STATE OF PLAY REPORT 03



STATE OF PLAY POLICY REPORT 03

Public Version.
September 2026

Inter-Observatory Coordinator: CERTH
Capabilities Observatory: FRMOI
Technology Observatory: ENG
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-report-feedback

Funded by
the European Union

Disclaimer

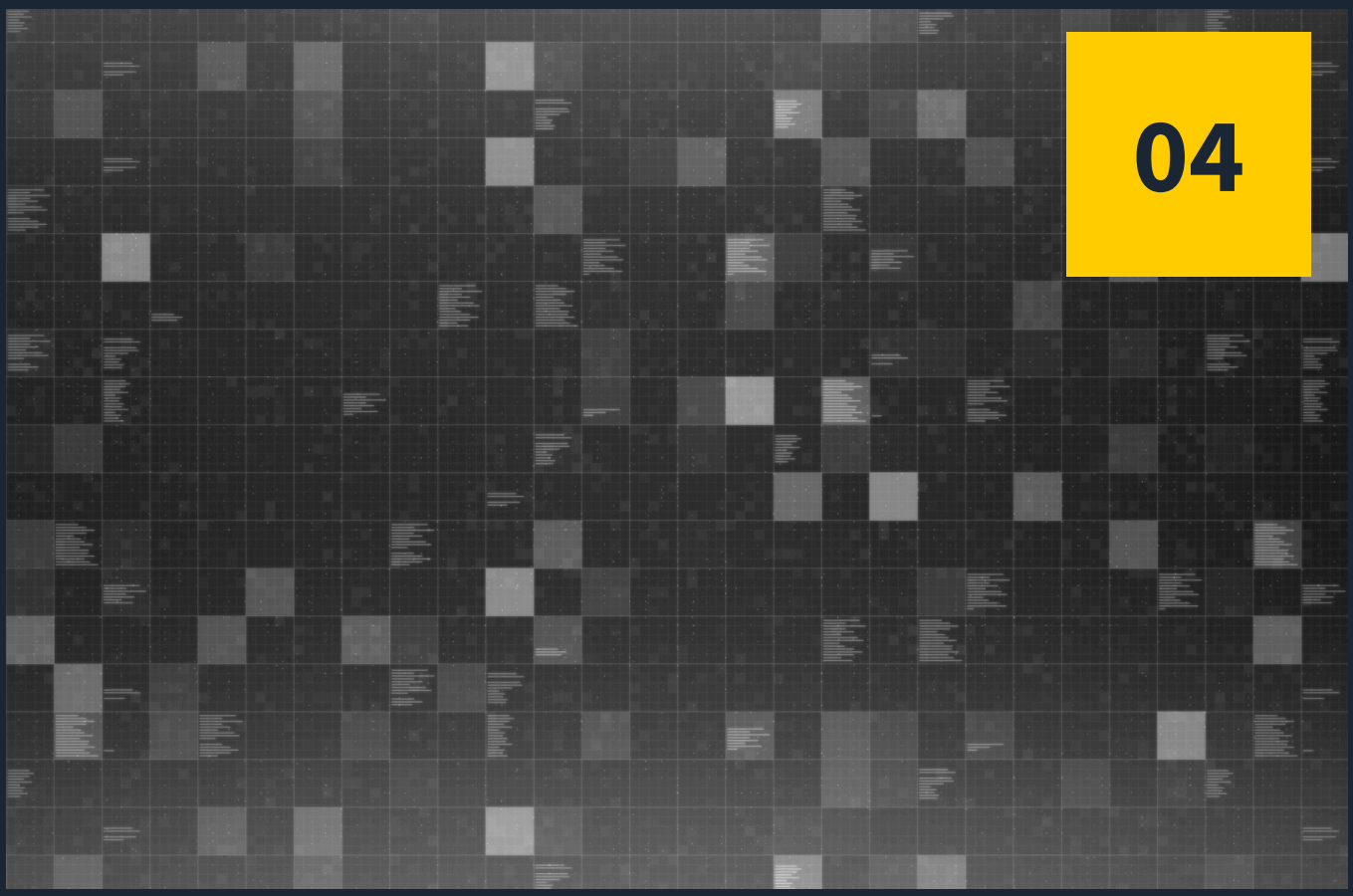
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

This report contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Acronyms

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
BM	Border Management
C-UAS	Counter-Unmanned Aircraft System
CapO	Capability Observatory
CEN	European Committee for Standardization
CENELEC	European Electrotechnical Committee for Standardization
CERIS	Community for European Research and Innovation for Security
CIR	Critical Infrastructure Resilience
CS	Cyber Security
CSA	Coordination and Support Action
DG-HOME	Directorate-General for Migration and Home Affairs
DRS	Disaster-Resilient Society
EC	European Commission
ECPAT	Every Child Protected Against Trafficking
EDIP	European Defence Industry Programme
ELSO	Ethical, Legal and Societal Observatory
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCS	European Union Civil Security
FCT	Fight against Crime and Terrorism
HEU	Horizon Europe
IA	Innovation Action
IoT	Internet of Things
ISO	International Organization for Standardization
JTC	Joint Technical Committee
L	Level
LLM	Large language Model
MFF	Multiannual Financial Framework
MktO	Market, Funding & Standardisation Observatory
R&D	Research and Development
R&I	Research and Innovation
RAN	Radicalisation Awareness Network
RIA	Research and Innovation Action
SEA	Sexual Exploitation and Abuse
SOC	Security Operations Center
SoP	State-of-Play
SRE	Security Research Event
TechO	Technology Observatory
WP	Work Package



04

STATE OF PLAY FCT POLICY REPORT 2026

The State of Play (SoP) Fight Crime and Terrorism (FCT) Policy Report, developed under the ENACT (European Network Against Crime and Terrorism) project, 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 2025 to July/August 2026. 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 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). The final ENACT SoP provides timely and relevant policy support tailored to the dynamic challenges of crime and terrorism.



05

INTRODUCTION

ENACT concept and approach

Knowledge is one of the most strategic assets available to the European Union (EU). The ability to anticipate threats, adapt to emerging challenges, and ensure evidence-based policymaking depends not only on technological capabilities or operational readiness, but also on the existence of robust, structured, and accessible knowledge ecosystems. Recognising this, the European Commission (EC), through Directorate-General for Migration and Home Affairs (DG HOME), launched a dedicated effort to establish Knowledge Networks in key security domains, including the fight against crime and terrorism, border management, disaster resilience, among others.

The creation of these networks responds to a fundamental challenge: while Europe has invested heavily in security research and operational innovation, the results of these efforts are often fragmented, difficult to access, or disconnected from the needs of practitioners. Valuable knowledge produced in EU-funded projects, national initiatives, or institutional bodies frequently remains isolated within specific communities, limiting their practical impact and slowing the uptake of innovation.

Knowledge Networks are intended to address this structural gap. By promoting cooperation, knowledge sharing, and strategic alignment among researchers, practitioners, policymakers, and industry, these initiatives seek to create long-term, service-oriented platforms that consolidate existing expertise and make it actionable. More than just repositories or research summaries, these networks are designed to foster dialogue, support policy development, and contribute to the long-term resilience and effectiveness of the security of the EU.

Through these efforts, DG HOME aims to ensure that the wealth of knowledge already produced, and still to come, can be better organised, better used, and ultimately better connected to the priorities of the Union and its citizens.

ENACT is one of the thematic Knowledge Networks aiming to strengthen Europe's capacity to fight crime and terrorism through structured knowledge, strategic collaboration, and innovation uptake. As a network, ENACT brings together law enforcement agencies, researchers, policymakers, and industry to collect, organise, and make sense of the vast and fragmented body of knowledge generated across the FCT landscape. It provides an online, open access, platform for sharing insights, identifying gaps, validating solutions, and aligning R&I with real operational needs, serving as both a knowledge hub and a bridge between research and practice. The knowledge gathered is also used to produce thematic Flash Reports, either from the project initiative or on demand from other stakeholders, on technologies, markets or ethics and social issues.

Purpose of this report

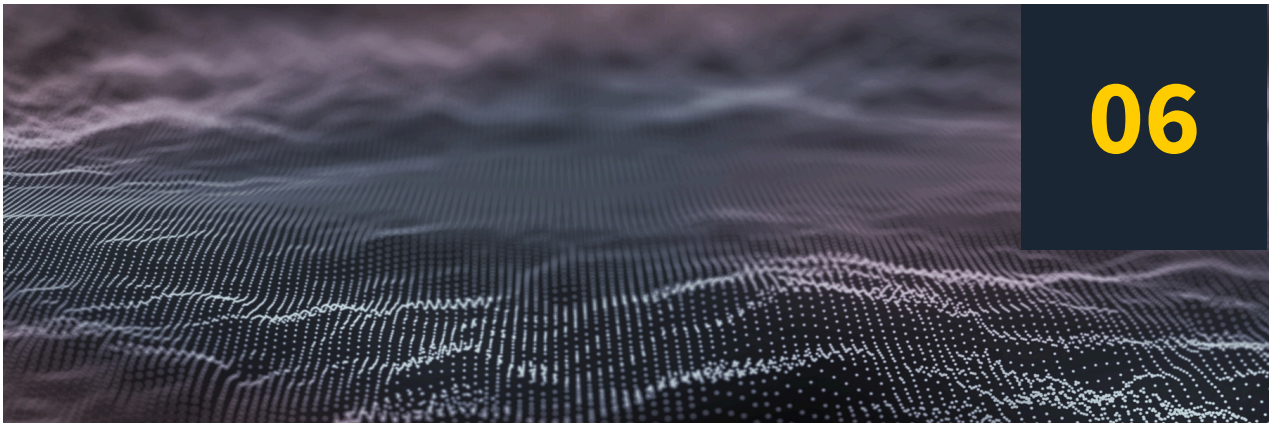
The present SoP FCT Policy Report offers a concise and targeted overview of recent developments, latest insights, and recommendations from various ENACT activities prepared during the final Full Implementation Cycle (from September 2025 to July/August 2026).

