STATE OF PLAY REPORT 02

STATE OF PLAY
POLICY REPORT 02

Public Version.
November 2025

Inter-Observatory Coordinator: ENG
Capabilities Observatory: FIMOI
Technology Observatory: CERTH
Markets and Standards Observatory: EOS
Ethics, Legal and Societal Observatory: KUL

ENACT.
European Network Against Crime and Terrorism

02

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.

Report Feedback

We're collecting feedback on this report through the EU Survey Platform, if you'd like to share your thoughts anonymously please click on the link below.

https://ec.europa.eu/eusurvey/runner/ENACT-StateOfPlayPolicy-2025

Funded by
the European Union

Disclaimer

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 European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

Acronyms

AI	Artifical Intelligence
AR	Analytical Report
CERIS	Community for European Research and Innovation for Security
CSA	Coordination and Support Action
CSE	Child Sexual Exploitation
CSEM	Child Sexual Exploiation Material
DORA	Digital Operational Resilience Act
EC	European Commission
ECPAT	Every Child Protected Against Trafficking
EDPB	European Data Protection Board
EDPS	European Data Protection Suprtvisor
EHDS	European Health Data Space
ELS	Ethical, Legal, Societal
ELSO	Ethical, Legal Societal Observatory
ENISA	European Union Agency for Cyber Security
EU	European Union
EUCS	European Union Civil Security
FCT	Fight against Crime and Terrorism
FRA	Fundamental Rights Agency
GDPR	General Data Protection Regulation
H2020	Horizon 2020
HE	Horizon Europe
HSI	Horizonal and Societal Issues
IA	Innovation Action

IOCTA	Internet Organised Crime Threat Assessment
JRC	Joint Research Centre
LEA	Law Enforcement Agency
LLM	Large Language Model
OSCE	Organisation for Security and Co-operation in Europe
PPDS	Public Procurement Data Space
PPE	Personal Protective Equipment
R&I	Research and Innovation
RIA	Research and Innovation Action
RAN	Radicalisation Awareness Network
SoP	State of Play
SRE	Security Research Event
TED	Tenders Electronic Daily
TE-SAT	Terrorism Situation and Trends
UNODC	United Nations Office on Drugs and Crime.

05

STATE OF PLAY FCT POLICY REPORT 2025

The State of Play (SoP) Fight Crime and Terrorism (FCT) Policy Report serves as a crucial resource for informing and guiding European Commission (EC) services by the latest relevant data on the evolving landscape of crime and terrorism. Designed as a policy support tool, the report aims to strategically support and shape FCT policy and research & innovation (R&I) programming by providing a condensed and focused overview of recent developments, key insights, and actionable recommendations from various ENACT activities from September 2024 to July 2025. By integrating findings from multiple sources and events, this report offers a holistic view of the current state of play in combating crime and terrorism within the EU context, based on robust and up-to-date analysis. Also, the report's primary purpose is to consolidate critical findings and policy recommendations derived from ENACT's outputs over the preceding cycle, notably Flash and Analytical Reports. Furthermore, it compiles and summarises the analytical support and outcomes from various high-level discussions, including CERIS FCT workshops, expert group meetings, Project2Policy events, and the Security Research Event (SRE).

06 POLICY VIEW

The 2025 policy view highlights the critical importance of both internal and external security, advocating for both for stronger EU resilience through integrated civilian and military capabilities [1] and emphasising the role of R&I and policy programs and the bridges between them [2].

KEY TRENDS IN THE POLICY AREA

Cybersecurity

Cybersecurity remains a top EU policy priority, though gaps persist in education and dedicated regulatory frameworks [3]. Ransomware and CSEM remain the most persistent cybercrime threats [4]. Policy responses emphasise the need for stronger cross-border cooperation, public-private partnerships, and investment in LEA capabilities [5]. Further policy actions target vulnerable groups such as children [6] and critical sectors [7].

Data Protection

EU digital policies, with EDPS And EDPB, continue to advocate for strong safeguards, compliance with GDPR and the ePrivacy Directive, through opinions on the EU Cyber Solidarity Act [8], Digital Euro Regulation [9], and EHDS [10]. EDPB Guidelines on Pseudonymisation support compliance, offering practical guidance [11]. The EDPB urges for better enforcement and resources rather than weakening data protection regulations.

Artificial Intellingence

The AI Act sets a global benchmark for trustworthy AI governance. Policy debate revolves around exemptions for national security and law enforcement [12]. Critics warn they create loopholes, undermine safeguards, and enable surveillance with limited accountability. Policy discussions call for clearer definitions, stronger oversight, transparency, and robust enforcement to fully respect privacy and fundamental rights. The EC guidelines [13] and their interpretation remain crucial to preventing the weakening of the Act's protections.

Racism

The FRA report on addressing Racism in Policing highlights persistent discrimination and ethnic profiling [14]. Policy recommendations include bans on discriminatory practices, robust accountability mechanisms, independent oversight, improved data collection, mandatory anti-racism training, and community engagement. Tackling racism in policing is essential for legal compliance and for protecting equality, dignity, and justice.

