D5.3 ENACT Annual Report v1

Lead Beneficiary	INOV
Dissemination Level	PUBLIC
Date	18/09/2024
Grant Agreement Number	101121152

Funded by
the European Union

Project Information

Grant Agreement Number	101121152
Acronym	ENACT
Name	European Network Against Crime and Terrorism
Call Topic	HORIZON-CL3-2022-SSRI-01-02 Knowledge Networks for Security Research & Innovation
Action Type	Coordination and Support Action
Start Date	01/09/2023
Duration	36 Months
Coordinator	PJ

Document Information

Work Package	WP5: Test implementation cycle
Deliverable	D5.3 ENACT Annual Report v1
Date	18/09/2024
Type	[REPORT]
Dissemination Level	[PUBLIC]
Lead Beneficiary	INOV
Main Author(s)	Inês Cunha (INOV); Sílvia Bogéa (INOV)
Contributors	André Alegria (PJ); Cyril Piotrowicz (FRMDLI); David Rios Morentin (VICOM); Dorothea Tsatsou (CERTH); Guillaume Brumter (EOS); Helen Gibson (CENTRIC); Isabela Rosal Santos (KUL); Marialuna De Tommaso (ENG); Peter van de Crommert (NP); Vincent Perez de Leon-Huet (EOS)
Document Reviewers	Helen Gibson (CENTRIC); Peter van de Crommert (NP)
Security Reviewer	Jarmo Puustinen (FIMOI); Rocío Carbayo (ESMIR); Patrick Hermans (NP)
Ethics Reviewer	Isabela Maria Rosal (KUL)

Revision History

Version	Date	Author	Comments
0.1	28/05/2024	Sílvia Bogéa (INOV); Inês Cunha (INOV)	ToC
0.2	05/07/202	Isabela Rosal Santos (KUL); Cyril Piotrowicz (FRMDLI)	ToC Revision
0.3	20/08/202	Inês Cunha (INOV); Sílvia Bogéa (INOV)	First Draft
0.4	30/08/202	André Alegria (PJ); Cyril Piotrowicz (FRMDLI); David Rios Morentin (VICOM); Dorothea Tsatsou (CERTH); Guillaume Brumter (EOS); Helen Gibson (CENTRIC); Isabela Rosal Santos (KUL); Marialuna De Tommaso (ENG); Peter van de Crommert (NP); Vincent Perez de Leon-Huet (EOS)	Contributions
0.5	10/09/2024	Inês Cunha (INOV); Sílvia Bogéa (INOV)	Final draft
0.6	12/09/2024	Helen Gibson (CENTRIC); Peter van de Crommert (NP)	Review
0.7	17/09/2024	Isabela Maria Rosal (KUL)	Ethical Review: accessibility, transparency, and non-discriminatory language aspects. Review mentions to ethical and legal aspects.
0.8	17/09/2024	Jarmo Puustinen (FIMOI); Rocío Carbayo (ESMIR); Patrick Hermans (NP)	Security Review: verify that no security-sensitive information is included in the document, ensure appropriate classification of the deliverable, and confirm that no security-relevant issues are present
1.0	18/09/2024	André Alegria (PJ)	Final
2.0	14/08/2025	Inês Cunha (INOV), Isabela Maria Rosal (KUL), André Alegria (PJ)	Updated in line with feedback from EAB and REA expert review.

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

Abbreviations

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
CDE	Communication, Dissemination and Exploitation
CERIS	Community for European Research and Innovation for Security
CINTiA	Criminal Intelligence – New Trends in Analysis
CSA	Coordination and Support Action
D	Deliverable
EC	European Commission
ELS	Ethical, Legal and Societal
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EU	European Union
EUCS	European Union Civil Security
EUDA	European Union Drugs Agency
FBI	Federal Bureau of Investigation
FCT	Fight against Crime and Terrorism
FP7	Seventh Framework Programme for Research and Technological Development
G2G	Government-to-Government
HES	Higher Education and School
H2020	Horizon 2020
IA	Innovation Action
ICT	Information and Communications Technology (ICT)
IOC	Inter-Observatory Coordinator
IOCTA	Internet Organised Crime Threat Assessment
IT	Information Technology
KER	Key Exploitable Results
KH	Knowledge Hub
KR	Knowledge Repository
KO	Knowledge Observatory
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
LLM	Large language model
MFS	Market, funding & standardisation
NATO	North Atlantic Treaty Organization
OSINT	Open-source Intelligence
OTH	Other (type of organisation)
PCP	Pre-Commercial Procurement

PNR	Passenger Name Record
PPE	Personal Protective Equipment
PRC	Private Company
PSE	Public Security Exhibition
PUB	Public Body
R&I	Research and Innovation
REC	Research Centre
RIA	Research and Innovation Action
RTO	Research and Technology Organisation
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*
WP	Work Package
UAS	Unmanned Aerial Systems
UAV	Unmanned flight vehicle
UK	United Kingdom
URL	Uniform Resource Locator

List of Figures

List of Tables

Table of Contents

Executive Summary

ENACT is a knowledge network dedicated to fighting crime and terrorism (FCT), with the mission to collect, aggregate, process, and disseminate valuable insights in the FCT domain. The ENACT network is built upon four key pillars: Networking, Research, Communication, Dissemination and Exploration (CDE), and Cooperation. In its first year, ENACT established and tested the strategies, methods, tools, and processes essential to each of these pillars, ensuring the effective operation of the Knowledge Network.