The report consolidates insights and recommendations derived from various ENACT products, including Flash Reports and Analytical Reports produced and compiles analyses carried out by ENACT in support of CERIS (Community of European Research and Innovation for Security), and FCT workshops, events, and discussions. This includes inputs from the FCT experts' group and other relevant FCT R&I events organised by the Commission, such as Project2Policy events and the Security Research Event (SRE). By summarising outcomes and recommendations from these and other Commission-organized events, supporting FCT R&I, this comprehensive approach ensures that policy recommendations are well-rounded and informed by a broad spectrum of expert insights and event outcomes.

The following sections aim to provide an overview of insights and recommendations gathered across four core domains of interest that constitute the Knowledge Observatories: i) capability needs, ii) technology R&I, iii) market, funding, and standardisation opportunities, along with iv) socio and legal-technical dimensions.

Intended audience

This report is intended for a broad audience, from policy-makers, such as DG HOME, to the European and Member State law enforcement community, the FCT R&I community, the general public and the media.





07

POLICY VIEW

This section provides a strategic overview of the extensive data compiled by ENACT, representing a valuable resource for policy analysis. While the selection of content reflects diverse perspectives, it offers crucial insights into the evolving security landscape.

The 2026 policy landscape in the FCT area is shaped by four main trends. Horizontal and societal issues account for 32% of high-relevance observations, followed by cybercrime at 30%, organised crime at 25%, and terrorism and radicalisation at 12%.

KEY TRENDS IN THE POLICY AREA

The policy trends are broadly reflected in the latest FCT Capabilities Maps [1] [2]. Data, information and intelligence gathering, management and exploitation, as well as investigation and forensics, are the most prominent functions. At technology level, artificial intelligence (AI), cybersecurity technologies, data analytics, digital forensics, and internet-based investigation are among the leading areas. This indicates a strong alignment between current policy priorities and R&I efforts to strengthen digital investigation, intelligence, and security capabilities. More specific policy trends can be found below.



Cybercrime and digital investigation

Cybercrime remains a major policy priority. Digital forensics, attacks against information systems, child sexual abuse, and darknet activities involving illegal markets and cryptocurrencies are the main areas of attention. These trends highlight the growing importance of digital investigations and the need to strengthen law enforcement capabilities in the online environment.

Disinformation and societal security

Horizontal and societal issues represent the largest policy category. Disinformation and fake news are the most prominent topic within this area, followed by conventional forensics, domestic and sexual violence, and hate speech. This reflects continued policy attention to threats affecting both public security and society.





Organised crime and trafficking

Organised crime accounts for 25% of high-relevance observations. Trafficking of humans and goods is the main concern, followed by economic crime, corruption and fraud. These priorities underline the continued need for cross-border cooperation and effective investigation of criminal networks and their activities.

Radicalisation, terrorist financing and public spaces

Terrorism and radicalisation account for 12% of observations. Within this area, radicalisation is the most prominent topic, followed by terrorist financing and the protection of public spaces. The findings point to continued attention to prevention, financial disruption, and the protection of citizens and public environments.





09

TECHNOLOGY VIEW

During the final full implementation cycle of ENACT's Work Package (WP) 7, the European security research and innovation ecosystem continued to be shaped by the growing convergence of artificial intelligence, advanced data analytics, cybersecurity, digital investigative technologies and information exploitation capabilities. Across the Fight Against Crime and Terrorism (FCT) domain, technological developments increasingly focused on enhancing the ability of law enforcement and security actors to collect, process, analyse, and manage large volumes of information, strengthen situational awareness, support evidence-based investigations and respond to rapidly evolving cyber and security threats.

The latest iterations of the FCT Technology Map [3][4] highlight a strong concentration of developments associated with C**onventional Forensics, Digital Forensics** and **Attacks against Information Systems**, confirming the continued importance of technologies supporting evidence collection, forensic investigations, cyber threat detection, and the protection of information infrastructures. From a functional perspective, the most prominent developments relate to **Data, Information and Intelligence Gathering, Management and Exploitation**, followed by **Monitoring and Surveillance of Environments and Infrastructures** and **Investigation and Forensics**. This distribution reflects the increasing importance of information-driven security capabilities, operational awareness and integrated investigative environments. These developments are also examined in ENACT Flash Report #08 [5], which provides an overview of digital tool supporting online monitoring and law-enforcement investigation.

A particularly significant trend remains the rapid expansion of Artificial Intelligence (AI) across both operational and research environments. Discussions held within CERIS events, the EU Innovation Hub for Internal Security and other European security initiatives increasingly focused on the practical deployment of AI-enabled capabilities, including Large Language Models (LLMs), advanced analytics and automated decision-support systems. At the same time, stakeholders emphasised the importance of ensuring that these technologies remain trustworthy, transparent and accountable.

The implementation of the EU Artificial Intelligence Act (AI Act) emerged as a recurring topic throughout the period, stimulating debate around explainability, human oversight, bias mitigation and regulatory compliance. These issues are explored in ENACT Flash Report #09 [6], which examines the implications of the AI Act for security and law-enforcement applications, and in ENACT Analytical Report #05 [7], which focuses on trustworthy AI, fundamental rights, transparency, accountability and human oversight.

Cybersecurity remains a major technology priority, driven by the increasing prevalence of attacks against information systems, online identity theft, digital fraud, and the growing complexity of cyber-enabled criminal activities. Across the broader technology landscape, a clear movement towards integrated, data-centric, and intelligence-led security ecosystems can be observed. These ecosystems increasingly combine AI-enabled analytics, information exploitation, advanced monitoring capabilities, digital forensics and operational decision support while maintaining alignment with European principles of privacy, transparency, accountability, and fundamental rights.

While these developments offer significant opportunities for law-enforcement and security actors, their strategic relevance must also be assessed in relation to the ways in which the same technologies are reshaping criminal and terrorist capabilities, organisational models and operational methods.

Strategic Threat Assessment Implications

The technological developments observed through the Technology Observatory not only strengthen the capabilities available to law-enforcement and security actors but are also reshaping the threat environment itself. Artificial Intelligence, advanced analytics, digital platforms and automated services are becoming increasingly accessible, enabling criminal actors to operate with greater scale, speed and adaptability. As highlighted by Europol's 2025 assessment [8], serious and organised crime is becoming increasingly enabled by digital technologies and accelerated by the growing availability of AI-driven capabilities.

A key development is the growing convergence between organised crime and cybercrime. Digital infrastructures increasingly support communication, recruitment, illicit trade, financial transactions and operational coordination across jurisdictions, while specialised cybercrime services are becoming accessible to a wider range of criminal actors. This evolution contributes to the emergence of more interconnected criminal ecosystems in which cyber-enabled and traditional criminal activities increasingly overlap. The proliferation of generative AI introduces additional challenges. Deepfakes, voice cloning, synthetic identities and AI-generated content can facilitate online fraud, identity theft, impersonation and social-engineering attacks, while also complicating the verification and evidential use of digital information. In parallel, crypto-assets and digital financial infrastructures continue to create opportunities for illicit financial transactions, money laundering and the concealment of criminal proceeds, reinforcing the need for enhanced digital-forensics and financial-investigation capabilities.

Emerging technologies may also be leveraged by terrorist and violent extremist actors to support propaganda, recruitment, financing and operational preparation activities. At the same time, cyberattacks, disinformation activities, illicit financing and other forms of malicious activity increasingly interact with broader hybrid-threat dynamics, blurring the boundaries between criminal, cyber and security challenges. Europol's recent assessment [9] further highlights the growing interaction between criminal networks, digital platforms and hybrid-threat actors.

Against this backdrop, a central strategic question concerns the ability of defensive and investigative capabilities to keep pace with rapidly evolving threats. The prominence of information exploitation, digital forensics, monitoring and surveillance technologies across the Technology Maps indicates a strong focus on capabilities designed to support intelligence-led investigations, situational awareness and evidence-based decision-making. Continued investment in technological innovation, operational readiness, interoperability, practitioner skills and governance frameworks will therefore remain essential to ensuring that European security actors can effectively respond to an increasingly interconnected and technology-enabled threat landscape.

Commercial and Operational Products

The commercial and operational technology landscape was characterised by the increasing maturity of solutions designed to support information exploitation, digital investigations, cyber resilience, situational awareness, and operational decision-making. Security vendors increasingly moved away from standalone tools towards integrated platforms combining AI, advanced analytics, automation, and data management capabilities to enhance operational effectiveness across law-enforcement and security environments.

Among the most visible developments were **AI-assisted Security Operations Centre (SOC)** platforms, capable of automating threat detection, anomaly identification and incident response activities. These systems use machine learning and behavioural analytics to process large volumes of security data and assist analysts in identifying malicious activity more efficiently. In parallel, digital investigation platforms increasingly integrated automated evidence processing, cryptocurrency tracing and intelligence extraction functionalities, responding to the growing complexity of cybercrime investigations.

Growing operational adoption was also observed in tools supporting the detection of **deepfakes**, synthetic media and AI-generated content. The increasing use of generative AI technologies has created demand for forensic solutions capable of verifying the authenticity of digital evidence and identifying manipulated multimedia content. Similarly, advanced intelligence tools supporting multilingual information analysis, document exploitation and the monitoring of online environments are increasingly becoming part of law-enforcement workflows. Telecommunications security represents a related area of operational development, particularly in response to impersonation and fraud facilitated through manipulated Caller IDs and Sender IDs. The ENACT Analytical Report #9 [10], examines relevant traceback and mitigation approaches, complementing the broader analysis of technologies designed to strengthen identity assurance, communication integrity and fraud prevention.

