



HELLENIC REPUBLIC  
Ministry of Citizen Protection



# CENTER FOR SECURITY STUDIES (KEMEA)

*"Global Catastrophic Risks"*  
Conference  
3-4/4/2025

**Manolis Kermitsis**

Head of Emergency Management  
& Civil Protection Sector





## Mission

The Research Center of the Hellenic Ministry of Citizen Protection (MCP) operates as a think tank of innovation and technology in the area of national security policies (cyber and physical), emergency management and civil protection.

National contact point with EC for ECIP (PD 39/2011)



## Objectives

- ✓ Consultation and scientific & technical support for the technological transformation of the MCP services.
- ✓ R&D on modern operational security solutions (Research Projects & Studies)
- ✓ Training of the operational services of the MCP and of other public or private bodies related to security and civil protection. Professional Certification of Private Security Personnel.



## Foundation Year



# KEMEA SECTORS

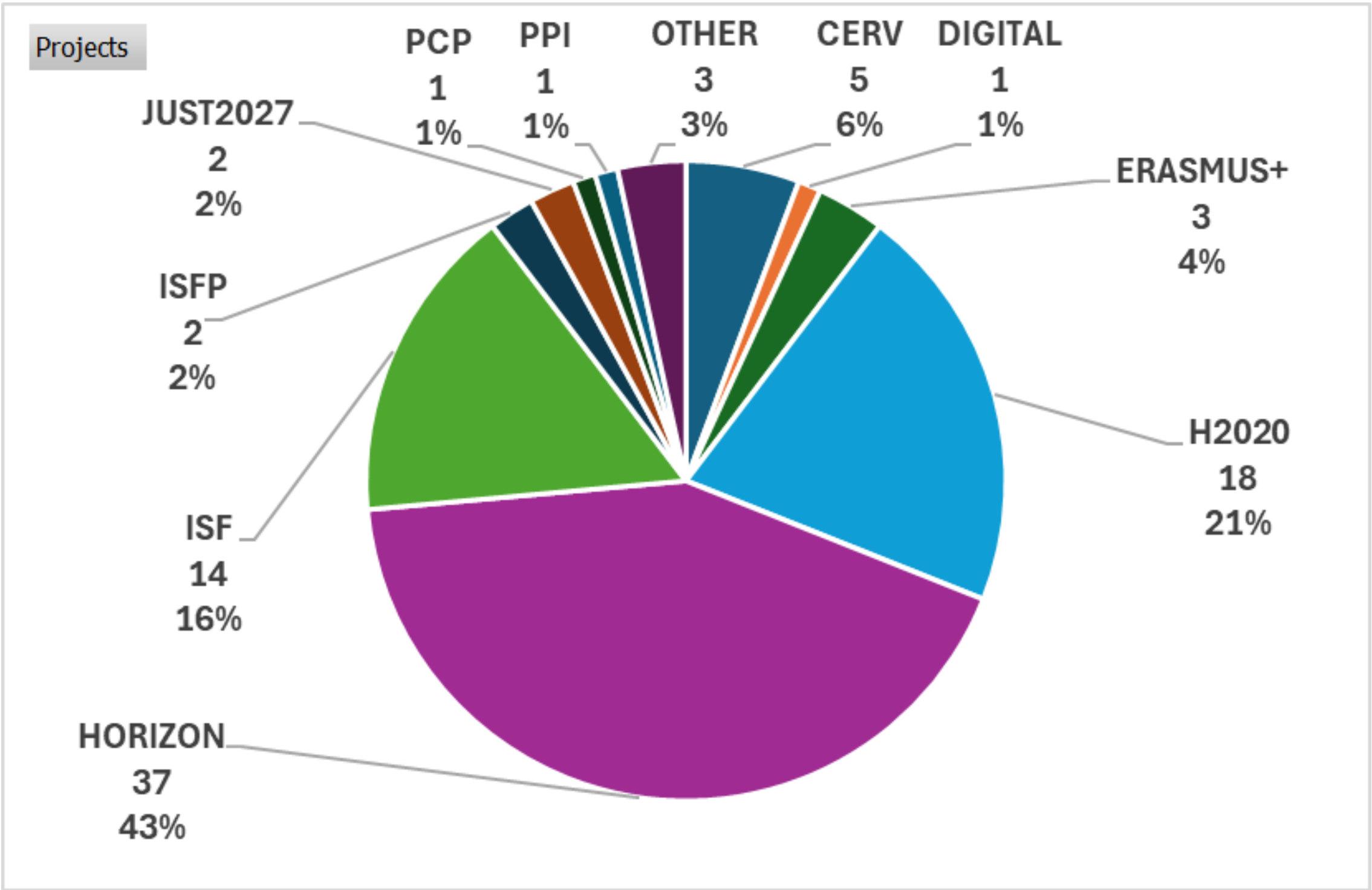
- 1 Border Security & Control (BES)
- 2 Emergency Management and Civil Protection (DRS)
- 3 Critical Infrastructure Protection (INFRA)
- 4 Anticrime Policy (FCT)
- 5 Cybersecurity (DS)
- 6 Institute of International Network and the study of extremism and terrorism (Radicalization)
- 7 Training & Professional Certification
- 8 Administrative Support