ENACT has implemented an Observatory system to extract, classify, and visualise information from the community through Knowledge Hubs (KHs), ultimately providing valuable feedback to stakeholders. The Observatory system consists of four main Knowledge Observatories (KOs), which cover the following domains of interest: i) Capabilities; ii) Technology; iii) Market, funding & standardisation (MFS); iv) Ethical, Legal & Societal (ELS). In addition to these four knowledge areas, a fifth observatory, the Inter-Observatory Coordinator (IOC), merges the knowledge delivered by the other Observatories and presents it as a comprehensive FCT research and innovation (R&I) knowledge picture.

The first ENACT Annual Report marks the project's inaugural year, sharing disclosable information about its network's activities and outcomes. This report highlights the ENACT products created to facilitate the exchange of knowledge and value across the broader FCT community. It is at the disposal of the stakeholders for their evaluation and use for decision making. One of these products, the Stakeholder Map (key exploitable result KER1), connects ENACT with major, pre-existing European Union (EU) FCT R&IKHs and organisations pivotal to the FCT community. In the first version of the Stakeholder Map, ENACT identified and registered 1013 stakeholders, primarily from Europe, representing various communities within the FCT ecosystem. This number is expected to grow substantially as the project progresses, driven by systematic identification and monitoring efforts, as well as active engagement in key events, particularly those focused on technology and security sectors.

ENACT also successfully created a comprehensive Periodic FCT map (KER2), which consolidates data from all four observatories, providing a comprehensive summary of the information collected over six months by the observatories. The FCT map compiles a total of 671 observations drawn from a wide array of sources and covering the period from 2014 onwards, aligning with major developments in the EU’s FCT R&I landscape and enabling the observatories to capture key trends, priorities, and challenges relevant to FCT policy and practice. Additionally, ENACT produced two Flash Knowledge Reports (KER3), which provide quick, on-demand insights focused on specific drivers such as policies, threats, functions, or technologies, and one Analytical Reports (KER4) prepared by the Consortium, offering detailed examinations of specific topics. Currently, ENACT is finalising three more flash reports and the Annual State-of-Play (SoP) FCT Policy Report (KER5), with a concise overview of recent developments, insights, and recommendations from various ENACT activities. These outputs are set to be presented at the ENACT Annual Event 2024, which will be held in Lisbon on September 20th.

The evaluation by the FCT community reflects positively on the ENACT products, with feedback highlighting the effectiveness and relevance of these efforts. After this first version, the subsequent ENACT Annual Reports will be presented yearly. ENACT outcomes will be

adapted based on the feedback received to maximise their relevance and contributions to the FCT community.

1 Introduction

1.1 ENACT Concept and Approach

Knowledge is one of the most strategic assets available to the European Union. 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, through 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 its 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 European Union.

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 – European Network Against Crime and Terrorism – 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 a platform for sharing insights, identifying gaps, validating solutions, and aligning research and innovation with real operational needs, serving as both a knowledge hub and a bridge between research and practice.

1.2 Purpose of this Deliverable and links with other Deliverables

ENACT is a knowledge network, funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society, focused on the FCT. The project aims to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area, targeting two major ambitions:

- Provide evidence-based support to the decision-makers in the EU R&I ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the FCT.

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

Considering these ambitions, ENACT follows a multidimensional approach in the delivery of the Knowledge Network services, by the means of four main pillars: i) Networking; ii) Research; iii) CCDE; and iv) Cooperation. The ENACT project laid the groundwork for its network implementation set-up, defining the project's overall direction and key components while formulating the methodology and strategic approach to achieve ENACT's objectives.

In brief, ENACT's Research pillar has four observatories, each led by a partner with expertise in the observatory's focus. These observatories systematically gather and integrate information into a Knowledge Repository (KR) that aligns with the EU Civil Security (EUCS) taxonomy (see **Appendix A**). A fifth observatory, the IOC is responsible for merging the knowledge delivered from the other four observatories and coordinate the production of a common FCT R&I knowledge picture, the ENACT Products, establishing an observatory system. The ENACT Consortium regularly compiles FCT capability, technology, market, ELS maps (**KER2**) every six months. Additionally, they promptly produce flash knowledge reports (**KER3**), in response to specific inquiries from the European Commission (EC), Member States, Community for European Research and Innovation for Security (CERIS), EU agencies, academia, and industry. These reports are prepared internally by ENACT and contribute to their knowledge base. Moreover, advanced research reports (**KER4**) are prepared by hired external experts to address emerging and critical topics relevant to the FCT R&I community. The compilation and analysis of this information are supported by ENACT's Networking activities. Partners are represented in the main FCT R&I community KHs identified on an ongoing Stakeholders Map (**KER1**). Utilising the insights from both Research and Networking pillars, ENACT provides tailored information and actionable recommendations every six months, to be documented in an annual FCT SoP policy report (**KER5**), which is a sensitive document with restricted access, primarily for the EC.