In parallel, increasing commercial attention is being devoted to platforms that integrate information gathering, intelligence management, forensic analysis, and operational monitoring functionalities into unified investigative and decision-support environments. The operational value of these technologies depends on their successful transition from technical availability to sustainable institutional adoption. The ENACT Analytical Report #4 [11], addressed this relationship between technological innovation and law-enforcement readiness.

Projects view

The European Research and Innovation (R&I) portfolio continues to demonstrate a strong focus on digital investigations, information exploitation, cybersecurity, trustworthy AI, and advanced forensic capabilities. Recent Horizon Europe Cluster 3 initiatives increasingly seek to transform research outcomes into operationally deployable solutions while addressing ethical, legal, societal, and regulatory requirements.

One example is **DETECTOR (Deepfake Evidence and Technology for Forensic Content Oversight and Research),** which addresses the challenges posed by generative AI and synthetic media. The project develops technologies and methodologies supporting the forensic analysis, detection and evidential exploitation of deepfakes and AI-generated content, reflecting the growing importance of digital evidence integrity and information authenticity in criminal investigations.





Illustrating the field of digital investigations, **SALUS (Strengthening Law Enforcement with IoT Forensic Tools)** focuses on forensic capabilities for Internet of Things environments. As connected devices become increasingly embedded in public and private environments, the project aims to strengthen the ability of law-enforcement authorities to collect, preserve and analyse digital evidence originating from complex IoT ecosystems.

The protection of public spaces and the response to emerging drone threats are addressed through initiatives such as **PRESERVE**, which develops technologies and operational concepts for countering hostile drones and improving situational awareness.





SHIELD PCP supports the validation and operational deployment of innovative security technologies for law-enforcement environments, reflecting the growing emphasis on innovation procurement and capability uptake across Europe.

The continuing relevance of Counter-UAS research and operational validation is reflected in ENACT Flash Report #23 [12] and complemented by the ENACT Analytical Report #7 [13] and the ENACT Analytical Report #8 [14]. Together, these reports examine the relationship between technological performance, regulatory feasibility, operational constraints and deployment readiness.

The broader project landscape also includes initiatives addressing cybercrime, intelligence sharing and organised-crime investigations

ARIEN is developing an AI-enabled framework supporting the monitoring of illegal drug production and trafficking, online and dark-market analysis, cryptocurrency-transaction analysis and cross-border information sharing. The project focuses on improving the operational intelligence picture relating to illegal drug production and trafficking and supporting law-enforcement authorities in identifying illegal markets and links to other forms of organised crime.



These themes connect closely with ENACT Flash Report #04 [15], which considers relevant research and innovation activities across the European project landscape.

These initiatives demonstrate a growing investment in AI, digital investigations, cybersecurity, intelligence exploitation, and information-sharing capabilities. Overall, the current EU project landscape illustrates a clear shift towards integrated, data-driven, and operationally deployable solutions designed to strengthen investigative processes, enhance situational awareness, improve cyber resilience, and support law-enforcement decision-making.

Science View

Scientific research concentrated on several rapidly evolving technology domains whose operational impact is expected to become increasingly significant in the coming years. Unlike ongoing projects, which focus on capability development and validation, scientific activities primarily explored emerging technologies, future risks and novel analytical methodologies.

A major research focus concerned the implications of **Generative Artificial Intelligence** and **Large Language Models (LLMs).** Scientific studies increasingly examined the detection of deepfakes, AI-generated misinformation, synthetic media manipulation and the broader security implications of generative AI. At the same time, researchers explored methods to improve explainability, transparency and trustworthiness of AI systems, reflecting the growing relevance of the AI Act and responsible AI principles within security research. These developments directly complement the governance and victim-oriented considerations examined in ENACT Flash Reports #09 [16] and #20 [17].

Another active area of investigation focused on **advanced digital forensics** and the analysis of complex digital environments. Research explored methods for evidence acquisition from cloud infrastructures, IoT devices, encrypted communications and distributed systems, while also examining AI-assisted approaches capable of supporting automated forensic triage and evidence correlation. As digital ecosystems continue to expand, scientific efforts increasingly seek ways to improve the scalability and reliability of forensic processes. The prominence of these topics is consistent with the findings of the latest FCT Technology Maps and with the investigative capabilities examined in ENACT Flash Report #08 [18].

Significant scientific attention was also devoted to **multi-modal sensor fusion** and **Counter-Unmanned Aircraft Systems (C-UAS).** Current research investigates the integration of radar, acoustic, thermal and radio-frequency sensing technologies with machine-learning techniques to improve the detection and classification of non-cooperative drones. These developments are particularly relevant in the context of increasingly autonomous and sophisticated drone threats. The corresponding operational and regulatory implications are examined in ENACT Flash Report #23 [19] and the Analytical Reports #07 [20] and #08 [21], creating a direct link between scientific development, operational readiness and deployment conditions.

Scientific research also increasingly examines the interaction between technological development and the changing methods used by criminal and malicious actors. This includes the analysis of AI-assisted social engineering, digitally mediated fraud, synthetic content, online criminal networks and behavioural patterns across open-web and dark-web environments. Such research can support the transition from reactive detection towards more adaptive approaches capable of identifying emerging patterns and changes in criminal behaviour.

Overall, the scientific landscape reveals a strong orientation towards AI-enabled analytics, trustworthy AI, digital forensics, information exploitation, and advanced investigative methodologies. Significant attention is devoted to improving the collection, analysis, management, and interpretation of large and heterogeneous datasets, reflecting the growing importance of intelligence-driven approaches within the European FCT ecosystem. These developments are expected to influence the next generation of security capabilities supporting cybersecurity, forensic investigations, operational awareness, and evidence-based decision-making.

14 MARKET & STANDARDS VIEW

The Markets and Standards Observatory (MktO) complements the insights provided by the Technology Observatory (TechO) and the Capability (policy-related) Observatory (CapO) by offering a detailed analysis of both demand and supply, as well as the evolving ecosystem. The meta-analysis of the latest ENACT Market and Standards Maps [22][23] surfaced the need to examine the landscape under the following facets: a) evolution of the Horizon Europe FCT R&I portfolio, b) the conditions affecting innovation procurement, and c) the standards supporting the European security market

FCT Research & Innovation

Considering Horizon Europe (HEU) FCT calls from 2021 and 2022, total net EU contributions made up about 90% of costs, or €81.6 million, across 21 signed grants covering 18 topics. Adding 2023 brings cumulative net EU contributions to 91.5%, or approximately €118.2 million, consistent with the trend reported through 2023.

With 2024 and 2025 data now included, the picture extends further. HEU 2024 added 11 signed grants (€45.3 million net EU contribution, a 95.5% net funding rate) and HEU 2025 has 9 grants signed (€31.4 million, 97.8%), the highest funding rate of any period to date. Across the full HEU 2021-2025 window, FCT R&I now totals 50 signed grants across 36 topics, €194.9 million in net EU contribution against €208.7 million total cost, a 93.4% net funding rate.

The shift toward Research and Innovation Actions (RIA) – funded at 100% of costs versus 70% for Innovative Actions (IA) – has continued well beyond the point where the 2025 report saw it levelling out. RIA's share of signed grants fell to 28.6% at the start of HEU 2021-2022 (from around 80% under H2020), then recovered to 66.7% in 2023, climbed to 72.7% in 2024, however coming back down to 66.7% in 2025. Taken cumulatively, RIA has now overtaken IA across the whole HEU 2021-2025 window (52% vs 46%), reversing the IA-heavy start of the framework. The share of Coordination and Support Actions (CSAs) remains minimal and confined almost entirely to the 2021-2022 calls (4.8%, versus 2.0% across the full period), reflecting FCT's continued priority on funding solutions and innovations close to market rather than coordination activity.

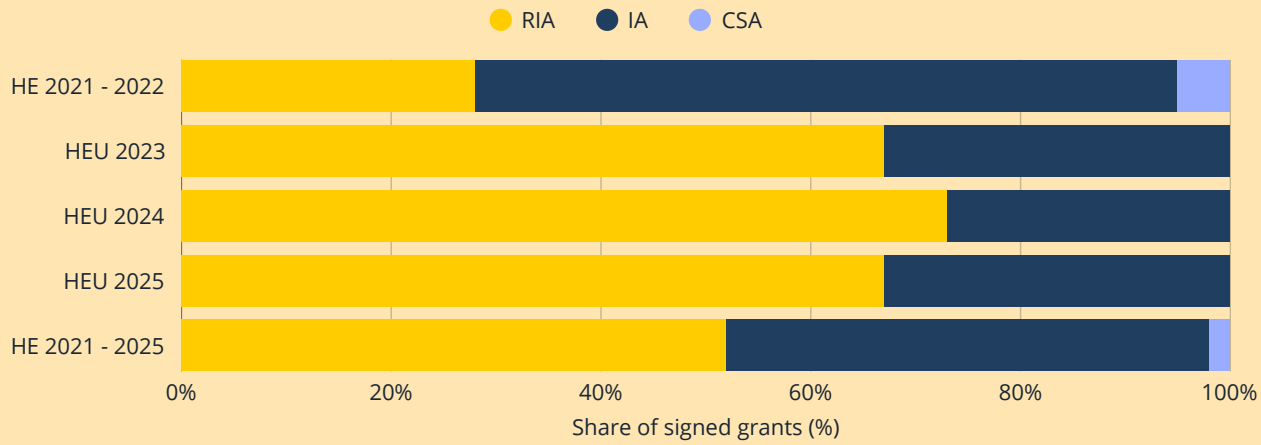


Figure 1: Share of signed FCT R&I grants by type of action, HEU 2021-2022 through HEU 2021-2025 (cumulative)