Human Trafficking

Policy efforts to combat human trafficking and forced labour emphasise stronger prevention measures (e.g., labour inspections), clear legal frameworks to protect victims' rights, and improved cross-border cooperation [15], as well as gender-sensitive labour policies [16], integrated approaches to counter-terrorism and anti-trafficking [17] and crisis preparedness. Countering technology-facilitated trafficking requires stronger legislation, enforcement, victim support, and cooperation with tech companies [19].

Child Sexual Exploitation

Policy efforts aim to disrupt online harm to children, call for stronger legislation and enforcement to criminalise all forms of online CSE, investment in victim support services, and improved training for law enforcement [19]. Key recommendations include digital literacy programs, cooperation with technology platforms, and robust data collection to inform policies.

Disinformation and Hate Speech

The EU Code of Conduct on Countering Illegal Hate Speech Online [20] promotes voluntary cooperation between the EC and major IT platforms to swiftly and transparently remove illegal hate speech. This initiative supports the broader EU strategy to combat racism and intolerance, complementing legislation like the DSA [21].

Crisis Management

Policy interventions address gender-based violence, with urgent calls for stronger laws, better data, and funding for survivor support to combat femicides [22]. Rising global terrorism deaths underscore the need for coordinated strategies addressing root causes like poor governance and economic instability [23], with regional security cooperation, community resilience, and human rights-compliant counter-terrorism measures.

Radicalisation

RAN highlights the growing influence of transnational extremist networks and online radicalisation [24]. Policy calls for stronger regional cooperation, improved monitoring of digital platforms, and tailored prevention strategies involving civil society. The TE-SAT 2023 [25] reinforces the need for cooperation, robust measures to counter radicalisation (especially online), and investment in protecting public spaces.

08

TECHNOLOGY VIEW

During the first full implementation cycle of ENACT, European civil security R&I efforts continued to emphasise technological solutions to emerging security challenges. Specifically, stakeholders focused on deploying “responsible” security solutions, i.e. effective technologies that also meet citizens’ expectations for privacy, transparency and accountability.

The EU Innovation Hub’s Annual Event [26] highlighted key technology priorities, including enhancing strategic foresight using Key Enabling Technologies, advancing biometric identification systems through dedicated testbeds, leveraging explainable AI for policing, and addressing encryption and lawful access while safeguarding fundamental rights. Experts stressed the need to “industrialise research results” so that lab innovations can be turned into deployable tools.

Commercial and Operational Products

Several new security technologies reached or neared operational readiness by the end of the first full implementation cycle of ENACT, with some being showcased as promising products for law enforcement. The EC announced the winners of its Security Innovation Awards 2023 [27], recognising innovative tools in the FCT domain. ENACT is providing financial support to these winners to accelerate their market uptake. Featured product highlights include:

T4i DOVER: A drone-mounted chemical detection system for reliable, real-time identification of hazardous chemicals during drone flights by addressing challenges like high speed, altitude changes, and environmental factors. It can detect vapor-emissions of dangerous substances in flight or hover and overlay geo-referenced, timestamped hazard alerts on a map, giving first responders a rapid airborne CBRN detection capability [28].

CRYPTOPOL: A cryptocurrency-tracing training platform that offers investigators a hands-on simulation environment to practice tracking illicit cryptocurrency transactions in realistic scenarios. By immersing officers in gamified investigations, it builds capacity in crypto forensics and financial crime investigation [29].

Drug Hunter Narcotic Analyser: A fast, field-deployable device for rapid drug identification. This portable analyser can detect narcotics quickly on-site, allowing police and border agents to immediately test suspicious substances, streamlining drug seizures and reducing reliance on lab turnaround times [30].

Projects view

Ongoing EU-funded projects in the FCT domain are tackling a diverse range of technological challenges, particularly in **cybercrime, digital forensics, AI security, and trafficking prevention**. Several initiatives are focused on enhancing the trustworthiness and explainability of AI systems: for example, the NeuralSentinel tool developed under the **KINAITICS** project [31] aims to improve the reliability of neural networks by detecting failure models and adversarial inputs, which is important in AI-assisted law enforcement decision-making. In technical malware analysis, the **CYBERSPACE** initiative [32] advances machine learning–driven malware classification and attribution, aiding LEAs in cyberthreat investigation and response. Meanwhile, **RAYUELA** project [33] uses gamification and behavioural analysis to combat cybercrime by engaging young users in a narrative-based video game designed to study online behaviours and inform prevention strategies. Collectively, these and similar projects showcase how Europe is building a robust ecosystem of AI-enabled and privacy-aware technologies to support law enforcement across digital and physical domains.

Science View

During the first full implementation cycle, scientific research in the FCT field focused on **digital threats, advanced forensics, and the growing use of AI** in security. Several papers examined how law enforcement can monitor the dark web using crawler technologies, while also highlighting legal and ethical challenges. Biometric research explored gait recognition for surveillance, and studies reviewed how to improve reliability in real-time identification systems.

