Etiqueta	Tipo	Sistema	Descripción	Abierto	Categoría	Creado	Actualizado	Opciones
□	▸	●	EPWS activated (7871 people remaining)	Evacuation	CR	EU-Alert level 1	●	physical	3/5/2023, 14:59:55	3/5/2023, 14:59:56	
□	▸	●	Drone Neutralized	UAV neutralization	PSA	The drone has been automatically neutralized: Jamming	●	physical	3/5/2023, 14:39:21	3/5/2023, 15:00:12	
□	▸	●	Explosion in the Oil terminal	Explosion	PSA	Explosion	●	physical	3/5/2023, 14:38:07	3/5/2023, 15:00:12	
□	▸	●	VHF detected by RF	Disruption	PSA	Very High Frecuency (VHF) detected by RF	●	physical	3/5/2023, 14:07:45	3/5/2023,	
□	▸	●	Emergency button pushed	emergency button detection	PSA	Emergency button pushed!	●	physical	3/5/2023, 14:04:03	3/5/2023,	

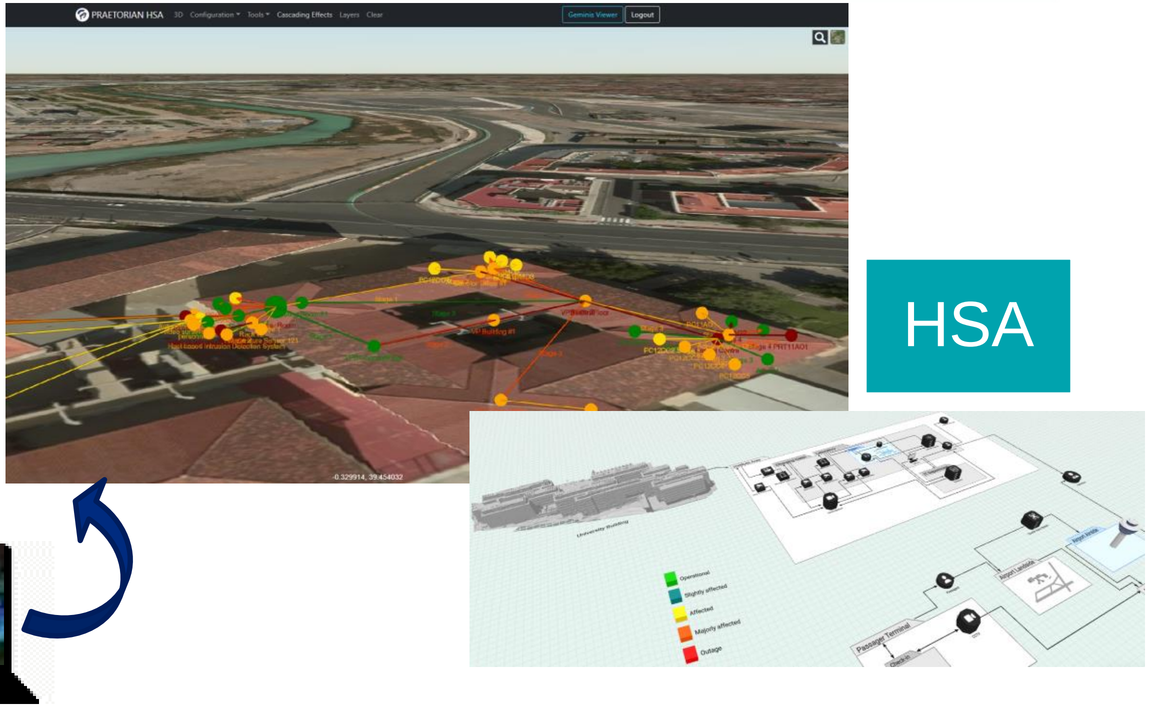
CR

PRAETORIAN Dashboards

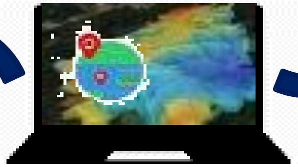
CSA

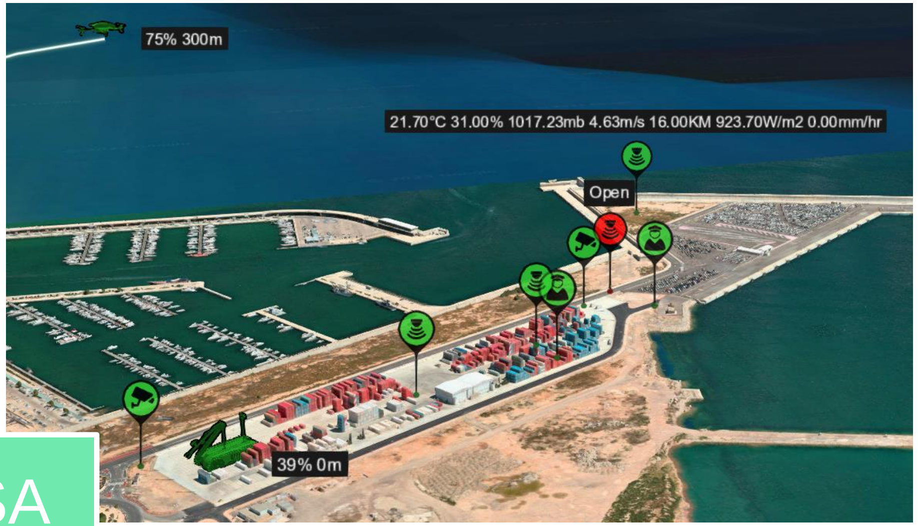
Impact on assets
End goal of attacker



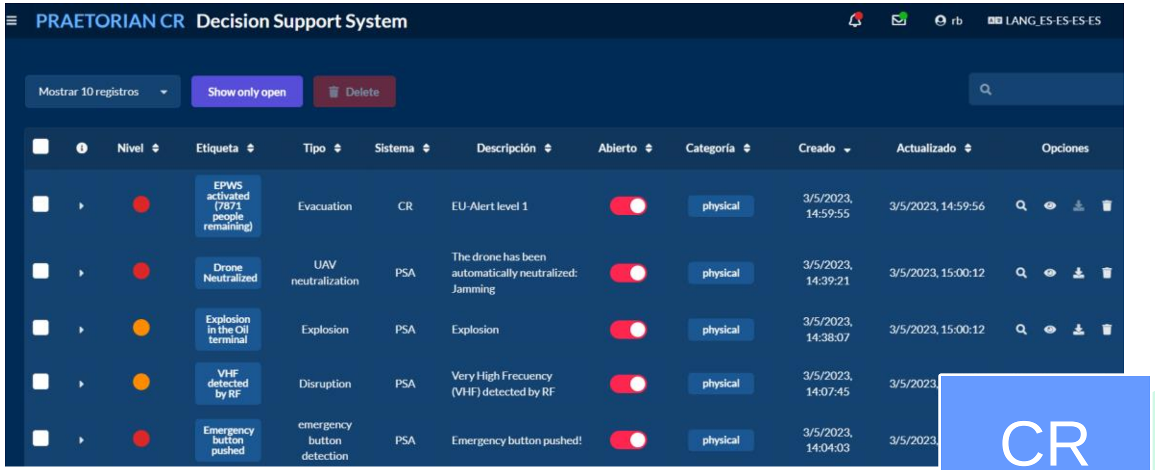


HSA




75% 300m
21.70°C 31.00% 1017.23mb 4.63m/s 16.00KM 923.70W/m2 0.00mm/hr
Open
39% 0m

PSA



≡ PRAETORIAN CR Decision Support System

rb LANG_ES-ES-ES-ES

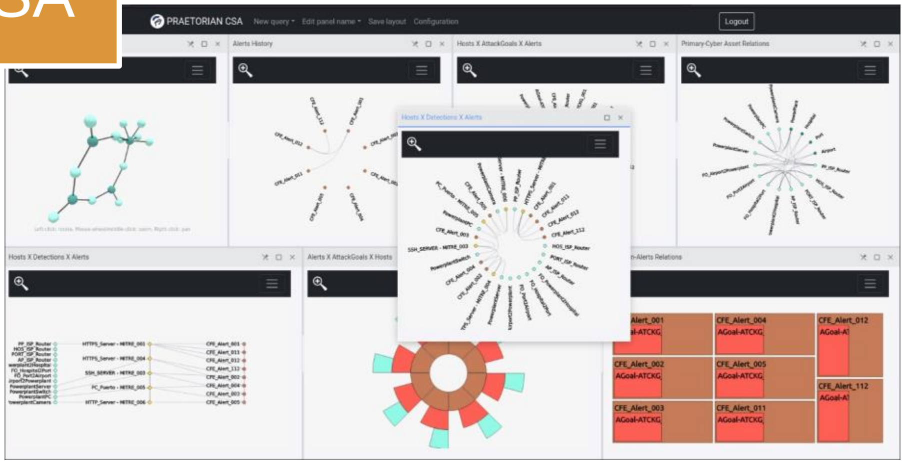
Mostrar 10 registros | Show only open | Delete

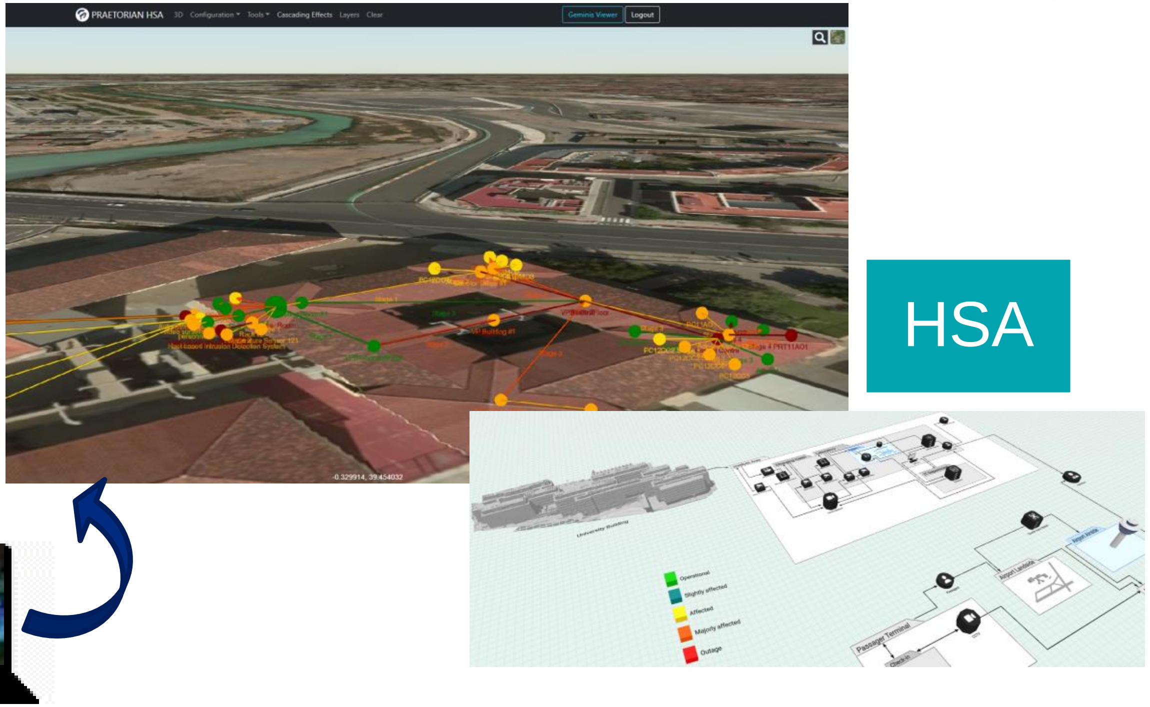
□		Nivel	Etiqueta	Tipo	Sistema	Descripción	Abierto	Categoría	Creado	Actualizado	Opciones
□	▸	●	EPWS activated (7871 people remaining)	Evacuation	CR	EU-Alert level 1		physical	3/5/2023, 14:59:55	3/5/2023, 14:59:56	
□	▸	●	Drone Neutralized	UAV neutralization	PSA	The drone has been automatically neutralized: Jamming		physical	3/5/2023, 14:39:21	3/5/2023, 15:00:12	
□	▸	●	Explosion in the Oil terminal	Explosion	PSA	Explosion		physical	3/5/2023, 14:38:07	3/5/2023, 15:00:12	
□	▸	●	VHF detected by RF	Disruption	PSA	Very High Frecuency (VHF) detected by RF		physical	3/5/2023, 14:07:45	3/5/2023,	
□	▸	●	Emergency button pushed	emergency button detection	PSA	Emergency button pushed!		physical	3/5/2023, 14:04:03	3/5/2023,	