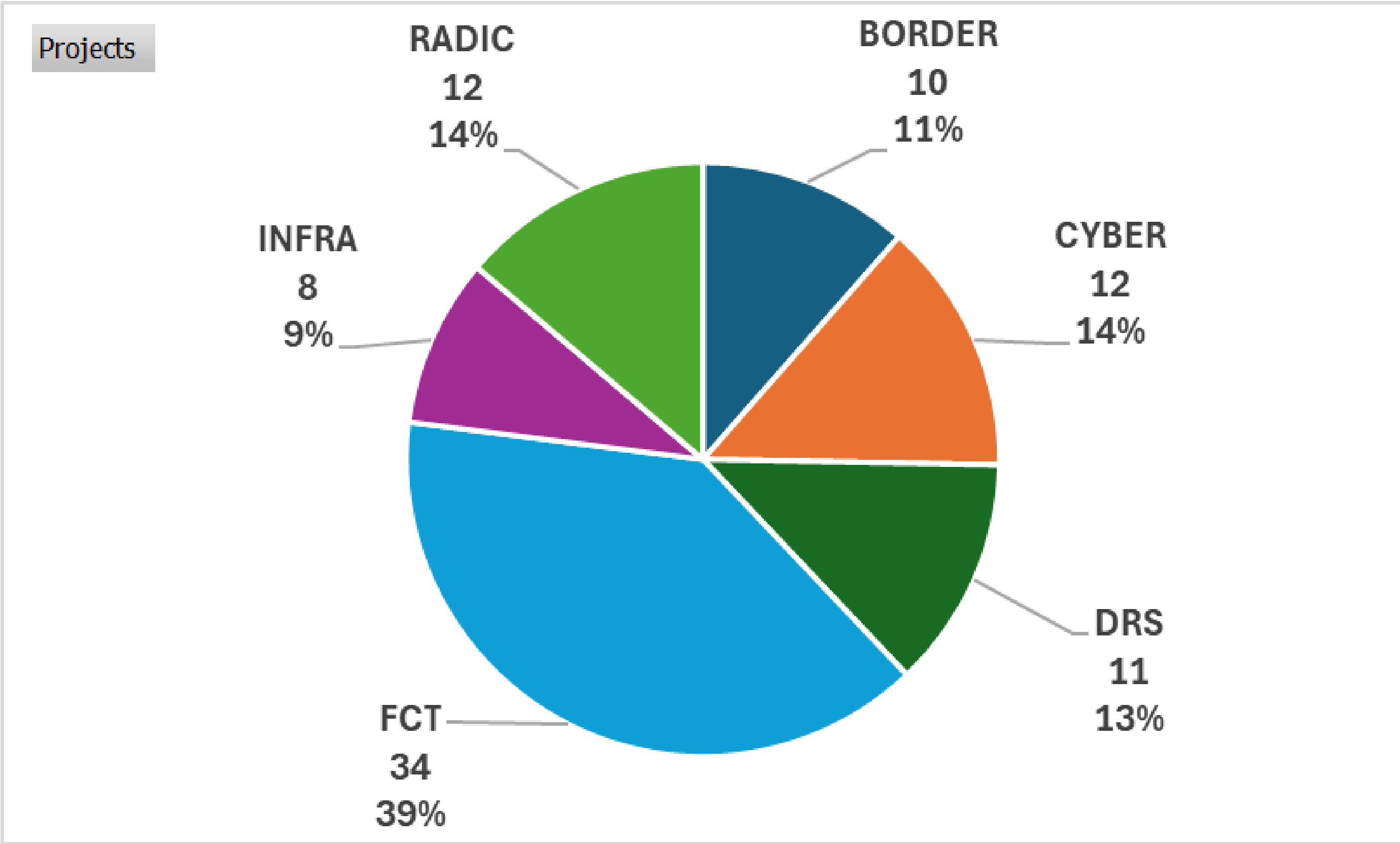
# KEMEA active projects distribution

## Per Programme

Total No of Projects (2024) : 87



## Per Sector/Topic



Funded by European Union Civil Protection and Humanitarian Aid



Erasmus+

Interreg





## KEMEA's INVOLVEMENT IN RESEARCH PROJECTS

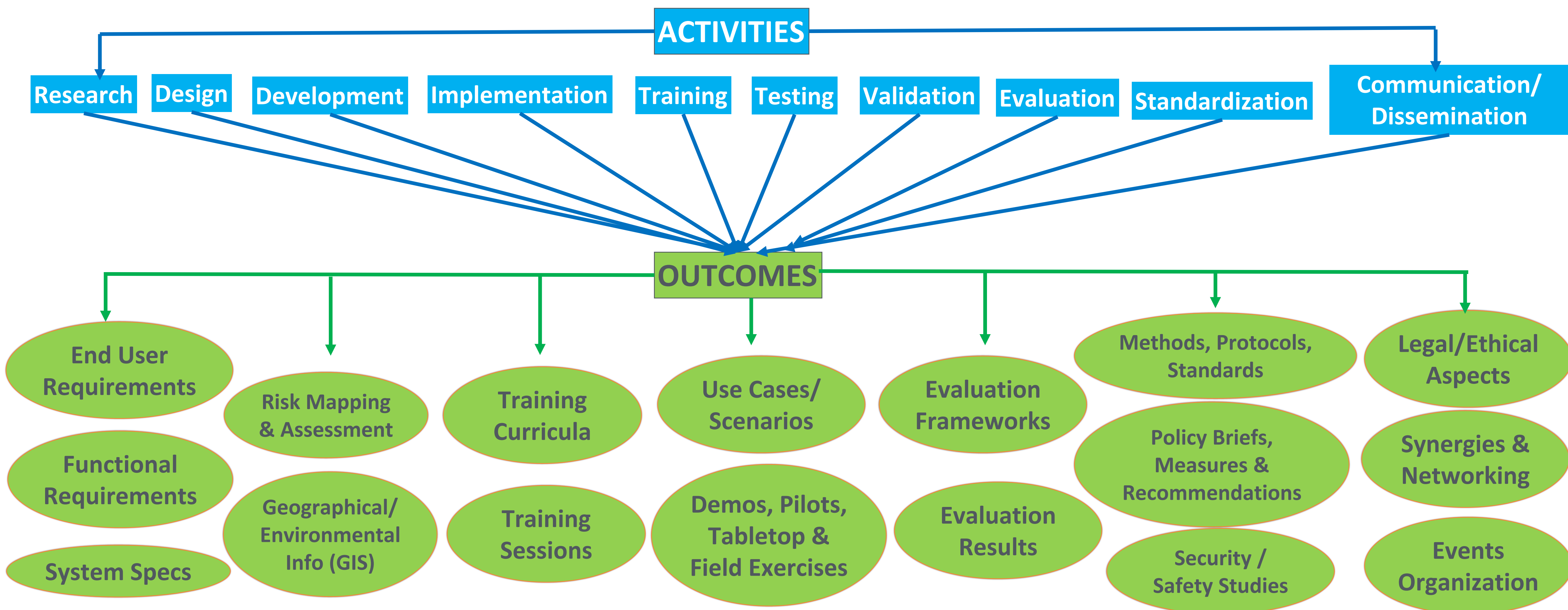
- End User and System Requirements
- Functional and Operational Analysis
- Training Curricula, Workshops & Hands-On Practicing
- Demonstrations, Pilots, Tabletop & Field-Testing Exercises
- Evaluations and Assessments
- Legal, Ethical and Societal Issues
- Communication, Dissemination and Exploitation
- Project Management





