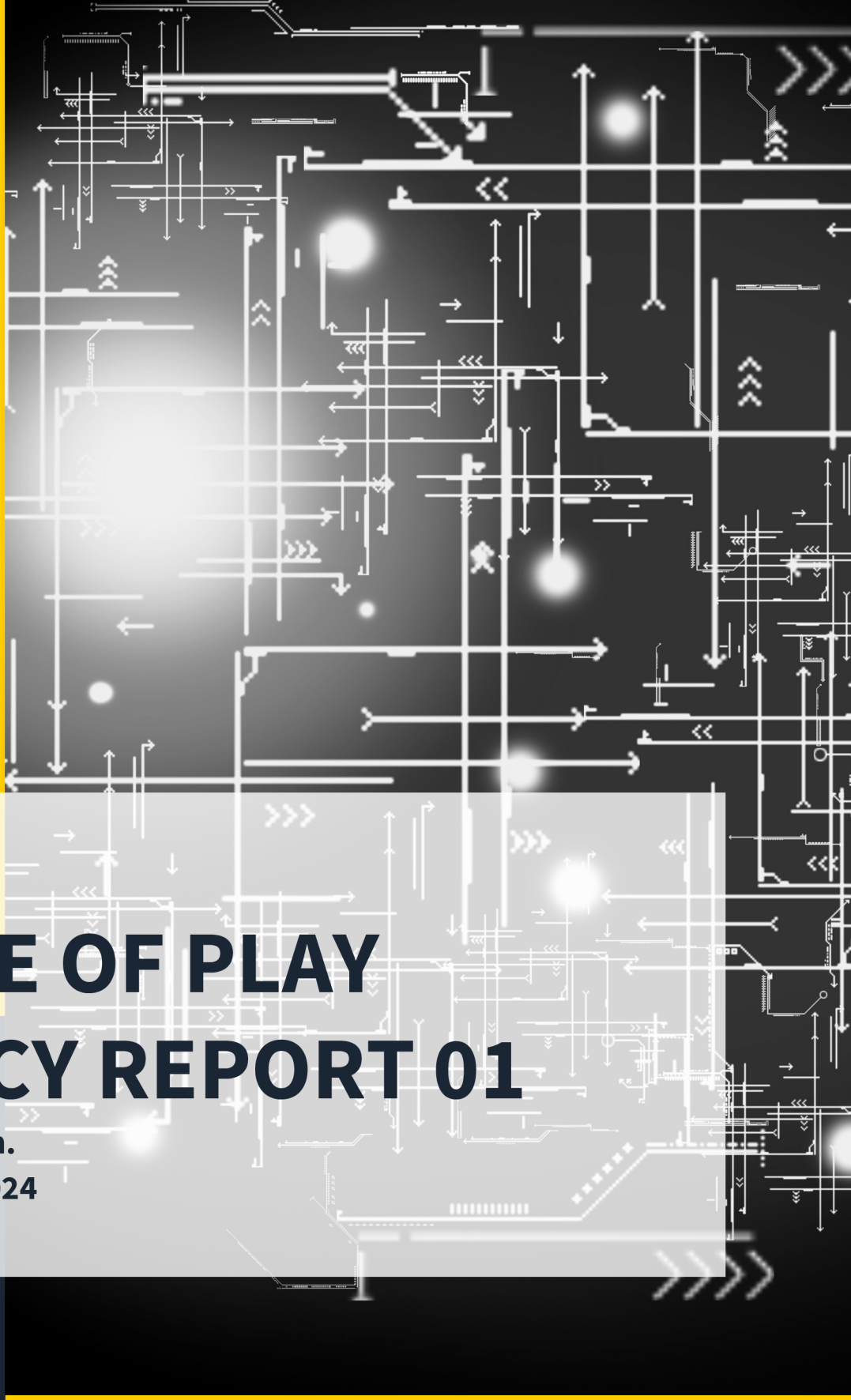
STATE OF PLAY REPORT 01



STATE OF PLAY POLICY REPORT 01

Public Version.
September 2024

Inter-Observatory Coordinator: INOV
Capabilities Observatory: PJ
Technology Observatory: CENTRIC
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-SoP-Report-2024-Public

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.