Digital forensics also saw important developments. Researchers proposed new ways to **recover evidence** from platforms like Discord, vehicle systems, and virtual machines. Other studies tackled issues like detecting tampered surveillance footage, analysing deepfakes, and dealing with fingerprint spoofing. There was growing attention on how **generative AI and large language models (LLMs)** could be misused to spread **misinformation**.

New uses of **digital twin technologies** were explored for simulating risks in public spaces, while **AI and sensors** were also used to track **environmental crimes**. Policy-focused research also looked at AI strategies in defence, access to encrypted data, and the **future impact of quantum computing** on cybersecurity.

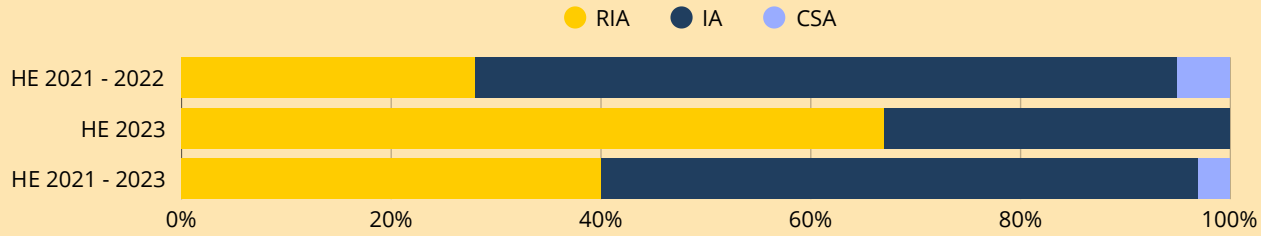
10 MARKET & STANDARDS VIEW

The Market Observatory offers a detailed analysis of both demand and supply, as well as the evolving ecosystem in the FCT domain. The initial focus is on assessing the size of the FCT market throughout its development cycle. This includes the creation of innovative solutions, and the support provided by EU funds. The analysis compares EU funding trends between the Horizon 2020 and Horizon Europe, examining the types of actions funded and the distribution of both public and private funding.

FCT Research & Innovation

Considering HE FCT calls from 2021 and 2022, the total net EU contributions made up about 90% or €81.6 million. When adding the 2023 total costs and net EU contributions, the total net of EU contributions accounts for 91.4%, or approximately €118.2 million. The number of grants for FCT R&I signed for 2023 (9) is also in line with the previous average established (10) [34].

While the share of Research and Innovation Actions (RIA), which are funded at 100% of costs compared to the Innovative Actions (IA), which are funded at 70% of costs, fell drastically to 28% in at the start of HE (from 80% in the H2020), there is evidence this is equalling out as the framework progresses (57% for IA and 40% for RIA. The share of coordination and support actions remains low, demonstrating the priority under FCT to focus on solutions and innovations, especially those closer to the market.



FCT Procurement

Based on information from the Public Procurement Data Space (PPDS) [35], listed under CPV code 35, Security, firefighting, police, and defence equipment, approximately 700,000 relevant procedures were identified, with around 20% related to the defence sector. **Germany** (by a large margin)**, Poland and Spain** were the largest procurers of **FCT equipment.**

Almost **80% of procedures were open calls**, rather than operating under a restricted or negotiated procedure, **increasing competition and choice** for the procuring entity; however, there are differences between Member States, with Netherlands and Austria having comparatively lower numbers of open calls while almost all calls in Portugal were open.

In terms of contract types, the **majority were for supplies** rather than for works or services, perhaps indicating a **greater need for equipment** while services are already provided by the public sector entity (police, ministry of interior, or similar). The majority of **contracting entities were central government authorities**, alongside local and regional entities. Furthermore, international or supranational bodies such as the EU had far fewer procedures for equipment, demonstrating a difference in their role.

Funding Opportunities

Following on the AR#1 'FCT R&I: An analysis of EU priorities 2014 – 2024[1] on Funding Priorities, the same methodology was applied to characterise the priorities of the 2025 HE Cluster 3 Work programme [36] and its Fighting Crime and Terrorism destination based on the 4 call topics.

1. Modern Information and Forensic Evidence Analysis (HORIZON-CL3-2025-01-FCT-01): focuses on enhancing the capabilities of security practitioners through modern tools and methods for forensic evidence analysis and frontline policing, emphasising advanced technology solutions that improve the efficiency and effectiveness of LEAs.

Policy Area	Function Area
Organised Crime	Data, Information & Intelligence Gathering, Management, and Exploitation
Cybercrime	Investigation and Forensics
Horizontal and Societal Issues	Training and Exercises

2. Prevention, Detection, and Deterrence of Crime and Terrorism (HORIZON-CL3-2025-01-FCT-02): aims to deepen the understanding of societal issues related to FCT, developing innovative tools and training, with a strong emphasis on community engagement and awareness-raising.