HEU Funding summary by period

Period	Topics	Grants	Net EU contr. (€M)	Total cost (€M)	Net/Cost (%)	RIA %	IA %	CSA %
HEU 2021-2022	18	21	81.6	90.5	90.2	28.6	66.7	4.8
HEU 2023	6	9	36.6	38.7	94.6	66.7	33.3	0
HEU 2024	8	11	45.3	47.4	95.5	72.7	27.3	0
HEU 2025	4	9	31.4	32.2	97.8	66.7	33.3	0
HEU 2021-2023	24	30	118.2	129.2	91.5	40	56.7	3.3
HEU 2021-2024	32	41	163.5	176.6	92.6	48.8	48.8	2.4
HEU 2021-2025	36	50	194.9	208.8	93.4	52	46	2

FCT Procurement

As part of the in-depth studies conducted by External Experts, ENACT commissioned a report on Innovation Procurement in the EU Security Sector, the ENACT 06 Analytical Report [24]. This report examines the legal and policy framework, national practices, and the pipeline between security research and deployment and provides key findings for the policymakers and the FCT community writ large to better understand innovation procurement and potential pitfalls. The policy framework remains under-developed EU-wide — the 2024 Commission benchmarking of thirty countries put the European average at just 33.05%, with Finland the sole "solid performer" and ENACT states ranging from Finland (1st) and Spain (4th) to Greece (16th) and Portugal (20th).

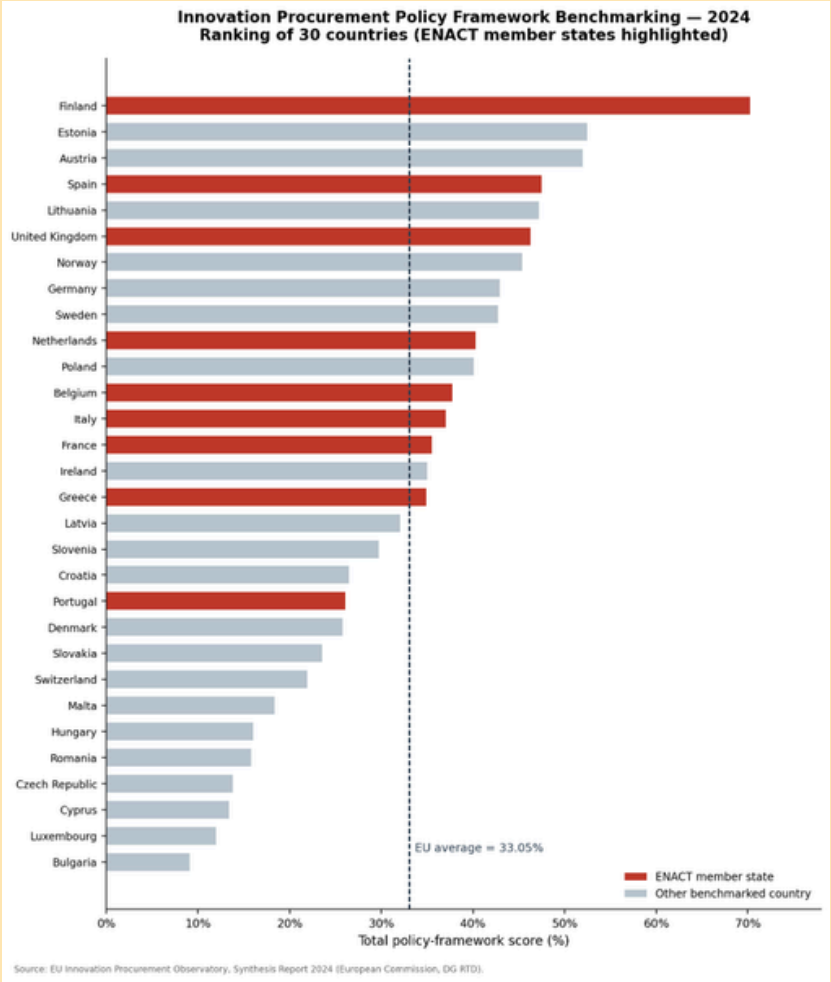


Figure 2: Innovation Procurement Policy Framework Benchmarking 2024 - ranking of the thirty countries assessed, ENACT member states highlighted [25]

While the security and defence sub-indicator has seen the second-largest sectorial gain since 2020 (from 12% to 40%), policy recognition still outpaces operational instruments: six key areas (sectorial policies, action plans, spending targets, monitoring, incentives, capacity building) all score below 35%. The principal legal gap is sitting at the acquisition stage rather than research, pre-commercial Research and Development (R&D) procurement is already available under Directive 2009/81/EC's [26] exclusion, but instruments like the innovation partnership are missing from the acquisition procedures, a gap the Commission's June 2025 proposal aims to close.

The report also covers the emerging EU framework for "European preference" in defence procurement, noting that Regulation 2025/2643 (EDIP) now caps non-EU component costs at 35% and requires EU-based design authority, though methodological and supply-chain questions remain unresolved. Having a national security research programme is a weak proxy for procurement capacity, since the five countries (Germany, Austria, Bulgaria, Czechia and Italy) with such programmes span very different performance levels and the programmes mostly operate at the research stage rather than deployment. The funding architecture itself is in flux, with the proposed 2028–2034 Multiannual Financial Framework folding security research into a new European Competitiveness Fund, a negotiation still ongoing as of mid-2026. Finally, the report distils concrete best practices from top-performing countries: dated spending targets, procurer-level KPIs, permanent competence centres, dedicated innovation agencies (e.g., Spain's CDTI, France's AID), and national strategies that explicitly name innovation procurement (Netherlands, Italy, France, Finland), as differentiators between stronger and weaker national frameworks.

A complementary perspective comes from ENACT's Analytical Report 03 [27], which maps the FCT priorities in the initial 2021–2027 ISF National Programmes. The findings show a strong emphasis on infrastructure serving multiple security threats, information exchange and institutional cooperation. Data and intelligence management emerge as the leading functional priority, alongside training, secure communications and forensic capabilities. Technological priorities centre on secure data storage and exchange, supported by data analytics, indicating a shared movement towards intelligence-led policing while retaining differences linked to national operational needs.

These priorities provide an indication of likely public procurement demand, since implementing the planned capabilities will often require Member States to acquire equipment, software, infrastructure and services. They therefore complement the innovation procurement report by identifying areas where operational funding could support the uptake of FCT research results. Such acquisitions may involve established solutions through conventional procurement, as well as innovative products or services where these meet identified needs. However, the ISF analysis captures planned priorities rather than awarded contracts or actual expenditure; translating this demand into deployment will depend on national project selection, procurement decisions and implementation capacity.

Standards

Standardisation can play an important role in ensuring the market avoid fragmentation side, such as standards being implemented into tenders or even regulation to ensure solutions are fit-for-purpose. In Europe, there are three standardisation bodies that produce standards affecting goods on the European market: the European Committee for Standardisation (CEN), the European Electrotechnical Committee for Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI). The International Standards Organisation (ISO), as the main global standardisation body, also produces standards that affect the European market, as CEN removes any duplicated standards and defaults to the ISO standard (see the 1991 Vienna Agreement).

In order to understand what currently exists in terms of standards for the FCT market, a review of the standards library was conducted for each of the bodies based on their classification of standards:

- For CEN/CENELEC, all of the standards originating from the technical bodies within the Defence and Security sector were compiled.
- For ETSI and ISO, all of the standards within their catalogue were downloaded, as they did not clearly demarcate the security sector.

All of the standards were then mapped to EU Civil Security Taxonomy, providing an overview of the existing standards, as seen in Figure 3 and Figure 4 below.

