ANALYTICAL REPORT 02

SECURITY OF MAJOR PUBLIC EVENTS

A report produced by the ENACT Consortium

Main Author
David Ríos Morentin (VICOMTECH)

ENACT.
European Network Against Crime and Terrorism

ABOUT ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 'Knowledge Networks for Security Research & Innovation', aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.

- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Funded by
the European Union

DISCLAIMER

COPYRIGHT

03

EXECUTIVE SUMMARY

The growing complexity and scale of major public events, such as international sporting championships, or large music events, present significant security challenges. While technology can be supportive in addressing these challenges, practitioners also need a good understanding of the dynamics of the threats and the capabilities required to address these before making strategic investment decisions on research, development or acquisition of advanced solutions.

This report has studied the evidence available within the ENACT Structured Knowledge Base and enriched it with the discussions that took place during the CERIS event on Security of Major Public events organised by the European Commission's DG HOME on December 2024. The results of the analysis show that certain threats, capabilities and technology areas might deserve particular attention during future Security R&I programming and implementation.

When looking at the main threats to the security of major public events, the analysis highlights mainly two sources of threat, namely terrorism and, to a lesser extent but still significant, petty crime and serious organised crime. Among the main types of threats leveraged by these two sources, the study has identified a non-exhaustive list of both physical and non-physical threats. Physical threats to major public events include CBRNE threats (e-g- unattended items, drones and aerial threats), physical attacks (e.g. firearms and other weapons, vehicle ramming), sabotage, public panic, trafficking of drugs and goods and Theft. Non-physical threats include cyber attacks, communications jamming and cascading effects.

To address the main security threats to public spaces and major public events, security agencies, infrastructure operators, and civil society need to develop a range of abilities, capabilities, and functions. The evidence found underlines four categories, namely: 1. Prevention capabilities: including Monitoring and surveillance, Detection of goods, substances, assets, people and incidents, Mobility and deployability, Security of information systems, networks and hardware, Identification and dentification of persons, assets and goods; 2. Preparedness capabilities: including Secure and public communication, data and information exchange (e.g. public awareness), Training (e.g. awareness raising), Data, information and intelligence gathering, management and exploitation (e.g. CMR planning), Physical

access control; 3. Response Capabilities: including Secure and public communication, data and information exchange (e.g. real time critical communications, reporting mechanisms), Data, information and intelligence gathering, management and exploitation, Data, information and intelligence gathering, management and exploitation (e.g. Command, control and coordination, and Incident Management); and 4. Recovery capabilities: including Investigation and forensics, Data, information and intelligence gathering, management and exploitation. Other cross-cutting capabilities have also been identified by experts, including Inter-agency collaboration, Technological innovation, Public education and Advocacy and policy influence.

According to the abovementioned threats and capabilities, a number of technologies emerge as crucial to ensure the security of major public events. These fall mainly in the categories of Access control and authentication, surveillance systems, digital security products and services, critical and interoperable communications, training and simulation, specialised management and control systems and data analytics.

The use of the above technologies pose, however some concerns in the legal, ethical and societal domain. Issues that are of particular importance in the development and use of technology for the protection of major public events include, among other, Privacy and Data Protection in relation with surveillance and monitoring and data security, Civil Liberties to ensure freedom of movement and assembly and avoid discrimination and bias, Legal and Regulatory Compliance at EU and Member States level in particular regarding accountability, transparency and human supervision, and other Ethical considerations linked to proportionality, transparency and public engagement.

An analysis of 25 EU-funded projects (including Horizon and ISF-funded), shows a comprehensive coverage of the abovementioned threats, capabilities and technologies during the period going from 2014 to 2023. Nevertheless, evidence suggest that there are areas which could benefit from additional research effort in order to match the potential future demand of practitioners for the protection of major public events. These are summarised in the table below:

Threats	• Sources of threat: Petty crime and Serious organised crime • Types of threat: Public panic, Sabotage, Trafficking and Theft, Communications jamming, Cascading effects
Type of threat:	• Investigation and forensics • Positioning and localisation, tracking and tracing • Identification and authentication of persons, assets and goods • Physical access control • Personal and other equipment for prevention, response and recovery • Mobility and deployability
Technologies	• Access control/authorisation: Integrated Security Systems, including video surveillance, access control, and emergency alert systems. • Training and simulation: Simulation and Training Tools, including Virtual reality (VR), augmented reality (AR), Digital Twins. • Specialised management and control systems: Command and Control Centers, including command centers equipped with Geographic Information Systems (GIS) and real-time data analysis capacity; and Incident Management Software, including software solutions for managing alerts, incidents, and crisis situations.

ACRONYMS

AI	Artificial Intelligence
AR	Augmented Reality
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CERIS	Community of European Research and Innovation for Security
CORDIS	Community Research and Development Information Service
ELS	Ethical, legal, societal
EU	European Union
EUCS	European Union Civil Security (taxonomy)
EUCCS	European Critical Communications System
FCT	Fighting Crime and Terrorism
GDPR	General Data Protection Regulation
GIS	Geographic Information Systems
IoT	Internet of things
IP	Intellectual Property
LEA	Law Enforcement Agency
LTE	Long Term Evolution
SKB	Structured Knowledge Base
R&I	Research and Innovation
URL	Uniform Resource Locator
VR	Virtual Reality

06 REPORT OBJECTIVE

This report presents the main threats to major public events and identifies the key capabilities needed to address them as well as the technologies that might enable the development of such capabilities. Comparing the results of the analysis presented herein with the scope of past and ongoing EU-funded actions on the subject matter will help identifying future research priorities and areas that deserve special attention by policymakers, security authorities, technology developers, researchers and civil society in general.

DISCLAIMER ON THE USE OF AI

Following the ENACT policy for the use of AI, the analysis carried out for this report has been supported by Microsoft Copilot given that the two following conditions were met:

- The data to be collected comes from a publicly available source, and
- The product being prepared is intended for open dissemination.

The main purpose of the use of AI for this analysis was to extract key information from the observations of interest. To do so, the AI was prompted to extract concrete references from the observations when these referred to relevant threats, capabilities, technologies and ethical, legal and societal issues relevant for the security of major public events. In order to provide contextual information, the AI was provided with a detailed description of the EU Civil Security Taxonomy (EUCS Taxonomy).

The outcomes of the AI-assisted analysis have been subject to human oversight to ensure their soundness, integrity and applicability to the objectives of the report.

08 INTRODUCTION

SCENE SETTER

This report has been produced as a follow up of the Community of European Research and Innovation for Security (CERIS) event on the security of Major Public Events held on the 12/12/2024 in Brussels [1]. The event focused on the challenges and solutions to ensure the safety and security of large gatherings. The discussions highlighted the importance of anticipating, adapting, and responding effectively to security threats at major public events, which attract significant international attention and pose various risks, including crime and terrorism.

On the other hand, the ENACT project maintains a system of Observatories which help to populate a Structured Knowledge Base (SKB) that contains open sources of information, including EU-funded projects. These ENACT Observations are mapped to the EU Civil Security (EUCS) Taxonomy by the experts involved in the observatories either manually or AI-assisted. From the content of the SKB, a total number of 51 open-source observations (See Appendix A) and 25 projects (See Appendix B) have been extracted as per being flagged as relevant by ENACT experts. These have been subject to analysis with the aim of reinforcing the outcomes of the discussions held under the abovementioned CERIS event.

METHODOLOGY

The document contains dedicated sections for the analysis of threats, capabilities, technologies and ethical & legal issues. Each of them contains a three-way analysis based on evidence extracted from **ENACT's Structured Knowledge Base** (statistical and AI-supported) and from the discussions held during the **CERIS event on the security of major public events**. Those aspects where the information extracted from ENACT's SKB and from the CERIS discussions coincide, serve as hard evidence on matters that are of relevance for the security of major public events. The findings presented in this report could be used to support decision making during the future planning and implementation of EU-funded security research.

[1] https://home-affairs.ec.europa.eu/whats-new/events/securing-major-public-events-2024-12-12_en

To be noted that the analysis carried out using the content of the ENACT SKB is two-fold:

1. **Statistical analysis of ENACT Observations:** Statistics have been generated and presented in figures that show the distribution of the mapping of the observations to the EUCS Taxonomy elements. This distribution shows which are the main domains contemplated in the recorded observations, which can also serve as a proxy measure of those aspects that are more closely linked to the security of major public events from a policy, functions/capabilities and technology perspectives [2].

2. **Content analysis of ENACT Observations:** Observations have been processed using generative AI, concretely Microsoft Copilot. In this case, Copilot was prompted with questions oriented to extract concrete references from the observations (list of URLs) when these referred to relevant threats, capabilities, technologies and ethical, legal and societal issues relevant for the security of major public events. In some cases, the AI was asked to classify the outcomes of its search in categories. For example, references to capabilities were structured in four categories, namely prevention, preparedness, response and recovery. The information provided by the AI was later analysed by a human expert, interpreted and in some cases, classified manually according to the categories of the EUCS taxonomy. The outcome of this processing offers a structured summary of the main themes addressed in the observations, offering a condensed view of the main aspects related with the security of public spaces addressed by the knowledge openly available to the community.

As mentioned above, only publicly available sources and general knowledge have been used to generate this analysis, i.e. information that is accessible to the public and not restricted by privacy or intellectual property rights. Publicly available sources include websites, articles, reports, and other materials that can be freely accessed online. General knowledge refers to widely known facts and information that are commonly understood and accepted.

In the context of the analysis provided, the information is derived from URLs registered in the ENACT SKB as “Open”, which are publicly accessible and contain content related to security threats, capabilities, and technologies. Intellectual property (IP) protected information, such as proprietary technologies, trade secrets, or copyrighted content, has not been included in the analysis.

THREATS LANDSCAPE

This section presents the threat landscape applicable to major public events according to the three-way analysis carried out by ENACT.

[2] Note: The mapping of some of the observations to the EUCS taxonomy was supported by AI using a hybrid curation method by which the automatic classification of the observations done by the AI was later verified and corrected, as necessary, by a human expert. The observations listed in Appendix A which followed a hybrid curation method are the following: 89,91, 96, 101, 116, 216, 556, 567.

STATISTICAL ANALYSIS OF ENACT OBSERVATIONS

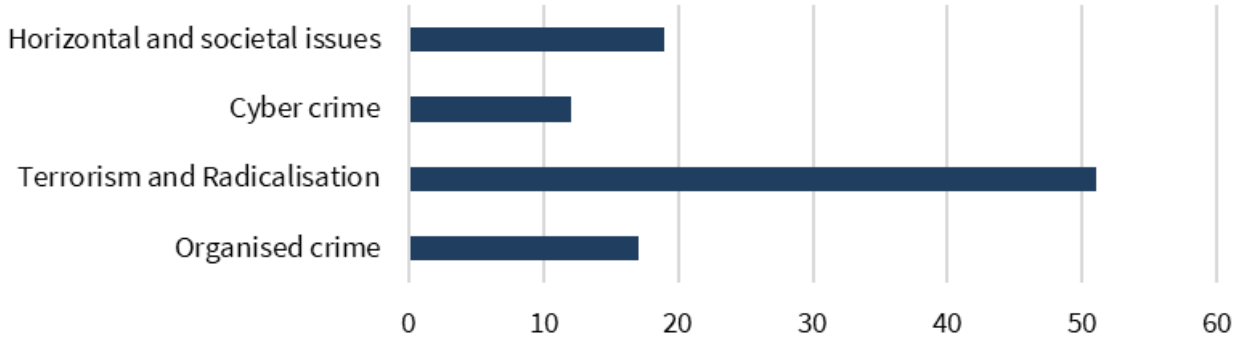


Figure 1 – Mapping of observations recorded in the ENACT SKB according to the EUCS Taxonomy Policy L2

The mapping of observations carried out by the ENACT experts shows that the security of major public events is predominantly linked to terrorist threats, with organised crime, cybercrime and other societal and horizontal security policy domains as secondary drivers. These secondary domains might entail security risks by themselves, or act as amplifiers of the primary terrorist threat.

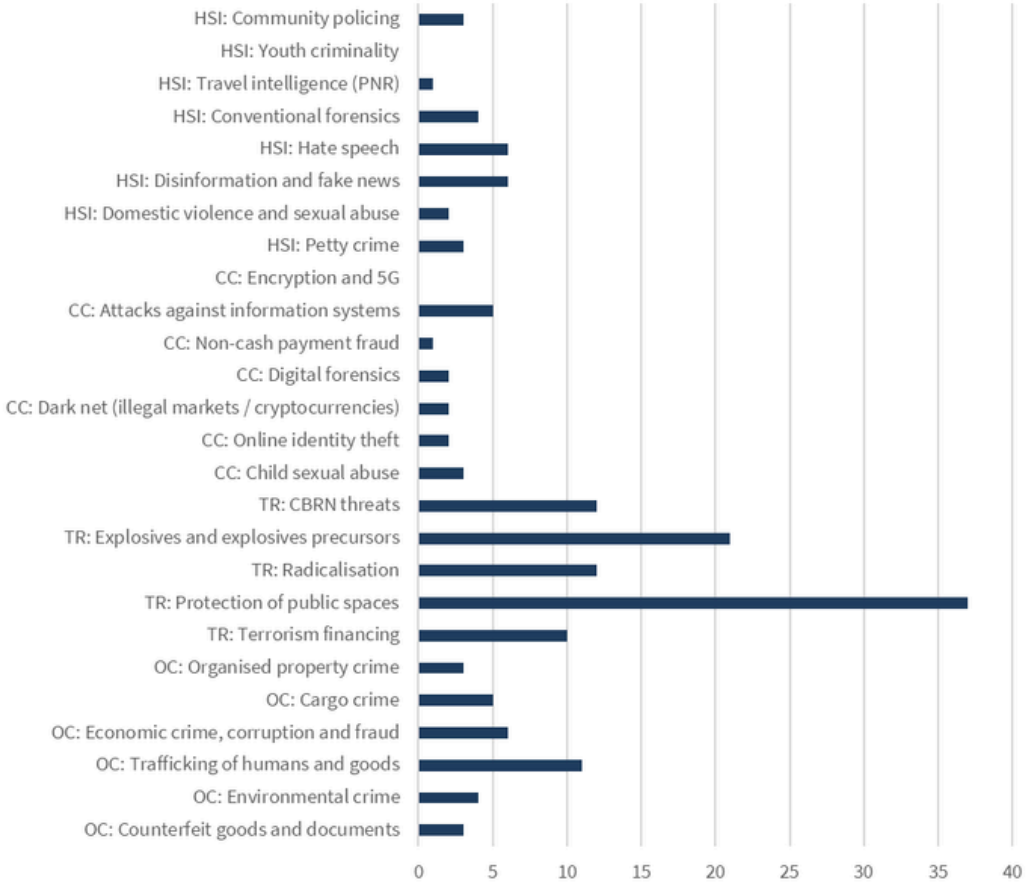
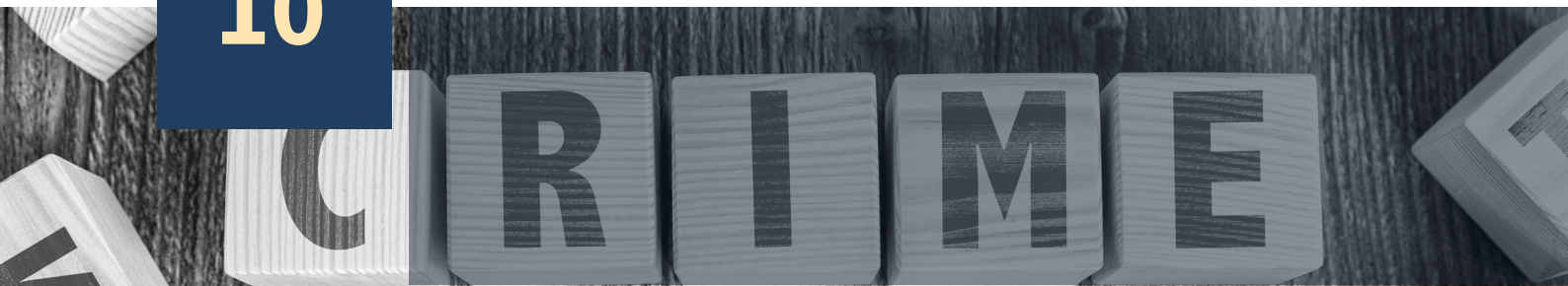