CR

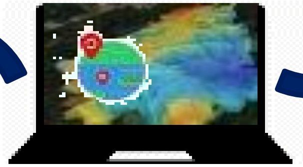
PRAETORIAN Dashboards

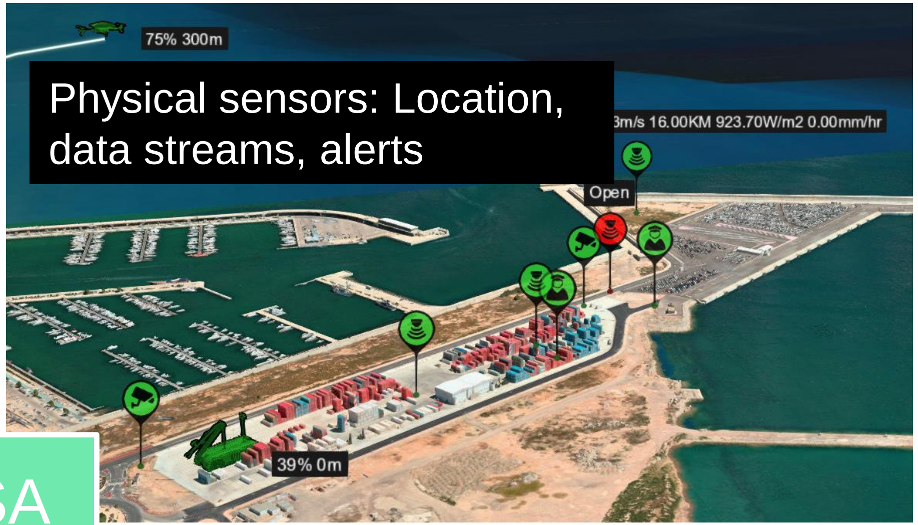
CSA


PRAETORIAN CSA
New query ▾
Edit panel name ▾
Save layout
Configuration
Logout
Alerts History
Hosts X AttackGoals X Alerts
Primary-Cyber Asset Relations
Hosts X Detections X Alerts
Alerts X AttackGoals X Hosts
Hosts X Detections X Alerts



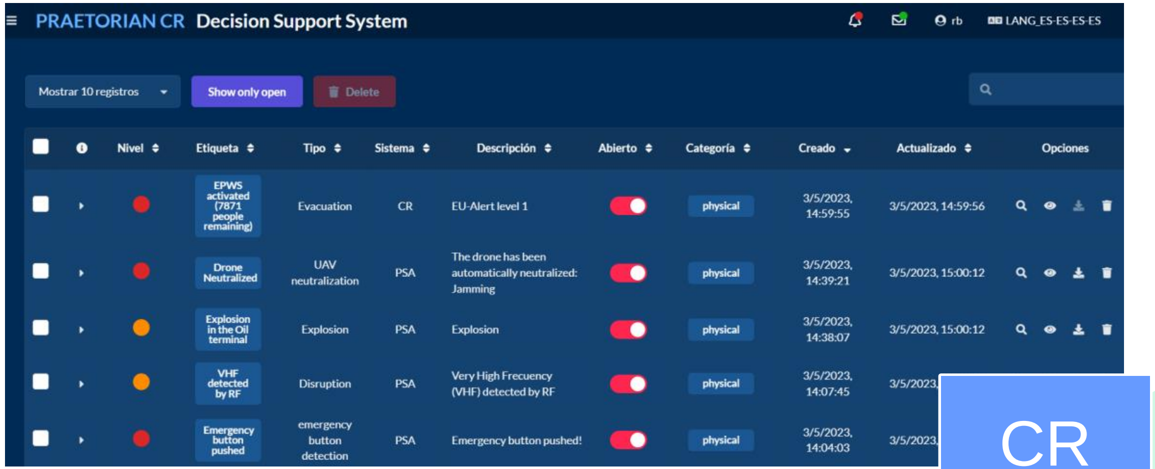
HSA





Physical sensors: Location, data streams, alerts

PSA



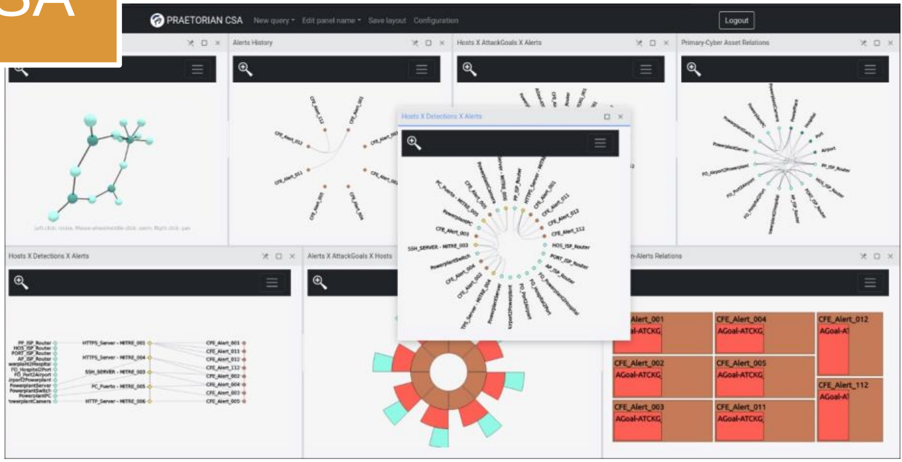
PRAETORIAN CR Decision Support System

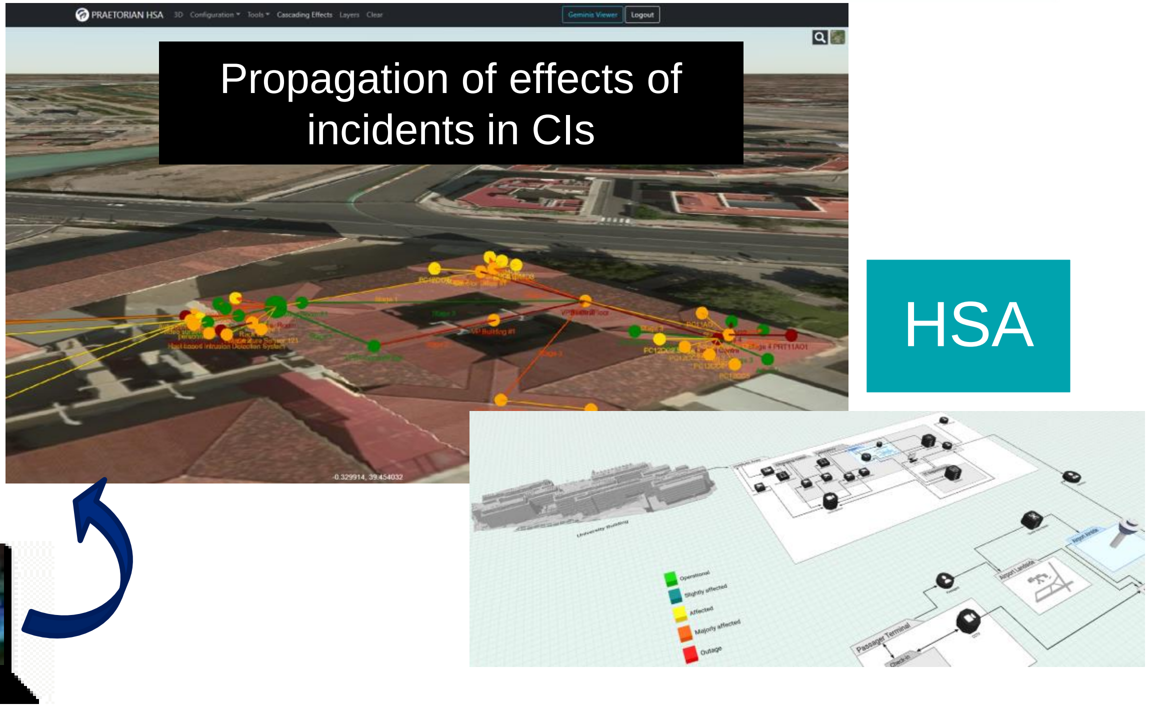
□		Nivel	Etiqueta	Tipo	Sistema	Descripción	Abierto	Categoría	Creado	Actualizado	Opciones
□	▸	●	EPWS activated (7871 people remaining)	Evacuation	CR	EU-Alert level 1		physical	3/5/2023, 14:59:55	3/5/2023, 14:59:56	
□	▸	●	Drone Neutralized	UAV neutralization	PSA	The drone has been automatically neutralized: Jamming		physical	3/5/2023, 14:39:21	3/5/2023, 15:00:12	
□	▸	●	Explosion in the Oil terminal	Explosion	PSA	Explosion		physical	3/5/2023, 14:38:07	3/5/2023, 15:00:12	
□	▸	●	VHF detected by RF	Disruption	PSA	Very High Frecuency (VHF) detected by RF		physical	3/5/2023, 14:07:45	3/5/2023,	
□	▸	●	Emergency button pushed	emergency button detection	PSA	Emergency button pushed!		physical	3/5/2023, 14:04:03	3/5/2023,	

CR

PRAETORIAN Dashboards

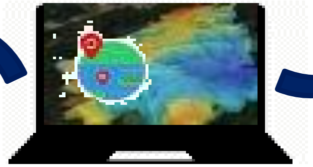
CSA

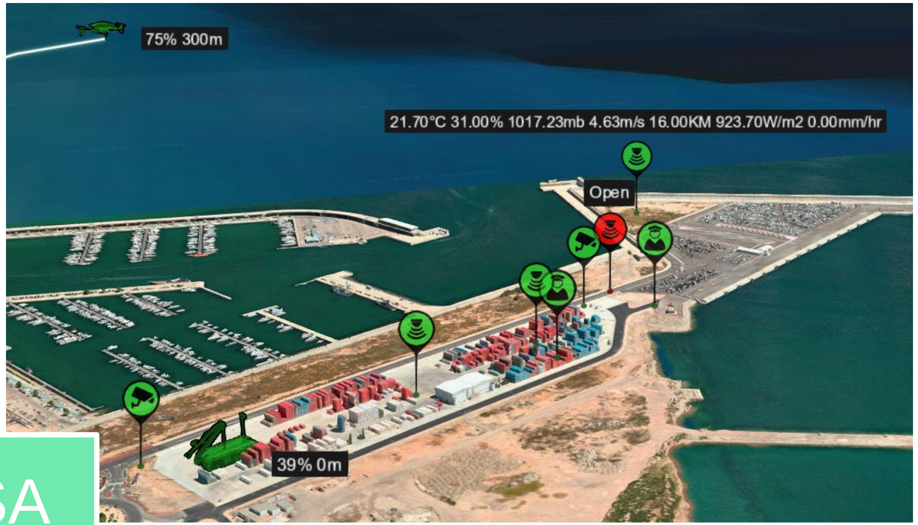

PRAETORIAN CSA
New query
Edit panel name
Save layout
Configuration
Logout
Alerts History
Hosts X AttackGoals X Alerts
Primary-Cyber Asset Relations
Hosts X Detections X Alerts
Alerts X AttackGoals X Hosts
Alerts Relations