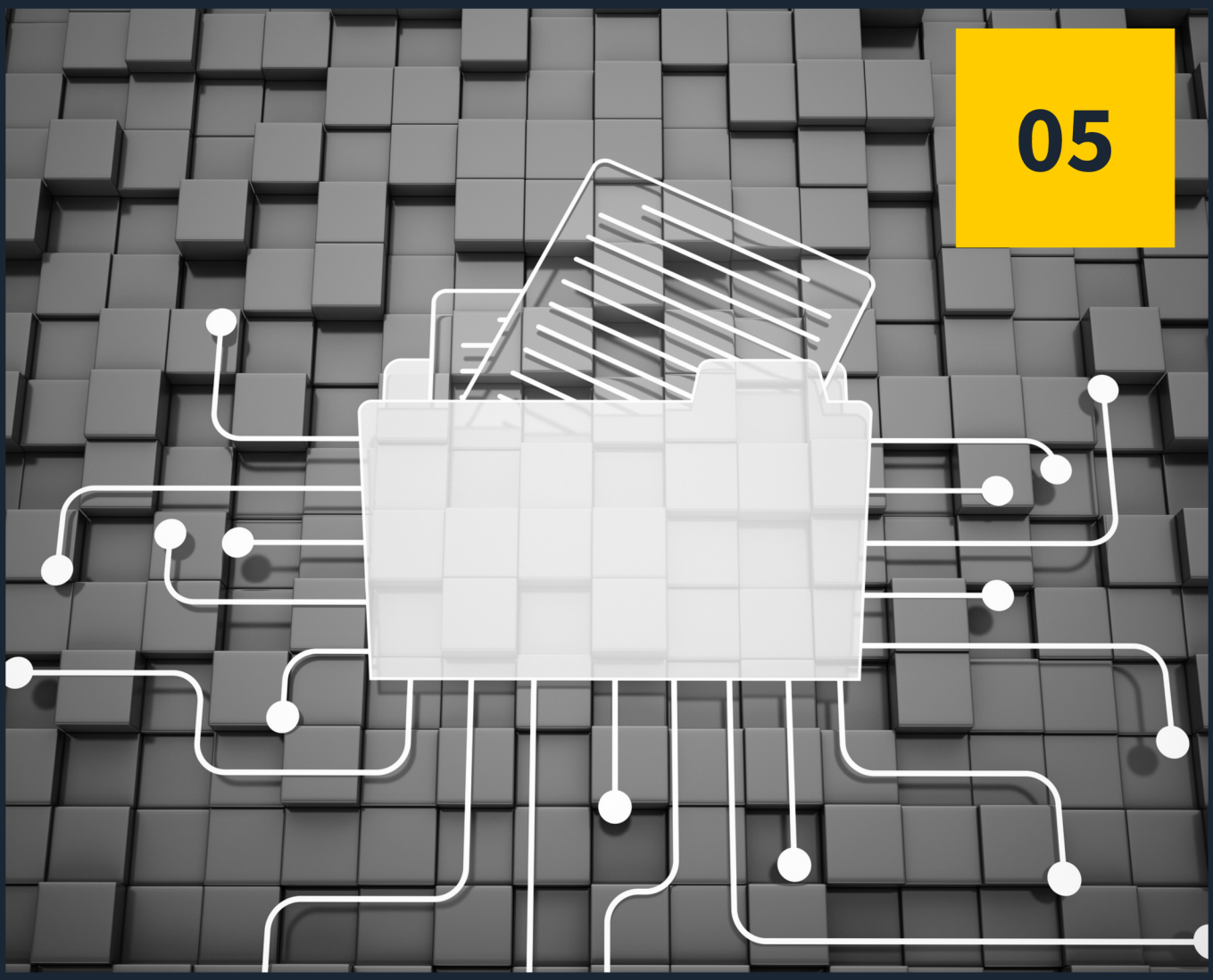
Copyright

Acronyms

ADS	Aerospace, Defence, Security & Space
AI	Artificial Intelligence
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CCTV	Closed-circuit Television
CERIS	Community for European Research and Innovation for Security
CINTiA	Criminal Intelligence – New Trends in Analysis
CSA	Coordination and Support Action
EC	European Commission
ELS	Ethical, Legal and Societal
EU	European Union
EUCS	European Union Civil Security
EUDA	European Union Drugs Agency
FBI	Federal Bureau of Investigation
FCT	Fight against Crime and Terrorism
FP	Framework Programme
G2G	Government-to-Government
H2020	Horizon 2020
IA	Innovation Action
ICT	Information and Communications Technology
IOC	Inter-Observatory Coordinator
IOCTA	Internet Organised Crime Threat Assessment

Acronyms

IT	Information Technology
KH	Knowledge Hub
KO	Knowledge Observatory
LEA	Law Enforcement Agency
NATO	North Atlantic Treaty Organisation
OSINT	Open-source Intelligence
PCP	Pre-Commercial Procurement
PNR	Passenger Name Record
PPE	Personal Protective Equipment
PSE	Public Security Exhibition
R&I	Research and Innovation
RIA	Research and Innovation Action
SICUR	Salón Internacional de la Seguridad
SKB	Structured Knowledge Base
SoP	State-of-Play
SPIE	Society of Photographic Instrumentation Engineers
TECNOSEC	Altas Tecnologías de Seguridad e Inteligencia, Drones y Antidrones
UAS	Unmanned Aerial Systems
UAV	Unmanned flight vehicle
UK	United Kingdom
URL	Uniform Resource Locator



05

STATE OF PLAY FCT POLICY REPORT 2024

The ENACT State of Play FCT Policy Report 2024 offers a concise and targeted overview of recent developments, latest insights, and recommendations from various ENACT activities from March to July 2024 in the FCT domain. This report consolidates insights and recommendations