Policy Area	Function Area
Organised Crime	Data, Information & Intelligence Gathering, Management, and Exploitation
Terrorism & Radicalisation	Monitoring and Surveillance of Environments and Activities
Horizontal and Societal Issues	Training and Exercises

3. Improved Intelligence Picture and Enhanced Prevention of Organised Crime (HORIZON-CL3-2025-01-FCT-03): targets the improvement of intelligence gathering and sharing mechanisms to better prevent, detect, and deter organised crime, including cross-border and training.

Policy Area	Function Area
Organised Crime	Data, Information & Intelligence Gathering, Management, and Exploitation
	Monitoring and Surveillance of Environments and Activities
	Training and Exercises

4. Humanitarian Demining and Unexploded Ordnance Disposal (HORIZON-CL3-2025-01-FCT-04): addresses the critical need for safe and effective demining activities in post-conflict areas, emphasising modern tools and methodologies for humanitarian demining, as well as risk education and awareness-raising activities to protect civilians.

Policy Area	Function Area
Horizontal and Societal Issues	Decontamination and Neutralisation
	Training and Exercises
	Detection of Goods, Substances, Assets, and People and Incidents

The priorities for 2025 build on the foundations from 2014 to 2024, to address new and emerging challenges. The emphasis on technology integration, training, and societal issues reflects a proactive and adaptive approach to enhancing security and combating crime in the EU. The continuity in focus areas underscores the persistent nature of certain threats, while the introduction of new priorities highlights the need for continuous innovation and adaptation in the face of evolving challenges.

Tender Opportunities

Around 9,000 relevant tenders were identified though EU TED, and mapped to the EUCS taxonomy. The largest category is **Personal & Other Equipment for Prevention, Response, and Recovery** (45%), indicating a significant investment in equipment for frontline personnel to handle emergencies. This is followed by **Monitoring and Surveillance of Environments and Activities** (37%), indicating a strong preference among MS for prevention and preparedness over post-event investigation or detection.

Considering EUCS technologies, the most prevalent is **General equipment**, including tools, vehicles, and field equipment, indicating a general operational readiness. The second, **PPE/Safety Equipment,** shows the importance of protecting personnel. Thirdly. **Surveillance systems** are used for real-time monitoring and dissuasion, combined with **Alarm/ warning systems,** creating an early warning and a rapid response. Investments in **Digital security products and services**, reflect digital transformation.

Overall, Member States and their investments are more aligned with the EC's crisis preparedness and physical security objectives, than digital, cyber and forensic-related ones.

[1] ENACT Analytical Report -FCT R&I: An analysis of EU priorities 2014 – 2024. https://enact-eu.net/wp-content/uploads/2024/04/ENACT-Analytical-Report-01-FCT-RI-An-analysis-of-EU-priorities-2014-2024.pdf

ETHICAL, LEGAL & SOCIETAL VIEW

The regulatory landscape is undergoing a significant transformation. Normative initiatives as responses to new technologies, opportunities, and challenges can be easily found, with actions at national, regional, and international levels. While the adoption of the AI Act still represents an important milestone, other norms also impact the FCT domain. Other countries are working on thematic regulations, and international bodies such as the UN, Organisation for Economic Co-operation and Development, and Council of Europe are also addressing the role of AI. Cybersecurity initiatives are becoming more relevant (e.g., Digital Operational Resilience Act, DORA, and UN Cybersecurity treaty), as are online children's protection, especially combating child sexual abuse. In topics that fall in a regulatory gap, best practices and ethical considerations still represent a significant role.

This section provides an overview of the key trends identified in the ELSO during the first Full Implementation cycle. To better capture the granularity of ELS topics, categories from the Joint Research Centre (JRC) cybersecurity ontology were selected.

Anonymity, pseudonymity, unlinkability, undetectability, or unobservability

This theme plays a central role in discussions surrounding cybercrime and personal data protection, not just in Europe but globally. Long-term observations are mainly connected to child sexual abuse in online environments, for example, the Global Threat Assessment [37] and cloud-based technology [38].

Biometric methods, technologies and tools

Biometrics are closely connected to the AI Act [39][40], while observations also relate to individual identification, especially in documents involving travel data. Observations come from different sources, especially scientific material and practitioners' reports [41]. Related topics, such as facial recognition or electronic identity cards, are part of the public debate [42][43]. Furthermore, new regulatory initiatives addressing specific systems and tools were also found. This category illustrates the increasing convergence of ELS topics and technical debates.

Citizen cooperation and reporting

The importance of cooperation between LEAs and citizens and their role in combating organised crime is predominant, especially in disappearances and human trafficking [44][45]. Furthermore, observations are also connected to cybercrimes, especially child sexual abuse [46]. Observations also show how citizen collaboration gains even more importance in situations involving vulnerable groups [47].

Cybersecurity technologies

This category encompasses a significant portion of ELSO's focus, covering data security, security tools, and other cybersecurity measures. The scope also connects to general technologies, such as LLMs [48], and addresses specific market needs, such as the financial sector [49]. Online security also represents a crucial and relevant sub-topic, reflecting the pervasive need to protect digital assets and activities.