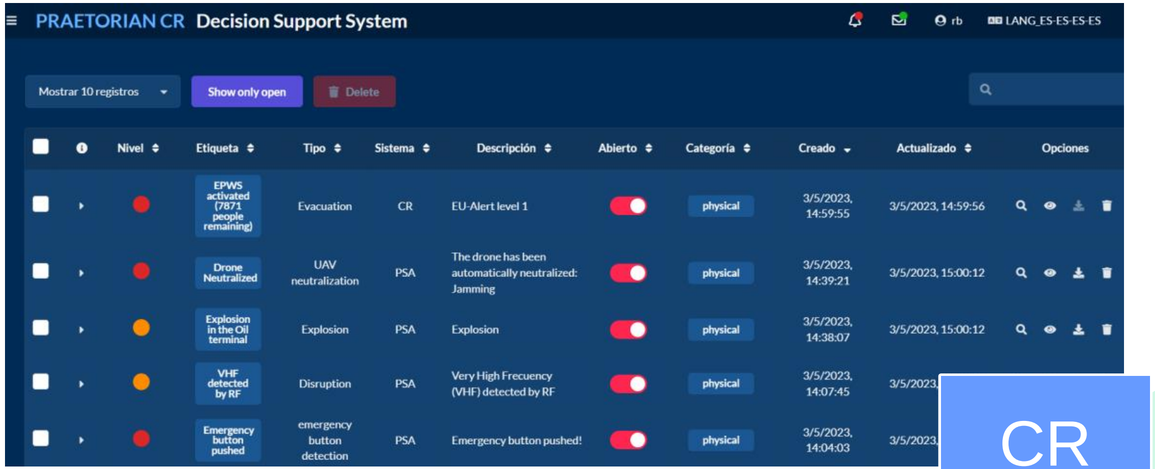
Propagation of effects of incidents in CIs

HSA




75% 300m
21.70°C 31.00% 1017.23mb 4.63m/s 16.00KM 923.70W/m2 0.00mm/hr
Open
39% 0m

PSA



PRAETORIAN CR Decision Support System

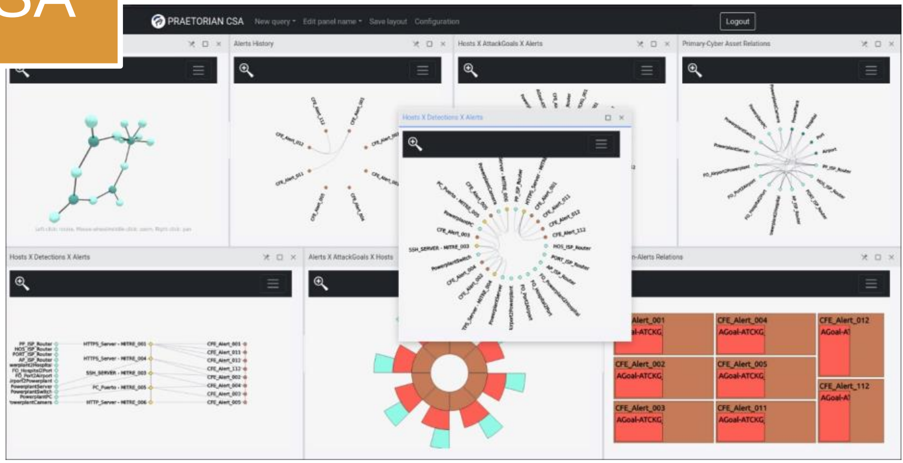
□		Nivel	Etiqueta	Tipo	Sistema	Descripción	Abierto	Categoría	Creado	Actualizado	Opciones
□	▸	●	EPWS activated (7871 people remaining)	Evacuation	CR	EU-Alert level 1		physical	3/5/2023, 14:59:55	3/5/2023, 14:59:56	
□	▸	●	Drone Neutralized	UAV neutralization	PSA	The drone has been automatically neutralized: Jamming		physical	3/5/2023, 14:39:21	3/5/2023, 15:00:12	
□	▸	●	Explosion in the Oil terminal	Explosion	PSA	Explosion		physical	3/5/2023, 14:38:07	3/5/2023, 15:00:12	
□	▸	●	VHF detected by RF	Disruption	PSA	Very High Frecuency (VHF) detected by RF		physical	3/5/2023, 14:07:45	3/5/2023,	
□	▸	●	Emergency button pushed	emergency button detection	PSA	Emergency button pushed!		physical	3/5/2023, 14:04:03	3/5/2023,	

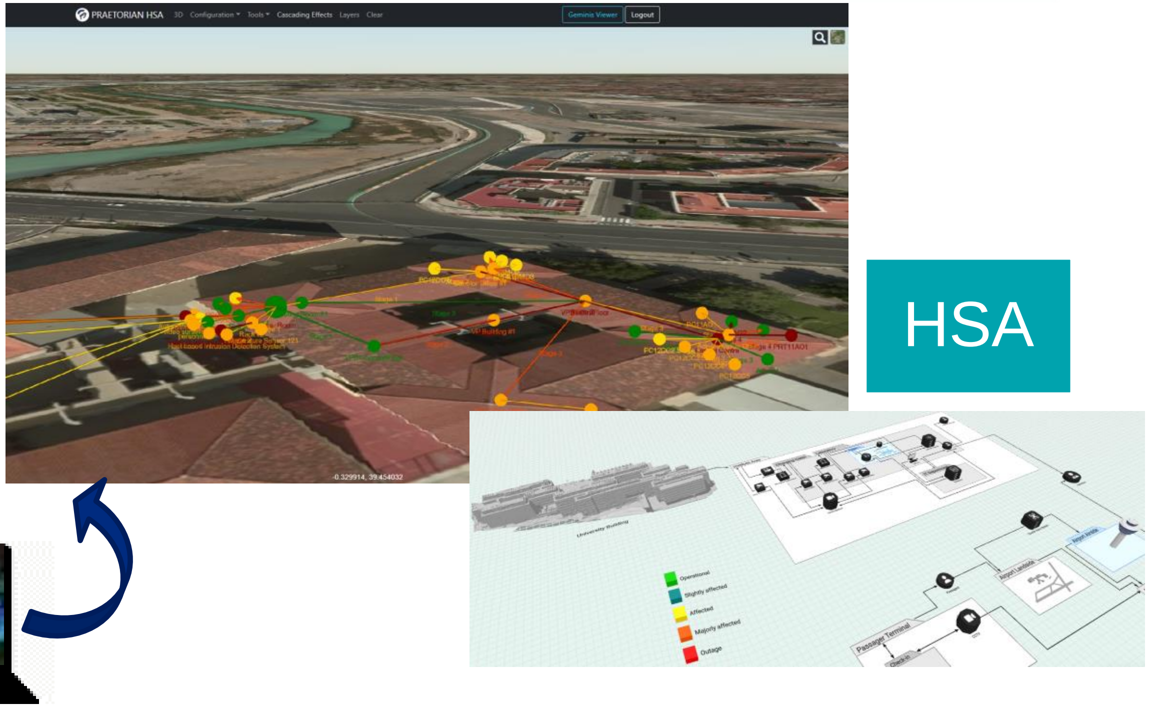
CR

PRAETORIAN Project Overview

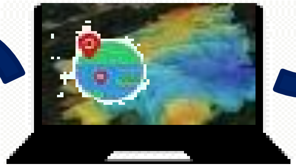
PRAETORIAN Dashboards

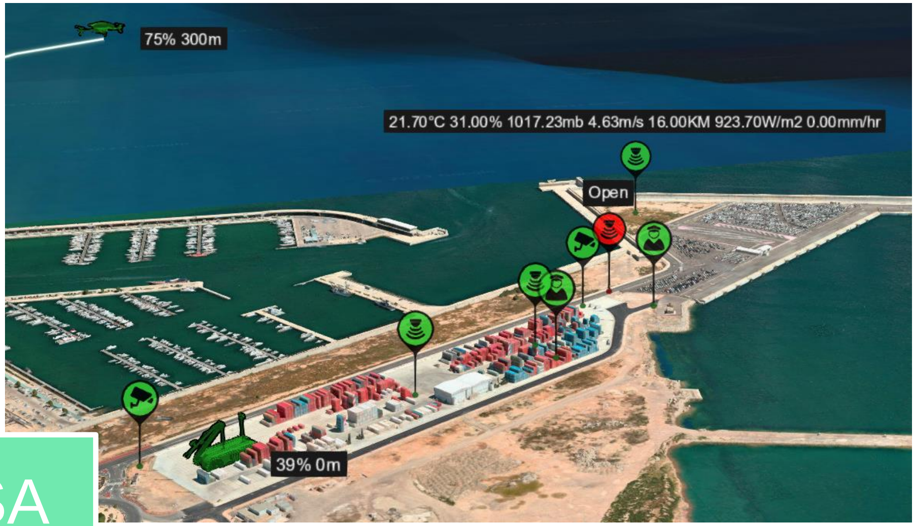
CSA



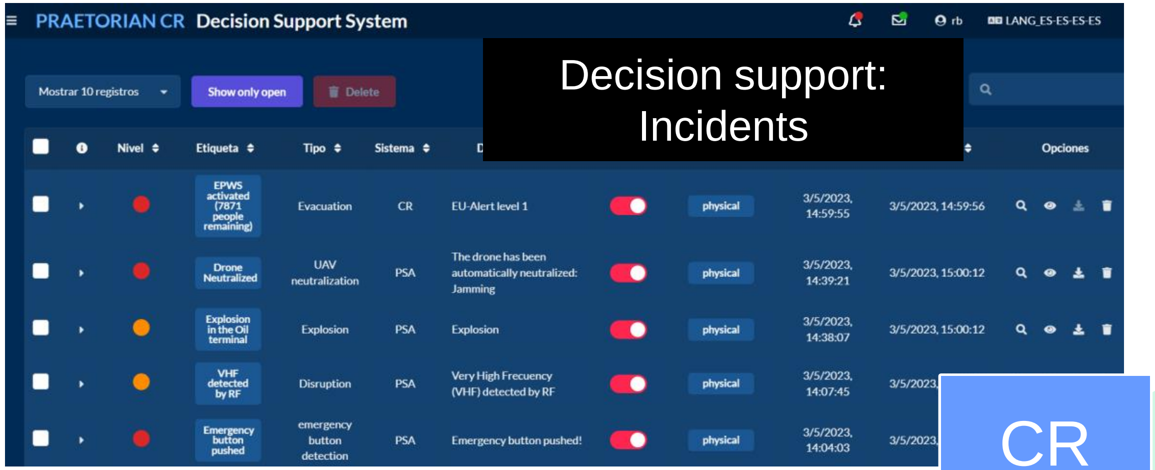


HSA




75% 300m
21.70°C 31.00% 1017.23mb 4.63m/s 16.00KM 923.70W/m2 0.00mm/hr
Open
39% 0m