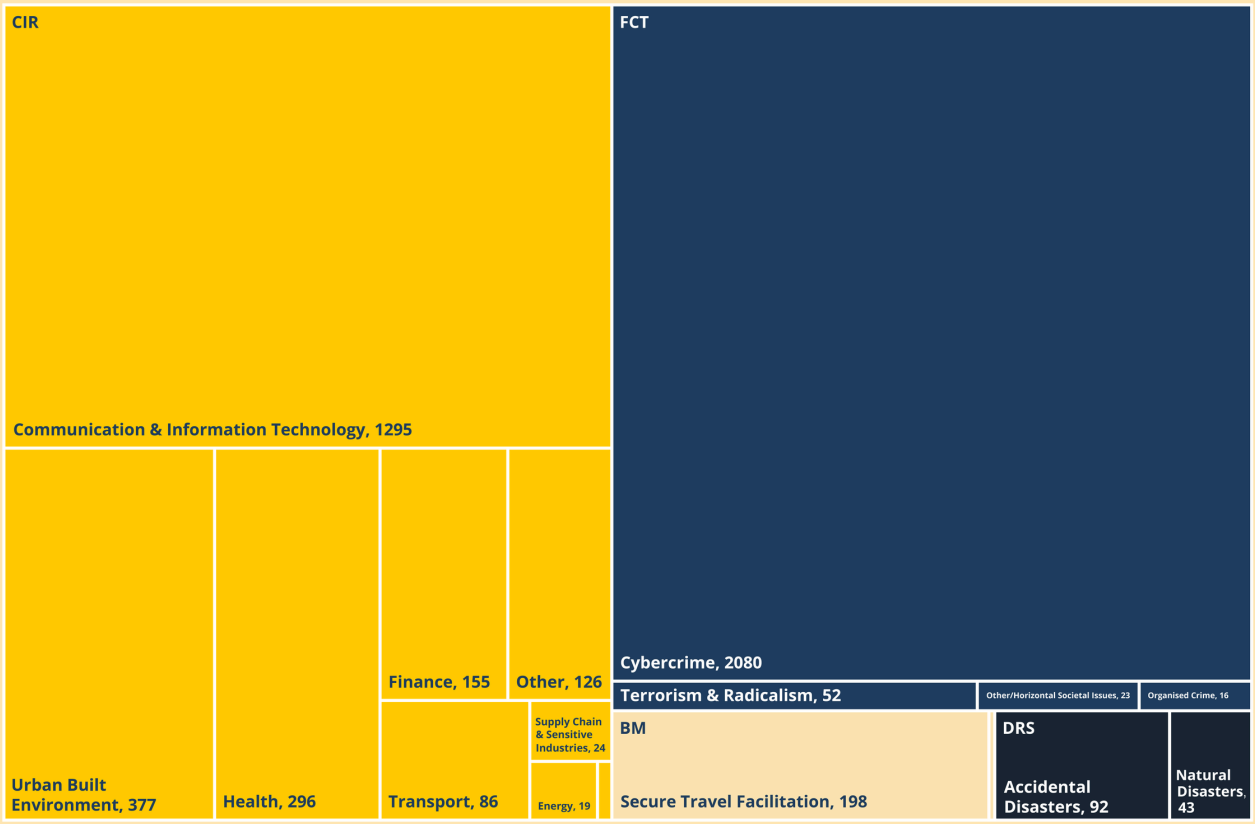


Figure 3: CEN/CENELEC, ETSI & ISO Standards by EUCS L2

Out of the four level 1 (L1) classifications for civil security, Fight against Crime and Terrorism (FCT) and Critical Infrastructure Resilience (CIR) largely surpassed Border Management (BM) and Disaster-Resilient Society (DRS) in terms of standards, representing 2171, 2382, 135, and 201 of the 5094 standards mapped, respectively (205 standards were considered not mappable). Part of the reason for this lies with the fact that ETSI is a body that largely focuses on telecommunication, and the ISO's Joint Technical Committee (JTC) 1 produces the most amount of standards in the realm of security. The large amount of CIR standards demonstrates technical standards representing the majority of security standards currently available.

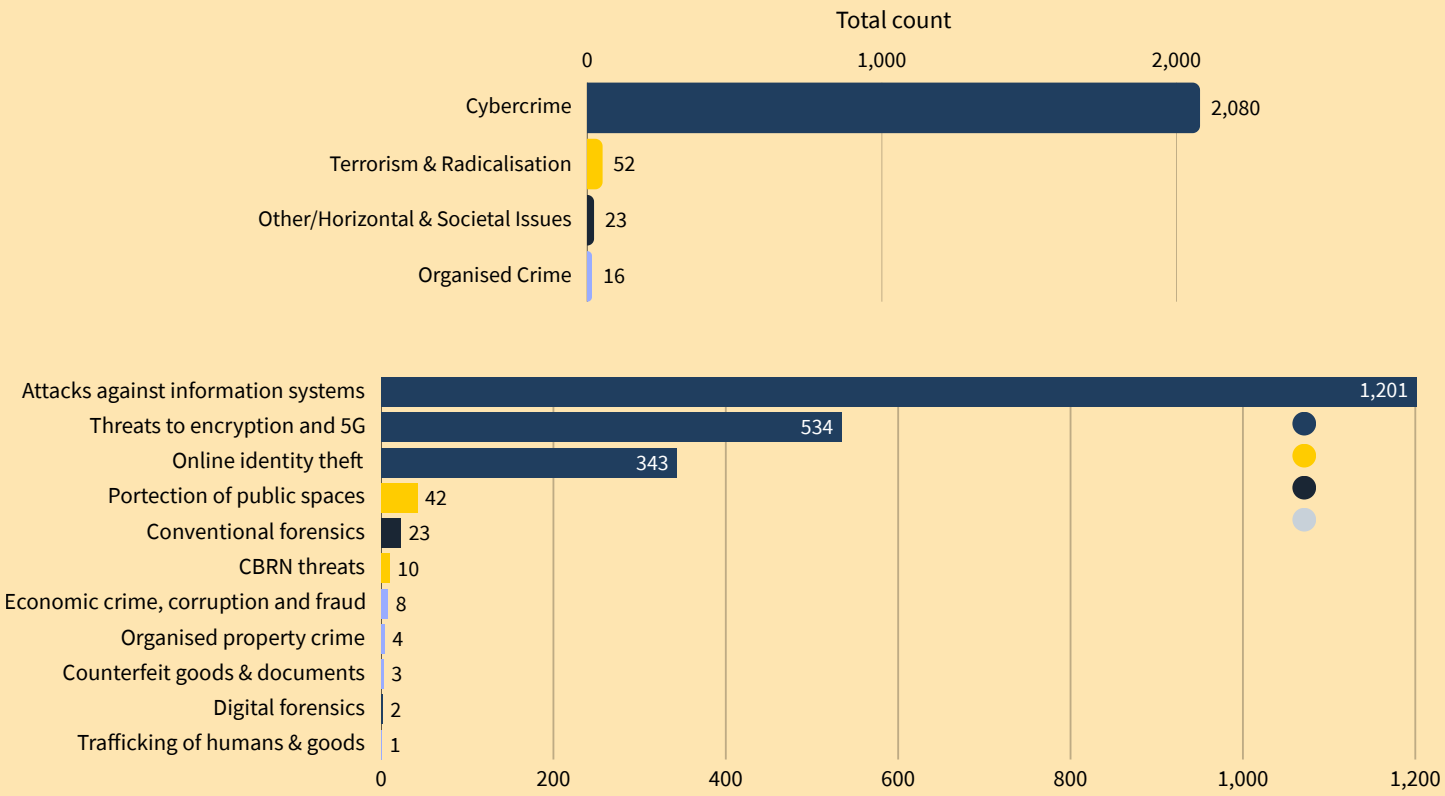


Figure 4: CEN/CENELC, ETSI & ISO Standards by EUCS FCT L3

This trend is also replicated in the FCT level 3 classification of the mapped standards. Cybercrime represents around 96% of the standards in the FCT domain, dominating over other categories. The FCT R&I community should arguably dedicate more effort into developing standards for other categories, particularly organised crime, which has the least. It should be noted that the categories are not always mutually exclusive, for example, organised crime groups will use dark net and non-cash payment fraud as part of their activities; however, this remains a gap.

It should be noted that this is a quick snapshot, and that a deeper analysis of existing standards is warranted, especially at the national level. This would provide a better understanding of what member states are currently developing, and current gaps between the national and European level, and how this currently affects the FCT market.

The rapid expansion of AI in FCT also makes the Commission's 2026 standardisation request[1] to CEN and CENELEC particularly relevant. It supports the development of harmonised standards for high-risk AI systems under the AI Act, with work coordinated through CEN-CENELEC's Joint Technical Committee 21. The standards address risk management, data quality, logging, transparency, human oversight, accuracy, robustness and cybersecurity, alongside quality management and conformity assessment. This work will have direct implications for FCT applications classified as high-risk, including certain law enforcement systems used to evaluate the reliability of evidence or profile individuals during criminal investigations. Once their references are published in the Official Journal of the European Union, compliance with these standards will provide a presumption of conformity with the AI Act requirements they cover. For the FCT community, their development therefore offers an opportunity to align research, testing and future procurement specifications with common European requirements, while ensuring that technical conformity is accompanied by the legal and fundamental-rights safeguards applicable to each use.



ETHICAL, LEGAL & SOCIETAL VIEW

During the final implementation cycle of ENACT, the ELSO was the Observatory with most relevant observations, considering both top relevance and other levels. Under those, certain trends were mapped and categorised accordingly.

Anonymity, pseudonymity, unlinkability, undetectability, or unobservability

Observations classified under the topic of **anonymity, pseudonymity, unlikability, undetectability, or unobservability** were heavily connected to aspects about online behaviours and artificial intelligence (AI) technologies. Online sexual harassment, toxic communication online, and cyberbullying and cyberstalking were some of the topics researched in the observations, mainly consisting of scientific publications. These topics illustrate the vulnerability of certain groups in online environments, including women and children. On the same lines, deepfakes, including the creation of fake sexual content, was a main topic found in the ELSO, showcasing the impacts to the victims and the need for regulatory answers to this topic. These themes are further explored in ENACT Flash Reports #20 [29], #11 [30] and #07 [31], which address AI-enabled victimisation, children's online safety and youth vulnerability to online harms, respectively.

Biometric methods

Under the biometrics umbrella, observations from scientific material and news and media addressed different aspects related to **facial recognition** and **new biometric tools** being used by law enforcement. Striking a balance between the potential and the risks derived from the use of these technologies within the FCT context remains as an ongoing challenge for both practitioners and researchers. These issues are further explored in ENACT Flash Report #09 [32], which examines facial recognition and remote biometric identification alongside their legal restrictions and implications for privacy and fundamental rights.

Citizen cooperation and reporting

Victims' perspectives and roles in the FCT domain was a topic heavily addressed in ENACT's last implementation cycle. Both ENACT Flash Reports 07 [33] and 20 [34] tackle the topic. Related themes were also found in different observations related to citizen cooperation and reporting, in different domains, including terrorism, digital or online crimes and crimes against vulnerable groups. Understanding how victims can or should impact the law enforcement work has become a reoccurring topic in the ELSO.

Cybersecurity and cybercrimes

In the ELSO, **cybersecurity** was mainly connected with legal developments and (new) cyberthreats. Under the regulatory framework, both specific and more general instruments were explored in the observations. Namely, international law [35] and, in the EU level, the AI Act, the Cyber Solidarity Act and the Cyber Resilience Act. Not a lot of emphasis was put on the new Digital Omnibus processe [36]. However, more discussions surrounding the changes on cybersecurity issues coming from the Omnibuses are expects.