Figure 2 – Mapping of observations recorded in the ENACT SKB according to the EUCS Taxonomy Policy L3



Looking at the correlation with the L3 level of the policy taxonomy, the domain "Protection of public spaces" stands out as the observations selected from the database where those that were mapped to that domain. However, given that one observation may be linked to multiple domains, other elements of the EUCS FCT Policy taxonomy might indicate secondary domains of relevance when considering the security of major public events. According to the figure, these include mainly sub-domains within the Terrorism and Radicalisation domain, and others such as Hate Speech, Disinformation and Fake news, Trafficking of humans and goods, Economic crime, Attacks against information systems or Community policing. These secondary should not be overlooked, as they allow to articulate the problem of the security of public spaces, notably major public events, from different perspectives and identify a variety of use cases that guide the development of flexible solutions for a multidimensional challenge.

AI-SUPPORTED ANALYSIS OF ENACT OBSERVATIONS

The AI-supported analysis of the content of the observations reveals a number of key security threats to public spaces which, to a large extent, correlate with the statistical analysis of the observations mapping:

- **Terrorism and Organized Attacks:** Terrorist attacks, whether high-intensity (using explosives and firearms) or low-tech (using vehicles or knives), pose significant threats to public spaces. These attacks can cause mass casualties, widespread panic, and long-term psychological effects on the public. At major public events, the risk is heightened due to the large number of people gathered in one place.

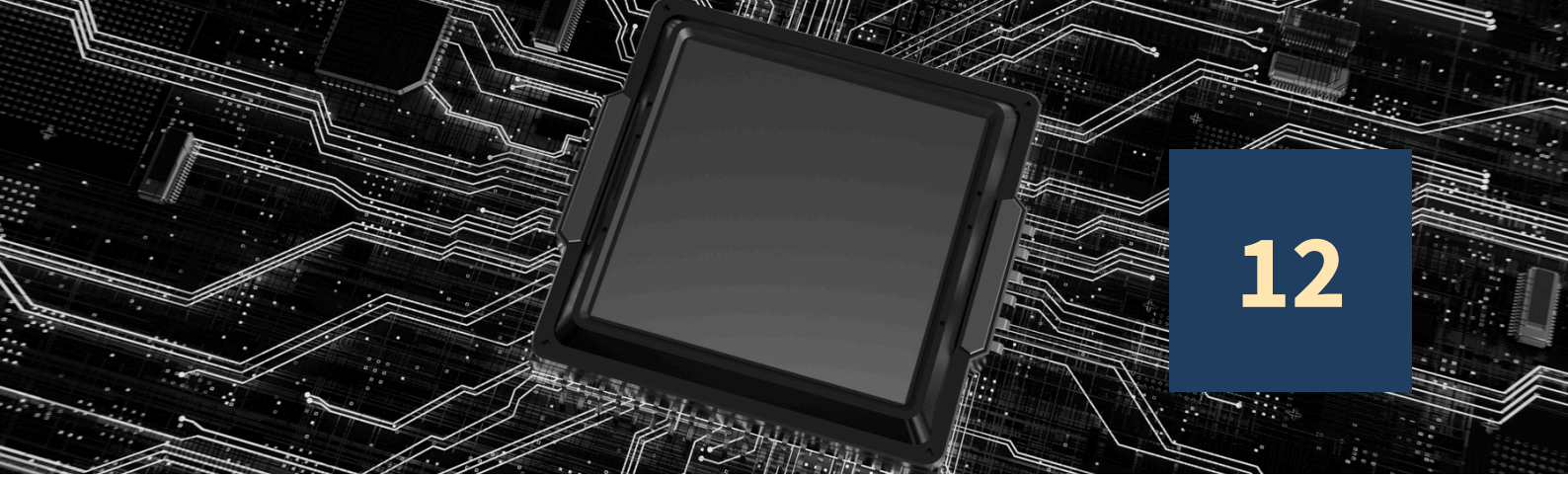
- **Cyber Threats:** Cyber threats can disrupt major public events by targeting critical infrastructure, such as power grids, communication networks, and transportation systems. A successful cyberattack could lead to power outages, communication breakdowns, and chaos, severely impacting the safety and security of the event.

- **Drones and Aerial Threats:** The misuse of drones poses a significant threat to public safety at major events. Drones can be used to carry weapons or hazardous materials, causing panic and potential harm to attendees.

- **Unattended Items:** Items such as bags or packages, can be used to conceal explosives or other dangerous devices. At major public events, the presence of unattended items can lead to evacuations, delays, and heightened security measures.

- **Public Panic:** Panic situations in crowded areas can lead to stampedes, injuries, and fatalities. Effective crowd management strategies, such as controlled entry and exit points, clear communication, and trained personnel, are essential to prevent and manage panic at major events. Understanding crowd dynamics and having contingency plans in place can significantly enhance safety.

- **Organized Crime and Serious Offenses:** Organized crime groups can exploit major public events for various illegal activities, such as drug trafficking, human trafficking, and theft. These activities can undermine the security and integrity of the event.



- **Cascading effects:** Protecting critical infrastructure, such as transportation hubs, power supplies, and communication networks, is vital to ensure the smooth operation of major public events. Any disruption to these infrastructures can have cascading effects, leading to chaos and compromising public safety. Coordinated efforts between public and private sectors are essential to safeguard these assets.

CERIS TAKE-OUTS

The growing complexity and scale of major public events, such as international sporting events, large music or cultural festivals, or even elections, present significant security challenges. These events attract global attention and large crowds, making them potential targets for a range of threats, from terrorism to cyberattacks.

During the conference panels, the following security threats were highlighted:

- **Cybersecurity Threats:** Cybersecurity threats were a major focus during the event. The discussions emphasized the importance of protecting communication networks and critical infrastructure from cyber-attacks. The transition to broadband public communications and the need for robust cybersecurity measures were highlighted as key priorities.

- **Physical Attacks:** Physical attacks, including sabotage and drone attacks, were also given significant attention. The event discussed incidents such as the sabotage of high-speed trains during the Olympics and the use of drones for malicious purposes. The need for technologies to detect and mitigate these threats was emphasized.

- **Jamming Communications:** The threat of jamming communications was addressed as a critical issue. The event highlighted the importance of maintaining communication integrity and the need for technologies to detect and locate the source of jamming.

- **Terrorist Attacks:** Terrorist attacks were recognized as a significant threat due to the high visibility and emotional significance of major public events. The discussions focused on the need for advanced security measures and counter-terrorism tools to prevent and respond to such attacks.

- **Petty Crime and Serious Organized Criminality:** While still important, petty crime and serious organized criminality were addressed with slightly less emphasis compared to the other threats. The discussions acknowledged the need for comprehensive security measures to prevent and respond to these types of criminal activities.

MAIN THREATS SUMMARY

13

Without going into the detail for all of them, the CERIS discussions corroborated the analysis of the observations. A summary of the threats landscape is as follows:

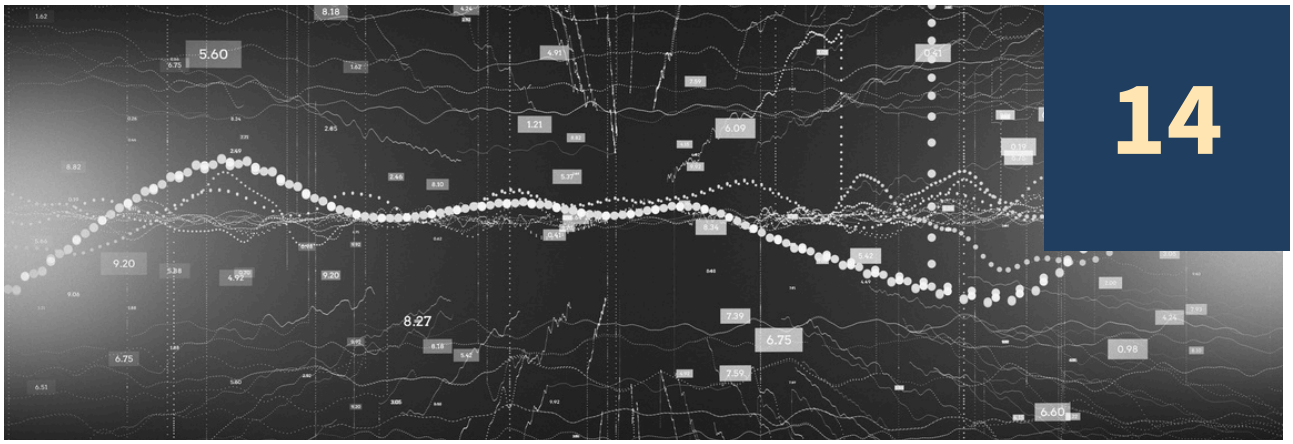
Source of threat:	• **Terrorism** • **Petty Crime and Serious Organised Crime**

Type of threat:	• **Physical threat**
	  ◦ CBRNE threats
	  ▪ Unattended items
	  ▪ Drones and aerial threats
	  ◦ Physical attacks
	  ▪ Firearms and other weapons
	  ▪ Vehicle ramming
	  ◦ Sabotage
	  ◦ Public panic
	  ◦ Trafficking and theft
	• **Non-Physical threat**
	  ◦ Cyber attacks
	  ◦ Communications jamming
	  ◦ Cascading effects

Correlation with EUCS L2 and L3 is not possible because the taxonomy is not structured on the bases of threats, but of EU policy lines/priorities. However, the threats can be primarily mapped to the EUCS L2 category of Terrorism and Radicalisation, and secondarily to the categories of Organised Crime and Horizontal/Societal Issues (petty crime).

CAPABILITIES

To address the main security threats to public spaces and major public events, security agencies, infrastructure operators, and civil society need to develop a range of abilities, capabilities, and functions. This section presents the key capabilities identified through the three-way analysis carried out by ENACT.



14

STATISTICAL ANALYSIS OF ENACT OBSERVATIONS

Figure 3 – Mapping of observations recorded in the ENACT SKB according to the EUCS Taxonomy Functions

The mapping of observations carried out by the ENACT experts shows that the security of major public events is **predominantly linked to the "Monitoring and surveillance of environments and activities"**. In a second level, other functions stand out as relevant for the protection of public spaces, such as **"Investigation and Forensics"**, **"Detection of goods, substances, assets and people and incidents"** and **"Data, information & intelligence gathering management and exploitation"**. The rest of the functions appear somewhat evenly in a third level of relevance.

AI-SUPPORTED ANALYSIS OF ENACT OBSERVATIONS

The AI-supported analysis of the content of the observations reveals a number of key capabilities, abilities or functions that need to be developed by Security Agencies and Infrastructure operators in order to cope with security threats to major public events.

The capabilities have been grouped according to the different stages of the resilience cycle applicable to security incidents, namely prevention, preparedness, response and recovery.

A. Prevention: Actions and measures taken to avoid or reduce the likelihood of security threats occurring in the first place

- **Advanced Surveillance and Monitoring:** Utilizing AI-powered video surveillance systems to detect suspicious behaviour, unattended items, and potential threats in real-time.
- **Drones and Aerial Surveillance:** Deploying drones equipped with high-resolution cameras and sensors to monitor large areas and detect suspicious activities from above.
- **Cybersecurity Measures:** Implementing robust cybersecurity protocols to protect critical infrastructure and communication networks from cyberattacks.
- **Perimeter Protection:** Implementing robust perimeter protection measures, including physical barriers, access control systems, intrusion detection systems, and regular security patrols to prevent unauthorized access.

B. Preparedness: The process of planning, training, and equipping to effectively handle potential security threats.

- **Crisis Management and Response Planning:** Developing comprehensive crisis management plans that include rapid response teams, evacuation procedures, and communication strategies to manage emergencies effectively.
- **Integration of Security Systems**: Combining video surveillance, access control, and emergency alert systems into a single platform for better coordination and situational awareness.
- **Simulation and Training Tools**: Using virtual reality (VR) and augmented reality (AR) to simulate emergency scenarios and provide realistic training for security personnel.

- Public Awareness Campaigns: Conducting public awareness campaigns, community engagement initiatives and training programs to educate citizens on recognizing and reporting suspicious activities. Leveraging mobile apps and social media platforms to educate the public about safety protocols and encourage vigilance.

C. **Response:** The immediate actions taken to address and manage security threats as they occur.

- **Real-Time Communication Systems:** Utilizing advanced communication systems, such as broadband trunk systems and LTE networks, to enable instant communication between security personnel and emergency responders.