# EMERGENCY MANAGEMENT & CIVIL PROTECTION SECTOR

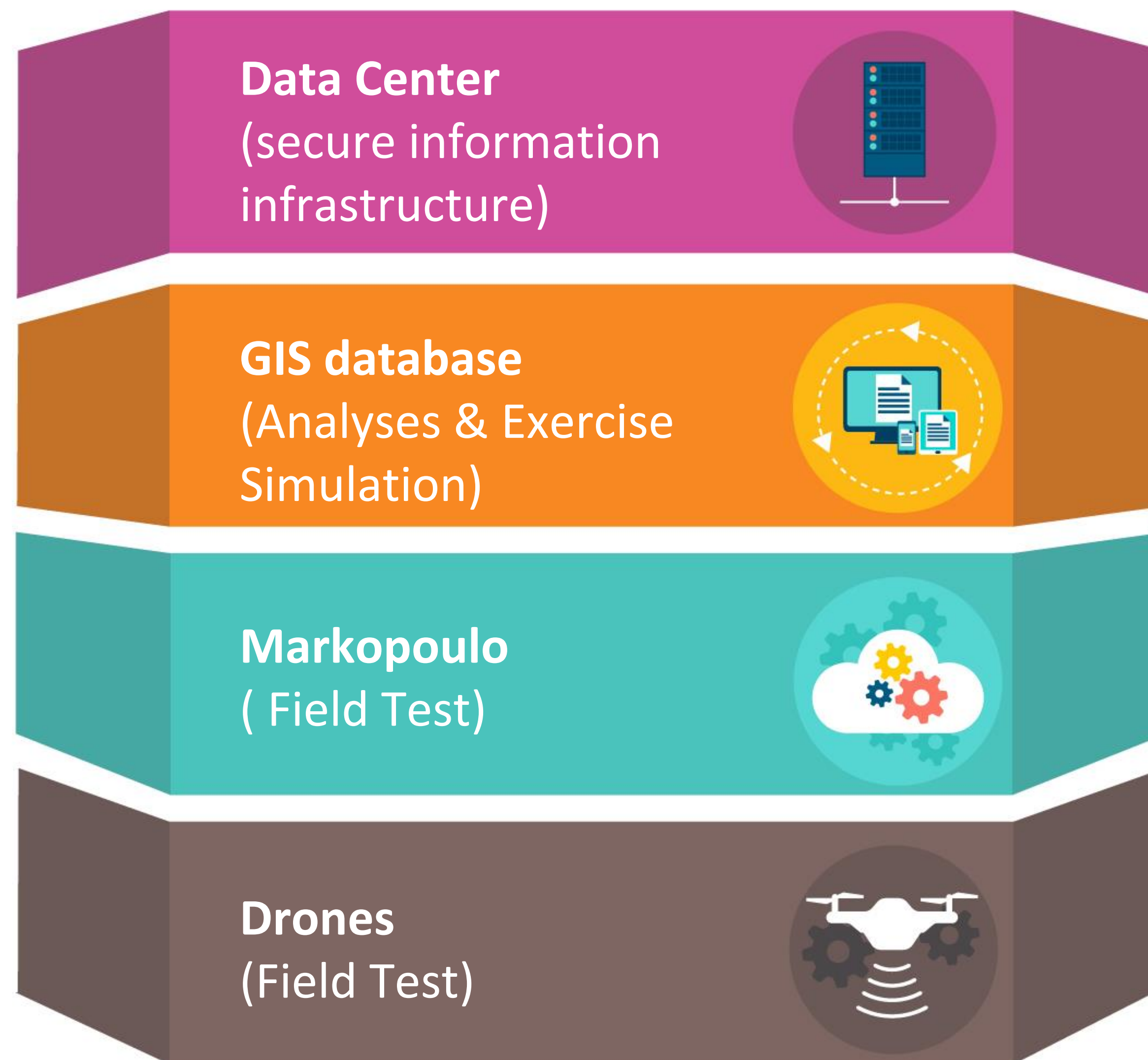
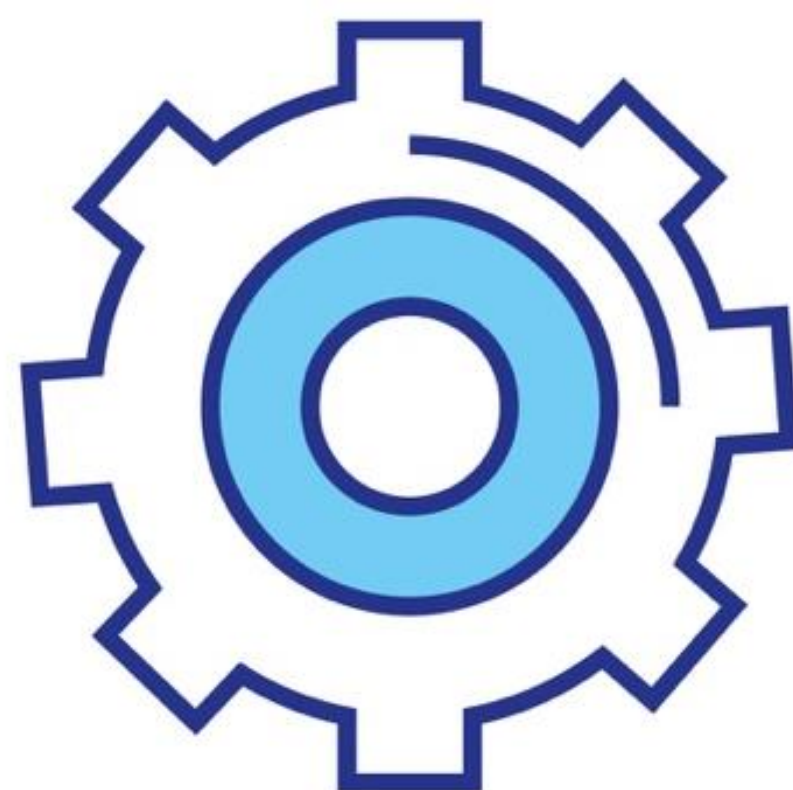
## Activities & Outcomes





# MODERN INFRASTRUCTURE

&  
EQUIPMENT







## Disaster Resilience and Civil Protection related EU Projects



<https://www.direktion-network.org/>



<https://www.enovation-project.eu/>



<https://firelogue.eu/>

<https://fire-in.eu/>



<https://www.eo4eu.eu/>



<https://civil-protection-knowledge-network.europa.eu/projects/collaris-network>



<https://www.riskpacc.eu/>



PANTHEON

<https://pantheon-project.eu/>



<https://tema-project.eu/>



<https://drmframeproject.eu/>



**STRATEGY**  
Interoperability for crisis management

<https://strategy-project.eu/>



**VALKYRIES**





HELLENIC REPUBLIC  
Ministry of Citizen Protection



# Thank you for your Attention!

Manolis Kermitsis, *Head of the Emergency Management & Civil Protection Sector*  
[m.kermitsis@kemea-research.gr](mailto:m.kermitsis@kemea-research.gr)

© KE.ME.A. 2025



[www.kemea.gr](http://www.kemea.gr)



[kemea@kemea.gr](mailto:kemea@kemea.gr)



HELLENIC REPUBLIC  
Ministry of Citizen Protection



# CRITICAL INFRASTRUCTURE PROTECTION

*“Global Catastrophic Risks”*  
Conference  
3-4/4/2025

Efstathios Skarlatos Meng, MSc

Head of Critical Infrastructure Protection Sector

CENTER FOR SECURITY STUDIES - KEMEA





## Critical Infrastructures

# An introduction to Critical Infrastructure Protection

- What is a Critical Infrastructure (CI) and what makes it important
- What are we trying to protect the CI's from
- What tools we have
- What challenges occur



# Critical Infrastructures



## Definition of a Critical Infrastructure and Critical Entities.



An asset, system or part thereof located in Member States which is **essential for the maintenance of vital societal functions**:

- **Health**
- **Safety**
- **Security**
- **Economic or social well-being of people**

and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

*«Directive 2008/114/EC»*



Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. it shall take into account the outcomes of its Member State risk assessment and its strategy and shall apply all of the following criteria:

- **the entity provides one or more essential services;**
- **the entity operates, and its critical infrastructure is located, on the territory of that Member State; and**
- **an incident would have significant disruptive effects,** as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.