PSA



≡ PRAETORIAN CR Decision Support System

rb LANG_ES-ES-ES-ES

Mostrar 10 registros ▾ | Show only open | Delete

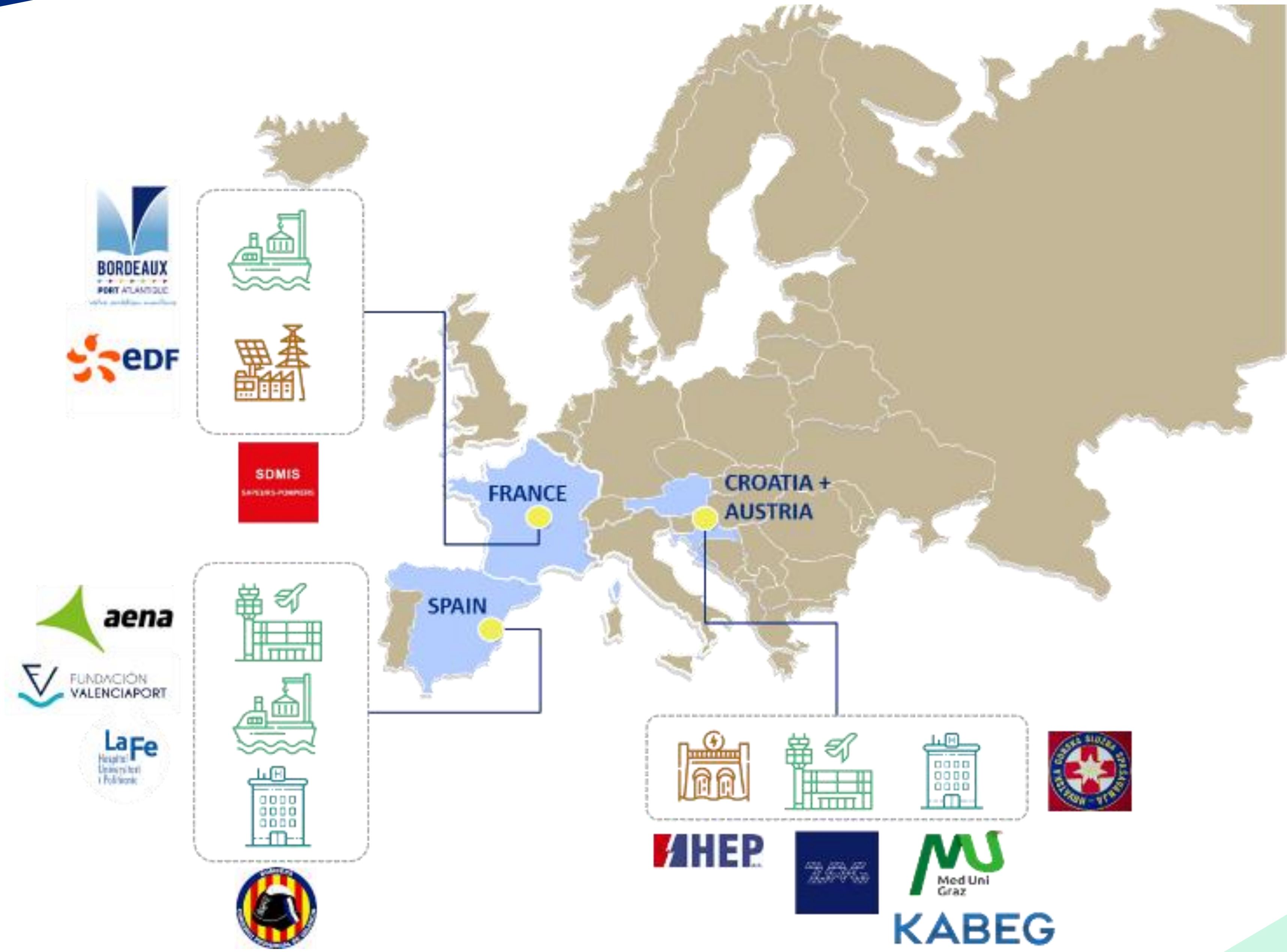
☐	ℹ	Nivel	Etiqueta	Tipo	Sistema	D					Opciones
☐	▸	🔴	EPWS activated (7871 people remaining)	Evacuation	CR	EU-Alert level 1		physical	3/5/2023, 14:59:55	3/5/2023, 14:59:56	
☐	▸	🔴	Drone Neutralized	UAV neutralization	PSA	The drone has been automatically neutralized: Jamming		physical	3/5/2023, 14:39:21	3/5/2023, 15:00:12	
☐	▸	🟠	Explosion in the Oil terminal	Explosion	PSA	Explosion		physical	3/5/2023, 14:38:07	3/5/2023, 15:00:12	
☐	▸	🟠	VHF detected by RF	Disruption	PSA	Very High Frecuency (VHF) detected by RF		physical	3/5/2023, 14:07:45	3/5/2023,	
☐	▸	🔴	Emergency button pushed	emergency button detection	PSA	Emergency button pushed!		physical	3/5/2023, 14:04:03	3/5/2023,	

Decision support: Incidents

CR

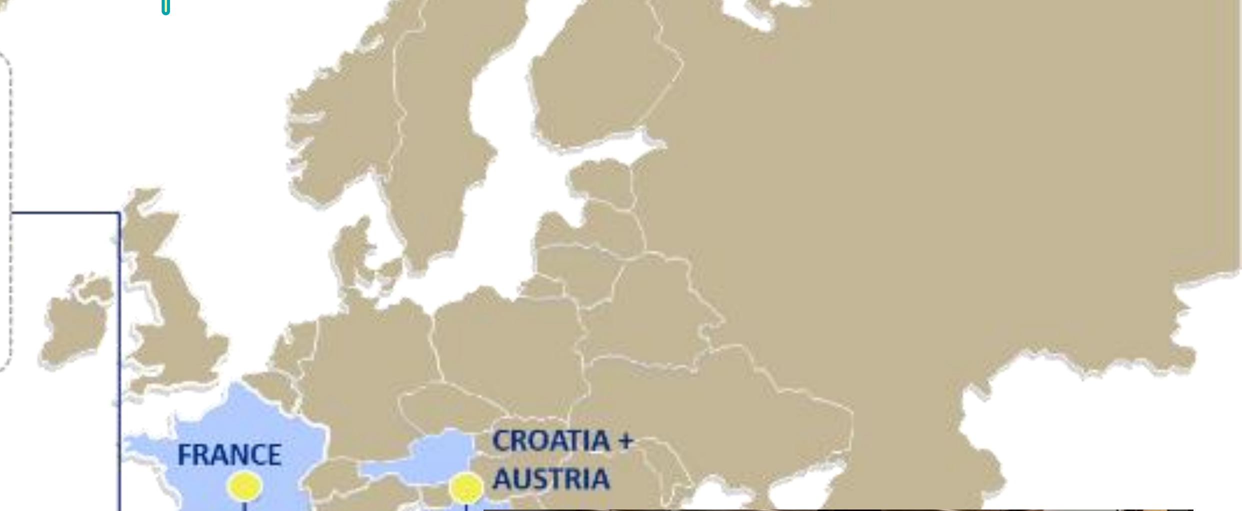
PRAETORIAN DEMO SITES

- 9 CI Operators
- 3 First Responders



Success story

- 9 CI Operators
- 3 First Responders



All recordings available at
PRAETORIAN YouTube channel

PRAETORIAN

Any questions or comments

Thank you!

Lazaros Papadopoulos - lpapadop@microlab.ntua.gr

https://praetorian-h2020.eu/

https://twitter.com/PraetorianH2020	@Praetorian2020
https://www.linkedin.com/company/praetorian-h2020	@praetorian-2020

This project has received funding from the European Union's Horizon 2020
Research and Innovation programme under Grant Agreement No 101021274

PRECINCT

Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats

PRESENTED BY.

Kevin Fleming (ICP, project coordinator)

Konnecta systems

Outline

01. PRECINCT Challenge & Vision

02. PRECINCT Digital Twin

03. Video Demonstration

04. Key Takeaways

01

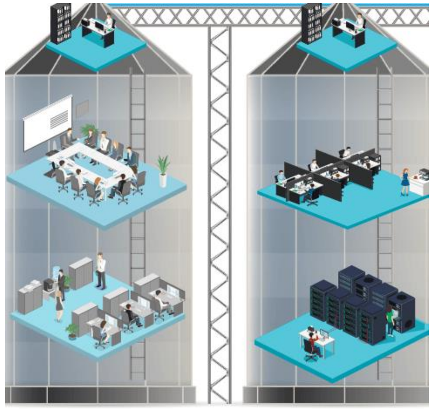
PRECINT
Challenge & Vision

PRECINCT

The Challenge

Lack of Information Connectivity across Critical Infrastructure systems

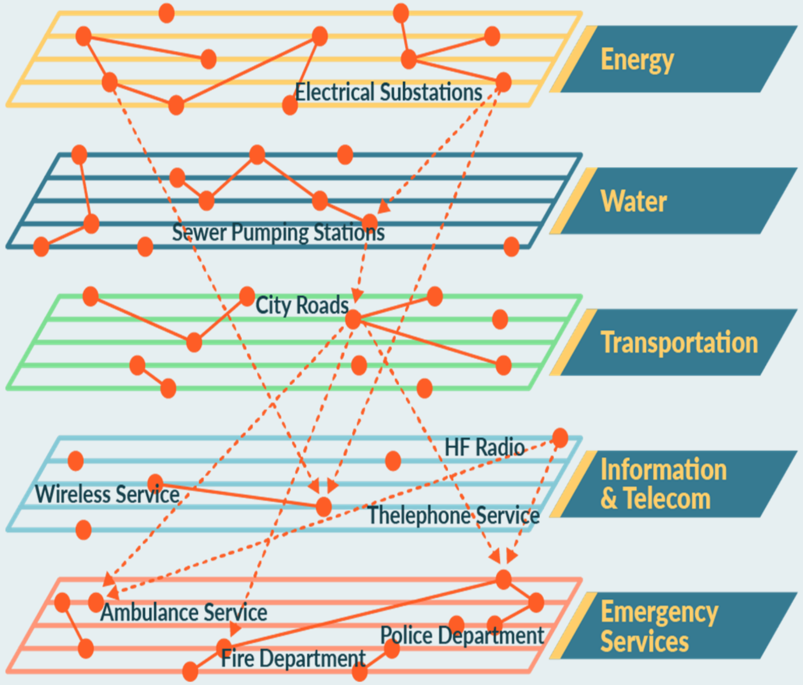
- ➢ Multiple stakeholders –> **siloed operations**
- ➢ Lack of **global situation awareness**
- ➢ Limited preparedness on **incident cascading effects** across systems



Information Silos

❑ Suboptimal **crisis management**

→ Siloed operations prevent **timely and coordinated response actions**



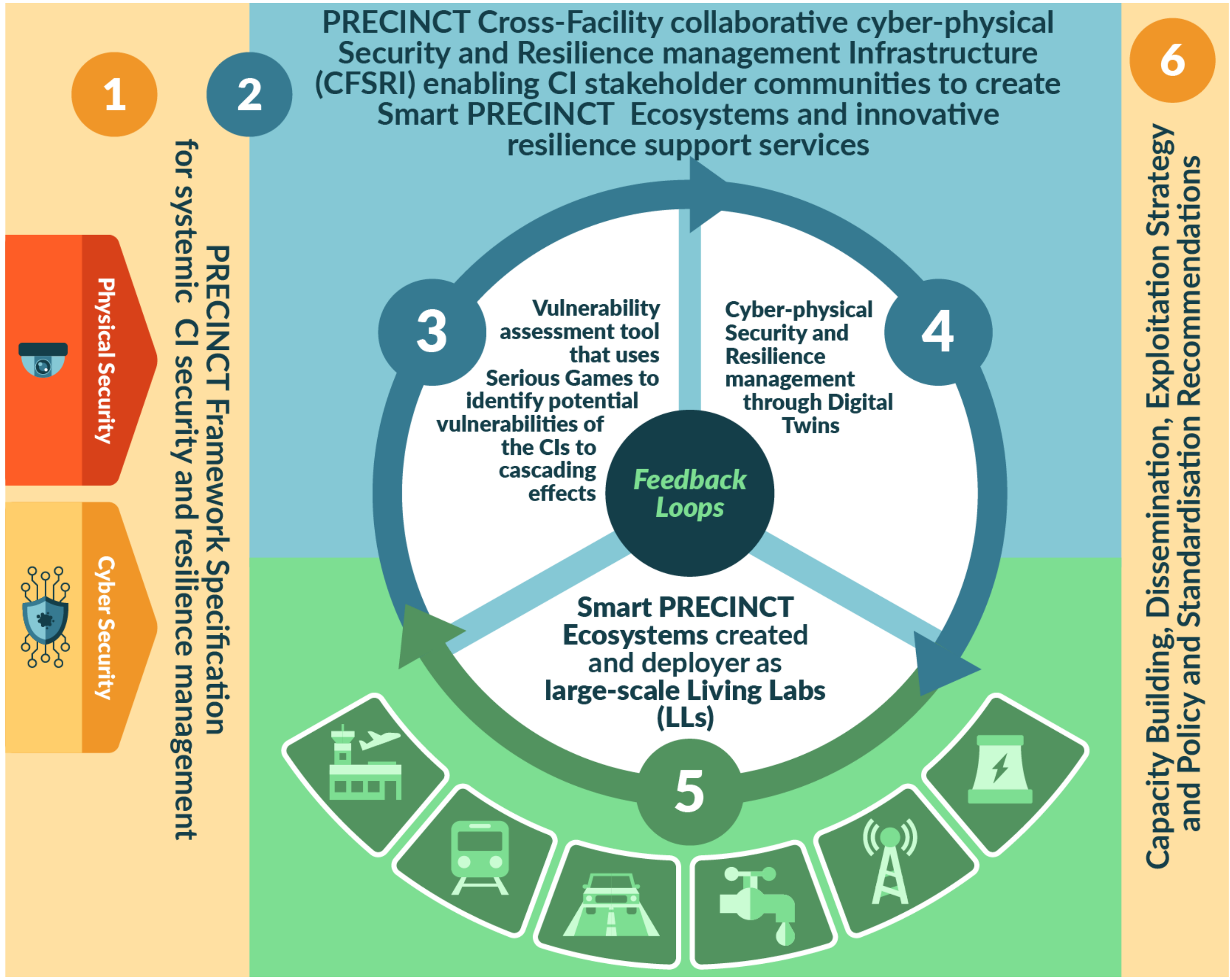
A single incident can have severe impact on multiple services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

PRECINCT Vision

- PRECINCT aims to **connect private and public CI stakeholders** in a geographical area to **a common cyber-physical security management approach** via **Digital Twins**

- **Enable interdependent CIs and Public authorities** to plan for, prevent, absorb, recover from and adapt efficiently and effectively to **cyber-physical threats / attacks** as well as **impede their cascading effects**.