Threats connected to financial online crimes were the main trend mapped by the Observatory, alongside new threats posed by AI tools. Best practices and use cases on how to investigate and prosecute cybercrimes were also added to the ELSO, in scientific materials in particular. These issues are reported in ENACT Flash Reports #12 [37], #08 [38], and #09 [39], covering financial-crime investigation tools, online investigative methods and AI-enabled threats, respectively, while the ENACT Analytical Report #09 [40], examines responses to communications-enabled scams and associated prosecution challenges.

Security, Safety, and Privacy

It is critical to notice that the FCT environment is composed by different actors who may be affected, in a positive or negative way, by the use of data-driven technologies. From victims to law enforcement agents and courts, risks and possibilities remain. While the potential of handling immense quantities of data becomes more evident with new technologies, the risks also increase, in particular when it comes to data breaches and effects to fundamental rights. Understanding the societal acceptance of these uses and technologies still remains as an ongoing challenge.

Applying the complex regulatory EU system of data governance [41] in the R&I for FCT remains a topic of interest and heavily addressed by the ELSO. Understanding what activities can rely on the flexibilities and opportunities offered to R&I initiatives in the context of law enforcement, security, defence, among others is still a challenge. In parallel, exploring the potential of AI tools and big data to support policing while recognising the risks related to it remains a relevant topic for data security and privacy. For instance, police officers have employed AI tools to generate reports and, more in general, to survey behaviours and better interpret big data information. How and whether these AI generated outputs can be used for law enforcement is still open. Also relevant to notice that the topic of **design** of systems that include security and privacy function was connected to reports of (dual-use) risks related to spyware.

On the citizens side, concerns remain regarding surveillance technologies, in particular when applied by other individuals to violate one's privacy. For instance, the topics of **deepfakes**, including for sexual content creation, and of **smart glasses** were continuously reported. Geo-location and other continuous surveillance mechanisms increase the risks of victimisation, including in domestic violence scenarios.

These concerns are further explored in ENACT Flash Reports #09 and #20, which address safeguards for police use of AI and victimisation through AI-generated sexual content, respectively, alongside Analytical Report #05 [42], on rights-based governance of AI-enabled intelligence tools.

Defence

In the last years, warfare, international armed conflicts, crises, and the role of technology in these scenarios have become part of the daily societal debates, being featured in different newspapers and even scientific publications. Considering this and unlike other cycles in ENACT, defence became a topic of relevance for the ELSO. Observations capture a glimpse of how international bodies, like the UN, NATO and Amnesty International have addressed the topic of defence. A study on the "UN Convention on the Prohibition of Development, Production and Use of Autonomous Weapons" [43] illustrates well how defence is perceived and evaluated in the ELSO. On the same lines, new political plans on defence matters and international relations have also been mapped in the ELSO, and reflected in ENACT's Flash Report #23 [44] and Analytical Report #08 [45]. Media plays a crucial role on updating society on crucial, and sometimes classified, defence matters.

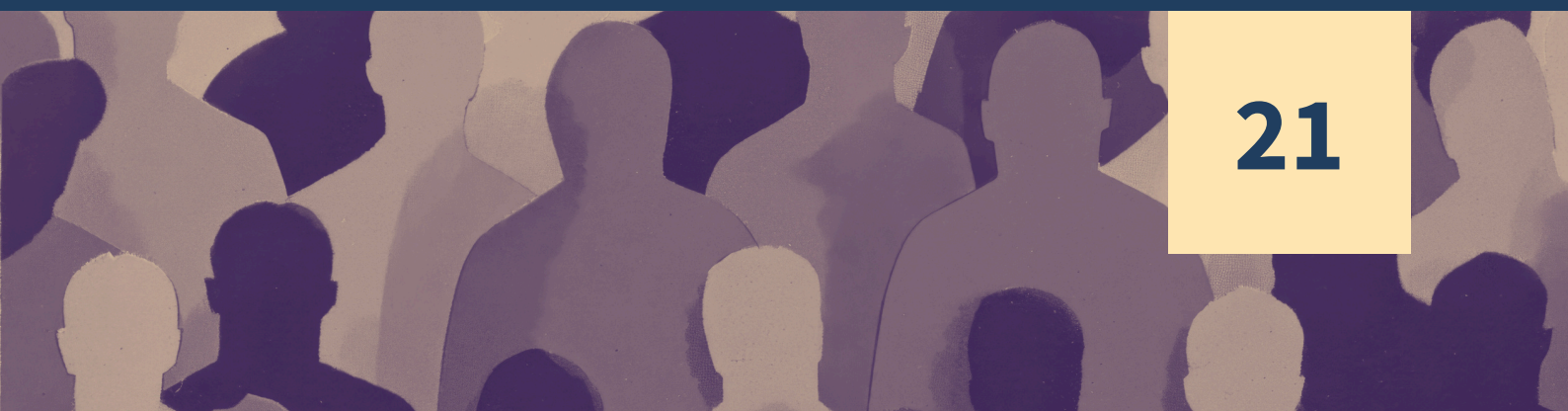
Regulation

A series of different topics were classified under **Legal Aspects**. A major trend on the observations gathered is related to the remaining regulatory gaps in specific domains. For instance, Generative AI and deepfakes, age requirements for using social media, quantum technologies and human rights and technologies. These were heavily influenced by digital sovereignty ideas. Environmental crimes represent a great part of legal observations, showcasing prosecution challenges on the matter. Also, company responsibility for malpractices were reported both on new technologies, like smart glasses and harms related to social media, as well as eco-crimes.

These regulatory issues are addressed in part in ENACT Flash Reports #09 (AI Act and Law Enforcement) and #20 (AI and Implications on Victims), as well as in FR 11 [46], which examine legal safeguards for AI use, responses to sexual deepfakes and AI-related victimisation, and the legal framework for protecting children online, respectively.

Relevant connections

An interesting aspect reported on ELSO were the possible connections between crimes, especially when it comes to organised crimes, but also between corruption and human trafficking and between environmental crimes and other criminal activities. Another important connection is related to technology use in facilitating certain crimes. As already mentioned, technology is an instrument for gender-based and domestic violence crimes. Research has also been developed surrounding time spent online and criminality or radicalisation. The relationship between disinformation and the aggravation of societal crisis, e.g., migration, was also recorded in the ELSO.





22

EU CIVIL SECURITY TAXONOMY

As analysed in the previous State of Play (SoP) report, the EUCS taxonomy was pivotal in the curation the FCT observations, stakeholders and projects landscape, and provided an invaluable tool to structure acquired knowledge. ENACT does not build, maintain or update the EUCS, nevertheless, because the taxonomy is central to ENACT's knowledge-curation and analytical activities, its systematic application across a wide range of sources places the project in a strong position to provide concise, practice-based recommendations. In addition to those presented in the previous SoP Reports [47][48] ENACT has gathered during its final implementation cycle the following specific recommendations:

Policy

Expand the policy dimension to represent areas of law-enforcement activities that are currently absent or only indirectly covered. This should include police cooperation under Horizontal and Societal Issues, consideration of missing persons as a distinct topic, and a broader understanding of the protection of public spaces that also encompasses public and vital or essential infrastructure

Technology

Give quantum technologies explicit and sufficient visibility within the technology dimension, while establishing a more flexible approach for incorporating emerging and enabling technologies as the security landscape evolves.

Functions

Broaden the functions dimension beyond its current emphasis on technical and operational capabilities. The Training and Exercises function seems too narrow and does not explicitly include aspects like collaboration, police cooperation, joint operations and patrols, exchanges of good practices, awareness raising and communication campaigns, which should have their own category. Administrative and enabling services, including translation and interpretation, also require appropriate coverage, while victim support, witness protection and liaison with stakeholder communities should be recognised through a distinct functional category.

ENACT overall observed the absence of FCT-pertinent topics and dimensions for describing the wider context in which security research, innovation and operational practice take place, since it's first iteration cycle. This prompted the creation of ENACT-specific categories and dimensions to further characterise its collected intelligence. To this end, these limitations are presented with a view to support future FCT-related EUCS updates.

Firstly, ENACT required broader categories for **emerging and enabling technologies**. The EUCS technology dimension is primarily structured around identifiable security products, equipment and services, whereas ENACT also needed to classify the underlying technological fields driving their development, e.g. AI, quantum technologies, robotics and autonomous systems, biotechnology, etc. This indicates a need for the EUCS to distinguish more clearly between security products and services and the foundational or emerging technologies on which they depend.

Additionally, ENACT needed a dedicated means of classifying **ethical, legal and societal** considerations related to the FCT domain. Existing Horizontal and Societal Issues mainly describe security problems or areas of intervention and cannot adequately capture matters such as privacy and data protection, anonymity, biometric governance, citizen cooperation, intellectual property, user acceptance, trust, regulatory design and risk management. Consequently, the EUCS provides limited support for recording the safeguards, constraints and societal conditions that influence how security technologies should be designed, evaluated and deployed.

Lastly, the EUCS does not contain a developed **market and innovation** dimension. ENACT therefore required additional coverage of funding, procurement, investment, industrial participation, supply and demand, barriers or drivers affecting innovation uptake, etc. These categories are necessary to understand whether research results can progress from development to procurement and operational deployment.

The EUCS remains an essential and highly valuable common reference for the European civil security community and ENACT looks forward to its continued evolution as it incorporates emerging technologies, operational experience and the wider conditions shaping European security research and innovation.