Data security and privacy

This category largely aligns with the EUCS Functions **Data, information & intelligence gathering management, and exploitation**. Within the FCT domain, this category addresses the use of data by LEA for the investigation and prosecution of crimes [50] [51].

Investigations of computer crime (cybercrime) and security violations

This category offers a more specific focus on the investigative actions of LEAs, complementing other classifications. Many observations relate to children, highlighting the challenges in understanding and leveraging technological tools used by minors on a daily basis [52]. Additionally, human trafficking and cybersecurity were also prominent themes in the relevant ELS observations [53][54].

Legal aspects

This is a broad category includes AI regulation, protection of fundamental rights, terrorism and radicalisation are some of key themes [55]. International regulatory initiatives and collaboration are also themes categorised under this umbrella [56].

Privacy concerns

Observations within this category primarily address the protection of children's privacy and the crucial parents' role in guaranteeing it [57]. Only one observation was not directly connected to family digital well-being, but rather to the challenge of reconciling privacy and innovation [58].

Safety and security

Observations under this category are highly correlated with terrorism and radicalisation, showing a strong connection between "Safety and Security" and national security [59]. Nonetheless, other topics are also addressed, particularly those concerning international organisations and the broader need for global security and collaboration on specific issues [60].

Trust and privacy

While this topic is complementary to others, such as "Privacy Concerns" or "User acceptance", this category serves as a means to classify ethical and societal aspects within the FCT domain including more specific categories, such as spyware [61], standardisation [62], and forensics [63].

User acceptance of security policies and technologies

Observations in this category focus on end-user acceptance, as well as public perception of certain approaches [64] and technologies in the FCT domain. Considerations around this topic are of utmost importance for the ELSO and policy development. Nevertheless, challenges in reconciling transparency and national security [65], and in assessing acceptance, are well-known.

14 HIGHLIGHTS

The latest updates highlight enhancing cybersecurity education and capacity building in Europe, alongside data protection, AI, and digital security innovation.

Capability Building through Education and Training: Recent initiatives include educational games, training resources, and frameworks to develop cybersecurity skills at all levels, building a resilient workforce.

Policy Directives in Education: Maturity assessments and frameworks align national and EU education strategies, balancing awareness with professional skills. New opinions from the EDPS and EDPB call for clearer safeguards, stricter purpose limits, and stronger oversight.

Governing AI: The EU AI Act has introduced bans on harmful practices such as social scoring and most real-time biometric identification, aiming to safeguard fundamental rights; however, broad exemptions for national security and serious crime investigations remain contentious and may face future tightening.

Operationalising Innovation: Operationally, the EU Innovation Hub for Internal Security actively fosters cross-border collaboration, creating opportunities for private sector partnerships, collaborative research, and pilot programs.

Broader Strategic Needs: Wider EU strategies signal future opportunities for secure cross-border data sharing, incident response, and trusted digital services.

These developments reflect a clear EU-wide trend towards balancing innovation and robust security with strong rights protections, creating opportunities for new technical solutions, compliance services, and cross-sector partnerships.

Four key topics emerged from the observations as highly relevant for ELSO.

Security of Children Online: Children are digitally native, developing tech skills early, before legal, psychological, or social maturity, leaving them vulnerable. Developments include rules for protecting children, fighting online child sexual abuse material, and managing children's access to digital platforms.

AI Regulation, Use, and Acceptance: Harnessing full potential of AI can offer solutions to diverse ELS challenges, but the risks associated with its are also well-documented in our observations, echoed by the EU AI Act.

Cybersecurity: The security of data and technology is increasingly essential, with efforts transcending countries, requiring collaboration. New regulations set minimum cybersecurity rules and guarantees, safeguarding fundamental rights.

Digital Literacy: Toolkits and best practices for children's online presence or use of AI tools by LEAs, are invaluable for addressing ELS. End-users and individuals affected by emerging technologies need to be empowered to better accept or critically evaluate these innovationsand learning from victims and specialists.

Several notable events took place in the FCT domain over the past months. **INTERPOL's 52nd European Regional Conference** [66], gathered 150 senior LEA officials from across Europe to address emerging transnational threats. Delegates discussed the evolving nature of crime, including the "dark side of AI" and links between organised crime and terrorism, and shared tools (like INTERPOL's new "Silver Notice" [67] for asset tracing) to strengthen international police cooperation. Another major event was **SRE 2025**. This flagship EU forum brought together over 600 participants from academia, industry, end-users, and policy under the theme "Boosting security through EU-based innovation", featuring discussions on EU security research priorities, live demonstrations of cutting-edge solutions, and an exhibition of 50+ EU-funded security projects.