- **Reporting Mechanisms**: Establishing easy-to-use reporting mechanisms for citizens to report suspicious activities or security concerns. This can include mobile apps, hotlines, and online platforms.

- **Command and Control Centers:** Equipping command centers with Geographic Information Systems (GIS) and real-time data integration to manage and coordinate responses to emergencies effectively.

- **Incident Management:** Streamline the response process by managing alerts, incidents, and crisis situations.

D. **Recovery:** The efforts to restore normalcy and rebuild after a security incident.

- **Data Analytics and Forensics:** Using data analytics and forensic tools for post-incident analysis to understand the cause of incidents and prevent future occurrences.

- **Resilient Infrastructure:** Enhancing the resilience of critical infrastructure with technologies such as redundant power supplies and backup communication systems to ensure essential services remain operational during and after an incident.

- **Community Engagement Platforms:** Facilitating communication and collaboration between the public, security agencies, and infrastructure operators to aid in recovery efforts.

Some capabilities are cross-cutting to the four stages mentioned above. These include:

- **Interagency Collaboration:** Establishing strong collaboration frameworks between different law enforcement agencies, infrastructure operators and civil society, both nationally and internationally, to share intelligence and coordinate responses to threats.

- **Technological Innovation:** Investing in innovative technologies, such as drones for aerial surveillance, AI for predictive analytics, and IoT devices for real-time monitoring of infrastructure.

- **Public Education:** Educating the public on safety protocols, emergency procedures, and the importance of vigilance in public spaces. This can be achieved through public service announcements, social media campaigns, and educational programs in schools.

- **Resilience Building:** Promoting resilience within communities by encouraging preparedness for emergencies and fostering a culture of mutual support and cooperation.

- **Advocacy and Policy Influence:** Engaging in advocacy to influence public policy and ensure that security measures are balanced with the protection of civil liberties and privacy rights.

CERIS TAKE-OUTS

The CERIS event stressed the critical need for cutting-edge security measures. It is essential to bring together experts, policymakers, and industry leaders to discuss how the latest advancements and strategies driven by EU-funded research can contribute to the development of security capabilities.

The following capabilities were mainly addressed during the event:

1. **Advanced Security Measures:**

- Monitoring and detection technologies to identify potential threats in real-time.
- Cybersecurity solutions to protect communication networks and critical infrastructure from cyber attacks.
- Counter-terrorism tools to prevent and respond to terrorist activities.
- Crisis management capabilities to handle emergencies effectively and ensure swift response.

2. **Drones and Sensors:**

- Deploying drones for surveillance, situational awareness, and detection of malicious activities.
- Using fixed and mobile sensors for real-time monitoring and fast reaction.

3. **Robust Communication Networks:**

- Building and operating resilient mobile broadband communications networks for public safety.
- Ensuring system robustness with physically distributed core infrastructure and logically redundant architecture.
- Implementing multi-layered cybersecurity defense mechanisms, including end-to-end encryption and direct links to cyber defense centers.
- Continuous innovation in communication technologies, such as ground-to-air communications, non-terrestrial networks, AI, and IoT.

4. **Digital Twins and AI:**

- Utilizing digital twins to understand complex scenarios and plan the deployment of resources optimally.
- Employing AI for surveillance, situational awareness, and training.
- Using digital twins and 3D models for remote preparation and simulation of various scenarios, including coverage of sensors and optimal distribution of human forces.

5. **Cyber-Physical Integration:**

- Ensuring the integration of cyber and physical situational awareness systems to detect and respond to threats effectively.
- Developing tools for dynamic risk assessment and automation of response to incidents.
- Training practitioners to understand the potential of new technologies, including AI and autonomous systems, and to use them effectively in stressful situations.

6. **Cooperation:** The panellists emphasized the need for enhanced cooperation among various stakeholders, including law enforcement agencies, event organizers, technology providers, and policymakers. They highlighted the importance of:

   - **Cross-border Cooperation:** Ensuring that different countries can communicate and coordinate effectively, especially in the context of the European Critical Communications System (EUCCS).
   - **Information Sharing:** Addressing the challenges of sharing information between public and private organizations, as well as between different types of practitioners. This is crucial for the protection of public events and for conducting effective risk assessments and crisis management.
   - **Standardization and Certification:** The emerging need for standardization and certification of security tools and technologies to ensure their reliability and interoperability across different contexts and jurisdictions.

7. **Training:** Training was identified as a critical component in preparing for and responding to security threats at major public events. The panellists discussed:

   - **Scenario-Based Training:** Using digital twins and simulation tools to conduct virtual exercises and prepare for various scenarios without being physically present at the event. This helps decision-makers understand the complexity of deployments and optimize resource allocation.
   - **New Skills for Law Enforcement Agencies (LEAs):** Emphasizing the need for LEAs to develop new skills to understand and utilize advanced technologies, including AI, autonomous systems, and cybersecurity tools.
   - **Collaboration Between Technicians and Users:** Encouraging collaboration between technology developers and end-users to ensure that practitioners are well-trained and can effectively use the new technologies in stressful situations.

8. **Awareness Raising:** Raising awareness among the public and practitioners was highlighted as essential for effective security management. The panellists mentioned:

   - **Public Awareness of Security Threats:** Educating the public about the potential security threats, risks, and ways to respond. This includes engaging with citizens to understand their concerns and expectations regarding the use of surveillance and other security technologies.
   - **Engagement with Society:** Conducting surveys and dialogues with citizens to gauge their acceptance of new technologies and to address any misconceptions or fears. This helps build trust and ensures that the deployment of security measures is transparent and justified.
   - **Avoiding Fake News and Disinformation:** Ensuring that society understands what is possible and not possible with technology, and combating the spread of fake news and disinformation related to security measures.

MAIN CAPABILITIES SUMMARY

The CERIS discussions addressed most of the capabilities identified through the mapping of observations at the ENACT SKB and the AI-supported analysis of the observations, which makes a coherent view of the capabilities required for the security of major public events.

The mapping of observations carried out by the ENACT experts in the ENACT SKB is less detailed than the other two, because the lower level of detail of the EUCS functions taxonomy does not allow to visualise lower level capabilities that could fall under one of the EUCS functions taxonomy categories. Additionally, the AI-supported analysis of the observations and the CERIS discussions make a high emphasis on some capabilities, such as Communications, while the mapping in the ENACT SKB does not show an equal relevance in the overall landscape (even if it does identify this particular one among the observations). Other capabilities that are strongly present in the mapping were also stressed as very relevant during the event and their relevance also appears clearly in the AI-supported analysis of the observations. Therefore, while the ENACT SKB mapping is not precise, it is indeed a good reference to filter out observations from the database and conduct follow-up and more detailed analysis based on them.

In order to present a summary of the key capabilities required to cope with security threats to major public event, all the outcomes of the three-way analysis (statistical, AI-based and CERIS discussions) have been merged and translated into the categories of the EUCS taxonomy for ease of reference and harmonisation.

PREVENTION:

- Monitoring and surveillance
- Detection of goods, substances, assets, people and incidents
- Mobility and deployability
- Security of information systems, networks and hardware
- Identification and authentication of persons, assets and goods

PREPAREDNESS:

- Secure and public communication, data and information exchange (incl. public awareness)
- Training (incl. awareness raising)
- Data, information and intelligence gathering, management and exploitation (incl. CMR planning)
- Physical access control

RESPONSE:

- Secure and public communication, data and information exchange (incl. real time critical communications, reporting mechanisms)
- Data, information and intelligence gathering, management and exploitation
- Data, information and intelligence gathering, management and exploitation (incl. Command, control and coordination, and Incident Management)

RECOVERY:

- Investigation and forensics
- Data, information and intelligence gathering, management and exploitation

Note that there are also other cross-cutting capabilities identified in ENACT analysis and CERIS discussion. It is also the case that these capabilities do not easily fit under any function category currently present in the EUCS taxonomy. Therefore, these might be taken into consideration for future updates of such taxonomy.

- **Interagency Collaboration**: Establishing strong collaboration frameworks between different law enforcement agencies, infrastructure operators and civil society, both nationally and internationally, to share intelligence and coordinate responses to threats.

- **Technological Innovation**: Investing in innovative technologies, such as drones for aerial surveillance, AI for predictive analytics, and IoT devices for real-time monitoring of infrastructure.

- **Public Education**: Educating the public on safety protocols, emergency procedures, and the importance of vigilance in public spaces. This can be achieved through public service announcements, social media campaigns, and educational programs in schools.

- **Advocacy and Policy Influence**: Engaging in advocacy to influence public policy and ensure that security measures are balanced with the protection of civil liberties and privacy rights.

TECHNOLOGIES

Technology can act as a capability enabler. The analysis presented in this section shows a number of technologies should be considered critical to prevent, prepare, respond and recover from a security incident at major public events.

STATISTICAL ANALYSIS OF ENACT OBSERVATIONS

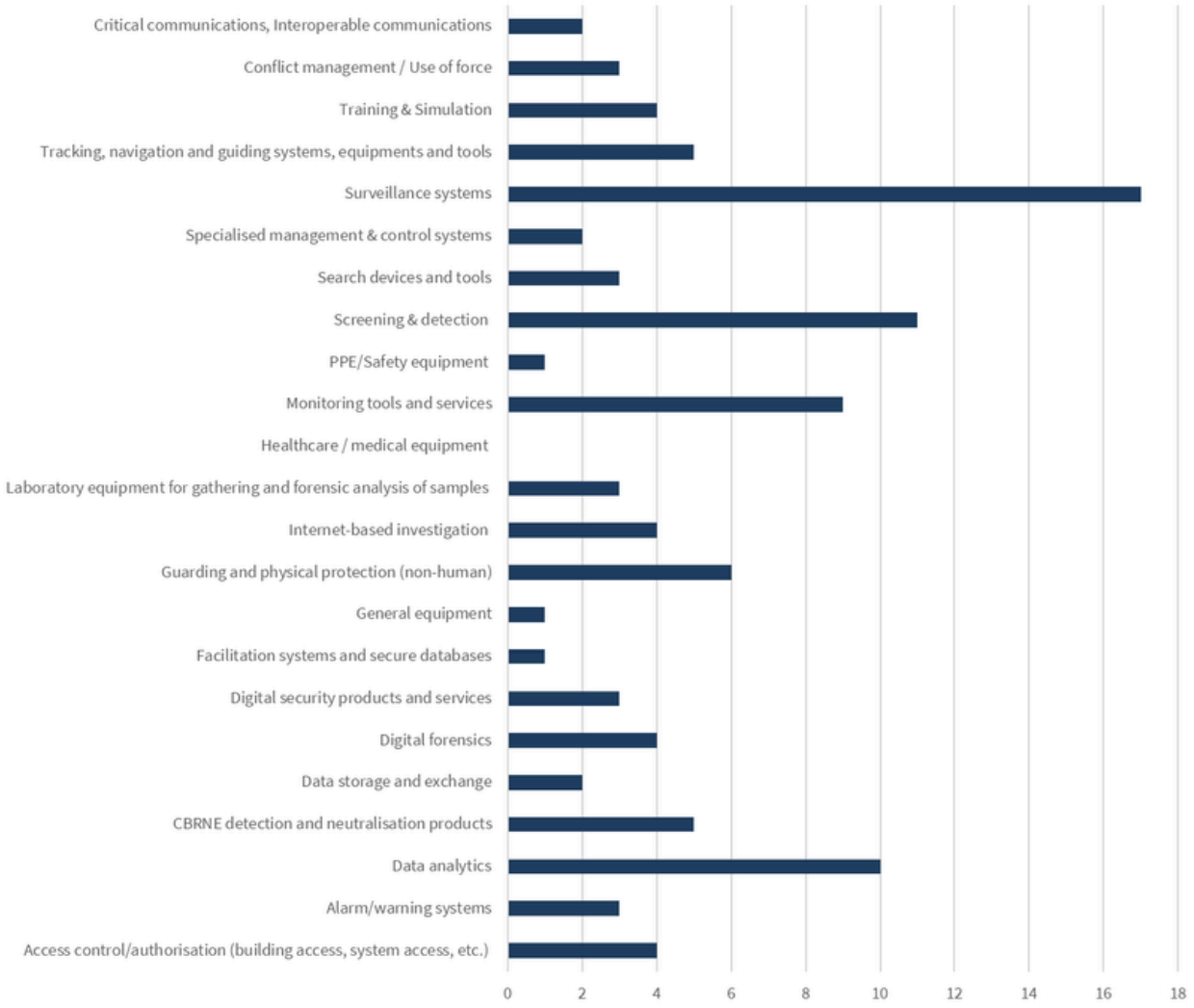


Figure 4 – Mapping of observations recorded in the ENACT SKB according to the EUCS Taxonomy Technologies

The mapping of observations carried out by the ENACT experts shows that the security of major public events is **predominantly linked to the technology category of "Surveillance systems"**. Technologies that appear in a second level of priority **include "Screening and Detection technologies"**, **"Monitoring tools and Services"** and **"Data analytics"**. A third level would include technologies such **"CBRNE detection and neutralisation products"**, **"Guarding and physical protection"** and **"Tracking, navigation and guiding system"** technologies.

AI-SUPPORTED ANALYSIS OF ENACT OBSERVATIONS

The AI-supported analysis of the content of the observations reveals several key technologies that could enable the development of capabilities to cope with security threats to major public events.

The technologies have been grouped according to the technology areas of the EUCS taxonomy. They have also been associated with the different stages of the resilience cycle for the security of major public events:

- **Access control/authorisation**
  - **Integrated Security Systems:** Integrated security systems combine video surveillance, access control, and emergency alert systems into a single platform. This allows for better coordination and situational awareness. These systems can provide real-time data and alerts to security personnel, enabling them to respond quickly to potential threats.

- **Surveillance systems:**
  - **Drones and Aerial Surveillance:** Drones equipped with high-resolution cameras and sensors provide real-time aerial views of large areas. They can be used to monitor crowds, detect suspicious activities, and track individuals from above. Drones are particularly useful in crowded events where ground surveillance might be limited.

- **Digital security products and services**
  - **Cybersecurity Solutions:** Robust cybersecurity measures are crucial to protect critical infrastructure and communication networks from cyberattacks. This includes the use of encryption, firewalls, intrusion detection systems, and regular security assessments. Cybersecurity solutions help prevent unauthorized access and ensure the integrity of data and systems.