As a result of these efforts, the main insights of these products are reported in the present **ENACT Annual Report 2024**, which captures the first batch of network outputs across the four Pillars, compiling all findings, outcomes, and recommendations.

1.3 Intended audience

This deliverable 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. It is also aimed at ENACT consortium partners, particularly the Work Package Leaders of WP6 and WP7, as it will serve as a tool to support the tasks to be carried out during the implementation cycles.

2 ENACT Products

Following the strategy, methodology, processes and tools developed and refined by the project, ENACT partners focused on systematically collecting, characterising and validating observations and mapping stakeholders for the preparation of several ENACT products. To ensure the timely and high-quality preparation of ENACT products, we relied on a rich and varied dataset for analysis and interpretation, that encompasses all observatories. The ENACT product's workflow was designed to efficiently address requests from external FCT entities and proposals from the Consortium.

During the first year of the project, considering the data acquired, classified and stored in the ENACT Structured Knowledge Base (SKB), we successfully produced insightful outcomes, which includes the preparation of a FCT R&I stakeholders map (**KER1**), an FCT map covering the four observatories (**KER2**), two flash reports (**KER3**), and an analytical report prepared by the Consortium (**KER4**). Currently, three additional flash reports and the annual SoP FCT Policy Report (**KER5**) are in progress and are planned to be completed by early-September, ahead of the **ENACT Annual Event 2024**[1] planned to take place in Lisbon on September 20th.

The upcoming sections detail the work done for the creation of each ENACT product, as well as the main results obtained.

2.1 FCT R&I Stakeholders Map (KER1)

The strategy defined for the Networking pillar focused on the identification and interaction with key stakeholders relevant to the project. This involved identifying and mapping key formal groups, entities, and organisations representing various communities of interest within the FCT ecosystem, with special focus on the most relevant KHs, engaging and interacting regularly with these groups, and keep updating and growing the **Stakeholders Map (KER1)**. In terms of mapping relevant stakeholders, while in the first six months the goal was to establish a register of players with whom ENACT should directly interface with, in the following six months this strategy was extended to incorporate a complete view of the FCT R&I ecosystem, encompassing every entity that has some kind of involvement in the development of security solutions and applications.

Regarding the liaising with relevant KH's and other important stakeholders, the strategy set up by ENACT was largely followed, ensuring ENACT could create the needed relationships with the community. These relationships were promoted across all types of stakeholders, from the end-user community to the academia, research and technology organisations (RTOs) and other EU projects, with a twofold purpose: collecting the needs and views of external parties to enable an unbiased analysis of the ecosystem and making sure that the work performed by ENACT is outward-looking and serving the community needs.

As shown in the **Figure 1**, ENACT has registered a total of 1013 stakeholders in the current version of the Stakeholders Directory, distributed across 52 countries worldwide, with 113 of them having unidentified geographical location. Of the total stakeholders, 819 are participating in EU projects funded by FCT calls between 2014 and 2022, with 68 of them serving as project coordinators. The majority of stakeholders were identified from the **EU Funding & Tenders**

[1] **ENACT Annual Event 2024:** https://enact-eu.net/enact-annual-event-2024/

Portal[2] using the “partner search” feature, designed to help organisations and individuals find and connect with potential partners for collaborative projects funded by the EU. This tool was refined to filter partners participating in EU projects from FCT calls between 2014 and 2022, either as beneficiaries or coordinators. Additional stakeholders were identified through monitoring key events within the FCT sector, including the SICUR (*Salón Internacional de la Seguridad*) and TECNOSEC (*Altas Tecnologías de Seguridad e Inteligencia, Drones y Antidrones*) & DRONExpo exhibitions. Recognising these events as highly significant for the FCT community, ENACT prepared two concise flash reports covering the main topics addressed, exhibitors, conferences, demonstrations, and other relevant details (see **KER3**). As such, the systematic identification, monitoring, and active participation in relevant events are essential for continually expanding the stakeholders' network and enhancing engagement within the FCT community, particularly in technology and security sectors.

Europe represents the largest share, encompassing a total of 855 stakeholders from 38 countries, of which 789 are actively involved in EU-funded projects, with 67 of them serving as coordinator's representatives. In contrast, Asia follows with 22 stakeholders across 6 countries, and 17 of these are engaged in FCT projects, including one as a coordinator. North America contributes with 11 stakeholders from two countries, while South America comprises 9 stakeholders from four countries with, all participating in EU FCT projects but none serving in coordination roles, and Africa and Oceania are represented by only three stakeholders combined.

This disparity of geographical distribution can be attributed to the sources used for mapping FCT stakeholders. Since Horizon Europe and its predecessors primarily target challenges faced by EU member states and associated countries, the specific focus on crime and terrorism tends to align more with issues that are pressing in Europe. Furthermore, engaging in Horizon Europe projects often necessitates substantial collaboration with EU entities, which can present significant challenges for organisations outside the EU in establishing these partnerships.