*«Directive 2022/2557/EU»*



# Critical Infrastructure

vital to the functioning of a society and its economy  
such as:

- Energy
- Telecommunications
- Transportation
- Water supply
- Healthcare
- Financial services, and
- Government services

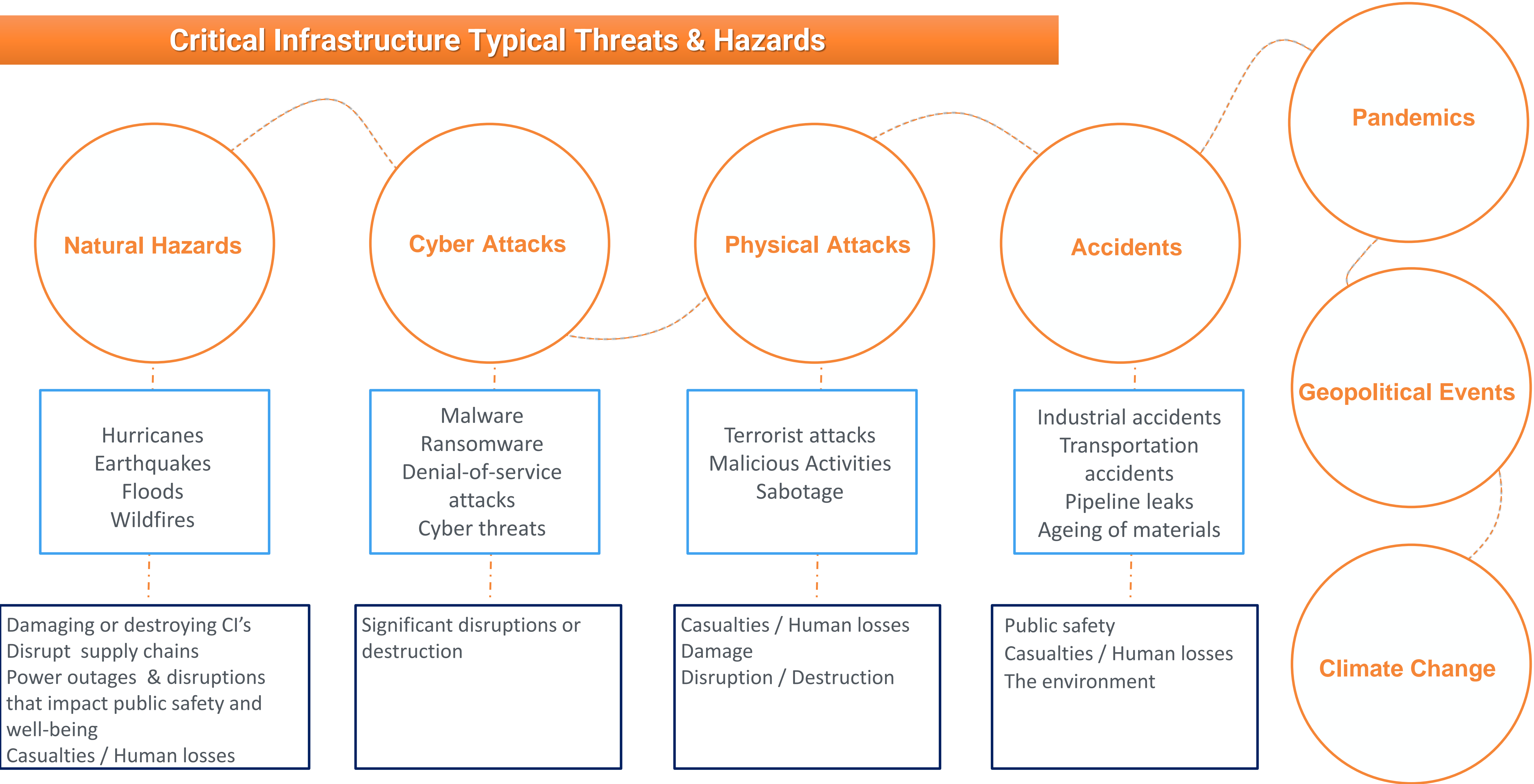
# Critical Entity

play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy.:

- Energy,
- Transport,
- Banking,
- Financial market infrastructure,
- Health,
- Drinking water,
- Waste water,
- Digital infrastructure,
- Public administration,
- Space,
- Production, processing and distribution of food



# Critical Infrastructure Typical Threats & Hazards







## Typical Factors influencing Threats and Hazards of CI's (with examples)

### Location:

- CI's highly exposed in hurricane prone, storm surge, and sea level rise areas (e.g. coastal areas), may be more vulnerable.
- CI's in seismic zones may be more vulnerable to earthquakes.
- CI's located in areas with a high risk of wildfires may be more vulnerable to those types of hazards.

### Sector:

- The energy sector may be vulnerable to cyberattacks targeting oil and gas pipelines.
- The financial sector may be vulnerable to cyberattacks targeting banking and financial systems.
- The transportation sector may be vulnerable to accidents and cyberattacks affecting airplanes, trains, or other modes of transportation.

### Criticality:

- Critical infrastructure that is essential for maintaining public safety and well-being, such as hospitals and water treatment plants, may be more vulnerable to targeted attacks or sabotage than infrastructure that is less critical.