HIGHLIGHTS

This section delves into the critical insights gathered from ENACT's dedicated Observatories, each providing a unique lens through which to analyse the complex FCT landscape. The **CapO** examines operational needs, capability gaps, emerging threats and priorities for European FCT research and innovation. Complementing this, the **TechO** and **MktO** offer detailed analyses of emerging technological trends and market dynamics within the FCT domain. Finally, the **ELSO** provides crucial perspectives on the ELS challenges and the implications of FCT policies and technologies for people and society, ranging across ethics, legislation, fundamental rights, privacy, accountability, public acceptance and impacts on vulnerable groups. Together, these observatories offer a comprehensive overview of the current state and future trajectory of FCTs, illuminating both opportunities and challenges for the FCT R&I community.



The Capability Observatory identified a growing emphasis on **data, information and intelligence management, investigation and forensics**, and **monitoring and detection** across the EU security landscape. These capabilities were relevant across organised crime, cybercrime, terrorism and radicalisation, and wider societal security challenges. Digital forensics, financial intelligence, crime linking and cross-border investigations featured prominently, reflecting the increasing volume and complexity of digital and financial evidence.

Artificial Intelligence increasingly appeared as an enabling capability across intelligence analysis, digital forensics, risk assessment, crime detection, training and operational decision-making. At the same time, growing attention was given to the ability of law enforcement authorities to **detect, identify and monitor threats**, including through biometrics, drones, satellite imagery, maritime surveillance and AI-supported detection systems.

The data also highlight the continuing importance of **training, skills development and organisational capacity.** Training frameworks, regional needs assessments, AI-related training and digital-forensics capacity were recurrent themes. **Secure information exchange, interoperability and cross-border cooperation** were similarly prominent, particularly in investigations involving organised crime, cybercrime and terrorism.

Overall, the findings point towards a shift from individual capabilities towards **integrated, data-driven and interoperable operational capabilities**, combining intelligence, investigation, detection, technology and human expertise.

The Technology Observatory identified a security innovation landscape increasingly shaped by the convergence of **Artificial Intelligence, cybersecurity, advanced analytics and digital investigation technologies**. Across the considered period, Digital Forensics, **Digital Security Products and Services,** and **Data Analytics** remained the most prominent technology areas, reflecting the growing importance of intelligence-driven approaches to crime prevention, investigation and threat detection.



A major trend observed throughout the year was the widespread adoption of A**rtificial Intelligence** across research, innovation and operational environments. Discussions within the **CERIS community**, the **EU Innovation Hub for Internal Security** and several European R&I initiatives highlighted both the opportunities offered by AI-enabled capabilities and the growing importance of ensuring compliance with the **EU Artificial Intelligence Act (AI Act)**. Explainability, transparency, human oversight and trustworthy AI emerged as recurring priorities for future capability development.

From a functional perspective, the strongest concentration of developments relates to Data, Information and Intelligence Gathering, Management and Exploitation, followed by Monitoring and Surveillance of Environments and Infrastructures and Investigation and Forensics. This reflects the increasing demand for technologies capable of transforming large volumes of heterogeneous information into actionable intelligence, enhancing situational awareness, supporting evidence-based investigations, and strengthening operational decision-making.

Cybersecurity remained a dominant area of technological activity, driven by the increasing prevalence of cyber-enabled crime, attacks against information systems and digital fraud. Significant advancements were observed in AI-assisted threat detection, digital forensics, cyber resilience technologies and advanced analytical tools capable of supporting the collection and exploitation of digital evidence.

The Observatory also identified growing interest in technologies supporting the detection and mitigation of **synthetic media, deepfakes and AI-generated content**, reflecting emerging challenges associated with Generative AI and information manipulation. In parallel, increasing attention was devoted to **Counter-Unmanned Aircraft Systems (C-UAS)**, where research and innovation activities focused on integrated solutions combining sensor fusion, artificial intelligence and advanced situational awareness capabilities to respond to evolving drone-related threats.

Overall, the findings reveal a clear shift towards **AI-enabled, data-driven and operationally deployable security capabilities**, while simultaneously highlighting the growing importance of ethical, regulatory and societal considerations in the development and adoption of future security technologies.



The Market Observatory identified a security market landscape increasingly shaped by **rising defence and security investment, intensifying digital market regulation**, and the **maturation of illicit online market structures**. Across the considered period, **Cybersecurity, Artificial Intelligence and advanced connectivity/digital technologies** emerged as the most prominent technology areas underpinning market activity, alongside growing attention to **robotics** and **autonomous systems, quantum technologies,** and **space** and **propulsion technologies**, reflecting a **security market that is diversifying** well beyond traditional equipment procurement, with a large **focus on dual-use**.

A major trend observed throughout the year was the **expansion of public and private investment** in defence and security capabilities. Observations on the EU's defence investment strategy, alongside selected NATO initiatives, provided wider context for developments in European security markets, particularly **private investment, supply-chain resilience** and **digital infrastructure**. The EU's Industrial R&D Investment Scoreboard and EU-funding observations further situated these developments within the broader research and innovation landscape. Their relevance to FCT lies in potential overlaps in technologies, suppliers and infrastructure. Within the FCT market, procurement, supply-chain dynamics and industry cooperation frameworks were consistently among the most frequently observed market subjects, underlining a market increasingly organised around translating **disruptive technologies** into deployable, **fundable capabilities.**

From a regulatory and competitive perspective, the Observatory recorded growing scrutiny of **digital markets** and **platforms** at EU level, including enforcement action against major e-commerce and social media players, debates on interoperability and "Big Tech" market power, and questions over the **governance of AI systems** entering defence and security use, such as the EU standardisation request on AI to CEN/CENELEC. These observations reflect a market environment where **commercial competitiveness** and innovation are increasingly weighed against compliance with EU digital and **AI regulation**, export controls, and legal accountability, echoed in ELSO-classified observations on cybersecurity regulation, data protection and legal aspects.

Mirroring the technology area, **cybersecurity** remained the dominant technology driver of market activity, but the Observatory also highlighted case studies of technology adoption and regulatory or investment frameworks, followed by observations on the disruptive potential of **emerging technologies, innovation dynamics, and industry cooperation**. A distinct and growing theme was the classification of technologies as **dual-use**, alongside a recurring focus on **regulatory sandboxes** (R&I sandbox), pointing to an increasing reliance on controlled testing environments to bring emerging and dual-use technologies to market under evolving regulatory conditions. **Supply chain, equipment, procurement and EU-funding observations** further mapped the concrete pathways through which technologies move from research into deployment, while repeated attention to barriers and drivers of adoption underscored ongoing analysis of what enables or constrains market uptake.

Overall, the findings reveal a security market **moving in two directions** at once: **strong technology-push** from AI, cybersecurity, quantum and dual-use innovation, and an equally **strong regulation-pull** from EU legal, privacy and AI-governance frameworks, with **regulatory sandboxes**, dual-use classification and EU funding instruments emerging as the practical mechanisms bridging the two.

During the final implementation cycle of ENACT, the Ethics, Legal and Societal Observatory mapped an increase relevance of ELS topics surrounding R&I in the FCT domain. A direct connection between the ELSO and new technologies found in the TechO can be traced. For instance, the ELSO found heavy reporting on the risks and distrust on **AI tools**, in particular **facial recognition** and **smart glasses**. This trend represents a continuity from what was found in the previous cycles of the project.



As a novelty, **defence** became a more prominent topic in the ELSO. Observations illustrate an interest in applying technologies, such as drones and satellites, in armed conflicts, while also recognising the risks related to this. With a direct connection to the current political climate, international bodies' actions were also mapped by the ELSO under the defence umbrella. Another new topic found in the Observatory is the possible regulation of **quantum technologies.**

Crimes against vulnerable groups represent the major trend observed by the ELSO, particularly in two fronts. First, the debate surrounding the regulation on **Child Sexual Abuse Material (CSAM)**. Considering the societal will of protecting children, especially in online environments, there is a lot of interest in providing more legal solutions for the topic. However, it is not clear if society accepts the risks related to continuous surveillance of their communications and how technology products can or not comply with the proposed solutions. On the same lines, usage of **AI** to produce sexual **deepfakes** was also the main topic of a great number of observations. Second, the ELSO found content on how new technologies facilitate gender-based crimes, including domestic violence.

The EU regulatory framework remains a main topic of interest of the ELSO. Although the Digital Omnibus was not yet heavily debated under the FCT domain, aspects surround human rights, cybersecurity, and privacy were and still are a topic heavily addressed in the ELSO. More research on how these legal instruments affect R&I in FCT is still needed, particularly- considering new technologies and crisis scenarios.





CONCLUSIONS AND STRATEGIC PRIORITIES FOR FCT POLICY AND R&I

The findings of this third ENACT State of Play report indicate that Europe's FCT priorities increasingly converge around digital investigation, financial intelligence, information exchange and AI-supported capabilities. Their strategic significance lies in the changing balance between criminal adaptability and institutional readiness. Generative AI, synthetic media and digitally connected criminal services can increase the scale of fraud, exploitation and manipulation while making identities, information and evidence harder to verify. For law enforcement, the operational consequence is a growing need to authenticate digital material, connect financial and investigative intelligence across jurisdictions, and respond to emerging threats without compromising evidential reliability or fundamental rights. The central policy challenge is therefore to ensure that investment in security R&I produces capabilities that practitioners can lawfully, reliably and sustainably use.