- **General equipment:**
  - **Resilient Infrastructure:** Technologies that enhance the resilience of critical infrastructure, such as redundant power supplies and backup communication systems, ensure that essential services remain operational during and after an incident.

- **Critical communications, Interoperable communications**
  - **Real-Time Communication Systems:** Advanced communication systems, such as broadband trunk systems and LTE networks, enable instant communication between security personnel and emergency responders. These systems ensure a coordinated and timely response to incidents. Real-time communication is critical during emergencies to share information and coordinate actions.

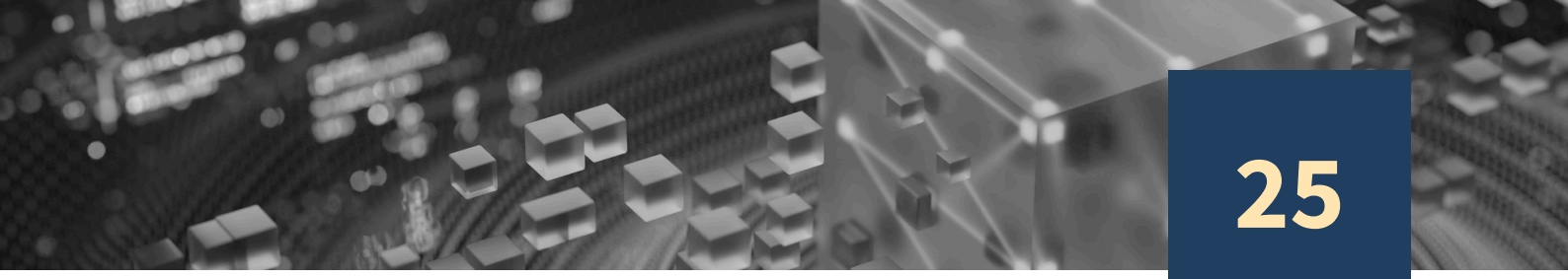
- **Public Awareness Campaigns:** Mobile apps and social media platforms can be used to educate the public about safety protocols and encourage vigilance. These technologies can disseminate information quickly and reach a wide audience, helping to prepare the public for potential threats.
- **Community Engagement Platforms:** Platforms that facilitate communication and collaboration between the public, security agencies, and infrastructure operators can aid in recovery efforts. These platforms can be used to disseminate information, coordinate volunteer efforts, and provide support to affected individuals. Engaging the community in recovery efforts helps build resilience and fosters a sense of collective responsibility.

- **Training and simulation:**
  - **Simulation and Training Tools:** Virtual reality (VR) and augmented reality (AR) technologies can simulate emergency scenarios, providing realistic training for security personnel. These tools help prepare for various threat situations and improve response strategies. For example, VR can be used to simulate a terrorist attack, allowing security teams to practice their response in a controlled environment.

- **Specialised management and control systems:**
  - **Command and Control Centers:** Modern command centers equipped with Geographic Information Systems (GIS) and real-time data integration can manage and coordinate responses to emergencies effectively. These centers can visualize incidents, allocate resources efficiently, and provide a central point for decision-making.
  - **Incident Management Software:** Incident management software solutions streamline the response process by managing alerts, incidents, and crisis situations. These systems can track the status of incidents, provide actionable insights to responders, and ensure that all necessary steps are taken to resolve the situation.

- **Data analytics:**
  - **Data Analytics and Forensics:** Post-incident analysis using data analytics and forensic tools helps understand the cause of incidents and prevent future occurrences. These tools can analyse data from various sources, such as video footage and sensor data, to reconstruct events and identify vulnerabilities.

As a general trend, observations underscore the relevance of Artificial Intelligence (AI) and Machine Learning as key enabling technologies. AI and machine learning technologies are essential for real-time surveillance and threat detection. These systems can analyse video feeds to identify suspicious behaviour, unattended items, and potential threats. For example, AI can be used to detect unusual patterns in crowd movements or identify individuals who may pose a risk. These technologies are also an invaluable enabler to detect and respond to cyber attacks, and to extract intelligence from larges amount of data during pre and post-incident investigations.



CERIS TAKE-OUTS

Discussions held during the event highlighted how innovative technologies and cross-border cooperation can be effectively applied to ensure the safety of these high-profile gatherings. Moreover, this event underscored the importance of continued investment in security research and innovation. Without sustained funding, the EU risks falling behind in its ability to secure public events and, by extension, its citizens. Continued research funding is vital to stay ahead of emerging threats, ensuring that the EU remains a global leader in event security. By fostering collaboration between research institutions, industry, and public agencies, the EU can develop and deploy the most advanced security solutions, making our public events safer for everyone.

The following are some of the most impactful technologies highlighted and showcased during the event:

- **Digital Twins and AI:** These technologies enable remote preparation, optimal deployment of resources, and simulation of various scenarios.
- **Drones:** Used for surveillance, detection of malicious activities, and situational awareness.
- **Sensors:** Both fixed and mobile sensors are essential for real-time monitoring and fast reaction.
- **Advanced Communication Networks:** Building and operating resilient mobile broadband communications networks for public safety, with a focus on cybersecurity and continuous innovation.
- **Cyber-Physical Integration:** Ensuring the integration of cyber and physical situational awareness systems to detect and respond to threats effectively.

MAIN TECHNOLOGIES SUMMARY

The AI-supported analysis of the observations revealed more technologies and with a higher detail than those discussed during the CERIS event, with the exception of Digital twins, which were more thoroughly addressed during the panel discussions. Therefore, the outcomes of the AI-supported analysis presented above serve as a good summary of the main technologies of interest for the protection of major public events:

- **Access control/authorisation:**
  - **Integrated Security Systems:** video surveillance, access control, and emergency alert systems.

- **Surveillance systems:**
  - **Drones and Aerial Surveillance:** equipped with high-resolution cameras and sensors.

- **Digital security products and services:**
  - **Cybersecurity Solutions:** encryption, firewalls, intrusion detection systems, and regular security assessments.

- **General equipment:**
  - **Resilient Infrastructure:** redundant power supplies and backup communication systems.

- **Critical communications, Interoperable communications**
  - **Real-Time Communication Systems:** broadband trunk systems and LTE networks.
  - **Public Awareness Campaigns:** Mobile apps and social media platforms.
  - **Community Engagement Platforms:** Platforms that facilitate communication and collaboration between the public, security agencies, and infrastructure operators can aid in recovery efforts.
-
- **Training and simulation:**
  - **Simulation and Training Tools:** Virtual reality (VR), augmented reality (AR), Digital Twins.

- **Specialised management and control systems**:
  - **Command and Control Centers:** command centers equipped with Geographic Information Systems (GIS) and real-time data processing capacity.
  - **Incident Management Software:** software solutions for managing alerts, incidents, and crisis situations.

- **Data analytics**
  - **Data Analytics and Forensics:** AI-powered data analytics and forensic tools.

ETHICAL, LEGAL AND SOCIETAL CONSIDERATIONS

Deploying new security technologies at major public events presents several ethical and legal challenges, particularly concerning privacy, data protection, and civil liberties. This section does not include a statistical analysis of the ENACT SKB observations because the EUCS taxonomy does not contain an ELS dimension, therefore the observations were not catalogued under this domain.

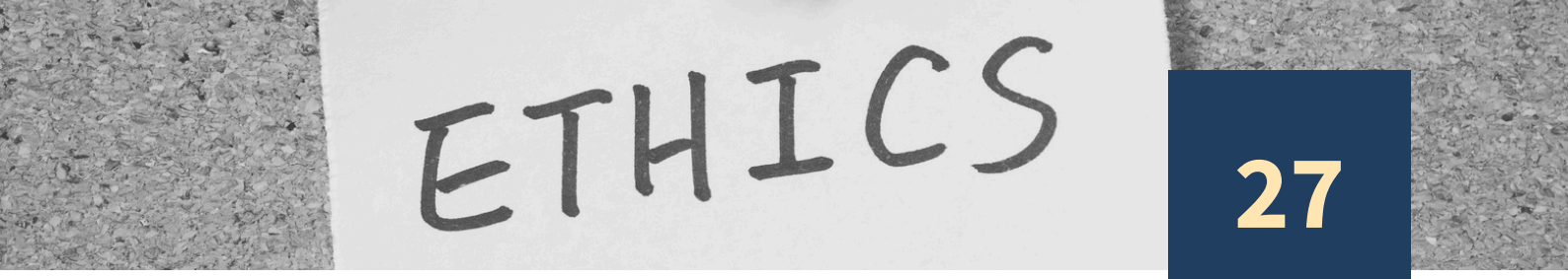
AI-SUPPORTED ANALYSIS OF ENACT OBSERVATIONS

The AI-supported analysis of the content of the observations reveals some of the most important ELS factors to be considered when dealing with the security of major public events. These are the following:

A. Privacy and Data Protection:

- **Surveillance and Monitoring:** The use of AI-powered video surveillance and monitoring systems can lead to extensive data collection, raising concerns about the privacy of individuals attending public events. The deployment of such technologies must comply with data protection regulations like the GDPR to ensure that personal data is collected, processed, and stored lawfully and transparently.

- **Data Security:** Ensuring the security of the collected data is crucial to prevent unauthorized access, breaches, and misuse. This includes implementing robust cybersecurity measures to protect against cyber-attacks and data leaks.



B. Civil Liberties:

- **Freedom of Movement and Assembly:** The deployment of security technologies, such as facial recognition and biometric systems, can potentially infringe on individuals' rights to freedom of movement and assembly. There is a need to balance security measures with the protection of civil liberties to avoid excessive surveillance and control.

- **Discrimination and Bias:** AI and machine learning algorithms used in security technologies can sometimes exhibit biases, leading to discriminatory practices. It is essential to ensure that these technologies are designed and implemented in a way that minimizes bias and promotes fairness.

C. Legal and Regulatory Compliance:

- **Compliance with Legal Frameworks:** Security technologies must comply with existing legal frameworks and regulations, such as the GDPR, the AI Act and other national and international norms. This includes obtaining necessary approvals and ensuring that the deployment of these technologies does not violate individuals' rights.

- **Accountability and Transparency:** There is a need for clear accountability and transparency in the deployment and use of security technologies. This includes informing the public about the use of such technologies, their purpose, and the measures taken to protect their rights.

D. Ethical Considerations:

- **Informed Consent:** Obtaining informed consent from individuals whose data is being collected and processed is a significant ethical challenge. This involves providing clear and accessible information about the data collection process and ensuring that individuals have the option to opt-out.

- **Proportionality and Necessity:** The use of security technologies should be proportionate to the threat and necessary for achieving the intended security objectives. Over-reliance on technology can lead to an erosion of trust and a sense of constant surveillance among the public.

CERIS TAKE-OUTS

The discussions during the event highlighted several important ethical, legal, and societal issues related to the security of major public events.

One of the primary ethical concerns is the balance between security and privacy. The use of advanced surveillance technologies, such as AI and biometric systems, raises questions about the extent to which personal data can be collected and processed. Ensuring that these technologies are used proportionately and justifiably is crucial to avoid infringing on individuals' privacy rights. Additionally, there is a need to consider the societal impact of surveillance, as different societal contexts may perceive the use of such technologies differently.

Overall, the discussions underscored the importance of a balanced approach that considers ethical, legal, and societal implications while implementing advanced security measures for major public events.

ELS SUMMARY

The AI-supported analysis of ENACT observations and the CERIS discussions highlight critical aspects related to the ethical, legal, and societal dimensions of the security of major public events. Both emphasize the importance of privacy and data protection, civil liberties, legal and regulatory compliance, and ethical considerations and stress the importance of a balanced approach.

A summary of the most critical aspects as perceived by the two analyses is the following:

- **Privacy and Data Protection:** There is a clear need to comply with data protection regulations like GDPR and ensure data security. Concerns exist about extensive data collection through AI-powered surveillance and the importance of using surveillance technologies proportionately and justifiably to avoid infringing on privacy rights.

- **Civil Liberties:** It is important to note the potential infringement on freedom of movement and assembly due to security technologies. There is a need to balance security measures with the protection of civil liberties and minimize bias in AI algorithms to avoid discriminatory practices.

- **Legal and Regulatory Compliance:** Despite the complexity of legal frameworks across jurisdictions, compliance with data protection laws at EU and national levels must be ensured. Accountability, transparency, and human supervision in the deployment and use of security technologies is mandatory.

- **Ethical Considerations:** Challenges exist for obtaining informed consent, ensuring proportionality and necessity, and avoiding over-reliance on technology. Public engagement, transparency, and educating the public to build trust and prevent disinformation are extremely important in this regard.

- **Additional Challenges:** Standardization and certification of security tools, ensuring data accuracy, and addressing legal barriers to the use of advanced AI technologies.

A VIEW ON EU-FUNDED PROJECTS

Following the analysis of threats, capabilities, technologies and ELS considerations, a number of projects have been selected from the ENACT SKB in order to assess the extent to which all the key aspects have been covered in EU-funded R&I actions conducted so far. The aim is to find gaps that could serve as a basis to propose additional research in the future addressing the security of public spaces, and in particular of major public events. The 25 projects selected from the ENACT SKB are listed in Appendix A.

The selection has been done based on the ENACT categorisation of those projects [3] . Given that the EUCS Taxonomy does not have a category for “Security of major public events”, projects categorised under the EUCS categories of “Protection of public spaces”, “Explosives and explosive precursors” and “CBRN threats” have been considered for this analysis. The reason is that these categories seem to be the ones closest to the topic addressed following the three-way analysis presented above.

This section does not include a statistical analysis of the coverage of the ethical, legal and societal dimension of the projects because the EUCS taxonomy does not contain an ELS dimension, therefore the projects were not catalogued under this domain. The AI-supported analysis of the projects does not address the ELS dimension either because the extent to which these matters were addressed by the projects under analysis is unclear from the publicly available information.

STATISTICAL ANALYSIS OF RELEVANT PROJECTS

The infographics in the following sections depict the distribution of the mapping Vs. EUSC taxonomy done by ENACT experts to the projects related to the protection of public spaces registered in the ENACT SKB. With the aim to assess if the projects are addressing those areas highlighted as relevant by the observations, the statistical analysis is shown as a comparison of the weight of the different EUSC taxonomy areas between observations and projects.