derived from various ENACT products, including Flash Reports and Analytical Reports produced, and also compiles analyses carried out by ENACT in support FCT workshops, events, and discussions. This includes inputs from the FCT experts' group and other relevant FCT R&I (research and innovation) events organised by the Commission. By summarising outcomes and recommendations from these and other Commission-organised 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.

06

POLICY VIEW

The current policy landscape in the FCT area is shaped by three key trends. Firstly, there is a prominent focus on **organised crime** and **cybercrime**. Organised crime remains the foremost concern, accounting for 38% of attention, particularly in areas such as human trafficking, smuggling of goods, economic crimes, corruption, and fraud. This is close followed by **cybercrime** which captures 31% of the focus, with a strong emphasis on countering activities on the darknet and the misuse of cryptocurrencies.

Secondly, the interconnected nature of threats is becoming increasingly apparent. Nearly a third of news reports about economic crimes also touch upon terrorism financing, underscoring the **links between organised crime and terrorism**. Additionally, 80% of reports on darknet activities are related to economic crimes, corruption, and fraud, highlighting how new technologies are facilitating criminal endeavours.

The third significant trend is the challenge of **disinformation and fake news**. This issue is particularly salient under the category of horizontal issues, with substantial attention given to the use of deepfakes and the mass dissemination of propaganda via social media. This reflects concerns over its impact on political stability and public trust, especially in the context of elections.