1

Physical Security

Cyber Security

2

PRECINCT Framework Specification for systemic CI security and resilience management

PRECINCT Cross-Facility collaborative cyber-physical Security and Resilience management Infrastructure (CFSRI) enabling CI stakeholder communities to create Smart PRECINCT Ecosystems and innovative resilience support services

3

Vulnerability assessment tool that uses Serious Games to identify potential vulnerabilities of the CIs to cascading effects

4

Cyber-physical Security and Resilience management through Digital Twins

Feedback Loops

5

Smart PRECINCT Ecosystems created and deployer as large-scale Living Labs (LLs)

6

Capacity Building, Dissemination, Exploitation Strategy and Policy and Standardisation Recommendations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

PRECINCT partners

PRECINCT

Prometni institut Ljubljana d.o.o.
Institute of Traffic and Transport Ljubljana l.l.c.

POLITIE ANTWERPEN

BSC Barcelona Supercomputing Center
Centro Nacional de Supercomputación

FS TECHNOLOGY
GRUPPO FERROVIE DELLO STATO ITALIANE

EOS
EUROPEAN ORGANISATION FOR SECURITY

LPP
Zapelji se na www.lpp.si

ATHENS
INTERNATIONAL AIRPORT
ELEFTHERIOS VENIZELOS

KEMEA

Tallinn

POLIS
CITIES AND REGIONS FOR TRANSPORT INNOVATION

ITL
ISTITUTO sui TRASPORTI
e la LOGISTICA

Slovenske železnice

ICS INSTITUTE FOR CORPORATIVE SECURITY STUDIES

ATTIKO METRO S.A.

ATTIKES DIADROMES S.A.

AKKA
PASSION FOR TECHNOLOGIES

NUROGAMES

ENGINEERING

Elektro
Ljubljana

CONCEPTIVITY
360 SECURITY

R S

Aeroporto di Bologna
Aeroporto Guglielmo Marconi di Bologna S.p.A.

TelekomSlovenije

imec

UITP
ADVANCING PUBLIC TRANSPORT

VLTN

UCD DUBLIN

tecnalia Inspiring Business

lepida
CUP2000

montimage

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

inlecom

KU LEUVEN

dlr
Comhairle Contae County Council

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

CORTE
Confederation of Organisations in Road Transport Enforcement

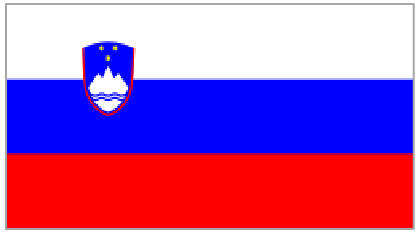
water-link

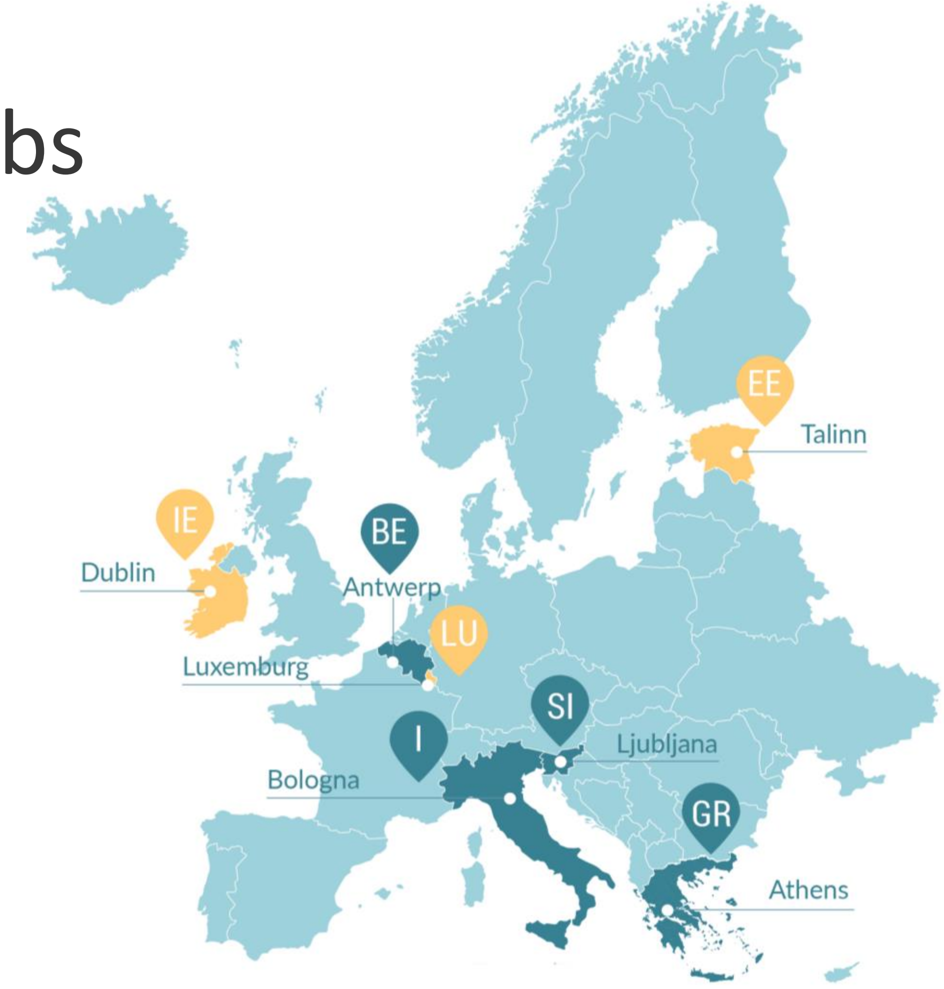
VIAS institute

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

PRECINCT Living Labs

PRECINCT





🟦 4 Precinct Living Labs

🟨 3 Transferability Demonstrators

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

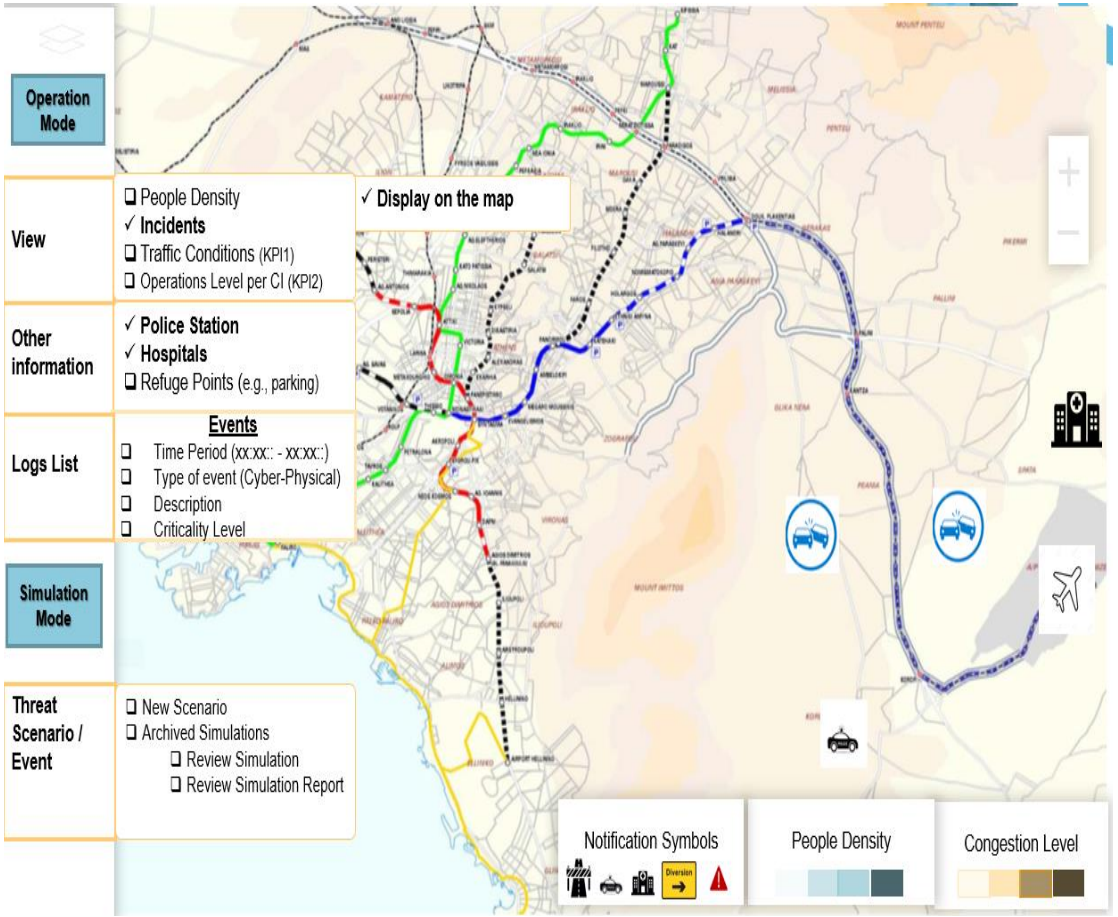
02

PRECINCT
Digital Twin

Digital Twin Goals

Build a software solution consolidating:

- ✓ Data across CIs in a **common representation**
- ✓ Inter-CI **incident dynamics**
- ✓ **Resilience** metrics
- ✓ **Incident detection & simulation** tools
- ✓ **Decision-support** for crisis management



View
- ❑ People Density
- ✓ **Incidents**
- ❑ Traffic Conditions (KPI1)
- ❑ Operations Level per CI (KPI2)

✓ **Display on the map**

Other information
- ✓ **Police Station**
- ✓ **Hospitals**
- ❑ Refuge Points (e.g., parking)

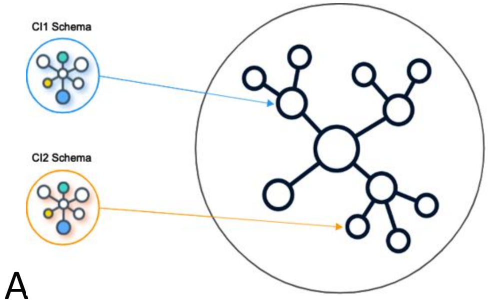
Logs List

Events
- ❑ Time Period (xx:xx:: - xx:xx::)
- ❑ Type of event (Cyber-Physical)
- ❑ Description
- ❑ Criticality Level

Threat Scenario / Event
- ❑ New Scenario
- ❑ Archived Simulations
  - ❑ Review Simulation
  - ❑ Review Simulation Report

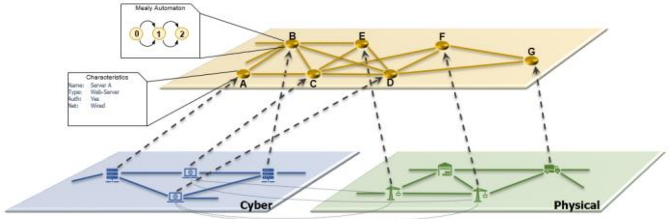
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

Building the Digital Twin



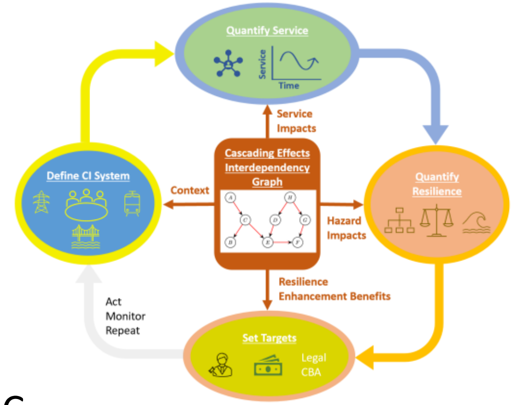
A

Define a **common representation** for CI data ingested from **different systems**