### Interconnectivity:

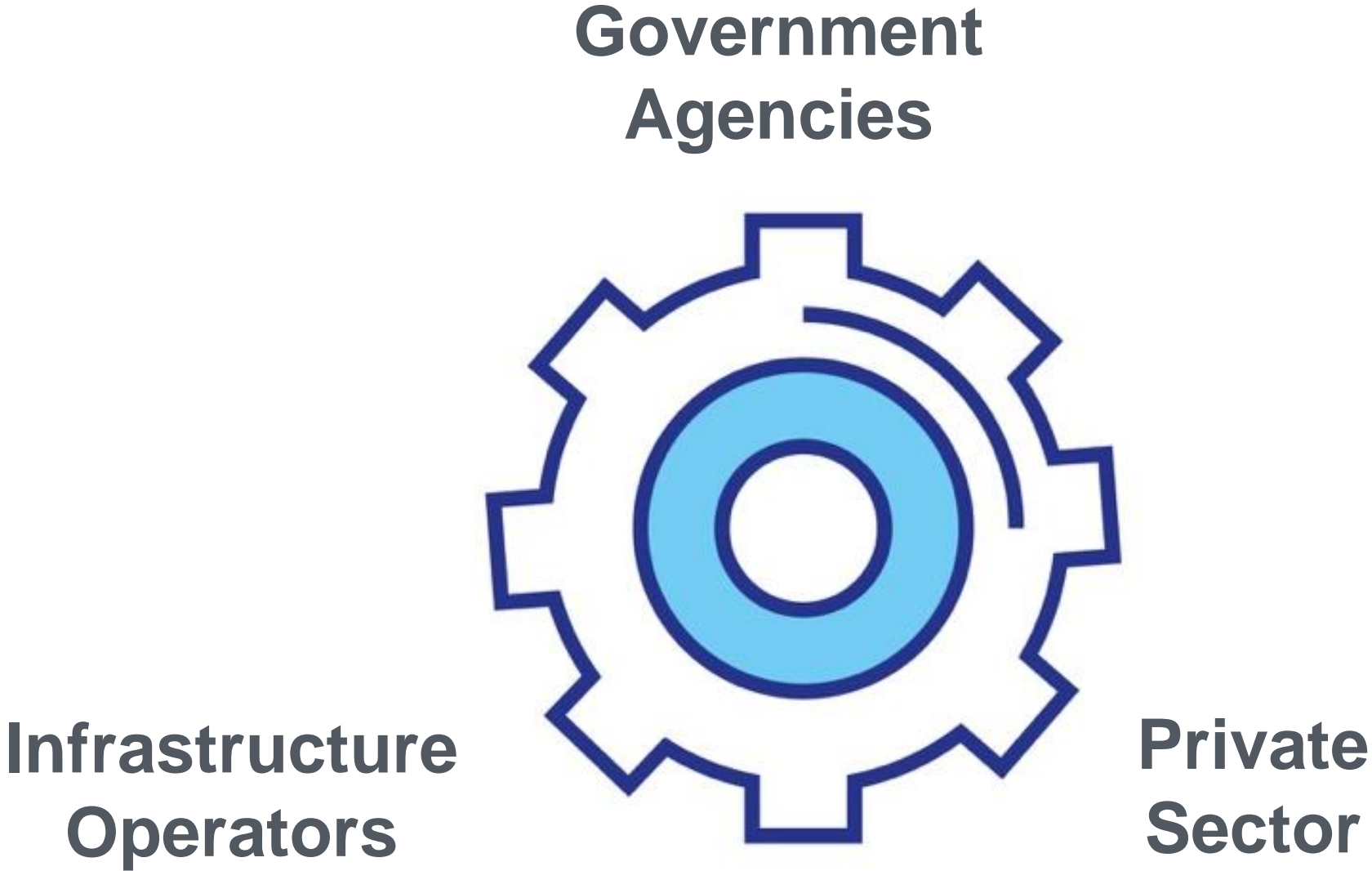
- A cyberattack targeting one critical infrastructure system may have ripple effects on other interconnected systems, potentially causing widespread disruptions.

### Resilience:

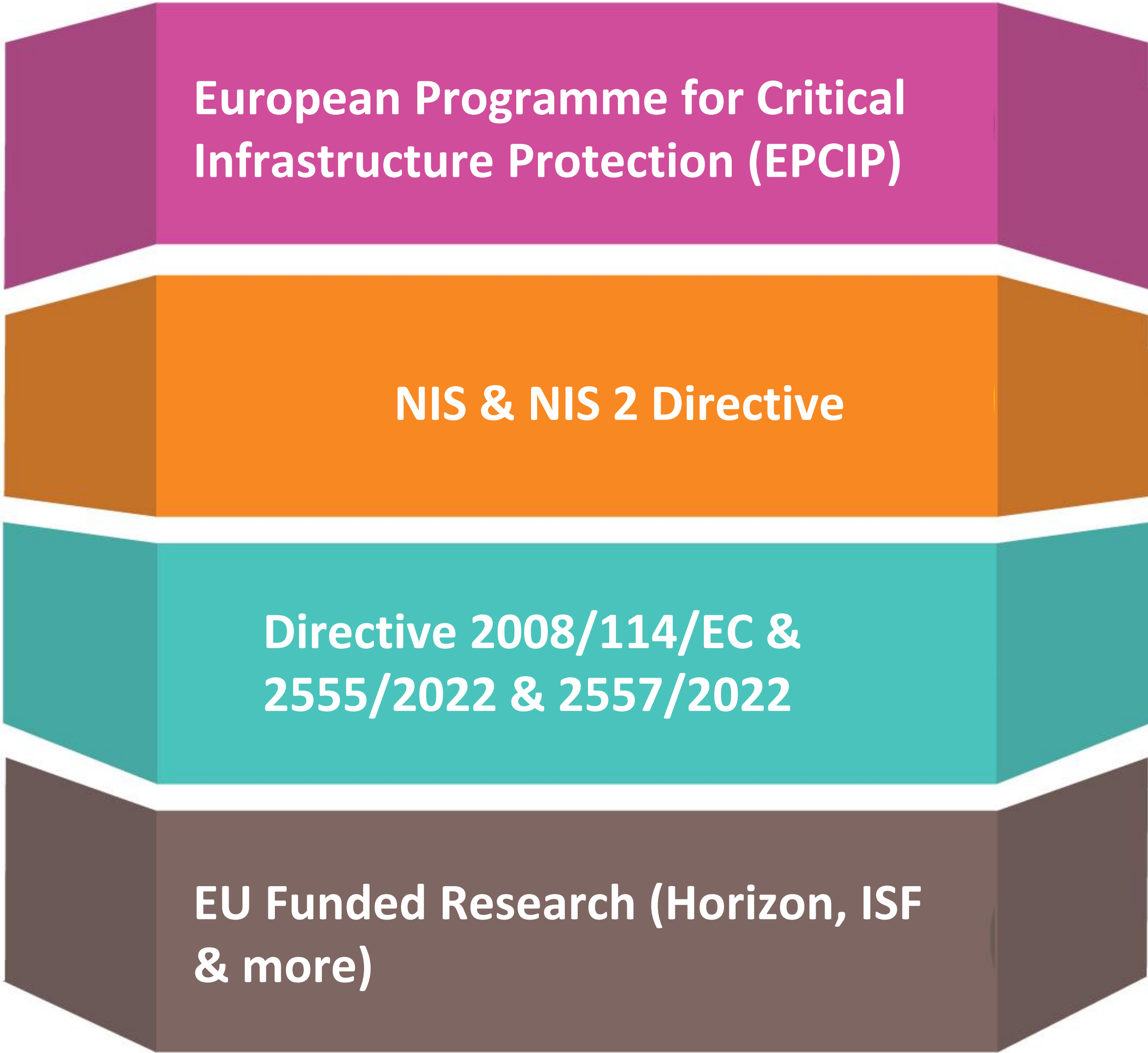
- Infrastructure that is designed to be resilient and able to withstand different types of threats and hazards may be less vulnerable to disruptions than infrastructure that is less resilient.