COMPARISON OF THE WEIGHT OF FCT POLICY AREAS

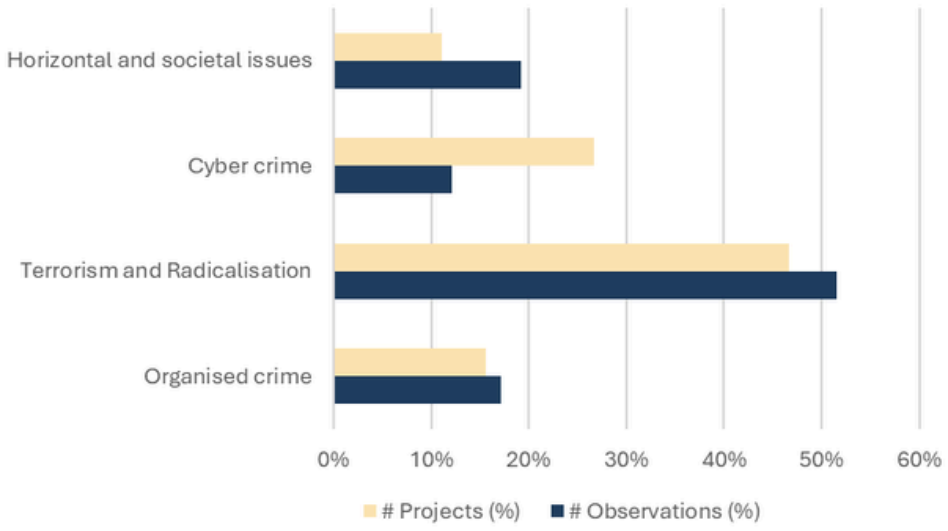


Figure 5 – Comparison of the weight of FCT policy areas L2: Observations Vs. Projects

[3] Projects inherited the categorisation of topics carried out under the 1st ENACT analytical report “FCT R&I: An analysis of EU priorities 2014- 2024” or were mapped manually by ENACT experts if they don’t belong to any of the Horizon FCT topics analysed in such report.

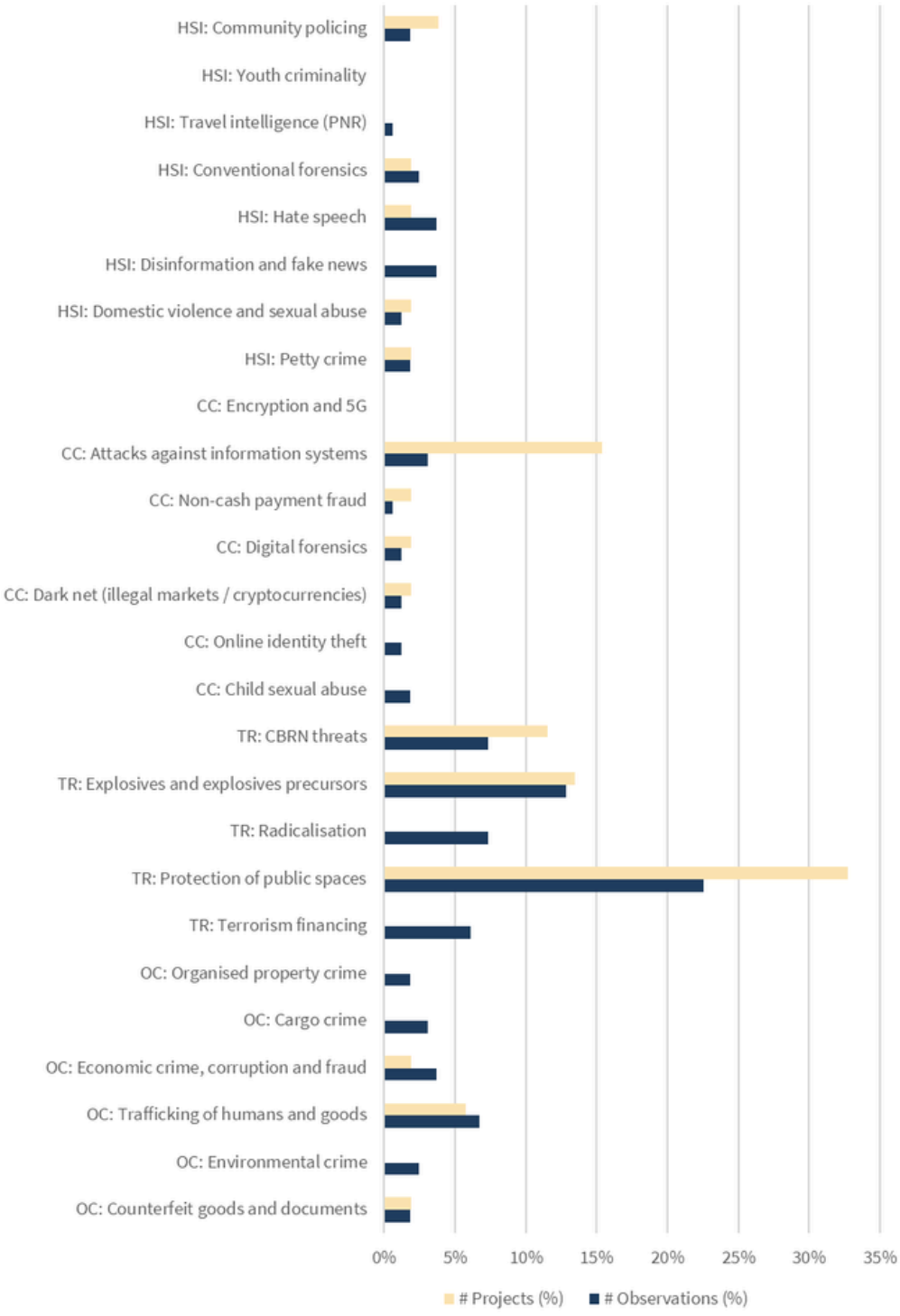


Figure 6 – Comparison of the weight of FCT policy areas L3: Observations Vs. Projects

The distribution of policy areas addressed by the identified projects mirrors largely the policy areas of interest revealed by the observations, which shows a good coverage of the policy domain. This means that no relevant policy area has been overlooked during the past years when funding projects dealing with the protection of public spaces.

COMPARISON OF THE WEIGHT OF FUNCTIONAL AREAS

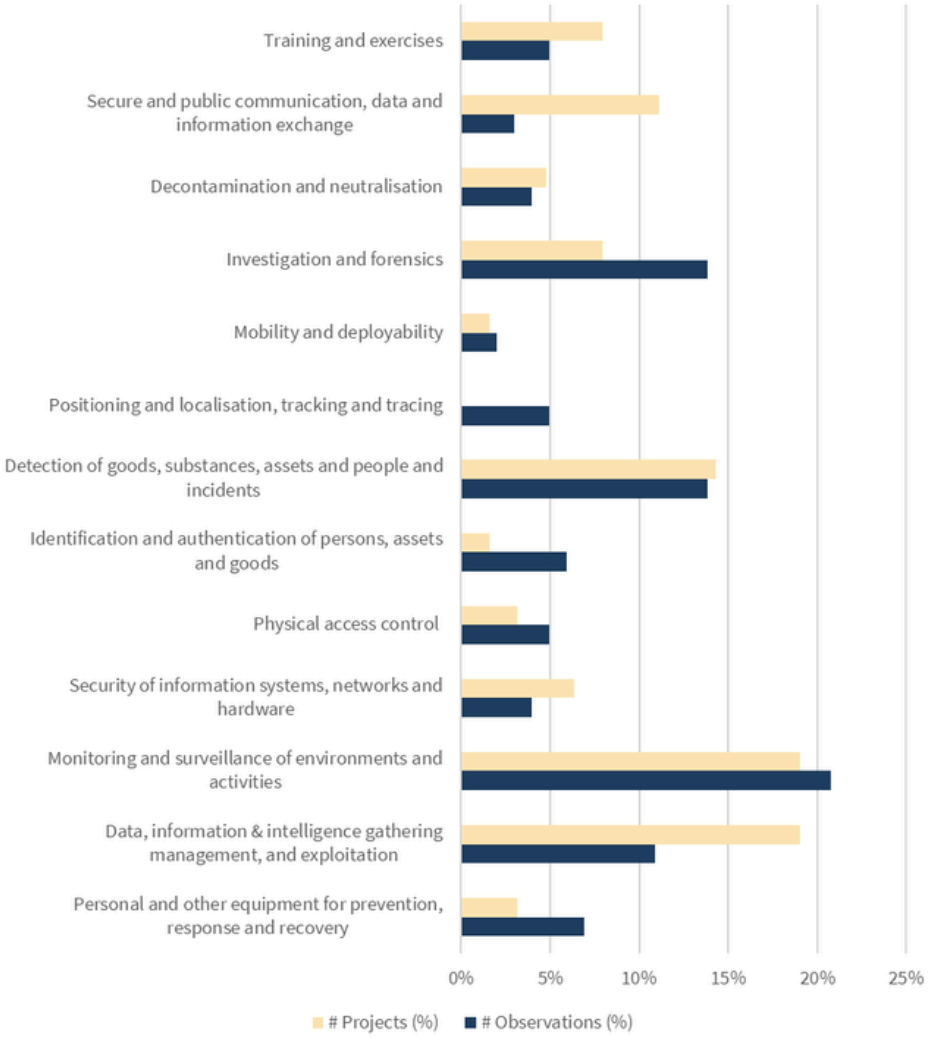


Figure 7 - Comparison of the weight of FCT Functions: Observations Vs. Projects

In the case of the functions addressed by the projects, the comparison with the mapping of the observations, considering also the outcomes of the AI-supported analysis of the observations and the CERIS discussions, shows that while most of the key capabilities have been addressed in past and ongoing projects, the following capability areas could be looked into with higher emphasis in the future:

- Investigation and forensics
- Positioning and localisation, tracking and tracing
- Identification and authentication of persons, assets and goods
- Physical access control
- Personal and other equipment for prevention, response and recovery

COMPARISON OF THE WEIGHT OF TECHNOLOGY AREAS

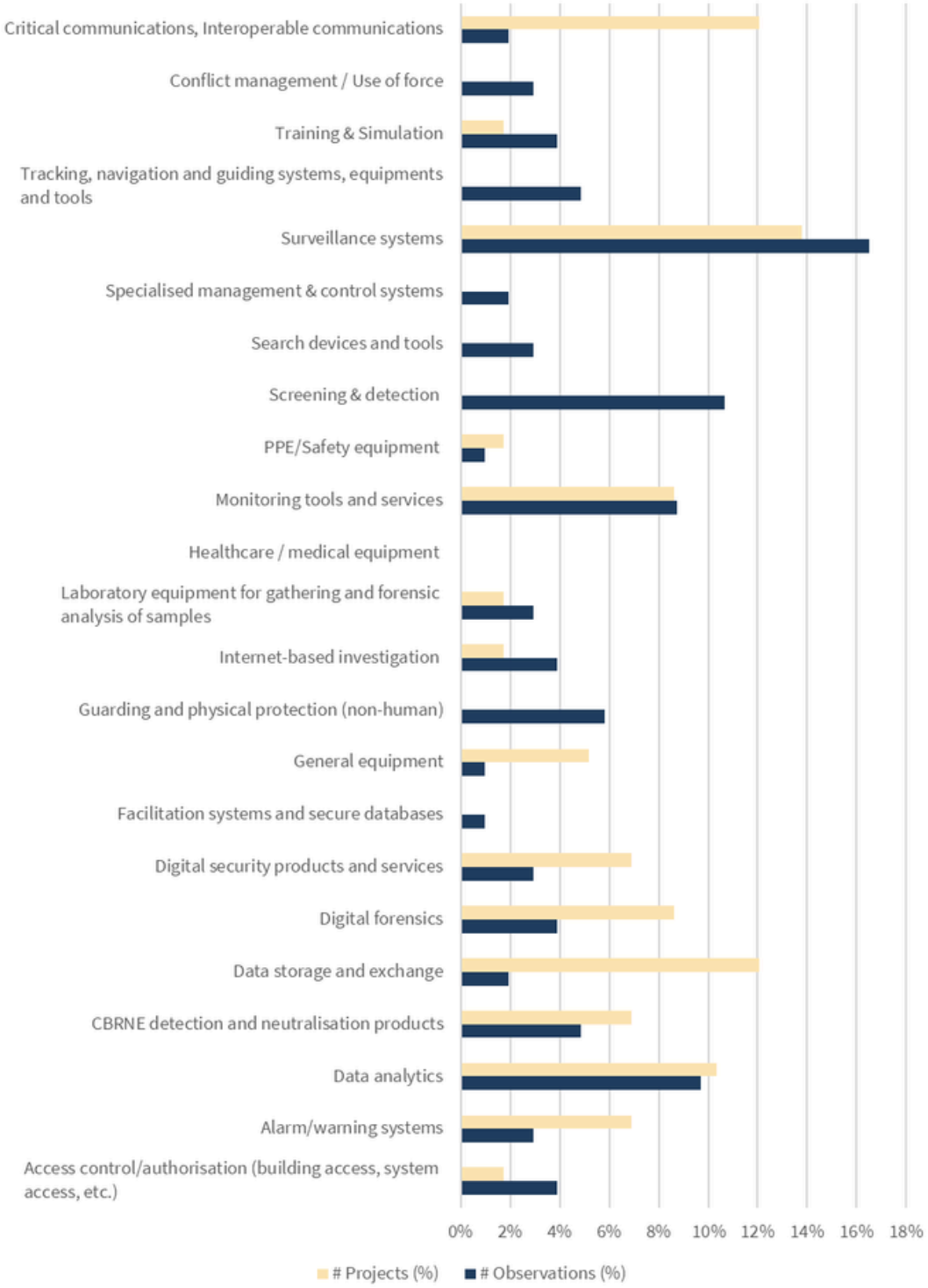


Figure 8 – Comparison of the weight of FCT technology areas: Observations Vs. Projects

In the case of the technologies addressed by the projects, the comparison with the mapping of the observations, considering also the outcomes of the AI-supported analysis of the observations and the CERIS discussions, shows that while most of the key technologies have been addressed in past and ongoing projects, the following technology areas could be looked into with higher emphasis in the future:

- Access control/authorisation
- Training and simulation
- Specialised management and control systems

AI-SUPPORTED ANALYSIS OF PROJECTS SCOPE

This section presents an AI-supported analysis of the coverage of the projects in terms of threats, capabilities and technologies. The objective of the analysis is to identify which of the critical aspects identified in sections above do not appear to be sufficiently covered by past and ongoing actions. This way, it would be possible to identify new untapped areas of research for the protection of major public events in future EU-funded R&I work programmes.