KEY TRENDS IN THE POLICY AREA

1 Main focus on organised crime and cybercrime

2 Strong links between economic crime and terrorist financing

3 Disinformation & fake news including deepfakes

Regarding policy trends, the focus on FCT is reflected in the media, where approximately 39% of news observations centre on **organised crime** and 29% on **cybercrime**. This concentration reinforces these areas as priority concerns. In response, the policy framework is geared towards adopting **digital forensic** tools, **internet-based investigations**, and advanced **data analytics**. These measures aim to bolster the capabilities of law enforcement agencies (LEAs) in detecting, monitoring, and disrupting criminal activities.

In parallel, R&I policies continue to prioritise investment in technological advancements related to **digital forensics**, **data analytics**, and **internet-based investigations**. These areas are prominently observed, accounting for 22% and 11% of news coverage respectively. Insights from ENACT's first Analytical Report #1 [1] suggest that EC-funded initiatives are predominantly targeting these technological areas and functions, which underscores the good alignment between the FCT R&I programming and the main policy trends observed by the ENACT Observatories. The goal is to develop robust and agile tools and methodologies that will enable LEAs to effectively address the evolving digital landscape of criminal threats.

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

07

TECHNOLOGY VIEW

Through the structured knowledge base (SKB), ENACT identifed four highly prevalent functions that align with the technology observatory.

Data, information & intelligence gathering management, and exploitation

Detection of goods, substances, assets and people and incidents

Monitoring and surveillance of environments and activities

Investigation and forensics

Commercial and Operational Products

ENACT's Flash Reports highlight the technology market for the security sector. These reports identified 95 and 113 companies, from the **TECNOSEC** [1] and **SICUR** [2] exhibitions, as significant contributors to FCT.

The key technologies showcased at SICUR focused on **access control/authorisation systems and surveillance systems,** specifically video surveillance systems (CCTV systems, cameras and sensors, video analytics). Within **surveillance systems**, technology included s**mall tactical drones** and **autonomous ground vehicles**; while **access control** included **control gates, biometric identification/ authentication, smart locks, personal protective equipment and safety equipment**. While, TECNOSEC focused on **surveillance systems data analytics** and **critical communications, interoperable communications** and **digital security products and services**.

Based on these reports, technologies related to **surveillance systems** are the most prevalent on the **safety and security market.** In events more oriented towards LEAs, **data analytics** and **communications** technologies emerge compared to those in the wider security sector.

Research and Innovation

In the project database, there are currently 44 active projects aligned to the FCT domain. In terms of the functional areas, **data, information & intelligence gathering management**, and **exploitation, investigation and forensics**, and t**raining and exercises** are each addressed by more than half of the projects present, indicating a high orientation to these areas in the previous years' funding cycle. This does not translate directly into commonalities in the technology areas, where **internet-based investigation** is addressed by 25% of these projects, **data analytics** by 13%, and all other technology areas by lower amounts.

Considering the observations included in the SKB regarding project results, these are somewhat skewed towards projects related to drugs (due to the preparation for the flash report for the European Union Drugs Agency (EUDA)) which prioritise sensing technologies – both for lab-based forensics and for larger scale such as maritime or customs use cases. Furthermore, the majority of these projects were funded under FP7 or H2020 and the technologies are no longer under active development within the project context.

[1] https://enact-eu.net/wp-content/uploads/2024/07/ENACT-FLASH-REPORT-2-TECNOSEC-EVENT.pdf
[2] https://enact-eu.net/wp-content/uploads/2024/04/ENACT-FLASH-REPORT-1-SICUR-exhibition.pdf

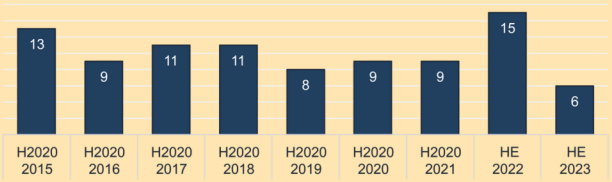
08 MARKET & STANDARDS VIEW

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.

Market Size

According to the data collected on **Horizon Dashboard** , the total EU funding granted to the participants of the selected projects was €367.4m over 7 years. The total cost of the selected calls, meaning the total costs of the projects including EU contribution but also other funding sources such as private investment, totalled €380m.