[2] **EU Funding & Tenders Portal:** https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home

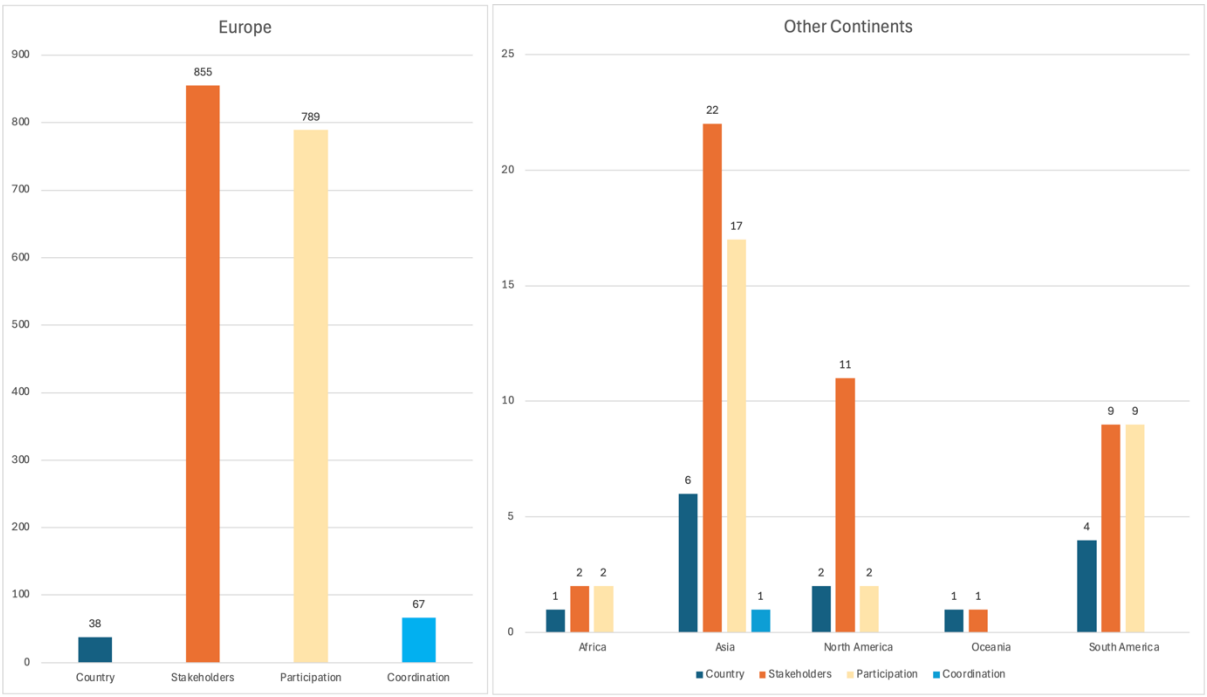


Figure 1 – Stakeholder count distribution by continent, EU FCT project participation, and coordination roles.

The ENACT stakeholders' distribution reveals a diverse range of organisational types, each contributing to the ENACT's objectives (see **Figure 2**). The largest group is represented by Private Companies (PRC), with 497 stakeholders involved, and Higher Education and Schools (HES) form the second-largest group, with 189 stakeholders referring to educational institutions such as universities and schools participating in or benefiting from the project. A total of 156 stakeholders are represented by Public Bodies (PUB), reflecting the importance of government and public sector involvement in ensuring the project aligns with public policy and societal needs. Research Centres (REC), often specialised research centres that offer focused expertise in specific areas relevant to the project, contribute with 92 stakeholders, and a catch-all category that includes any other types of organisations or entities (Other - OTH) that do not fit into the above categories but are involved in the project.

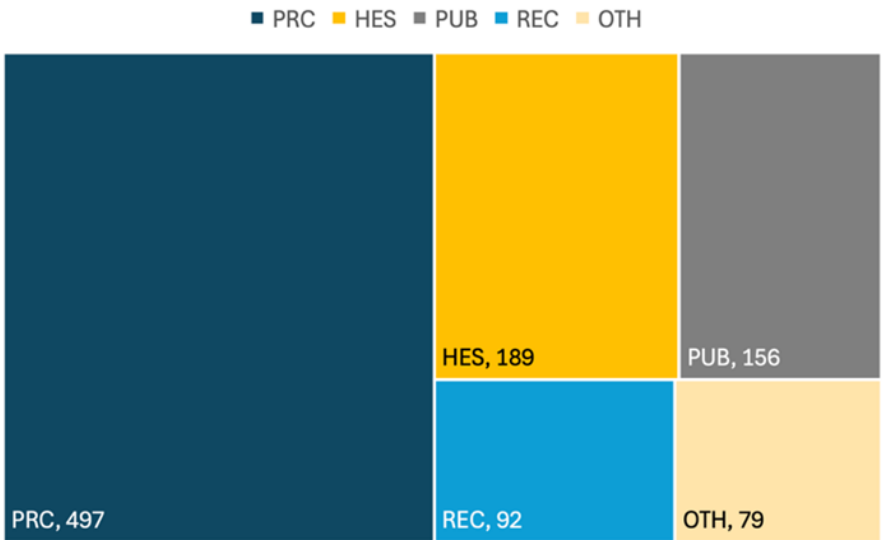


Figure 2 - Stakeholder count distribution per organisation type.