It should be noted that the analysis relies uniquely on information publicly available at CORDIS or at the project websites, therefore there might be deviations from the actual coverage of the projects and this analysis should only be taken as a reference to be further checked if needed.

THREATS

Regarding the two sources of threat identified previously, all the projects in the list seem to address Terrorist Threats, while none of them seems to focus particularly on Petty Crime and Organised crime. This could be a potential line of research for future projects.

Regarding the threat types, there are some predominant threats that have been broadly addressed by the projects.

- **Physical threats:** CBRNE threats are the most addressed (6 projects). Physical attacks and Public panic have been marginally addressed (2 and 1 project respectively), while Sabotage and Trafficking and theft does not seem to have been explored by the projects.
- **Non-Physical threats:** Cyber attacks are the most widely addressed (11 projects), while Communications jamming does not seem to have been explored by any project. Regarding cascading effects, while this is a recurrent theme under R&I related to critical infrastructure, it does not seem to have been significantly addressed by projects related with protection of public spaces.

CAPABILITIES

Considering the key capabilities identified previously, the analysis shows that the ones that have been more widely addressed by the projects are the following:

- Detection of goods, substances, assets and people and incidents: Addressed by 9 projects.
- Data, information & intelligence gathering management, and exploitation: Addressed by 4 projects.
- Monitoring and surveillance of environments and activities: Addressed by 4 projects.
- Security of information systems, networks and hardware: Addressed by 4 projects.

The rest of the functions appear to have been marginally addressed or not addressed at all. This correlates with the mapping comparison presented previously, and confirms that the following functions could be subject to further research in the future:

  - Investigation and forensics
  - Positioning and localisation, tracking and tracing
  - Identification and authentication of persons, assets and goods
  - Physical access control
  - Personal and other equipment for prevention, response and recovery
  - Mobility and deployability (which does not seem unbalanced in the mapping comparison, but which shows poor coverage in the AI-supported analysis)

TECHNOLOGIES

As per the key technologies identified previously, the analysis of the projects shows that all of them have been addressed to a larger or lesser extent.

However, there is a concentration on a number of technologies that have been more intensively addressed by projects. These are the following:

- **Surveillance systems:**
  - **Drones and Aerial Surveillance -** equipped with high-resolution cameras and sensors.

- **Digital security products and services**
  - **Cybersecurity Solutions,** including - encryption, firewalls, intrusion detection systems, and regular security assessments.

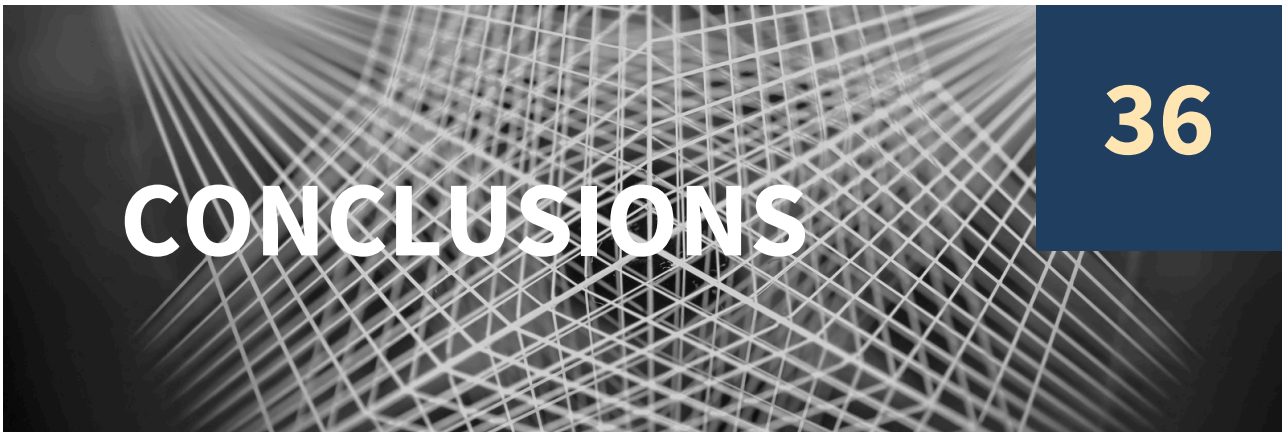
- **Critical communications, Interoperable communications:**
  - **Real-Time Communication Systems,** including **-** broadband trunk systems and LTE networks.
  - **Public Awareness Campaigns,** including - Mobile apps and social media platforms.
  - **Community Engagement Platforms,** including - platforms that facilitate communication and collaboration between the public, security agencies, and infrastructure operators can aid in recovery efforts.

However, and also in correlation with the mapping analysis, the following key technologies appear to have been addressed more marginally:

- **Access control/authorisation**
  - **Integrated Security Systems,** including **-** video surveillance, access control, and emergency alert systems.

- **Training and simulation:**
  - **Simulation and Training Tools,** including - virtual reality (VR), augmented reality (AR), Digital Twins.

- **Specialised management and control systems:**
  - **Command and Control Centers,** including - command centers equipped with Geographic Information Systems (GIS) and real-time data.
  - **Incident Management Software,** including - software solutions for managing alerts, incidents, and crisis situations.



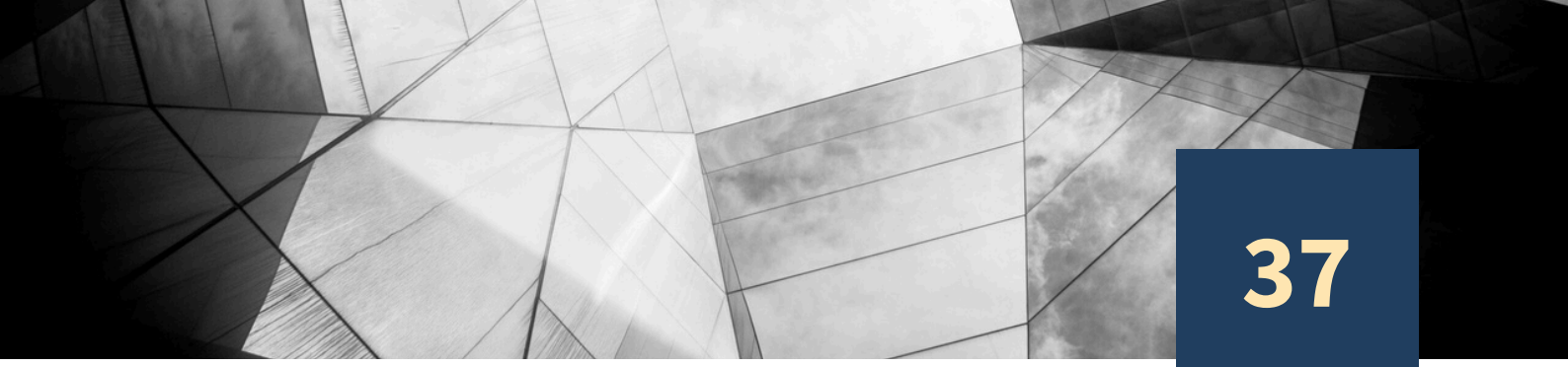
36 CONCLUSIONS

This report has presented a three-way analysis carried out by using observations extracted from the ENACT Structured Knowledge Base (statistical analysis and AI-supported analysis) and the outcomes of the discussions held at the CERIS event on Security of Major Public Events. This analysis has revealed key threats, capabilities and technologies related to the security of major public events.

The three-way analysis of the observations has been compared with the main threats, capabilities and technologies addressed by a set of 25 EU-funded projects selected from the ENACT SKB. This comparison shows that there are some areas that have been widely covered by past or ongoing EU-funded projects, but there are others that were not addressed so intensively. These could constitute elements of future research actions related with the security of major public events.

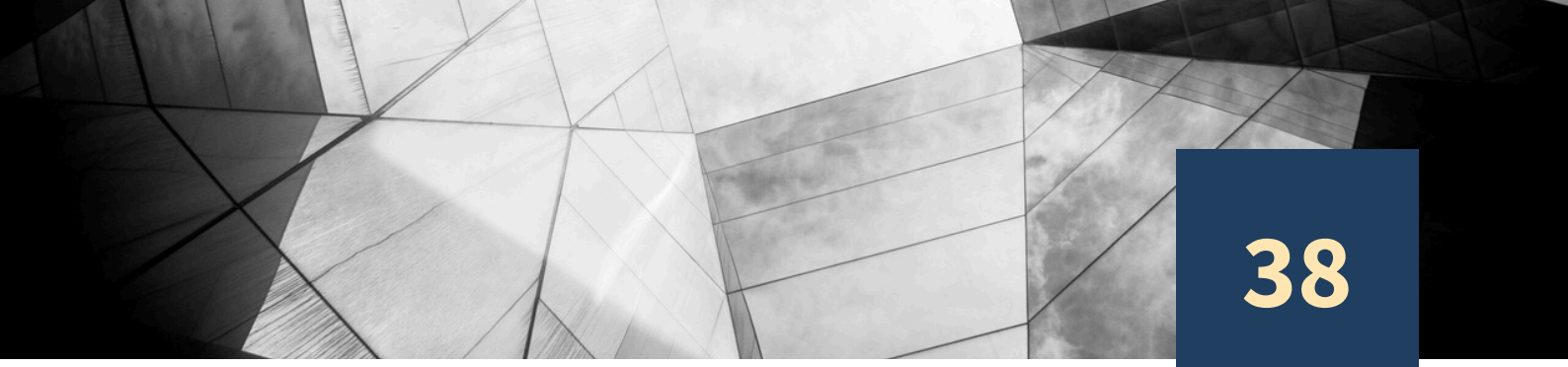
Threats	• Sources of threat: Petty crime and Serious organised crime • Types of threat: Public panic, Sabotage, Trafficking and Theft, Communications jamming, Cascading effects
Capabilities	• Investigation and forensics • Positioning and localisation, tracking and tracing • Identification and authentication of persons, assets and goods • Physical access control • Personal and other equipment for prevention, response and recovery • Mobility and deployability
Technologies	• Access control/authorisation: Integrated Security Systems, including - video surveillance, access control, and emergency alert systems. • Training and simulation: Simulation and Training Tools, including - virtual reality (VR), augmented reality (AR), Digital Twins. • Specialised management and control systems, including - Command and Control Centers, centers equipped with Geographic Information Systems (GIS) and real-time data), Incident Management Software: (software solutions for managing alerts, incidents, and crisis situations.

Even if this report has not provided an analysis of the extent to which ELS aspects have been addressed in the EU-funded projects considered, the analysis of observations has shown that there are some ELS-related issues that are critical when developing and deploying technology for the security of major public events. ELS-related issues that should also be subject to consideration in future research actions, include Privacy and Data Protection, Civil Liberties, Legal and Regulatory Compliance, Ethical Considerations and additional challenges such as standardization and certification.



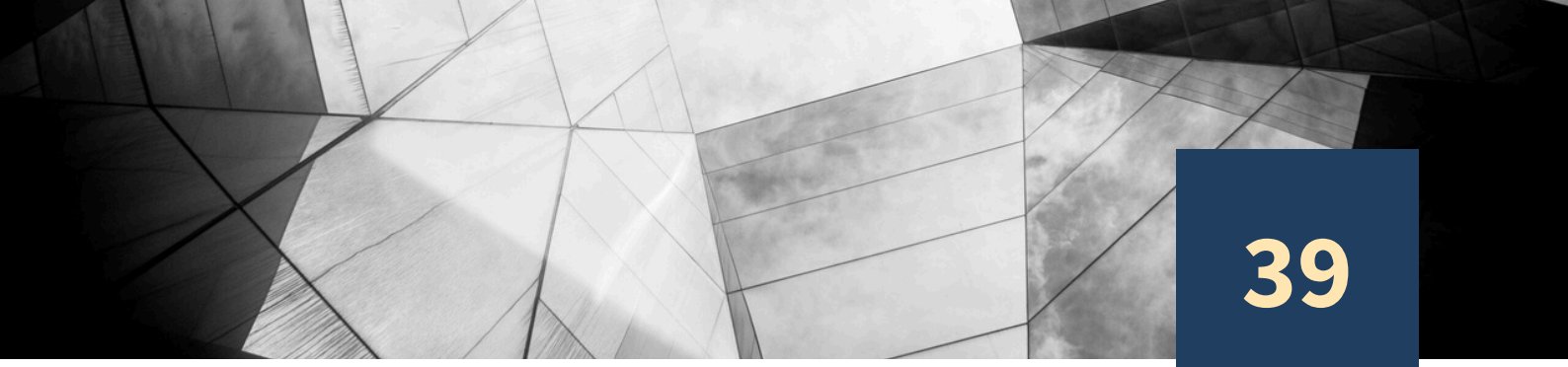
APPENDIX A: LIST OF ENACT SKB OBSERVATIONS

Metadate Mapping	TITLE	PUBLISHER	SOURCE
4	Las empresas llevan el vídeo con IA más allá del entorno de la seguridad	DIGITAL SECURITY MAGAZINE	https://www.digitalsecuritymagazine.com/2024/02/21/las-empresas-llevan-el-video-con-ia-mas-alla-del-entorno-de-la-seguridad/
7	Phase 2 Prototype Development for Unattended Items Detection Successfully Completed	PREVENT PCP PROJECT	https://prevent-pcp.eu/news/phase-2-prototype-development-for-unattended-items-detection-successfully-completed/
22	EU Terrorism Situation & Trend Report	EUROPOL	https://www.europol.europa.eu/publications-events/main-reports/eu-terrorism-situation-and-trend-report
24	Serious and Organised Crime Threat Assessment (SOCTA)	EUROPOL	https://www.europol.europa.eu/publications-events/main-reports/serious-and-organised-crime-threat-assessment
32	COM(2020) 795 COMMUNICATION FROM THE COMMISSION A Counter-Terrorism Agenda for the EU	EUROPEAN COMMISSION	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0795
34	Solutions for Public Space Safety & Crowd Management	SHIELD4CROWD	https://shield4crowd.eu/update/new-catalogue-available-solutions-for-public-space-safety-crowd-management/
35	The 3 Most Challenging Security Scenarios in the Context of Crowd Management	SHIELD4CROWD	https://shield4crowd.eu/update/the-3-most-challenging-security-scenarios-in-the-context-of-crowd-management/
38	El Ejército de Tierra compra a Grupo Etra 36 sistemas antidron para la Guardia Civil	El Radar	https://www.elradar.es/sistemas-antidron-guardia-civil-etrair/
43	Málaga acoge las pruebas de un robot diseñado por la UMA para ayudar a los cuerpos de seguridad	eSMARTCity.es	https://www.esmartcity.es/2024/04/04/malaga-acoge-pruebas-robot-disenado-uma-ayudar-cuerpos-seguridad
50	Compressed images and Video interpolation and enhancement for legal evidence – IMPROVED	France's National Agency for Scientific Research	https://anr.fr/en/funded-projects-and-impact/funded-projects/project/funded/project/b2d9d3668f92a3b9fbbf7866072501ef-a1d6b5de82/?tx_anrprojects_funded%5Bcontroller%5D=Funded&cHash=66086d3ab3bed53be5908989633a70cf