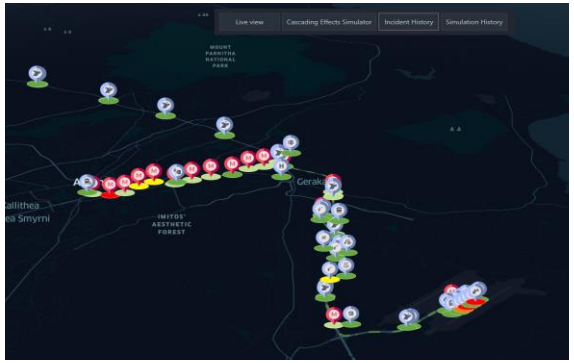
B

Model **incident dynamics** and **cascading effects** for simulations



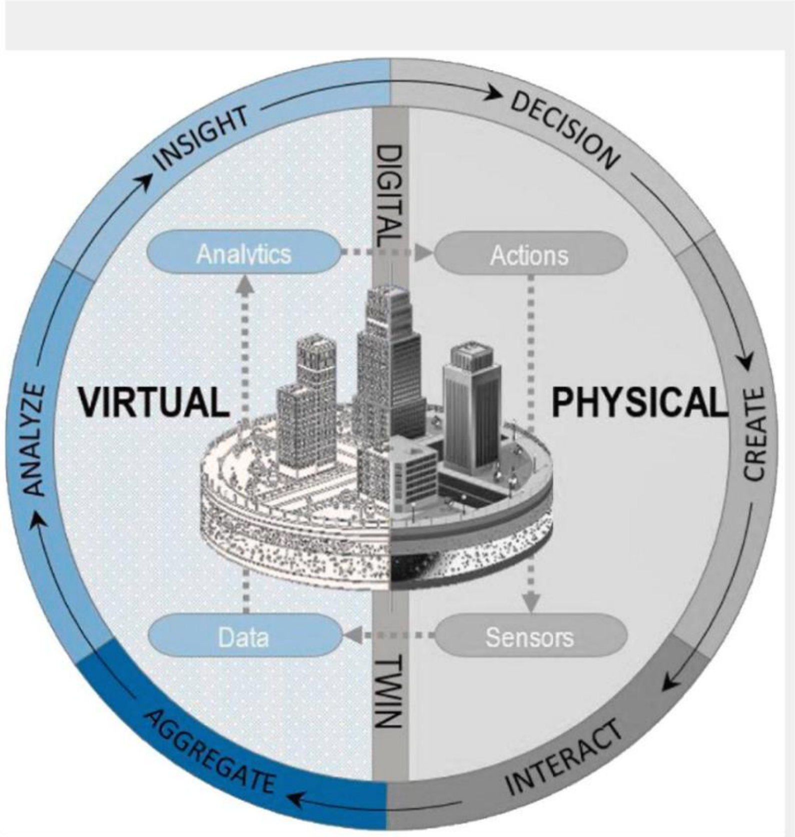
C

Quantify **operational resilience** for **decision-support**



D

Expose in **unifying user interface**



Digital Twin

Digital Twin Features

Live Situational Awareness

Simulation of Cascading Effects

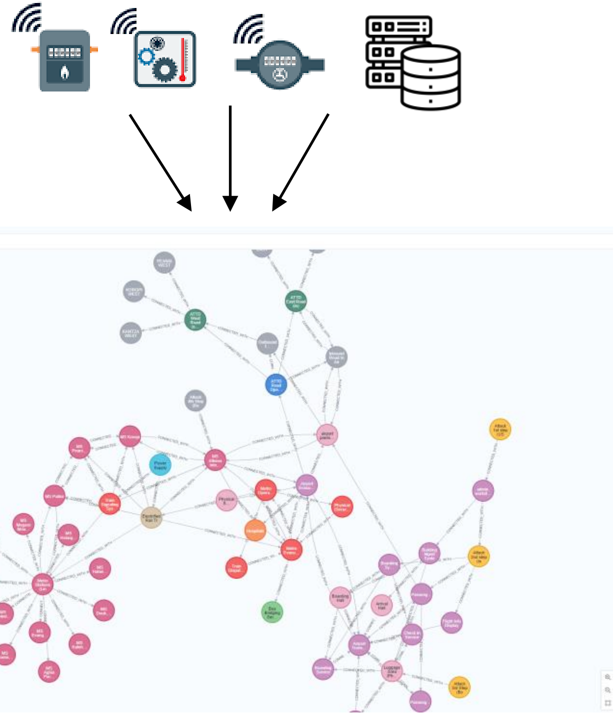
Incident Detection & Reporting

Decision-Support for Crisis Management

Live Situational Awareness

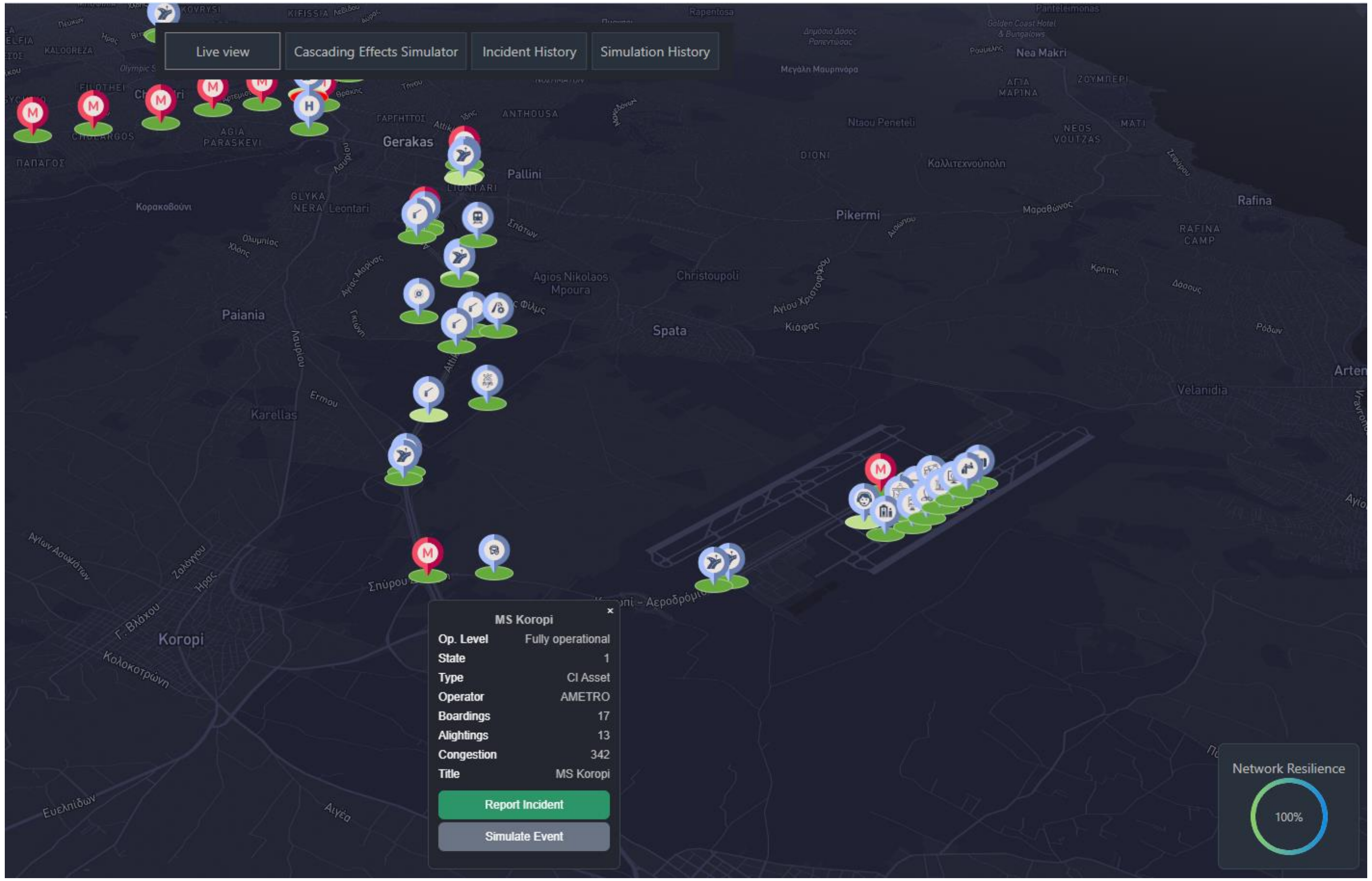
PRECINCT

CI Systems



neo4j

Multi-CI
Knowledge Graph



MS Koropi

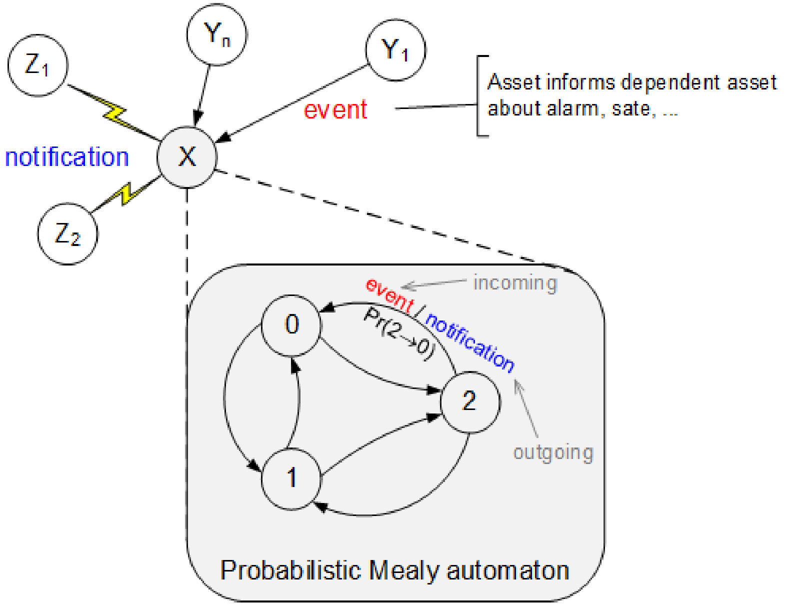
Op. Level	Fully operational
State	1
Type	CI Asset
Operator	AMETRO
Boardings	17
Alightings	13
Congestion	342
Title	MS Koropi

Digital Twin Dashboard

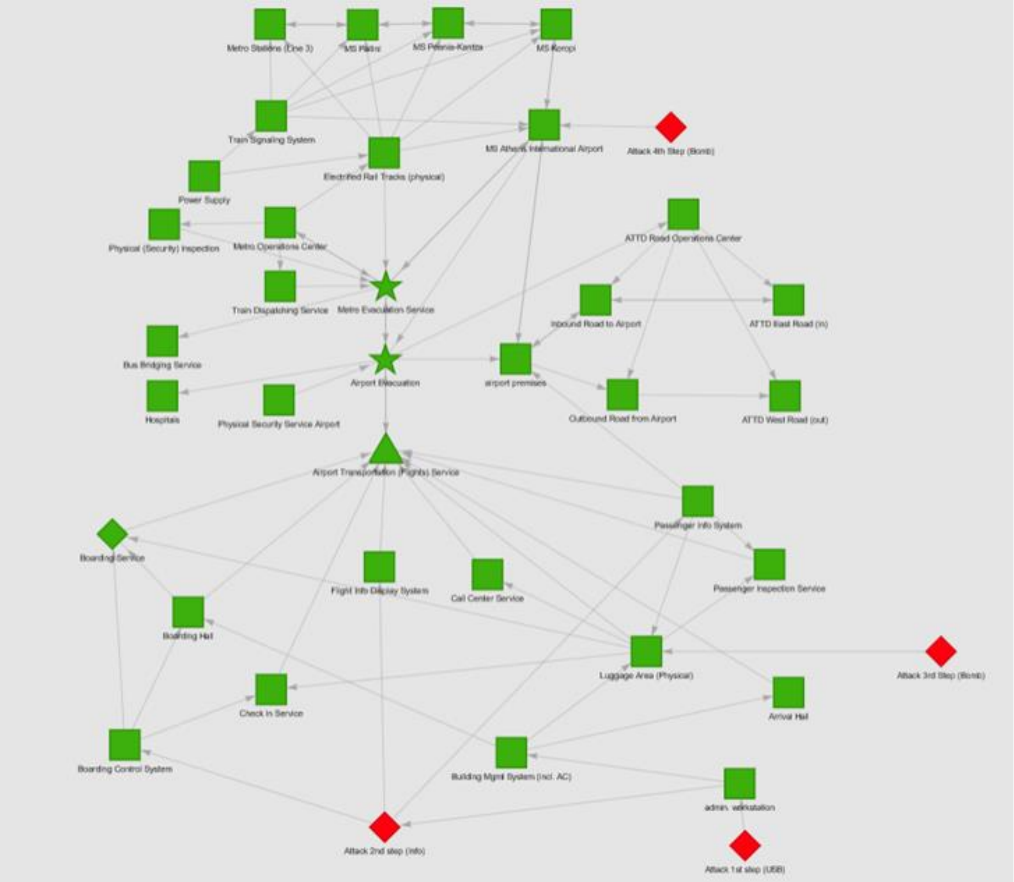
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