One key added value of the mapping carried out under the Stakeholders Directory has been their categorisation and classification according to the EUCS Taxonomy. This categorisation will facilitate (once the Stakeholder Directory is fully operational and interactive) the identification of stakeholders with expertise in specific taxonomy areas. The categorisation of the stakeholders who have participated in EU-funded FCT R&I projects has been done using as a basis the categorisation of the FCT topics of the last 10 years presented in the first ENACT Analytical Report. The categorisation of the stakeholders identified in fairs and exhibitions (SICUR and TECNOSEC) has been done manually by enact experts.

Considering the EUCS taxonomy (see **Section 2.5.5**), ENACT stakeholders' interest areas significantly focus on various aspects of crime and security. Among these interest areas, **cybercrime** stands out for its relevance to the FCT policy domain, followed by **horizontal and societal issues**, **terrorism and radicalisation**, and **organised crime** (see **Figure 3**).

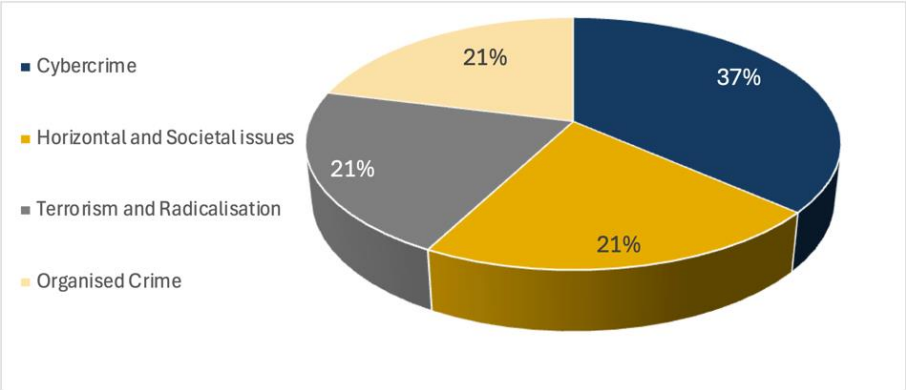


Figure 3 – Mapping of stakeholder's interest areas in the Policy domain, according to the EUCS taxonomy.

Within the Cybercrime policy domain, a detailed breakdown reveals specific sub-areas of interest (as shown in **Figure 4**). The most representative sub-area is the **dark net (illegal markets/cryptocurrencies)**, attracting 602 stakeholders, indicating a substantial concern around this topic. **Digital forensics** also commands significant attention, with 300 stakeholders engaged in this area, highlighting its importance in the cybercrime landscape. Child sexual abuse is another critical area, with 279 stakeholders focusing on this issue. Other areas of interest include **other forms of cybercrime** (364 stakeholders), **non-cash payment fraud** (98 stakeholders), **encryption and 5G** (61 stakeholders), **attacks against information systems** (42 stakeholders), and **online identity theft** (23 stakeholders).

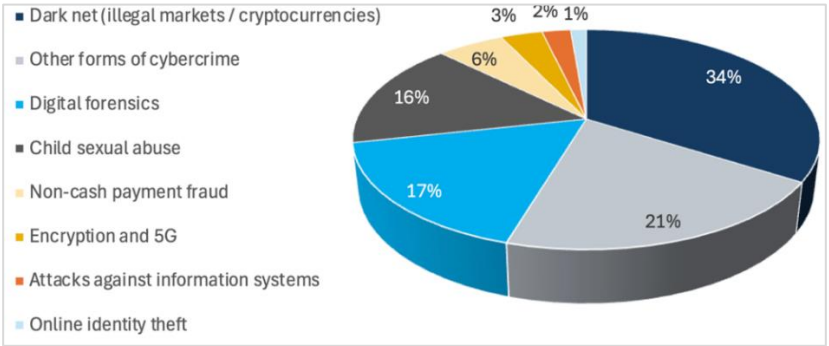


Figure 4 - Mapping of stakeholder's interest areas in the Cybercrime Policy sub-level domain, according to the EUCS Taxonomy.

Within the functional areas domain, a significant stakeholder number is interested in the **investigation and forensics** (F10), followed by **data, information & intelligence gathering management** (F02). The functional area of **training and exercises** (F13) shows considerably lower interest than the other two, suggesting that stakeholders might prioritise operational and analytical capabilities over other functional areas (see **Figure 5**).