Regarding the upcoming events, **Europol's Cyber Innovation Forum** 2025 [68] brings together law enforcement, academia, and industry to explore innovative solutions for combating cyber-enabled crime, including online child exploitation and encrypted communications. The **International Security Expo 2025** [69] features a dedicated Counter Terrorism Zone, live demonstrations, and expert briefings on AI surveillance, hybrid threats, and protective technologies. It offers a platform for FCT end-users to engage with the solutions and operational needs.

Observations gathered during this period highlighted a strong interplay between science, technology, and policy in shaping the European FCT market.

AI and Data Analytics: AI and big data solutions are now key for surveillance, forensics, and cybersecurity, used in vehicle recognition and forensic labs with speech-to-text tools. Their adoption shows technological advances and procurement strategies focused on efficiency and cross-border interoperability.

Cybersecurity and Digital Resilience: Protecting digital infrastructures is a key market driver. Investments focus on cryptography, infrastructure security, and digital evidence against cybercrime. Policy, research, and procurement trends emphasise the need for resilient cybersecurity in Europe.

Emerging and Dual-Use Technologies: Beyond mainstream solutions, attention shifts to frontier innovations like quantum communication, advanced navigation, robotics, and drones. These serve civilian and security needs, but raise ethical, standardisation, and sustainability questions.

Innovation and Procurement: Procurement plays a key role in shaping the market. Public procurement of innovation fosters partnerships and accelerates the adoption of technologies. EU funding, like HE, guides resource allocation, focusing on AI governance, supply chain resilience, and counter-terrorism.

The strategic adoption of AI, cybersecurity, and emerging technologies shows a response to threats and a commitment to creating a resilient, innovation-driven security market in Europe.

16

EU CIVIL SECURITY TAXONOMY

The use of the EUCS Taxonomy as the backbone of ENACT's analytical approach has been consolidated throughout the first implementation cycle. The taxonomy has proved to be an invaluable tool to systematically assess the vast and scattered information landscape, allowing ENACT to deliver structured knowledge directly mapped to the defined categories. The work presented in flash reports, advanced reports, and maps (notably the stakeholders map) demonstrates how the taxonomy facilitates the elaboration of sound, traceable, and comparable analyses, and significantly improves communication while minimising information loss.

ENACT has continued to meticulously document the potential weaknesses of the taxonomy, forming the basis for a detailed analysis and several recommendations.

Policy

The policy category mixes policies, security threats and operational activities, leading to **redundant classifications**. Furthermore, some policy areas do not have **sufficient visibility**, e.g., the production and trafficking of drugs, the narrow classification of hate speech rather than hate crime, the opportunity to bundle explosives with CBRN. The **horizonal and societal issues** class are not fully aligned to FCT and lack sub-classifications, as well as functional and technological sub-categories

ELS

ELS topics are not well represented at policy levels two and three; for example, **biometrics** is not considered under FCT. A topic on **fundamental rights** would fit well under **horizontal and societal issues.**

Products / Services

Many technology areas are not well represented, e.g., drones or vehicles. From an R&I perspective, key enabling technologies could be included, while communications technology should also include messaging applications and there lacks a category for key services such as translation, transcription and interpretation.

Functions

Functions are often mixed with technologies and equipment, leading to overlapping and redundant classifications. Functions also lack aspects related to **citizen engagement, awareness raising, societal issues, research and victim support**. A function that represented command, control, organisation and coordination could be beneficial.

Overall, there are also inconsistencies across the online and Excel versions of the taxonomy, a bottom-up approach could better help identify and resolve gaps, whilst it is also important to be mindful of the relationship to the Border Management, Disaster Resilience and Critical Infrastructure categories.

17 REFERENCES

[1] Niinistö, S. et al. (2024) Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness. UCP Knowledge Network. https://civil-protection-knowledge-network.europa.eu/media/safer-together-strengthening-europes-civilian-and-military-preparedness-and-readiness

[2] Report of the CERIS Expert Group (2024). Building resilience in the civil security domain based on research and technology. Publications Office of the European Union. https://data.europa.eu/doi/10.2837/06076

[3] ENISA publications. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications

[4] Europol (2024) Internet Organised Crime Threat Assessment 2024 (IOCTA 2024). https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024#downloads

[5] EU Innovation Hub for Internal Security. Europol. https://www.europol.europa.eu/how-we-work/innovation-lab/eu-innovation-hub-for-internal-security

[6] European strategy for a better internet for kids - BIK+. https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids

[7] European action plan on the cybersecurity of hospitals and healthcare providers. https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

[8] EU Cyber Solidarity Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

[9] Digital euro package. https://finance.ec.europa.eu/publications/digital-euro-package_en

[10] European Health Data Space (EHDS) Regulation.https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

[11] European Data Protection Supervisor Guidelines 01/2025 on Pseudonymisation: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

[12] EU AI Act. https://ai-act-service-desk.ec.europa.eu/en/ai-act-explorer

[13] European Commission (2025) Guidelines on AI systems: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

[14] Fundamental Rights Agency (2024) Addressing Racism in Policing: https://fra.europa.eu/en/publication/2024/addressing-racism-policing