# EU APPROACH TO CIP



## RELEVANT STAKEHOLDERS





Developing Resilience Strategies & Building Robust Response

RISK  
ASSESSMENT

INTER-  
DEPENDENCY  
ANALYSIS

RESILIENCE  
PLANNING

BUSINESS  
CONTINUITY  
PLANNING

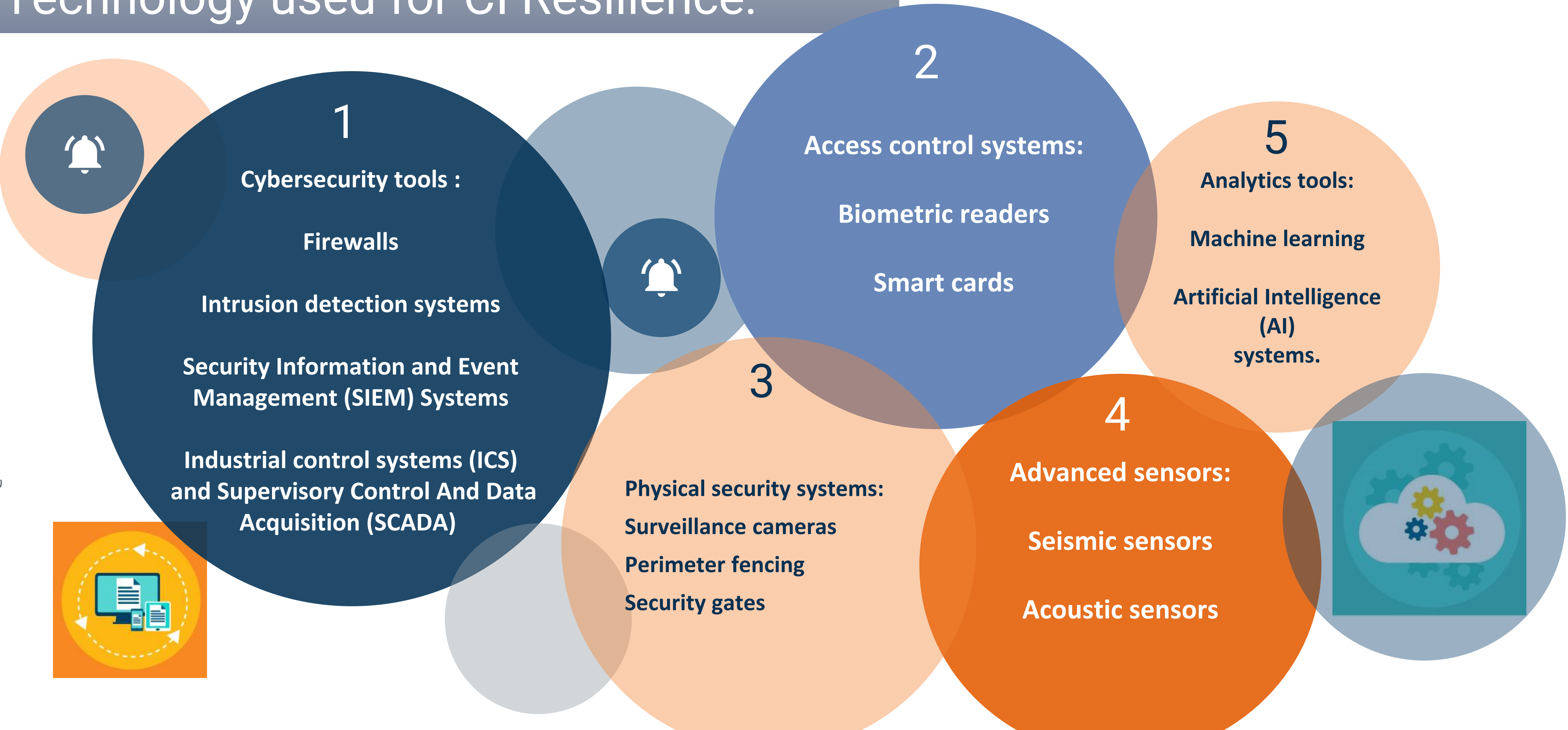
CRISIS  
MANAGEMENT  
PLANNING

TRAINING AND  
EXCERCISES

INFORMATION  
SHARING



# Technology used for CI Resilience:





# KEMEA Critical Infrastructure (CI) and Public Spaces (PS) related projects

## HOTHREAT

- Tailored CBRNe protection measures for hotels and conference centres.

<https://hothreat.eu/>

## POWERBASE

- Low-Emission Power supply for Emergency Shelters and Bases of Operation

<https://www.powerbaseproject.eu/>

## HELOISA

- Water Quality Monitoring, Water Quantity Monitoring, Maritime Surveillance

Greek National Satellite Space Project

## ATLANTIS

- Improved resilience of Critical Infrastructures Against Large scale transNational and systemic risks

## Western Balkans CIP

- Allow the Western Balkans and participating EU Member States to work together to better anticipate, prevent, protect and respond to terrorist threats on public spaces and to critical infrastructures.