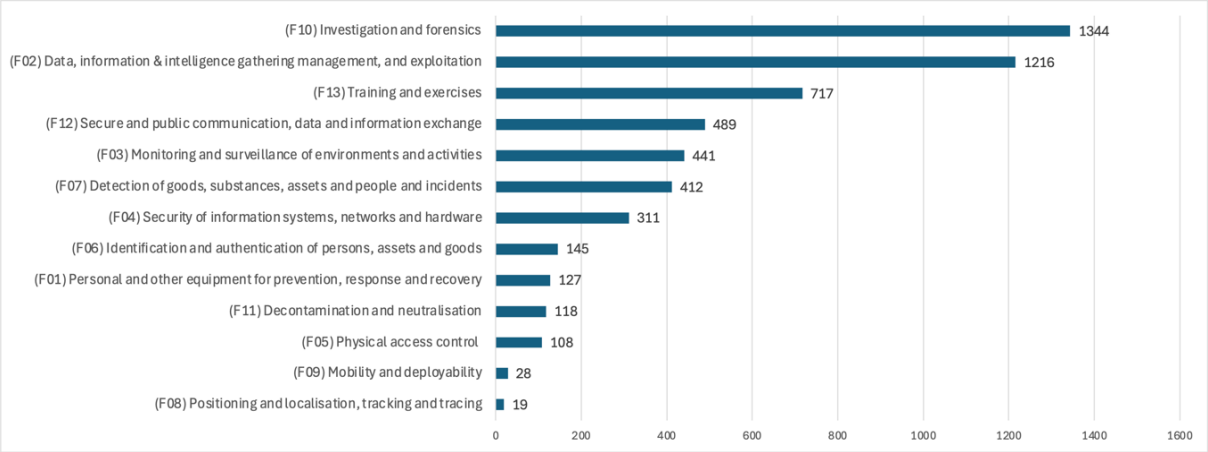


Figure 5 - Mapping of stakeholder's interest areas in the functional areas domain, according to the EUCS taxonomy.

The EUCS Taxonomy products and services are identified in the first level by a total of 23 technology areas. **Internet-based investigation** is of the highest interest to the stakeholders, indicating a strong focus on technologies that support online data gathering and analysis, followed by **data analytics**, emphasising the importance of processing and analysing data to derive insights, likely due to the increasing volume and complexity of data in security contexts. **General equipment**, **critical and interoperable communications**, **data storage and exchange**, and **digital forensics** technology areas are still significant, indicating essential operational needs (see **Figure 6**).

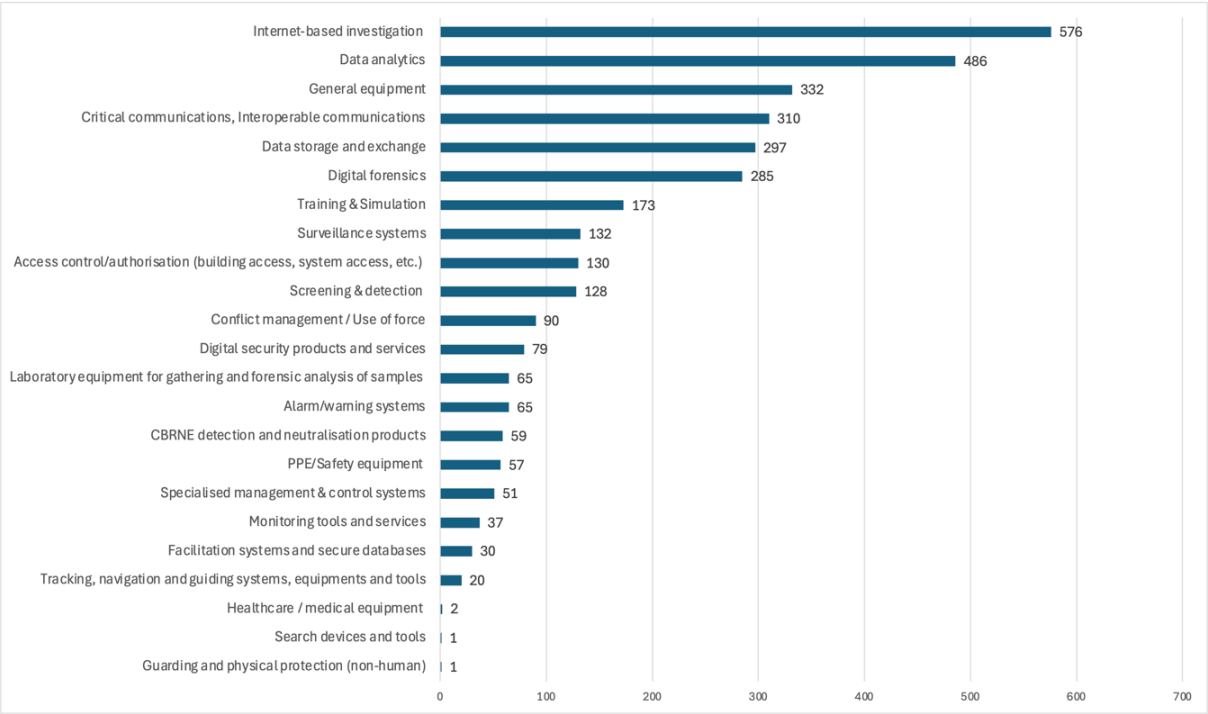


Figure 6 - Mapping of stakeholder's interest areas in the technology areas domain, according to the EUCS taxonomy