[15] Council of Europe (2020) Compendium of good practices in addressing trafficking in human beings for the purpose of labour exploitation. https://edoc.coe.int/en/trafficking-in-human-beings/10984-compendium-of-good-practices-in-addressing-trafficking-in-human-beings-for-the-purpose-of-labour-exploitation.html

[16] Organisation for Security Cooperation in Europe (OSCE) (2009) Guide on Gender-Sensitive Labour Migration Policies: https://www.osce.org/files/f/documents/b/4/37228.pdf

[17] Organisation for Security Cooperation in Europe (OSCE) (2021) Trafficking in Human Beings and Terrorism: https://www.osce.org/files/f/documents/2/7/491983.pdf

[18] COM(2025) 8 final - Progress made in the European Union in combating trafficking in human beings (Fifth Report). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0008

[19] EPCAT. Disrupting Harm: https://ecpat.org/disrupting-harm/

[20] The EU Code of Conduct on countering illegal hate speech online. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[21] Digital Services Act Package. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

[22] UN Women (2023) The Gender Snapshot 2023. https://www.unwomen.org/sites/default/files/2023-09/progress-on-the-sustainable-development-goals-the-gender-snapshot-2023-en.pdf

[23] Institute for Economics and Peace (2024) 2024 Global Terrorism Index. https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf

[24] Radicalisation Awareness Network (2024) RAN digital small-scale expert meeting. https://home-affairs.ec.europa.eu/whats-new/publications/ran-digital-small-scale-expert-meeting-violent-right-wing-extremism-western-balkans-07-may-2024_en
[25] Europol (2023) European Union Terrorism Situation and Trend report 2023 (TE-SAT). https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat
[26] DG Home (2024) EU Innovation Hub's Annual Event. https://home-affairs.ec.europa.eu/news/eu-innovation-hub-internal-security-wrap-annual-event-2024-2024-12-02_en
[27] DG Home (2023) Security Research Event 2023. https://home-affairs.ec.europa.eu/news/security-research-event-2023-2023-10-25_en
[28]T4i DOVER Project: https://www.t4ieng.com/winner-of-the-2023-EC-security-innovation-award/
[29] CRYPTOPOL: https://www.europol.europa.eu/media-press/newsroom/news/game-for-europol-and-centric
[30] Drug Hunter Analyser: https://www.drughunter.eu/
[31] KINAITICS (2024) Introducing NeuralSentinel: A Tool for Safeguarding Neural Network Reliability and Trustworthiness. https://kinaitics.eu/introducing-neuralsentinel-a-tool-for-safeguarding-neural-network-reliability-and-trustworthiness/
[32] CYBERSPACE (2024) From Similarity to Attribution: Machine Learning-Driven Malware Analysis. https://cyberspaceproject.eu/from-similarity-to-attribution-machine-learning-driven-malware-analysis/
[33] DG Home (2024) Project RAYUELA helps combat cybercrime through gaming. https://home-affairs.ec.europa.eu/news/project-rayuela-helps-combat-cybercrime-through-gaming-2024-12-18_en
[34] European Commission. Horizon Dashboard: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard
[35] Public Procurement Data Space: https://api.public-procurement-data-space.europa.eu/dashboard/list/
[36] European Commission. (2025) Horizon Europe Work Programme 2025. Civil Security for Society. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf
[37] WeProtect Global Alliance (2023) Global Threat Assessment 2023. https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf
[38] Westlake B. et al. (2024) Benefits and risks of implementing cloud-based technology for child sexual abuse investigations in Australia. Trends & issues in crime and criminal justice no. 699. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77550
[39] Sumer, B. (2024). The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?. European Data Protection Law Review, 10(2), 150-161. https://doi.org/10.21552/edpl/2024/2/6
[40] Santalu, N. (2023) Biometrics under the EU AI Act. IAPP. https://iapp.org/news/a/biometrics-under-the-eu-ai-act
[41] Miniadou, K. et al. (2024). Enhancing secure cross-border collaboration among law enforcement agencies for facial biometric search. In 2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE) (pp. 1-6). IEEE. https://doi.org/10.1109/EEITE61750.2024.10654447
42] European Data Protection Board. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en
[43] European Data Protection Board. Opinion 21/2024 on Proposal for a Council Regulation on strengthening the security of identity cards. https://www.edps.europa.eu/system/files/2025-01/2024-0652_opinion_en.pdf
[44] Organisation for Security and Cooperation in Europe. Recommendations on enhancing efforts to identify and mitigate risks of trafficking in human beings online as a result of the humanitarian crisis in Ukraine. https://www.osce.org/files/f/documents/4/c/516423_0.pdf
[45] Organisation for Security and Cooperation in Europe (2024) Invisible victims: The nexus between disabilities and trafficking in human beings. https://www.osce.org/files/f/documents/c/7/568150.pdf
[46] EPCAT (2022) Child sexual exploitation and abuse online: Survivors' Perspectives. https://ecpat.org/wp-content/uploads/2022/01/05-01-2022_Project-Report_EN_FINAL.pdf
[47] Council of Europe (2024) Missing migrants, refugees and asylum seekers – A call to clarify their fate. https://rm.coe.int/as-mig-2024-11-draft-report-missing-migrants-refugees-and-asylum-seeke/1680b090c3