Number of signed grant agreements over time 2015 - 2023



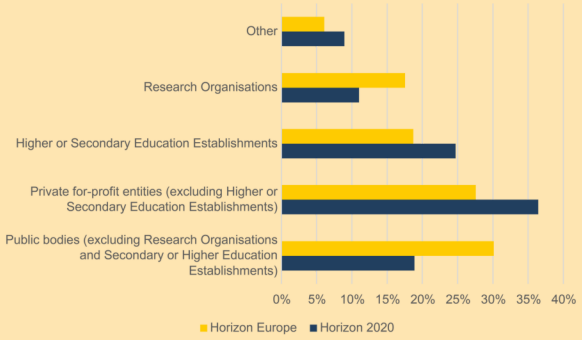
Looking at the type of action and funding scheme used to support FCT R&I under Horizon 2020, 80% of the grants were research and innovation actions (RIA). Coordination and support action (CSA) and innovation actions (IA) represent 2% of the total grants, and pre-commercial procurement (PCP) represents 18%. In comparison, Horizon Europe sees an increase for IA, which covers 70% of the eligible costs of the action.

The comparison between the Horizon 2020 and the first two years of the Horizon Europe, allows to make two observations. Firstly, the total budget allocated to FCT R&I is decreasing. Secondly, the share of IA is increasing. This trend could indicate solutions developed to address FCT issues are closer to the market, thus requiring more innovation actions (IA); or by the decreased budget allocated to FCT R&I, which may have prompted a focus on market-ready solutions.

Market Actors

The evolution of the beneficiaries' organisation type between Horizon 2020 and the first two years of the Horizon Europe shows the share of public bodies has significantly increased under Horizon Europe. On the contrary, the share of both private for-profit organisations and higher or secondary education establishments has decreased.

Distribution of organisation types in H2020 and Horizon Europe



Funding Opportunities

The EU provides FCT R&I funding opportunities to support both end-users and solution providers. The available options can be used to facilitate research, development and innovation activities, as well as pilots, testing, or procure-ment of innovative solutions. These can be delivered through **direct management, shared management** or **indirect management.** FCT-related funding programmes include Horizon Europe, Internal Security Fund, Digital Europe, Connecting Europe, Border Management and Visa Instrument, Customs Control Equipment Instrument, Customs Programme, EU Anti-Fraud Programme, Programme for the Protection of the Euro against Counterfeiting, and the Union of Civil Protection Mechanism.

09

ETHICAL, LEGAL & SOCIETAL VIEW

Ethical, legal and socetial (ELS) aspects are a part of everyday activities and concerns of actors involved in FCT. Considerations on these topics are part of all development phases of a new technology, procedure or activity. From R&I to the enforcement activities, actors must be aligned with values and rights that must be considered in all activities that may affect individuals.

Ethical and Societal Issues

Data exchange is still highly relevant in FCT Specifically, international cooperation has a central role in investigating and preventing crime, especially **organised crime** and **cybercrime**. With transnational crime, global cooperation is essential for LEAs. However, challenges such as the protection of human rights across jurisdictions, lack of trust in data-based technologies, and observing the necessity of processing data for each purpose exist. Also, **disinformation** is a hot topic in the area of societal issues.

Societal engagement can guarantee civil representation and safeguard the interests of society. Therefore, evaluating the societal impact of a new procedure or technology reoccurs in research and projects (e.g., human rights and societal impact assessments). Practitioners' reports (over 50% of high-relevance observations) mention societal impacts periodically. These reports usually relate to actions and results of operations, technologies and forms of investigation. The ELS Observatory lacks material on how to practically assess societal impacts and guarantee social engagement.

FCT events do tackle ELS topics, but in a more lateral and generalized manner. For the best development of good practices in the FCT domain, it is crucial to have more events involving different actors, including ethics and legal specialists and law enforcement agents.