2.2 Periodic FCT Capability, Technology, Market, ELS Maps (KER2)

ENACT partners have routinely extracted relevant and diverse data on targeted topics of interest identified and prioritised during the last six months. Most observations cover the period from 2014 onward, capturing a pivotal phase in the EU's R&I efforts in the FCT domain, which aligns with key developments under Horizon 2020 and Horizon Europe Cluster 3, when major policies, funding decisions, and research priorities were established. Both data sources and collected data were systematically analysed and characterised according to EUCS taxonomy and SKB "vocabulary". A protocol was developed using Artificial Intelligence (AI) as tool for assisting in a part of the data characterisation according to the observatory relevance and EUCS taxonomy to ensure consistency and reliability in data processing. Finally, data was meticulously verified and validated by Knowledge Observatory (KO) leaders, ensuring its accuracy, consistency, and reliability, and eliminating any errors or inconsistencies, and finally compiled in the SKB for easy access and later use for preparation of ENACT products.

The **periodic FCT maps (KER2)** were prepared by KO leaders, which consists of a compilation of detailed statistical analysis, time evolution data, and key highlights of validated data classified as highly relevant for the Observatory they are overseeing. The prepared periodic FCT maps (KER2) provides a comprehensive summary of all the information collected by the observatories from March to July 2024 on FCT-relevant security threats, police functions and policy, product/services, ongoing research and scientific breakthroughs, on funding, procurement and standardisation opportunities and on ELS issues.

Overall, the ENACT Research Pillar successfully aggregated data from a diverse range of sources (201 data sources), with a total of 671 observations, highlighting a rich and varied dataset. As shown in **Figure 7,** the observations show a varied distribution across different observatories. Each observation is assigned to a single observatory with the high-relevance (other observatories can be selected, but they will be considered as secondary options with less relevance). The distribution shows a concentration of highly relevant observations in the Capability Observatory and Technology Observatory categories, while the ELS Observatory has a significant but lesser concentration, and the Market, Funding & Standardisation Observatory has the smallest share, accounting for only 9% of the total observations.

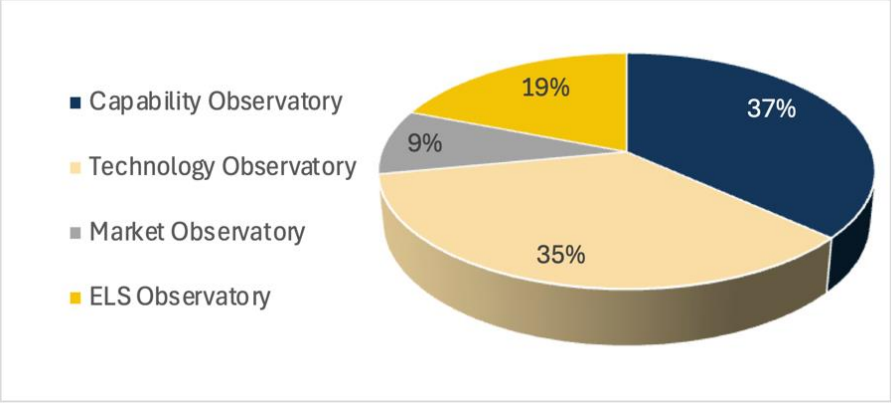


Figure 7 - Percentage distribution of observations by observatory relevance.

As presented in **Figure 8**, the collected data includes project results, practitioner reports, public databases, policy papers and updates, news and media, scientific literature, and consultation results from identified primary sources. Among these, the distribution strongly emphasises **project results** (167 observations), followed by **news and media** coverage (137 observations), and **scientific materials** (113 observations). **Policy papers** are also well-represented with 110 observations, and **practitioner reports** contribute 71 observations. In contrast, **consultation results** are notably less represented, with only three observations.

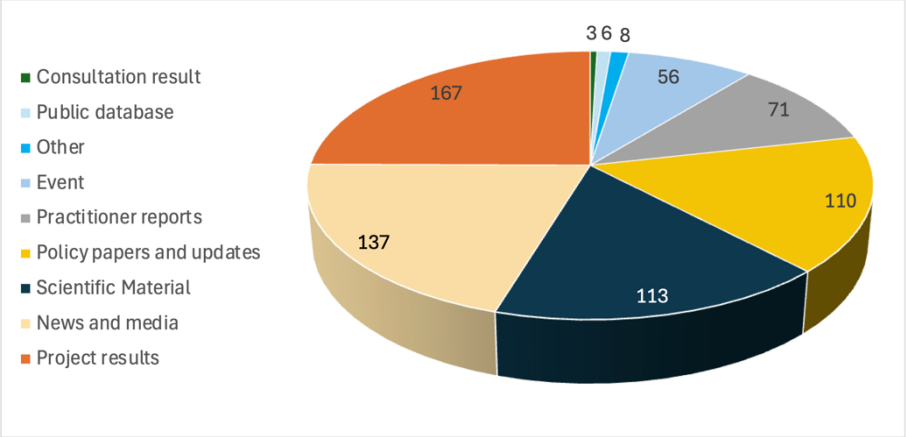


Figure 8 – Distribution of observations by category.