[48] Europol (2024) ChatGPT - the impact of Large Language Models on Law Enforcement. TechWatch Flash Report. https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement
[49] ENISA (2025) EU financial entities cybersecurity upgrade: DORA is now alive and kicking. https://www.enisa.europa.eu/news/eu-financial-entities-cybersecurity-upgrade-dora-is-now-alive-and-kicking
[50] European Data Protection Board. Statement 5/2024 on the Recommendations of the High Level Group on Access to Data for Effective Law Enforcement. https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf
[51] Court of Justice of the European Union (2024) Access by the police to data contained in a mobile telephone is not necessarily limited to the fight against serious crime. https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-10/cp240171en.pdf
[52] Blokland, A. et al. (2024). Why do users continue to contribute to darknet Child Sexual Abuse Material forums? Examining social exchange, social capital, and social learning explanations using digital forensic artifacts. Child Abuse & Neglect, 153, 106815. https://doi.org/10.1016/j.chiabu.2024.106815
[53] Organisation for Security and Cooperation in Europe (2024) Policy action to address technology-facilitated trafficking in human beings. https://www.osce.org/files/f/documents/8/d/579190_0.pdf
[54] Rahman, M. M., & Das, T. K. (2024). Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them. Journal of Digital Technologies and Law, 2(4), 973-1002. https://doi.org/10.21202/jdtl.2024.46
[55] Staniforth, A. (2024) Regulation risk: The challenges facing smaller service providers in tackling terror online. Policing Insight. https://policinginsight.com/feature/innovation/regulation-risk-the-challenges-facing-smaller-service-providers-in-tackling-terror-online/
[56] European Data Protectio Supervisor. Opinion 19/2024 on two Proposals for Council Decisions on the signing and conclusion of an Agreement between the EU and Lebanon on cooperation between Eurojust and the authorities of Lebanon competent for judicial cooperation in criminal matters. https://www.edps.europa.eu/system/files/2024-09/24-08-28_opinion_lebanon_eurojust_en_0.pdf
[57] Family Online Safety Institute – Digital Parenting Program. https://fosi.org/parenting/
[58] Centre for Information Policy Leadership (CIPL) (2024) Reconciling Privacy and Innovation: The Path Forward on AI in the EU. https://www.euractiv.com/opinion/reconciling-privacy-and-innovation-the-path-forward-on-ai-in-the-eu/
[59] Staniforth, A. (2024) Understanding radicalisation and gender: Terrorist motivation of women and girls. Policing Insight. *https://policinginsight.com/feature/understanding-radicalisation-and-gender-terrorist-motivation-of-women-and-girls/*
[60] Organisation for Economic Co-operation and Development (OECD) - OECD AI Incidents Monitor. https://oecd.ai/en/incidents
[61] Panagiotopoulos, V. (2025) EXCLUSIVE: Spyware firm behind new surveillance of journalists, civil society operates from the EU. Euractiv. https://www.euractiv.com/news/exclusive-spyware-firm-behind-new-surveillance-of-journalists-civil-society-operates-from-the-eu/
[62] Laux, J., Wachter, S., & Mittelstadt, B. (2024). Three pathways for standardisation and ethical disclosure by default under the European Union Artificial Intelligence Act. Computer Law & Security Review, 53, 105957. https://doi.org/10.1016/j.clsr.2024.105957
[63] Romsos, E. L. et al. (2025). Development of a forensic DNA research grade test material. Journal of Forensic Sciences, 70(1), 276-283. https://doi.org/10.1111/1556-4029.15639
[64] United Nations Interregional Crime and Justice Research Institute (2024) “Not Just Another Tool" Report on Public Perceptions of AI in Law. https://unicri.org/Publications/Public-Perceptions-AI-Law-Enforcement
[65] Staniforth, A. (2024) What works: Evidence-based approaches and tackling teenage terror. Policing Insight. https://policinginsight.com/feature/analysis/what-works-evidence-based-approaches-and-tackling-teenage-terror/
[66] Interpol (2025) Emerging criminal threats targeted by INTERPOL’s European Regional Conference: https://www.interpol.int/News-and-Events/News/2025/Emerging-criminal-threats-targeted-by-INTERPOL-s-European-Regional-Conference
[67] Interpol (2025) Silver Notice targeting criminal assets: https://www.interpol.int/News-and-Events/News/2025/INTERPOL-publishes-first-Silver-Notice-targeting-criminal-assets
[68] Europol - Cyber Innovation Forum 2025. https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2025
[69] International Security Expo 2025. https://www.internationalsecurityexpo.com/

ENACT.

European Network Against Crime and Terrorism

@enact-network

enact-eu.net

Scan the QR code to visit ENACT online and read this report in digital format.

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.