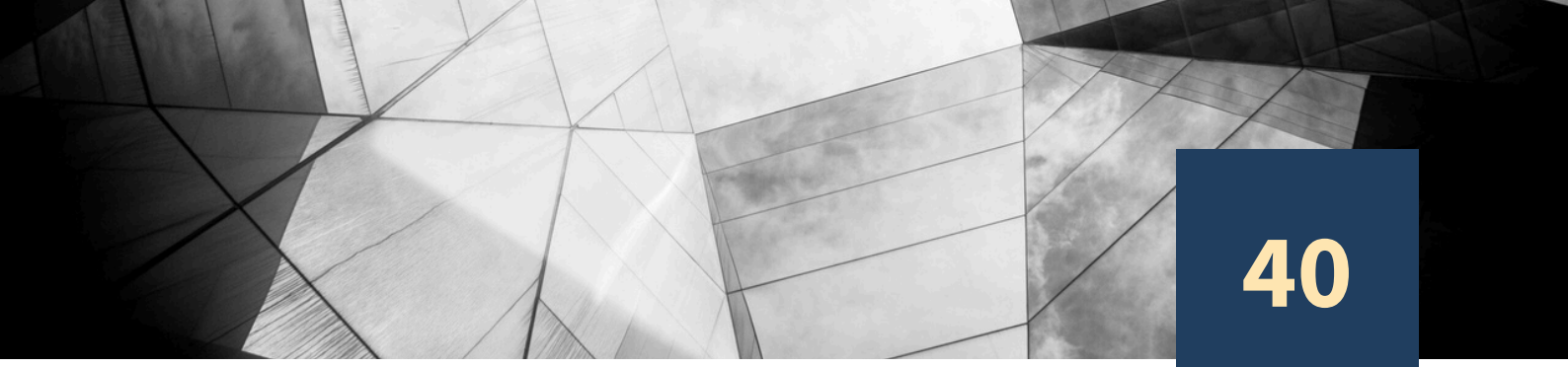
APPENDIX A: LIST OF ENACT SKB OBSERVATIONS

Metadate Mapping	TITLE	PUBLISHER	SOURCE
53	Detection of explosives and drugs by AbsoRpTion in the infrared rAnGe enhanced by arrays of NANoresonators – DARTAGNAN	France's National Agency for Scientific Research	https://anr.fr/en/funded-projects-and-impact/funded-projects/project/funded/project/b2d9d3668f92a3b9fbbf7866072501ef-d470bbcf33/?tx_anrprojects_funded%5Bcontroller%5D=Funded&cHash=256be4709a474e91a803dce729a3ccc7
89	CRIM-TRACK - Sensor system for detection of criminal chemical substances	CORDIS	https://cordis.europa.eu/project/id/313202/reporting
91	DIRAC - rapid screening and identification of illegal Drugs by IR Absorption spectroscopy and gas Chromatography	CORDIS	https://cordis.europa.eu/article/id/91459-new-rapid-drug-sniffer-developed
96	SYSTEM - SYnergy of integrated Sensors and Technologies for urban sEcured environMent	CORDIS	https://cordis.europa.eu/article/id/441968-a-stealth-sensor-network-locates-clandestine-drug-labs-and-explosives-makers
101	CUSTOM - Drugs and Precursor Sensing by Complementing Low-Cost Multiple Techniques	CORDIS	https://cordis.europa.eu/article/id/147269-portable-chemical-sensor-for-multiple-applications
116	C-BORD - effective Container inspection at BORDer control points	CORDIS	https://cordis.europa.eu/project/id/653323/reporting
167	The use of mantrailing dogs in police and judicial context, future directions, limits and possibilities – A law review	Forensic Science International: Synergy	https://www.sciencedirect.com/science/article/pii/S2589871X23001262
175	The European Convention on Human Rights and Policing	EUROPEAN COURT OF HUMAN RIGHTS	https://www.echr.coe.int/documents/d/echr/Handbook_European_Convention_Police_ENG
186	Report on Emerging Terrorist Threats in Europe	Council of Europe Council of Europe Committee on Counter-Terrorism	https://rm.coe.int/-1445-10-2b-cdct-cm-2022-149-adde/1680a9ad62



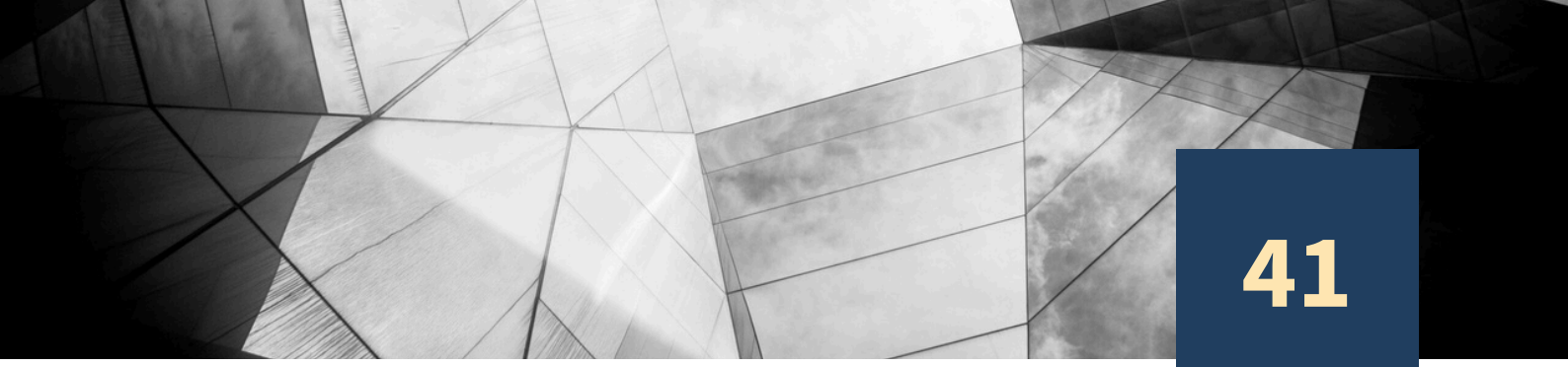
APPENDIX A: LIST OF ENACT SKB OBSERVATIONS

Metadate Mapping	TITLE	PUBLISHER	SOURCE
190	Convention on the Prevention of Terrorism	Council of Europe	https://rm.coe.int/16808c3f55
192	Additional Protocol to the Convention on the Prevention of Terrorism	Council of Europe	https://rm.coe.int/168047c5ea
198	Guidelines on the links between terrorism and transnational organised crime	Council of Europe	https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a19655
204	From Threat to Threat: Terrorism and the Protection of Public Spaces	PRECRISIS Project	https://precrisis-project.eu/wp-content/uploads/2023/10/PRECRISIS-From-threat-to-threat.pdf
205	Newsletter March 2024 | Issue #1	PRECRISIS Project	https://precrisis-project.eu/wp-content/uploads/2024/03/N1_.pdf
215	PRECRISIS Attended the Counter Terrorism Preparedness Network (CTPN) Conference in London	PRECRISIS Project	https://precrisis-project.eu/news/precrisis-attended-the-counter-terrorism-preparedness-network-ctpn-conference-in-london/
216	Bioterrorism in National Counter-Terrorism Legislation: Developments Since 2004 by Barry de Vries	UNICRI	https://unicri.it/sites/default/files/2024-04/ART_7.pdf
217	Seventh Progress Report on the implementation of the EU Security Union Strategy for 2020-2025.	DG HOME	https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2565
239	PRECRISIS Seminar: Protecting Public Spaces – Innovation Challenges and Priorities	PRECRISIS Project	https://precrisis-project.eu/news/precrisis-seminar-protecting-public-spaces-innovation-challenges-and-priorities/
256	Foresight and Key Enabling Technologies	DG HOME - CERIS (Community for European Research and Innovation for Security)	https://home-affairs.ec.europa.eu/news/foresight-and-key-enabling-technologies-2024-03-12_en



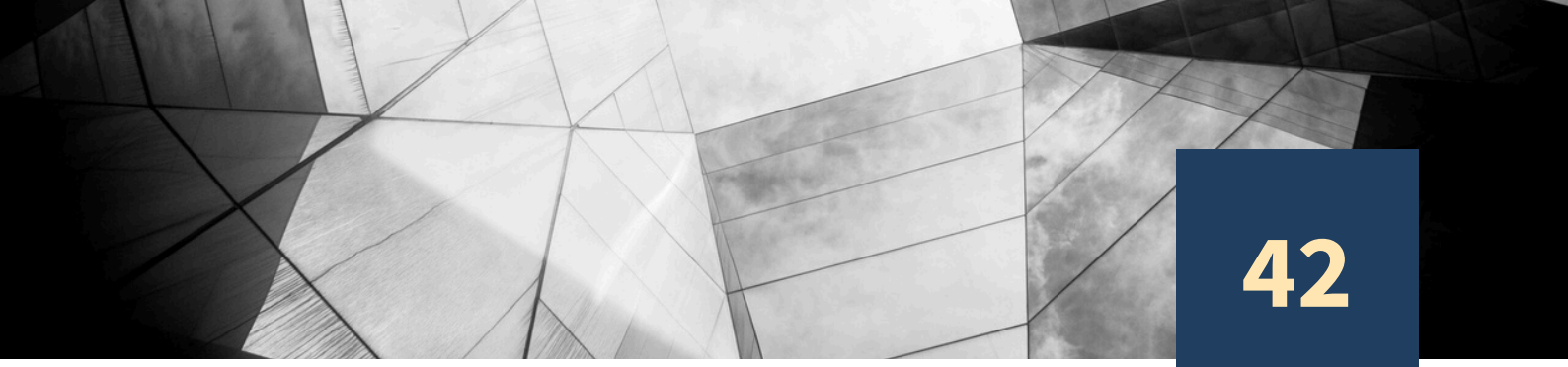
APPENDIX A: LIST OF ENACT SKB OBSERVATIONS

Metadate Mapping	TITLE	PUBLISHER	SOURCE
283	CIVILIAN USES OF UNMANNED AERIAL VEHICLES (UAVs): A THREAT TO NATIONAL SECURITY	FRMDLI	https://cel.hal.science/CREOGN/hal-04026578v1
283	CIVILIAN USES OF UNMANNED AERIAL VEHICLES (UAVs): A THREAT TO NATIONAL SECURITY	FRMDLI	https://cel.hal.science/CREOGN/hal-04026578v1
286	HUMAN INTELLIGENCE IN THE AGE OF NEW INFORMATION AND COMMUNICATION TECHNOLOGIES (NICT)	FRMDLI	https://cel.hal.science/CREOGN/hal-04295440v1
287	OVERVIEW OF THE FRENCH EXTREMIST MOVEMENTS IN 2022	FRMDLI	https://cel.hal.science/CREOGN/hal-04023473v1
298	Hybride dreigingen en Veiligheidsbeleid Nederland 2023-2029	Rijksoverheid	https://www.rijksoverheid.nl/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden
308	Standardisation of crime prevention can be effective and fun	DSP-DISSS	https://disss.one/publications/Standardisation-in-crime-prevention-can-be-effective-and-fun.pdf
309	Routine Activity Theory: how to protect public places	City Security Magazine	https://citysecuritymagazine.com/security-management/routine-activity-theory-how-to-protect-public-places/
334	ENFSI Annual Report 2023	ENFSI	https://enfsi.eu/wp-content/uploads/2024/06/ENFSI_Annual_Report_2023-1.pdf
338	Facing the future: The rise of facial recognition in policing	Policing Insight	https://policinginsight.com/reports/facing-the-future-the-rise-of-facial-recognition-in-policing/
348	Still Aiming at the Harder Targets: An Update on Violent Non-State Actors' Use of Armed UAVs	Perspectives of Terrorism	https://www.jstor.org/stable/27301123
385	One-shot logo detection for large video datasets and live camera surveillance in criminal investigations	STARLIGHT Project	https://zenodo.org/records/10417738



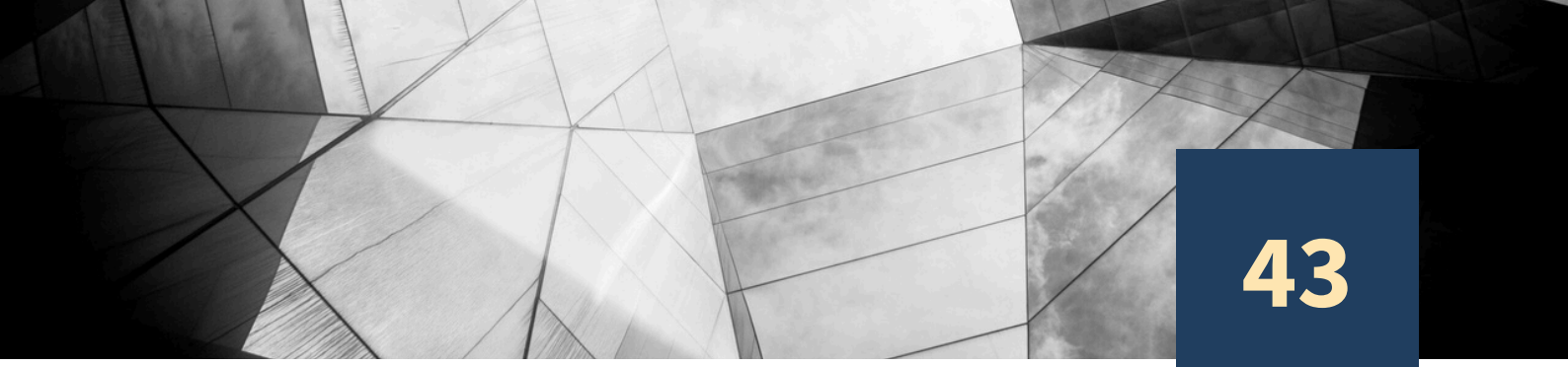
APPENDIX A: LIST OF ENACT SKB OBSERVATIONS