For policy-makers, an immediate priority should be to translate these developments into a focused capability agenda for future FCT programming. Particular attention should be given to digital evidence integrity, including synthetic-content detection, financial investigation linked to organised crime and terrorist financing, secure cross-border information exchange and the protection of children and other vulnerable groups exposed to technology-facilitated harm. Counter-drone capabilities warrant targeted support where civilian operational needs, deployment conditions and legal responsibilities are clearly established. These priorities should be developed with practitioners and assessed against existing project results, so that new funding addresses unresolved needs and supports the uptake of promising solutions. The evolving EU funding architecture also makes it important to maintain clear routes between civil security research, operational validation and deployment, with civilian FCT needs remaining explicit

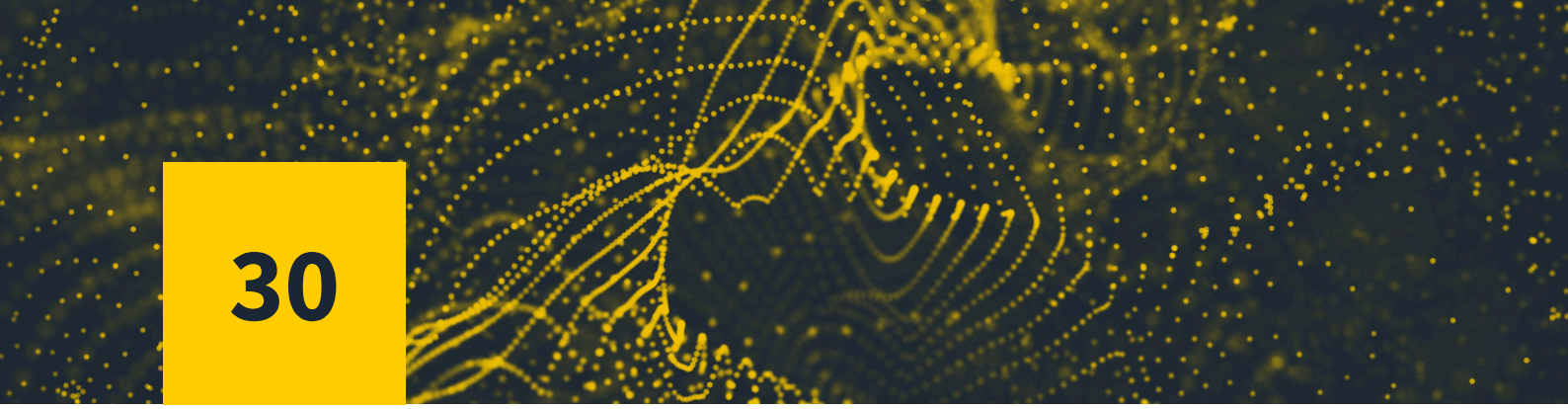
For Member States, the priority is to connect national capability planning with implementation capacity and procurement. The ISF National Programmes provide a useful indication of planned demand, particularly for data infrastructure, information exchange and training, but this demand must be translated into defined requirements, responsible authorities, budgets and delivery plans. National authorities should assess the readiness of intended users before acquiring new tools, including staffing, technical infrastructure, legal expertise and the ability to maintain systems throughout their lifecycle. Joint testing and, where appropriate, coordinated procurement can help address shared needs and reduce fragmentation. Procurement specifications should include interoperability, cybersecurity, data portability and lifecycle support, alongside performance and applicable legal safeguards. Conventional and innovation procurement should be selected according to the maturity of available solutions and the capability required.

For LEAs, effective adoption requires organisational change alongside technical investment. Agencies should prioritise training in digital forensics, financial investigation, AI literacy and the assessment of synthetic or manipulated evidence. Agencies should test AI-supported outputs in defined operational scenarios, with documented limitations, meaningful human oversight, and clear accountability for their use. Cooperation with judicial authorities is particularly important where tools influence evidence assessment or investigative decisions. Interoperability should be evaluated through practical cross-border workflows, including the preservation, interpretation and lawful exchange of information. Without these measures, integrated platforms risk adding complexity, dependence on suppliers and new sources of error to already demanding investigative environments.

For the security R&I ecosystem, operational validation and governance should become central measures of success. Researchers and industry should involve end users early, test against realistic and evolving threats, and provide evidence of reliability, usability, security and compliance. Evaluation should extend beyond technical accuracy to include false positives, bias, explainability, workload and integration with existing procedures. AI governance and relevant standardisation work should inform system design and procurement readiness from the outset. The concentration identified in the standards mapping also warrants closer examination of operational requirements in less represented FCT areas before specific standardisation priorities are selected. Where defence and civilian security technologies overlap, proposed transfers should be assessed against the distinct legal, operational and societal conditions of civilian law enforcement.

Across these actions, victim protection and public trust should be treated as conditions of operational effectiveness. Responses to sexual deepfakes, online exploitation and technology-facilitated domestic violence require accessible reporting, appropriate support and coordination between authorities and relevant service providers. Privacy, proportionality and accountability should be reflected in design choices, testing and deployment decisions. Expanding surveillance or analytical capacity without demonstrating necessity and effectiveness risks undermining the cooperation on which prevention and investigation depend.

ENACT's final observations provide a structured basis for identifying priorities. The findings call for closer alignment between FCT research, operational needs, procurement and governance, with particular attention to practitioner readiness, interoperability and fundamental rights. Progress should be judged by whether these efforts deliver reliable capabilities that improve prevention, investigation and victim protection.



30

REFERENCES

[1] ENACT 2026-1 FCT Maps – Capabilities Observatory

[2] ENACT 2026-2 FCT Maps – Capabilities Observatory

[3] ENACT 2026-1 FCT Maps – Technology Observatory

[4] ENACT 2026-2 FCT Maps – Technology Observatory

[5] ENACT Flash Report #08 - Digital Tools for Online Crime Monitoring: Investigative Technologies Supporting Law Enforcement Agencies

[6] ENACT Flash Report #09 – AI Act and Law Enforcement

[7] ENACT Analytical Report #05 – From Compliance to Trust: Operationalising rights-based governance for AI-enabled intelligence support technologies in the EU FCT domain

[8] EU Serious and Organised Crime Threat Assessment

[9] European Union Terrorism Situation and Trend report 2025

[10] ENACT Analytical Report #9 - Methods to Facilitate the Traceback and Mitigate the Spoofing of Telecommunications

[11] ENACT Analytical Report #4 - Digital Capability Readiness in EU Law Enforcement: Evidence from Horizon FCT Projects

[12] ENACT Flash Report #23 – Counter-UAS Capabilities in the EU

[13] ENACT Analytical Report #7 - UAV Detection Technologies for Law Enforcement: Operational Readiness and Regulatory Feasibility against RF-Silent Targets at Bounded, Resource-Constrained Sites

[14] ENACT Analytical Report #8 - Structural Barriers to the Deployment of RF-Based Counter-UAS Systems for Critical Infrastructure Protection in the EU

[15] ENACT Flash Report #04 - Drug Production, Distribution, and Forensics Research in Horizon 2020 and Horizon Europe

[16] ENACT Flash Report #09 – AI Act and Law Enforcement

[17] ENACT Flash Report #20 – AI and implications on victims

[18] ENACT Flash Report #08 – Digital Tools for Online Crime Monitoring: Investigative Technologies Supporting Law Enforcement Agencies

[19] ENACT Flash Report #23 – Counter-UAS capabilities in the EU

[20] ENACT Analytical Report #07 - UAV Detection Technologies for Law Enforcement: Operational Readiness and Regulatory Feasibility against RF-Silent Targets at Bounded, Resource-Constrained Sites

[21] ENACT Analytical Report #08 – Structural Barriers to the Deployment of RF-Based Counter-UAS Systems for Critical Infrastructure Protection in the EU

[22] ENACT 2026-1 FCT Maps – Markets and Standards Observatory

[23] ENACT 2026-2 FCT Maps – Markets and Standards Observatory

[24] ENACT Analytical Report #6: Innovation Procurement in the EU Security Sector: State of Play, the Use of Available Tools across EU Member States, and Best Practices

[25] Source: 2024 benchmarking of national policy frameworks for innovation procurement, Table 1.

[26] Directive on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defense and security.

[27] ENACT Analytical Report #3: Internal Security Fund – Analysis of EU Member State Priorities

[28] The 2026 annual Union work programme for European standardisation

[29] ENACT Flash Report #20: AI and Implications on Victims

[30] ENACT Flash Report #11: Web Traps and Digital Resilience

[31] ENACT Flash Report #7: Youth and Criminality

[32] ENACT Flash Report #9: AI Act and Law Enforcement

[33] ENACT Flash Report #7: Youth and Criminality

[34] ENACT Flash Report #20: AI and Implications on Victims

[35] The Regulation of Cybercrime in International Law: Discussing the Legal Frameworks and Challenges in Regulating Cybercrime, available at: https://doi.org/10.59075/ijss.v3i2.1267

[36] MEPs give mixed reception to omnibus' single cyber reporting plan, available at: https://www.euractiv.com/news/meps-give-mixed-reception-to-omnibus-single-cyber-reporting-plan/.

[37] ENACT Flash Report #12: Europol Industry and Research Days

[38] ENACT Flash Report #8: Digital Tools for Online Crime Monitoring

[39] ENACT Flash Report #9: AI Act and Law Enforcement

[40] ENACT Analytical Report #9: Methods to Facilitate the Traceback and Mitigate the Spoofing of Telecommunications

[41] AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union, available at: https://doi.org/10.1016/j.cose.2025.104628.

[42] ENACT Analytical report #5: From Compliance to Trust

[43] Available at: https://www.lawjournal.digital/jour/article/view/628.

[44] ENACT Flash Report #23: Counter-UAS Capabilities in the EU

[45] ENACT Analytical Report #8: From lab to Field: Structural Barriers to the Deployment of RF-Based Counter-UAS Systems for Critical Infrastructure Protection in the EU

[46] ENACT Flash Report 11: Web Traps and Digital Resilience

[47] ENACT 2024 FCT State of Play Policy Report

[48] ENACT 2025 FCT State of Play Policy Report



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.