Simulation of Cascading Effects

- Building of **Interdependency Graph**


Z₁
Yₙ
Y₁
X
Z₂
notification
event
Asset informs dependent asset about alarm, sate, ...
incoming
event / notification
Pr(2→0)
0
1
2
outgoing
Probabilistic Mealy automaton

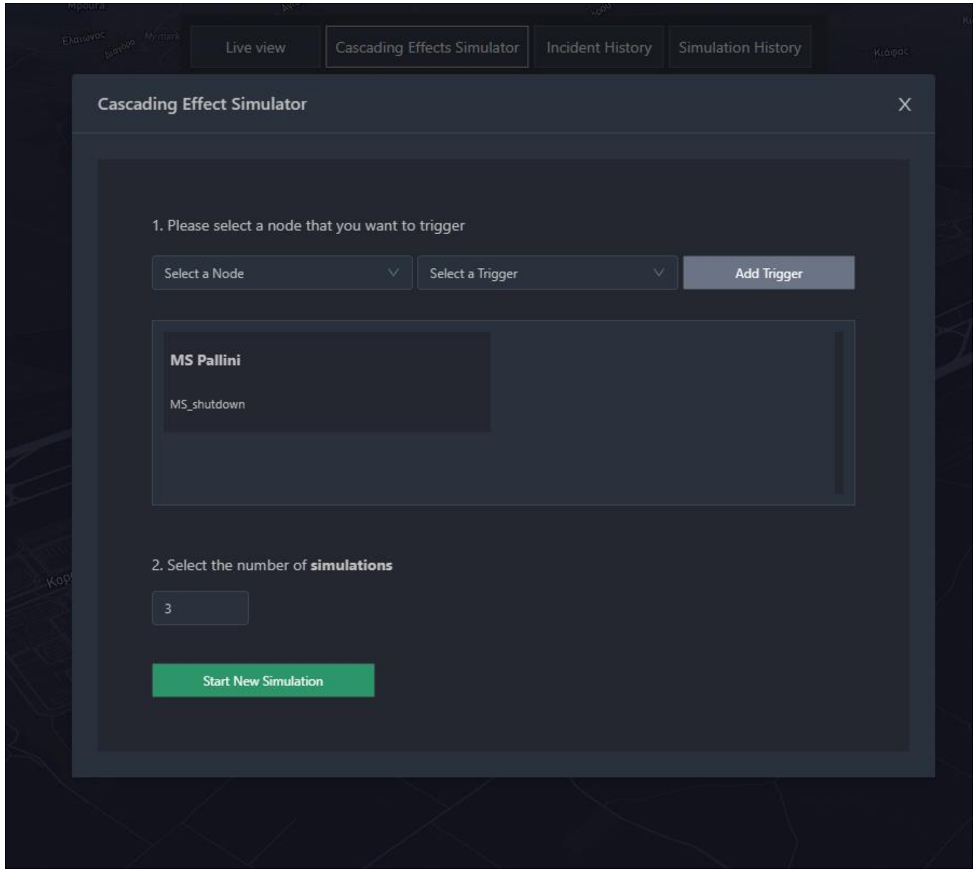
Modelling of incident propagation



Graph of CI assets and their interdependencies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

Simulation of Cascading Effects



Cascading Effect Simulator

1. Please select a node that you want to trigger

Select a Node | Select a Trigger | Add Trigger

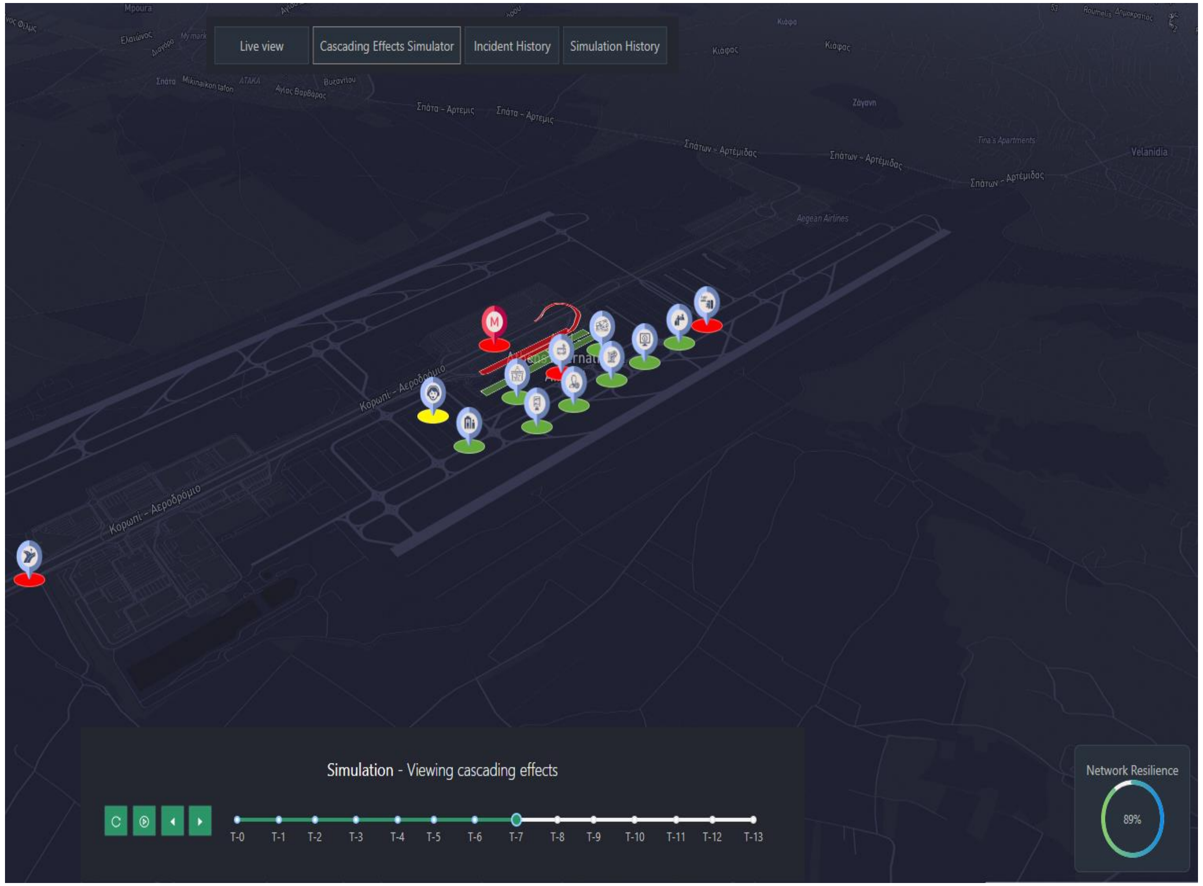
MS Pallini

MS_shutdown

2. Select the number of **simulations**

3

Start New Simulation

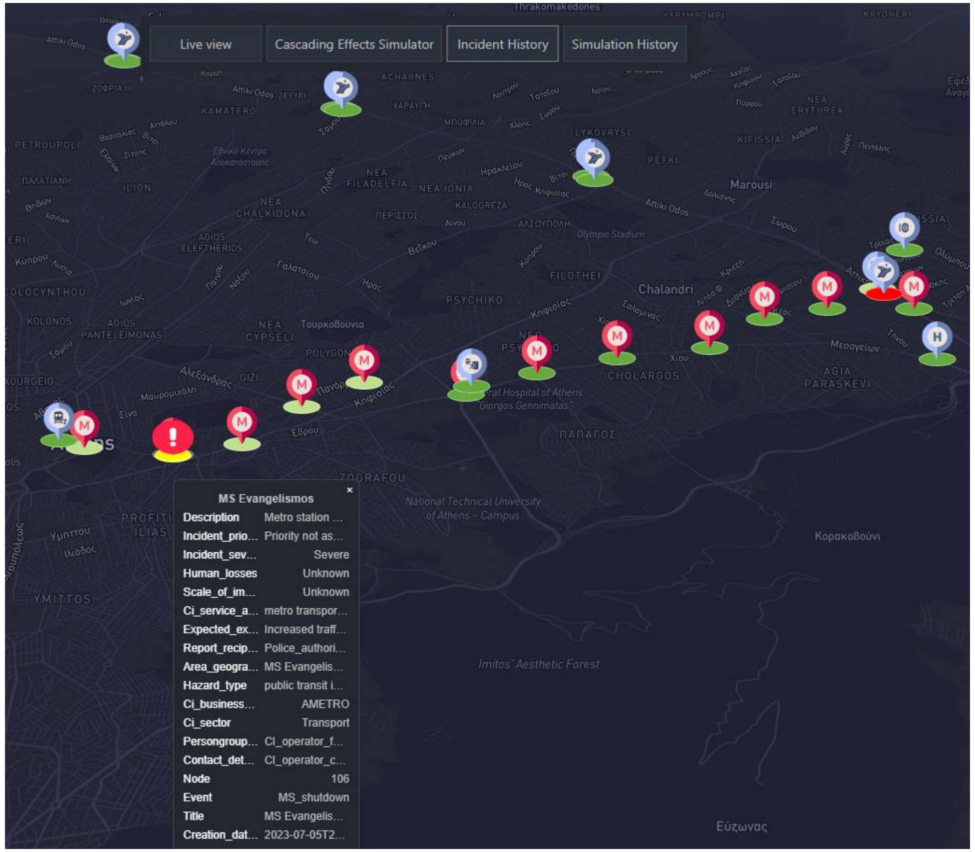


- ✓ Simulation parameterization
- ✓ Visualization of Cascading Effects

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

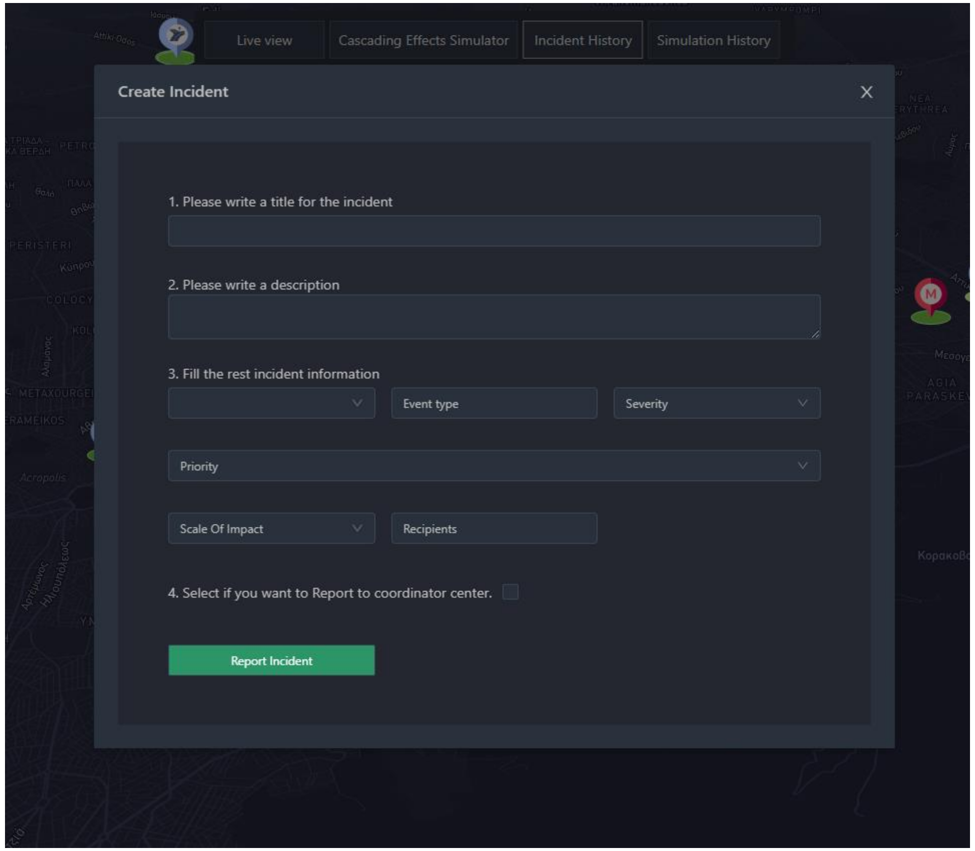
Incident Detection & Reporting

PRECINCT



MS Evangelismos

Description	Metro station ...
Incident_prio...	Priority not as...
Incident_sev...	Severe
Human_losses	Unknown
Scale_of_im...	Unknown
Ci_service_a...	metro transpor...
Expected_ex...	Increased traff...
Report_recip...	Police_authori...
Area_geogra...	MS Evangelis...
Hazard_type	public transit i...
Ci_business...	AMETRO
Ci_sector	Transport
Persongroup...	CI_operator_f...
Contact_det...	CI_operator_c...
Node	106
Event	MS_shutdown
Title	MS Evangelis...
Creation_dat...	2023-07-05T2...