EU & Member States Legal Framework

The AI Act was a major development in the EU legal framework bringing decisive rules for the use of AI. Surveillance and identification and authentication of persons, assets and goods were closely linked to the observations involving AI regulation while discussing possible biases, inaccuracies and risks. Considering the prohibitions in the AI Act, biometric identification and use of biometric data in AI technologies are central themes to FCT. Data use, re-use and exchange persists in the EU frame-work, with various acts put into place and the developments of the EU Data Strategy. Additionally, regulations not directly focused on law enforcement also impact the uses, limits and possibilities of equipment, technology, information exchange, among other practices.

Another relevant regulatory development was the proposal to prevent and combat child sexual abuse. The protection of children is of utmost relevance. Nonetheless, other values and rights could be affected, media and academic results report risks in possible surveillance mechanisms. which could affect a large group of people.

Organised crimes, tax fraud and money laundry are significant topics, which link to cryptocurrencies. Thus, regulatory and international bodies have been working to ensure the security of digital currencies, and guarantee the legal use of these assets. Limits to privacy when designing surveillance measures for digital currencies and payments must be considered alongside these regulatory developments.

10

EU CIVIL SECURITY TAXONOMY

The use of a taxonomy to structure and classify the knowledge acquired and produced by the ENACT observatories was considered crucial from the inception of the project. ENACT aimed to systematically assess the vast and scattered information landscape and deliver structured knowledge mapped to the categories defined in a well-known taxonomy. This helps in ensuring that the information collected, and the knowledge produced could be seamlessly exchanged with and integrated in the work of other FCT R&I stakeholders outside the Consortium, thus managing and facilitating the communication and reducing the loss of information. The reference taxonomy chosen by ENACT for this purpose is the one elaborated under the **EU Security Market Study** [1] commissioned by DG HOME.

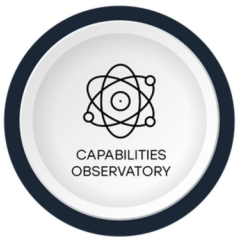
Several ENACT partners had contributed in consultations to the drafting and validation of the taxonomy produced in the study. The project then used the material gathered during this validation process as an initial reference for the definition of the ENACT taxonomy, which was translated to the 2021 version of the EU Civil Security (EUCS) Taxonomy. Some additional material related to the EUCS Taxonomy was also made available by DG HOME through the CERIS website [2], including an **EUCS market segmentation model** [3] and an **EUCS taxonomy and taxonomy explorer** [4]. This material is hereinafter referred to as the 2022 version of the EUCS taxonomy. Given that one of the objectives of ENACT is also to contribute to improving the quality of this taxonomy, the intention of the project is to be flexible in its use and issue recommendations regarding possible variations in upcoming versions delivered by DG HOME in future studies. It should therefore be noted that the EUCS taxonomy is, in itself, a subject of study for the ENACT project.

The Research Strategy of ENACT utilised the 2021 version of the EUCS taxonomy as a starting reference to structure knowledge. The v2021 taxonomy adopted (last update: 19/11/2021) is represented by its three main dimensions Policy, Function and Technology dimensions.

Finally, ENACT has informed the community about our approach to the use of the taxonomy, via documents, publications and presentations, for example, and this has raised some interest. It would be advisable that the EC continues to give visibility to the taxonomy and promote its use.

[1] **EU Security Market Study**: https://op.europa.eu/en/publication-detail/-/publication/db2efbc8-070a-11ed-acce-01aa75ed71a1
[2] **CERIS - Community for European Research and Innovation for Security.** https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en
[3] **EUCS market segmentation model**: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-market-segmentation-model_en
[4] **EUCS taxonomy and taxonomy explorer**: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en

11 HIGHLIGHTS



In July 2024, Europol released its **Internet Organised Crime Threat Assessment (IOCTA)** [1], shedding light on the increasing complexity and fragmentation of the cybercriminal landscape. The report emphasises how organised crime groups adopt more sophisticated cyber tools, making detection and prevention more challenging. A key finding is the interconnected nature of various criminal activities, such as organised crime, economic crime, terrorism financing, and the spread of disinformation, all increasingly converging in the digital realm.