## UNICOPS

- Universal CBRNe Protection System Supporting the Safety and Open Nature of Higher Education Institutions

KEMEA.CIP Presentation @ 2025  
KEMEA.C. Corporate Presentation @ 2025





HELLENIC REPUBLIC  
Ministry of Citizen Protection



# Thank you for your Attention!

Efstathios Skarlatos, *Head of the Critical Infrastructure Protection Sector*  
[e.skarlatos@kemea-research.gr](mailto:e.skarlatos@kemea-research.gr)

© KE.ME.A. 2025



[www.kemea.gr](http://www.kemea.gr)



[kemea@kemea.gr](mailto:kemea@kemea.gr)





HELLENIC REPUBLIC  
Ministry of Citizen Protection



# GOOD PRACTICES FOR SECURITY & PROTECTION OF PUBLIC SPACES

*“Global Catastrophic Risks”*  
Conference  
3-4/4/2025

**Konstantinos Apostolou**  
Research Associate

CENTER FOR SECURITY STUDIES - KEMEA





# Public Spaces and Soft Targets

|                      | Examples  |
|----------------------|---|
| Transport Hubs       | Train stations, bus hubs, underground metro stations, etc.  |
| Squares              | Public squares where many events take place, are next to important buildings, have regular big markets, festivals, etc. |
| Shopping Areas       | Shopping malls, main shopping streets in city centre, etc.  |
| Nightlife Areas      | Area with a high density of bars, pubs and/or nightclubs, restaurants, coffee shops, small concert halls                |
| Cultural Venues      | Concert hall, museum, monuments, sport events, stadiums, amusement parks, tourist sites, etc.                           |
| Business Venues      | Big hotels with meeting rooms, large offices, conference centres, etc.  |
| Places of Worship    | Churches, Mosques, Synagogues, etc  |
| Institutional Venues | Governmental / Municipal buildings, health buildings, education buildings, etc.   |

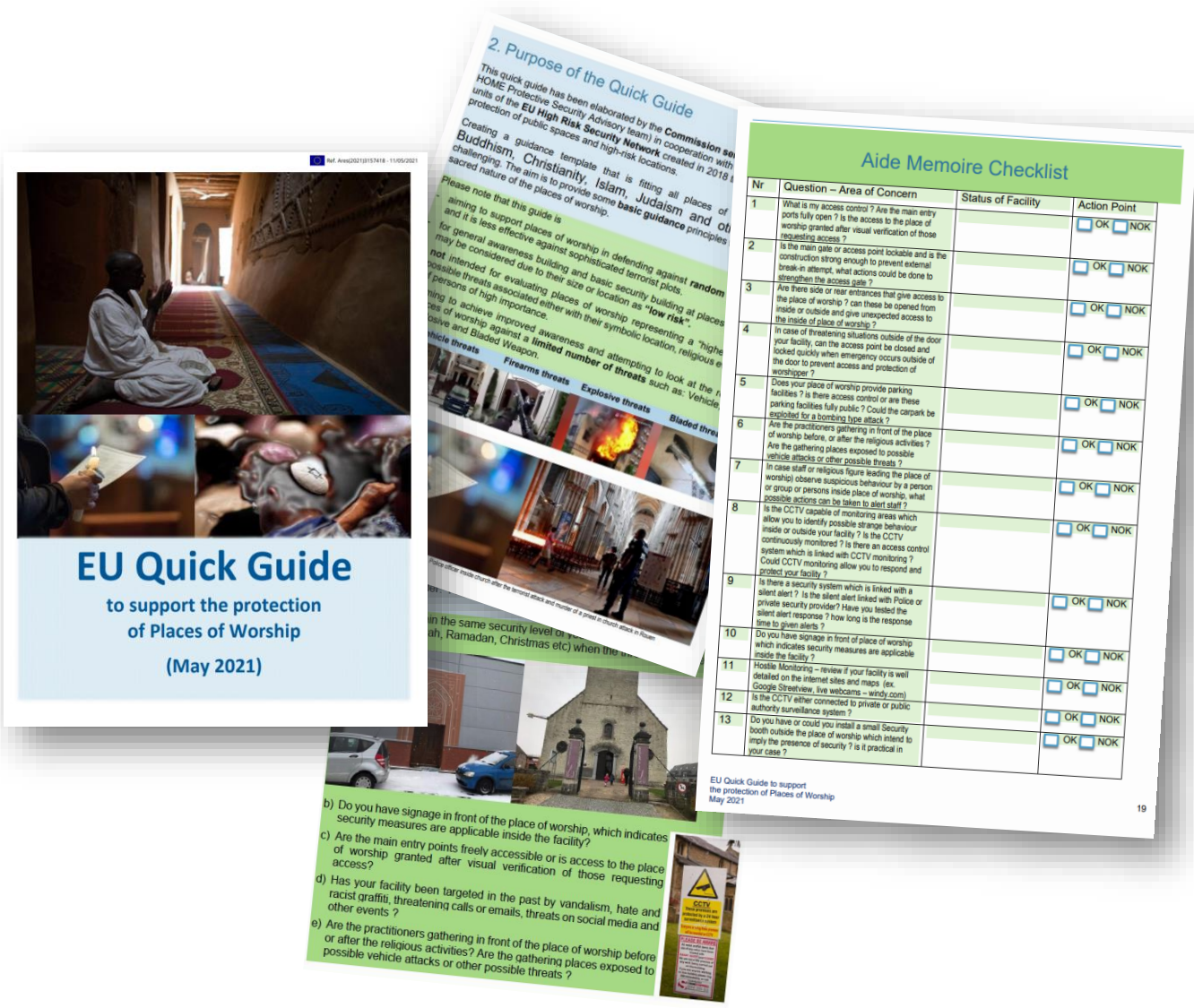






# EU Documentation

- Action Plan to support the protection of public spaces (Commission, 2017)
- COMMISSION STAFF WORKING DOCUMENT **Good practices** to support the protection of public spaces (2019)
- **EU Counter-terrorism Agenda: Anticipate, Prevent, Protect, Respond** (2020)
- **EU Guide Quick Guide (DG HOME, 2021)** to support the protection of Places of Worship
- **EU Vulnerability Assessment Checklist - VAC** (EU PSA, Under development)



[EU quick guide to support the protection of places of worship](#)



[EU VAC](#)





# General Good Practices in the EU

## Multistakeholder Collaboration

- Establishment of cooperation between **local authorities, LEAs, first responders, site operators, local officials, urban planners.**
- Regular **risk / vulnerability assessments** for identification of vulnerabilities.

## Awareness & Training

- **Public involvement** through awareness campaigns (e.g., "See Something, Say Something").
- **Theoretical training** for security personnel, general staff, managers and event organizers.

## Incident Response & Crisis Management

- Guidelines and recommendations for establishment of **emergency response protocols** for large gatherings (e.g., festivals, sports events).
- **Simulation exercises** to test preparedness for terrorist threats or mass evacuations.

## Security by Design (or CPTED)

- Incorporating protective measures directly into urban planning and infrastructure.
- Example: Installing **bollards, reinforced street furniture, and blast-resistant glazing** without disrupting aesthetics.