Create Incident ×

1. Please write a title for the incident

2. Please write a description

3. Fill the rest incident information

Event type

Severity

Priority

Scale Of Impact

Recipients

4. Select if you want to Report to coordinator center. □

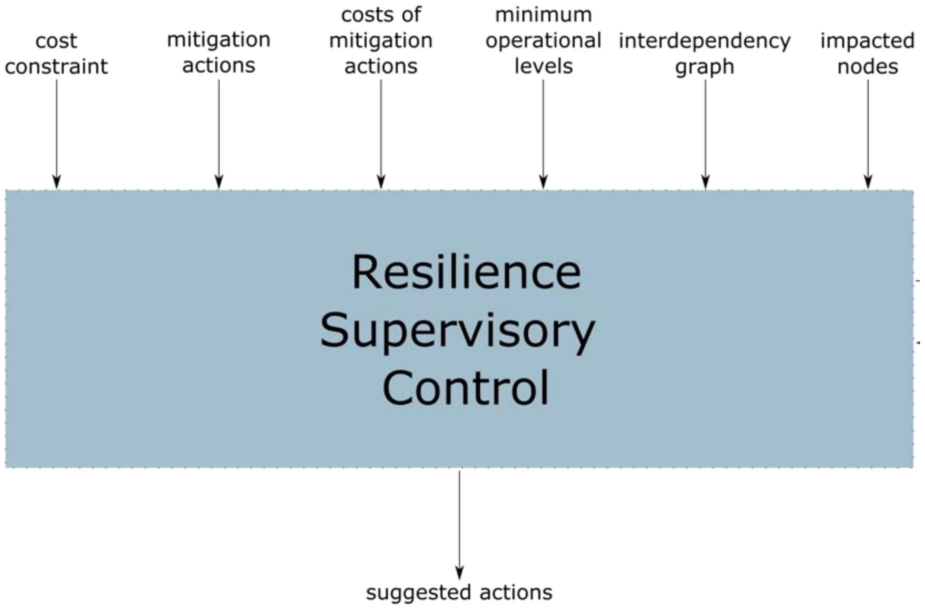
Report Incident

- ✓ Incidents detected by PRECINCT security monitoring tools

- ✓ Manual reporting of incidents by CI operators

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

Decision-Support in Crisis Management



cost constraint

mitigation actions

costs of mitigation actions

minimum operational levels

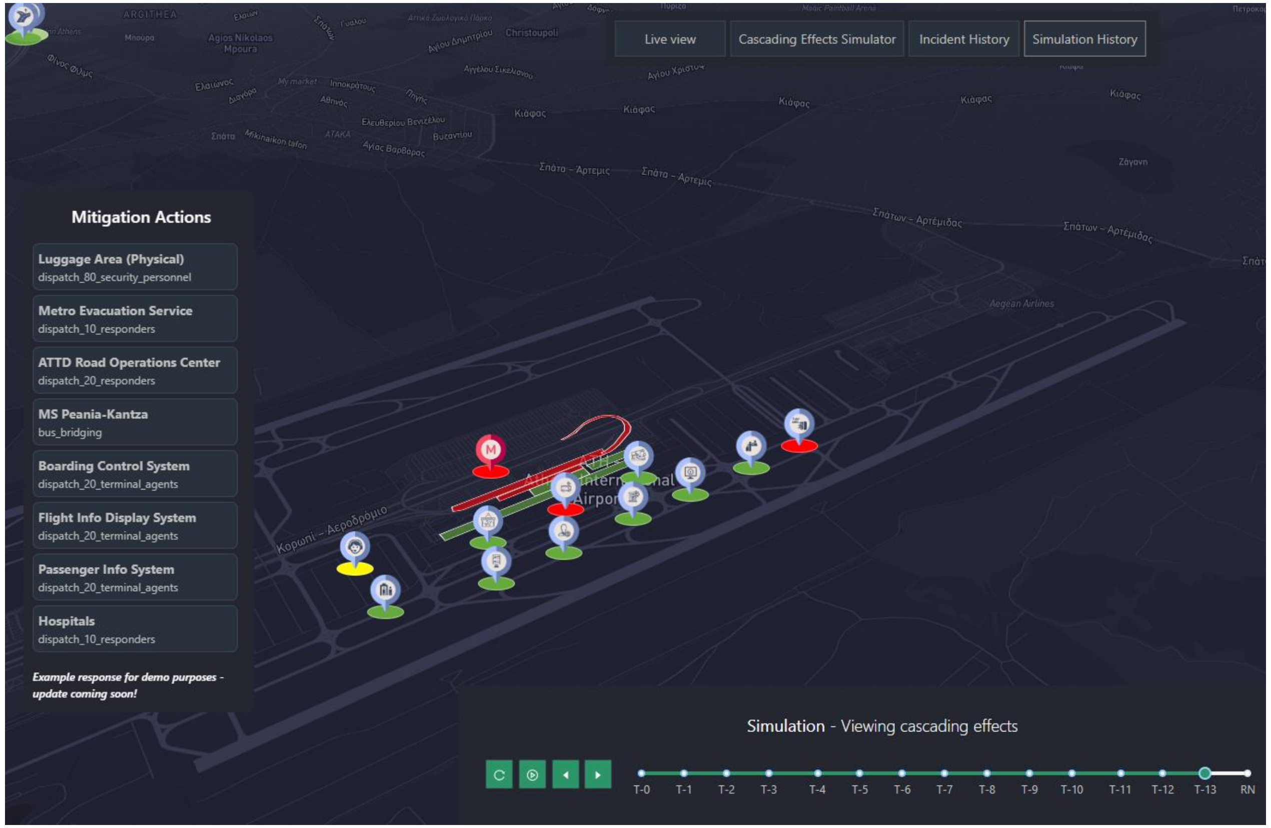
interdependency graph

impacted nodes

Resilience Supervisory Control

suggested actions

- ✓ Calculation of optimal mitigation actions to restore resilience



Mitigation Actions

Luggage Area (Physical)
dispatch_80_security_personnel

Metro Evacuation Service
dispatch_10_responders

ATTD Road Operations Center
dispatch_20_responders

MS Peania-Kantza
bus_bridging

Boarding Control System
dispatch_20_terminal_agents

Flight Info Display System
dispatch_20_terminal_agents

Passenger Info System
dispatch_20_terminal_agents

Hospitals
dispatch_10_responders

Example response for demo purposes - update coming soon!

- ✓ Feature integrated in the CI DT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

03

Video Demonstration

PRECINCT

PRECINCT LL3 - Athens Digital Twin

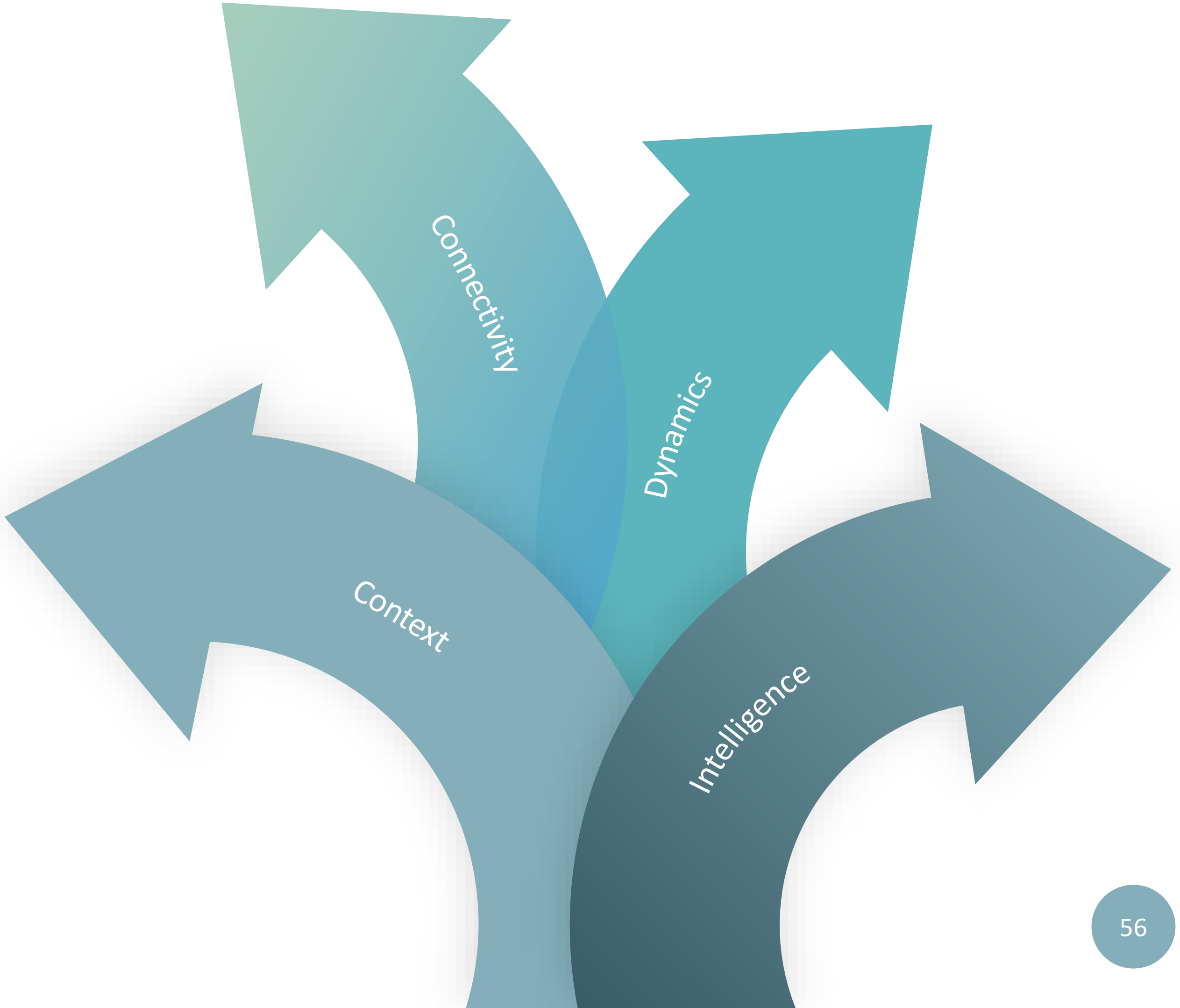
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 101021668.

04

Key Takeaways

Key Takeaways

- Significant value lies in **bridging the silos** and leveraging **inter-system dynamics**
- CI systems are **highly interconnected**; optimal **operational resilience** depends on achieving **connected intelligence**
- The **PRECINCT** project tackles the above by building a **unifying DT framework** for CIs, focused on **cyber-physical threats**



Questions

Thank you

THE END