Similarly, at the end of 2023, the **FBI's Internet Crime Report** [2] highlighted the alarming growth of cyber threats in the United States, noting a substantial rise in ransomware attacks and other forms of cybercrime. The FBI reported an 18% increase in ransomware incidents and a 74% increase in associated losses, mirroring trends identified by Europol. Both reports underscore the global nature of these challenges, with organised crime groups exploiting digital tools to perpetrate cybercrimes on an unprecedented scale. This convergence shows the critical need for international cooperation to address the cyber threat landscape.

Europol's IOCTA 2024 and the FBI's Internet Crime Report 2023 highlight the convergence of traditional organised crime with cybercrime, mainly through ransomware and other digital tools, demonstrating that cybercriminals and organised crime groups are increasingly sophisticated and resilient, adapting quickly to law enforcement efforts and exploiting the global reach and anonymity provided by the internet. The growing complexity of these threats underscores the urgent need for international cooperation and robust strategies to combat the ever-evolving landscape of cybercrime, which now transcends national borders and impacts both public and private sectors worldwide.

The European Council formally adopting the EU AI Act and its publication illustrates well how regulatory frameworks currently focus on risks and opportunities of developing and using new technologies in different domains, including the FCT. The same rationale also applies to the regulatory framework involving data use and re-use for public interests. Practitioners recognise the challenges brought by cryptocurrencies in the investigation of cybercrimes, due to their anonymity and lack of centralised control, creating a strong need for new regulatory measures to enhance law enforcement capabilities. While promoting that ethics must be embedded in all phases of procedures, technologies and actions in the FCT domain, practitioners should also understand that international cooperation and modern regulations are needed to meet the societal needs for respecting fundamental rights and values and guarantee the proper investigation and enforcement against illegal activities.

[1] **IOCTA 2024**: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
[2] **FBI's Internet Crime Report 2023**: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

As the use of AI in crime prevention continues to expand, the complexity of combating criminal activities has also increased. AI enables law enforcement agencies to process and analyse vast amounts of data, identifying crime patterns that would be impossible to detect manually. As criminal actors increasingly exploit sophisticated tools to further their illicit activities, law enforcement and security practitioners must similarly adopt advanced technologies to prevent, respond to, and mitigate these threats effectively.

The integration of AI into law enforcement operations makes it increasingly difficult for criminals to conceal their activities, as these advanced tools enhance the ability to predict and respond to criminal behaviour with greater precision. Since 2022, **INTERPOL's Project CT-Tech** [1] has underscored the critical importance of advanced technology in combating modern threats such as terrorism and organised crime. This initiative focuses on enhancing the capabilities of global LEAs by integrating new technologies, including facial recognition and open-source intelligence (OSINT), and employing tools like digital forensic software to gather and analyse digital evidence more effectively.

Supported by the EU, Project CT-Tech aims to improve law enforcement's operational, investigative, and analytical capacities through comprehensive training on these technologies. The project highlights the necessity of understanding how terrorists use technology while simultaneously adopting advanced tools to counter these threats effectively, ensuring that LEAs remain one step ahead in the fight against crime and terrorism.

Other recent publications, such as **Europol's IOCTA 2024** highlight the abuse of technology by criminals. The abuse of AI, cryptocurrencies and the dark web all remain high on the agenda of LEAs and consequently need to technologies to counteract such crime threats. Furthermore, in their **First Report on Encryption** [2], Europol are also calling for more research into cryptography and telecommunications as well as biometrics.