Metadate Mapping	TITLE	PUBLISHER	SOURCE
397	E-commerce security and countering illicit transactions	DG Home CERIS News	E-commerce security and countering illicit transactions - European Commission (europa.eu)
399	Bulgaria and Cyprus receive funding to upgrade external sea borders	DG Home News	Bulgaria and Cyprus receive funding to upgrade external sea borders - European Commission (europa.eu)
415	Exploring AI's Role in Security with Michalis Lazaridis from CERTH	STARLIGHT project	https://www.starlight-h2020.eu/news/2024-07/exploring-ais-role-security-michalis-lazaridis-certh
416	Anonymisation and Pseudonymisation as Solutions for the Protection of Personal Data	PREVENT PCP Project	https://prevent-pcp.eu/wp-content/uploads/PREVENT-PCP-Article-Anonymisation-and-pseudonymisation-as-solutions-for-the-protection-of-personal-data.pdf
469	Enhancing Urban Safety & Counter-Terrorism through Satellite Security	City Security Magazine	https://citysecuritymagazine.com/security-technology/enhancing-urban-safety-counter-terrorism-through-satellite-security/
488	Digitale Maatschappelijke Onrust	DISSS	https://disss.one/publications/20231228-Digitale-Maatschappelijke-Onrust-(def).pdf
489	Perspectieven op Maatschappelijke Onrust Interviews met experts	DISSS-DSP	https://disss.one/publications/Interviews-over-Maatschappelijke-Onrust-versie-1-feb.pdf
516	All tags	Open Security Data Europe	https://opensecuritydata.eu/tags?p=1&limit=25
522	Strengthening the institutional capacities in dealing with cultural heritage and environmental crimes – MK 21 IPA JH 01 23	Eutalia	https://www.eutalia.eu/progetti-internazionali/eu-twinning/strengthening-the-institutional-capacities-in-dealing-with-cultural-heritage-and-environmental-crimes-mk-21-ipa-jh-01-23/
556	Current threats in big cities	USEC - Universal Security & Emergency Channel	https://canalnoticias.usecim.es/amenazas-actuales-en-las-grandes-ciudades/troncal-seguridad/plan-suscripcion-seguridad-usecim/
567	Middle East pager attacks ignite fear of supply chain warfare	Politico	https://www.politico.com/news/2024/09/19/pager-attacks-supply-chain-warfare-00180136



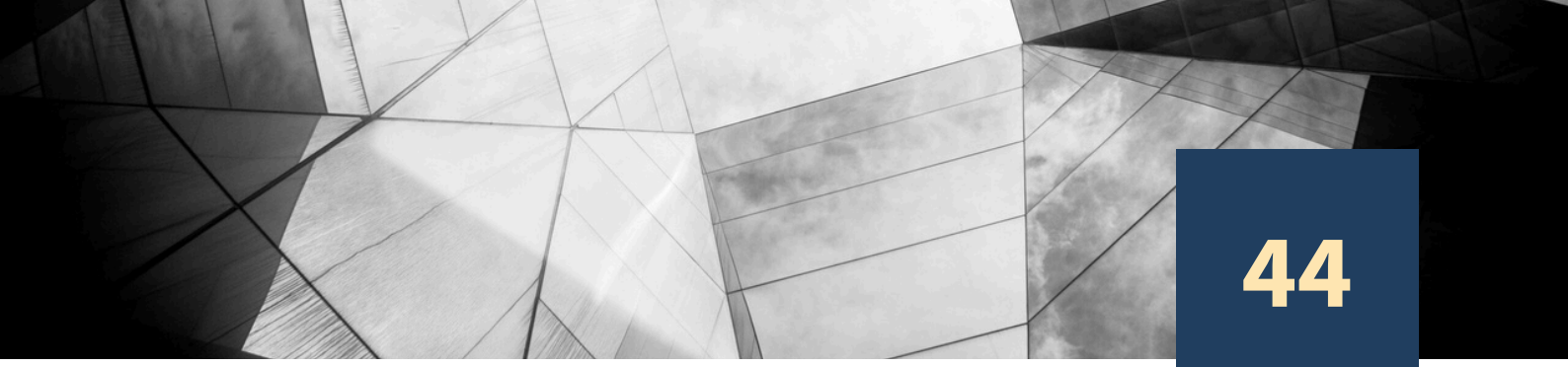
APPENDIX B: A.2 LIST OF PROJECTS

PROJECT ACRONYM	TITLE	ID	TEASER
ENTRAP	Enhanced Neutralisation of explosive Threats Reaching Across the Plot	740560	ENTRAP will deliver combined operational research (OR) methods for assessing and identifying emerging and future counter-measures. The tools will be used for identifying the needed step-changes for countering present, emerging and future explosive threats. The OR tools will...
LETS-CROWD	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings	740466	LETS–CROWD will overcome challenges preventing the effective implementation of the European Security Model (ESM) with regards to mass gatherings. This will be achieved by providing the following to security policy practitioners and in particular, LEAs:(1) A dynamic risk...
ODYSSEUS	PREVENTING, COUNTERING, AND INVESTIGATING TERRORIST ATTACKS THROUGH PROGNOSTIC, DETECTION, AND FORENSIC MECHANISMS FOR EXPLOSIVE PRECURSORS	101021857	ODYSSEUS aims to increase the knowledge on explosive precursors and homemade explosives (HMEs), including precursors not previously studied, and develop effective and efficient prognostic, detection, and forensic tools to improve the capabilities of LEAs towards the...
ROCSAFE	Remotely Operated CBRNe Scene Assessment Forensic Examination	700264	The overall goal of ROCSAFE is to fundamentally change how CBRNe events are assessed, in order to and ensure the safety of crime scene investigators by reducing the need for them to enter high-risk scenes when they have to determine the nature of threats and gather forensics...
SAFE-CITIES	riSk-based Approach For the protEction of public spaces in European CITIES	101073945	Over the past decades, Europe has experienced several terrorist attacks, proving that this threat is still real and serious, while perpetrators are finding new methods to penetrate current security measures. Although grave attacks have so far been rather infrequent, it is...
MELCHIOR	Mechanical Impedance and Multiphysics concealed and hidden objects interrogation	101073899	This project aims to improve substantially a novel technology for fast detection of drugs, explosives, weapons and illicit goods concealed on individuals and in critical cavities of the human body based on infrasound mechanical impedance interrogation, optionally complemented with other harmless and non-contact technologies. Mechanical Impedance interrogation was validated in lab -TRL4- in the multiply awarded H2020 MESMERISE Project, detecting items concealed on trunk under clothes -including critical cases like warm molded materials that remain undetected to other technologies.



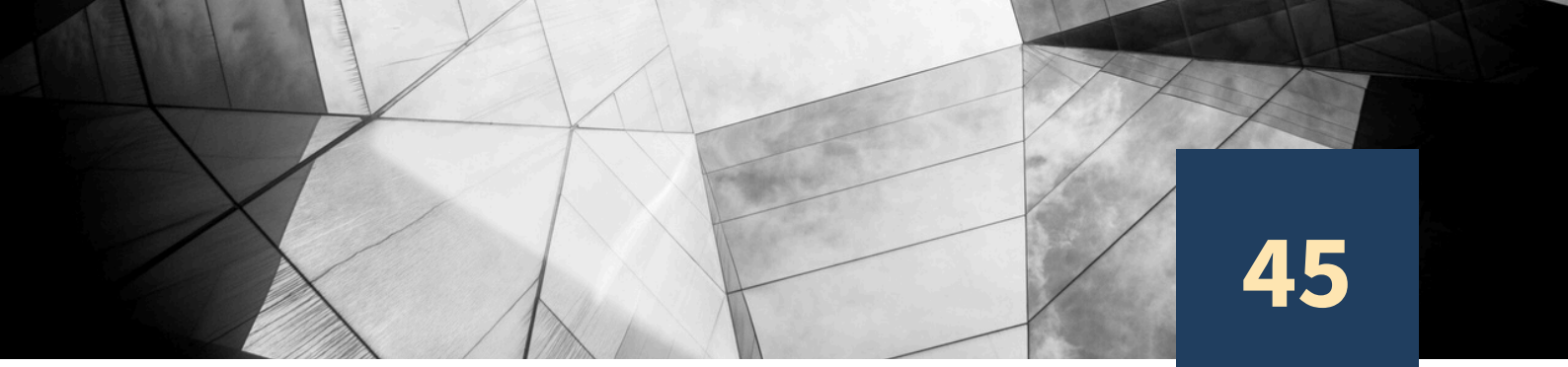
APPENDIX B: A.2 LIST OF PROJECTS

PROJECT ACRONYM	TITLE	ID	TEASER
SHIELD4CROWD	Heightening Innovation Procurements and Setting a Baseline for a Pre-Commercial Procurement (PCP) to Increase Crowd Management Security in EU Public Spaces	101121171	SHIELD4CROWD establishes a baseline for European pre-commercial procurement and technical innovation to protect public spaces.
PRECRISIS	Protecting Public Spaces Through Integrated Smarter Innovative Security	101100539	PRECRISIS aims to strengthen the protection of public spaces by preventing terrorist attacks and violent crimes and mitigating their impacts.
PREVENT PCP	(PROCUREMENTS OF INNOVATIVE, ADVANCED SYSTEMS TO SUPPORT SECURITY IN PUBLIC TRANSPORT)	101020374	PREVENT PCP focuses on augmenting the security in public transport and public areas in the vicinity through innovative procurement of technology solutions that will allow timely automatic detection of potentially dangerous unattended items, identification and tracking of perpetrators, and advanced crisis management system.
DARTAGNAN	Detection of explosives and drugs by AbsoRpTion in the infrared rAnGe enhanced by arrays of NANoresonators		The development of this sensor, capable of identifying chemical molecules thanks to their infrared signature, has many applications that go far beyond the applications to CRBN-E threats and the fight against criminality: biology, detection of food poisoning, medicine, pollution monitoring.
PRESERVE	Protecting euRopean public spaces against Emergent hoStile drone thrEats thRough an adVanced multidimensional shield and cross-border intelligEnce	101168392	PRESERVE will deliver a trustworthy, transparent, and easy-to-use Hybrid C-UAS C2 platform supporting Police Authorities with the prevention, early detection and optimal management of operational response against current and emergent threats in drone technology.
TRANSCEND	Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption	101168023	The transport network is among the so-called Critical Infrastructures' (CIs), which are essential to maintaining the vital functions of the Single Market. While it is by nature a large-scale interconnected and interdependent system to efficiently move people and goods.
TESTUDO	Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention	101121258	As its surroundings changes radically and climate conditions deteriorates, Europe and its Members adapt to these current challenges. To this end and in order to maximise their usability, the EC established a framework of a common policy (EU Security Market study) by...



APPENDIX B: A.2 LIST OF PROJECTS

PROJECT ACRONYM	TITLE	ID	TEASER
PRECINCT	Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection	101021668	EU Critical Infrastructures (CIs) are increasingly at risk from cyber-physical attacks and natural hazards. Research and emerging solutions focus on the protection of individual CIs, however, the interrelationships between Cis has become more complex for example in smart...
IMPETUS	Intelligent Management of Processes, Ethics and Technology for Urban Safety	883286	An interconnected city grid of sensors, such as of cameras or environmental sensors, offers a wealth of actionable Big Data. In addition to better managing traffic and public transit, as well as controlling pollution, they can be used for enhanced policing, crowd control, and...
PRAETORIAN	PROTECTION OF CRITICAL INFRASTRUCTURES FROM ADVANCED COMBINED CYBER AND PHYSICAL THREATS	101021274	PRAETORIAN strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project will provide a multidimensional (economical, technological...
SUNRISE	Strategies and Technologies for United and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe	101073821	The COVID-19 pandemic has highlighted the importance of the continuity of vital services, has shown the need to work together for the common good. It has proven that a pandemic is not only a health crisis and that it does not only disrupt Critical Infrastructures (CIs), but...
S4AllCities	Smart Spaces Safety and Security for All Cities	883522	Smart cities have frontline responsibility to ensure a secure and safe physical and digital ecosystem promoting cohesive and sustainable urban development for the well being of EU citizens. S4AllCities integrates advanced technological and organizational solutions in a market...
SAFETY4RAILS	Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS	883532	Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are becoming even more important means of transportation given the need to address climate change. However, being such critical infrastructures turns metro and railway...
POPART	Protection of public spaces by means of an advanced security platform	N/A	The POP-ART project addresses the domain of Terrorism and Radicalisation. It focuses on enhancing the security of public spaces and large gatherings in Europe, which includes measures to prevent and respond to terrorist threats



APPENDIX B: A.2 LIST OF PROJECTS

PROJECT ACRONYM	TITLE	ID	TEASER
B-prepared	Building PREPAREDness with Collaborative Knowledge Platform, Gamification and Serious Game in Virtual Reality	101121134	Recent disaster events, like the 2021 flood in Germany showed clearly, that even the best alert systems and top first responder organisations can not prevent fatalities and serious damage on property without having prepared the citizens how to act and react during disaster...
TRACY	Data analytics and AI solutions for LEAs	101102641	TRACY aims to gain a deeper understanding of the operational procedures involved in resolving crimes, particularly focusing on data-driven evidence processing. This includes investigating the methods, tools, and type of evidence data utilized.
SAFEGUARD	SAFEguardinG pUblic spAces through intelligent thReat Detection tools	N/A	SAFEGUARD aims at integrating, validating, and demonstrating a next-generation holistic suite of tools that significantly improve LEA capabilities to protect public spaces through the entire lifecycle of their operations, by investigating, detecting, assessing, and preventing terrorist and extremist activities targeting public areas.
GATHERINGS	Balancing security, privacy and cost	N/A	GATHERINGS will investigate the surveillance of public gatherings in order to: Make public events safer, balancing the effects of surveillance on citizens, Law Enforcement Agencies (LEAs), and security professionals; Improve fairness and transparency in surveillance, enhancing the respect for privacy; Promote cost-effective surveillance with a balanced approach that prioritises both security and privacy.

ENACT.
European Network Against Crime and Terrorism

@enact-network

enact-eu.net

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.