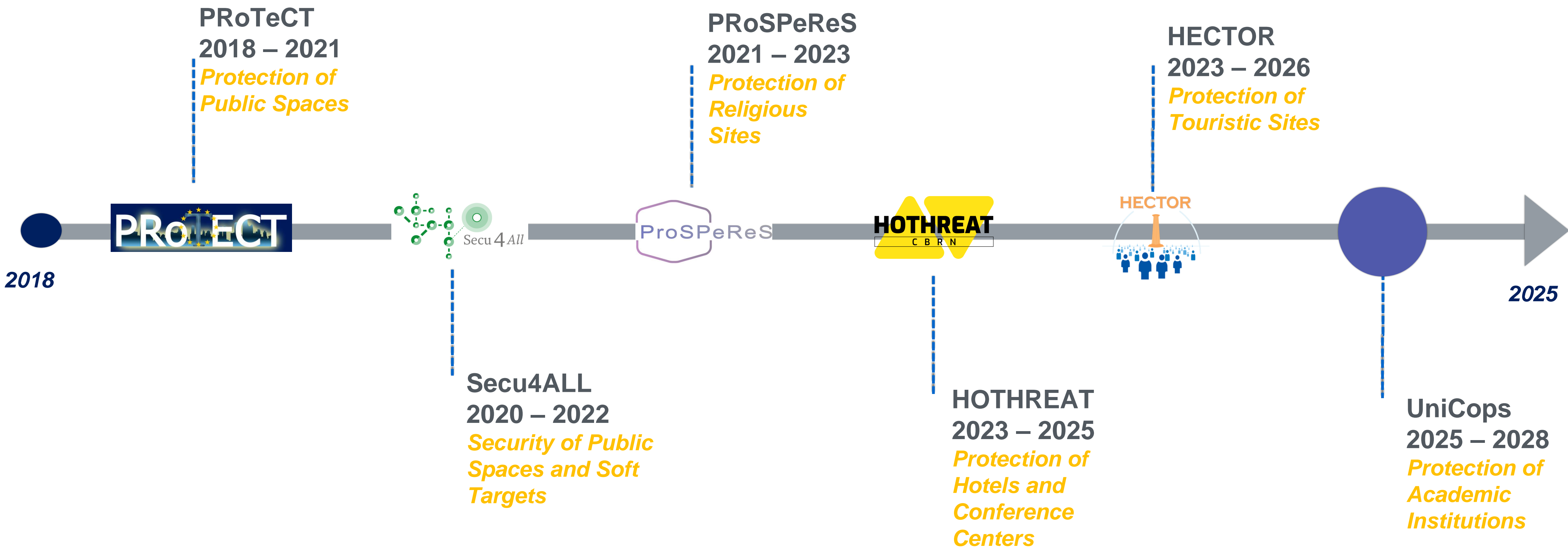
## Surveillance & Technology Integration

- Use of **AI-powered video surveillance, real-time incident detection, and drone monitoring.**
- Deployment of **CCTV analytics** to detect suspicious behavior in crowded places.





# EU Initiatives - Research Projects (ISFP / ISFP)







## Insights from EU Research Projects (1/2)

### Enhancing Urban Security through the incorporation of modern technology

- UAVs for extended area surveillance during events
- UAVs for 3D modelling of sites of interest

### Vulnerability Assessment (VA) of Public Spaces

- VA for sites of interest with the involvement of the site's staff
- Multidisciplinary VA training workshops with the participation of site operator staff, local LEAs and first responders

### Theoretical Training

- Training of public space operators' staff in security issues (e.g. VAs, suspicious persons and items, emergency response and available solutions.
- Development of tailor-made Training Curriculums for public space staff, LEAs and first responders

### Practical Training

- Practical training in anticipation of, preparedness for, prevention of threats and incident & emergency response through based on multi-threat hypothetical and realistic scenarios through TTX and multi-stakeholder field exercises







## Insights from EU Research Projects (2/2)

### Development of Guidelines

- Guidelines for emergency incident response (anticipation)
- Guidelines about techniques and available tools for the protection of public spaces
- Guidelines for Security-by-Design

### Development of Tools

- Development of novel tools to assist emergency response and VAs (e.g. HECTOR – “safeEU platform”, ProSPeReS - “Quick VAT”

### Strengthening Private-Public Partnerships (PPP)

- Enhancement of **cooperation** between **municipal authorities**, **LEAs** and **private security** at large-scale events improved threat response time.
- Enhancement of PPP through organization of awareness conferences, technology demonstrations, and solutions’ testing pilots

### Addressing the Challenge of Balancing Security & Openness

- Over-securitization can negatively impact public perception and usability of spaces.
- Solution: Implement discreet and proportionate security measures (e.g., discreet surveillance, architectural barriers).



[ProSPeReS - VAT Lite](#)



[HECTOR - safeEU Platform](#)





# Conclusions

## Conclusion & Recommendations

- Public spaces **must remain safe yet open** and **accessible**.
- **Recommended Approach:** a **layered security model** combining training, design, technology, collaboration, and security awareness.
- EU institutions, local governments, and private operators must continue to **share knowledge** and **foster their collaboration** through joint initiatives

### RUN

Escape, if you can



- Consider the safest options;
- Is there a safe route? RUN, if not HIDE;
- Can you get there without exposing yourself to greater danger?

Help other people to escape, but don't let their indecision slow you down



Leave belongings behind



Do not attempt to film the incident – RUN!



Alert people around you and deter them from entering the danger zone



### HIDE

If you cannot run, HIDE



- Find cover from gunfire e.g., substantial brickwork / heavy reinforced walls;
- If you can see the attacker, they may be able to see you. Cover from view does not mean you are safe. Bullets go through glass, brick, wood and metal.

You must still hide, even if you are behind a locked door



Turn off light and mute the devices



Be quiet, silence your phone and turn off vibrate



Lock / barricade yourself in and move away from the door



If you can't run or hide during a life-threatening situation, thwart the attack!

### TELL

Call 112



- If you cannot speak or make a noise, listen to the instructions given to you by the call taker.

What do the police need to know?



- What's happening?
- Where exactly?
- Where are the suspects?
- Description of suspects;
- Info about casualties / hostages;
- Info about the building / surroundings.

Follow police instructions



- Remain calm;
- Avoid sudden movements that may be considered a threat;
- Keep your hands open and in view.

Police may...



- Point guns at you;
- Treat you firmly;
- Question you;
- Be unable to distinguish you from the attacker;
- Officers will evacuate you when it is safe to do so.

**RUN,HIDE,TELL** **Flyer**  
(ProSPeReS, 2023)



## Projects' Websites



<https://prosperes.eu/>



<https://hothreat.eu/>



<https://hector-project.com>





HELLENIC REPUBLIC  
Ministry of Citizen Protection



# Thank you for your Attention!

Konstantinos Apostolou, *Research Associate*  
[k.apostolou@kemea-research.gr](mailto:k.apostolou@kemea-research.gr)

© KE.ME.A. 2025



[www.kemea.gr](http://www.kemea.gr)



[kemea@kemea.gr](mailto:kemea@kemea.gr)