Upcoming events in the technology area include the **Forensic Experts Forum 2024 Conference** [3] which focuses on highlighting current best practices in digital forensics, the on-going CYCLOPES [4] practitioner workshops that dually identify practitioner needs and technology capabilities and gaps, with the next workshop focused on OSINT. Broader events also include the SPIE (Society of Photographic Instrumentation Engineers) conference on **AI for Security and Defence Applications II** [5] and **CINTiA 2024 ("Criminal Intelligence – New Trends in Analysis Conference 2024)** [6]. All of these events highlight a significant emphasis towards digital forensics and analytics.

[1] **Project CT-Tech**: https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech
[2] **First Report on Encryption**: https://www.europol.europa.eu/publications-events/publications/first-report-encryption
[3] **Forensic Experts Forum 2024 Conference**: https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference
[4] **CYCLOPES project**: https://www.cyclopes-project.eu/events/workshop-enhancing-digital-forensic-investigations-using-osint-cyber-intelligence
[5] **SPIE conference**: https://spie.org/ESI24D/conferencedetails/artificial-intelligence-security-defence
[6] **CINTiA 2024**: https://ppbw.pl/en/cintia-2024-we-are-opening-registration-for-companies/

13

September 2024 is packed with key FCT-relevant security events across Europe, offering a range of opportunities for networking, learning, and showcasing the latest innovations in the field.

Event	Location & Date	Description
SANS Brussels	2-7 Sept. 2024 Brussels, Belgium	At SANS, their mission remains steady. They continue to deliver relevant cyber security knowledge and skills, empowering students to protect people and their assets. Register for SANS Brussels September 2024 (2-7 September) and continue to build practical cyber security skills users can implement immediately.
Counter UAS Homeland Security Europe	9-10 Sept. 2024 London, UK	Drawing on knowledge gained from major Homeland Security experts from key UK, European and International security organisations, governments, military, police and industry, Counter UAS Homeland Security Europe 2024 conference will showcase the very latest technology in the market to ensure that civilians, domestic infrastructure, borders and all aspects of homeland security are protected from the criminal use of drones.
Public Security Exhibition	11 Sept. 2024 Brussels, Belgium	The PSE is co-organised by ADS and the British Embassy. This PSE will be focused on showcasing cutting-edge UK security capabilities to help meet current security challenges in Belgium. This event will be an excellent opportunity to network and build relationships in-country, as well as capitalise on the international setting of Brussels through G2G, EU and NATO engagements in the security and resilience sector.
Security Essen 2024	17-19 Sept. 2024 Essen, Germany	As the most important event and impulse-giving platform for innovations, contacts, and deals, security Essen attracts exhibitors and visitors from all over the world. The following topics will be presented: Special-purpose vehicles, civil protection and defence, special forces, video, perimeter protection, entrance/mechatronics, Fire/intrusions, Services, digital networking security.
BruCON Security Conference	19-20 Sept. 2024 Linter, Belgium	BruCON is an annual security and hacker conference providing two days of an interesting atmosphere for open discussions of critical infosec issues, privacy, information technology and its cultural/technical implications on society. Organised in Belgium, BruCON offers a high-quality line up of speakers, security challenges and interesting workshops. BruCON is a conference by and for the security and hacker community.
International Cyber Expo	24-25 Sept. 2024 London, UK	International Cyber Expo bursts with networking and business opportunities with a highly sophisticated visitor base.
International Security Expo	24-25 Sept. 2024 London, UK	International Security Expo will immerse visitors in a dynamic environment that is focused on protecting nations, critical infrastructure, and citizens.
Annual event on research for FCT	24-25 Sept. 2024 Brussels, Belgium	DG HOME is organising a two-day annual event with the aim of facilitating and stimulating the discussion and exchanges among security research practitioners, policy makers, researchers, civil society and industry on cross-cutting topics that have a broad and horizontal impact on research and innovation in this domain.

ENACT.
European Network Against Crime and Terrorism

@enact-network

enact-eu.net

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