Following this, we explore the classification of observations using the EUCS taxonomy within FCT classification, depicted through a tree-map that visually represents the project's observations providing a comprehensive overview focusing on various crime and security aspects (**Figure 9**). The tree-map is organised into the four categories from the Level 2 EUCS Taxonomy policy domain: i) organised crime, ii) cybersecurity, iii) terrorism and radicalisation, and iv) horizontal and societal Issues. This visualisation effectively demonstrates the distribution of observations at Level 3 within policy domain. **Cybercrime** accounts for 30% of the total observations. It stands out as a dominant area, representing the highest percentage in Technology Observatory at 27%, Market Observatory at 39%, and ELS Observatory at 30% of the high relevance level observations. In the Capability Observatory, **cybercrime** accounts for 30% of the high relevance level observations, representing the second percentage, and **organised crime**, with 38%, is a dominant area in this Observatory.

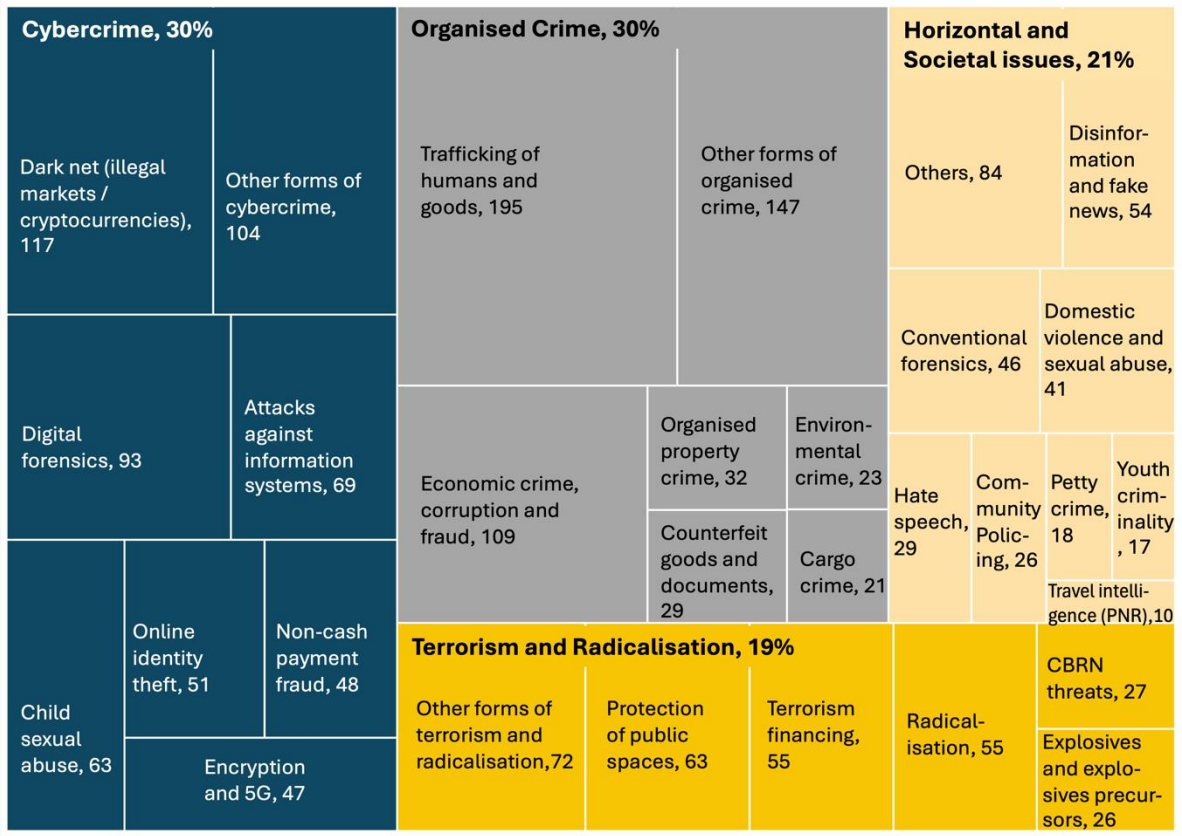


Figure 9 – Distribution of Observations per element of the EUCS Taxonomy Policy Level for FCT.

Subsequently, the data is further analysed through horizontal bar charts, which detail observations categorised by EUCS Taxonomy functional (**Figure 10**) and technological areas (**Figure 11**) within the ENACT general view. The analysis shows that the **investigation and forensics** (F10) and **data, information & intelligence gathering, management, and exploitation** (F02) functional areas are the most frequently observed and significant in terms of activity and focus within the project. In contrast, the **decontamination and neutralisation** (F11) functional area has fewer observations, indicating lower engagement or priority in this domain.

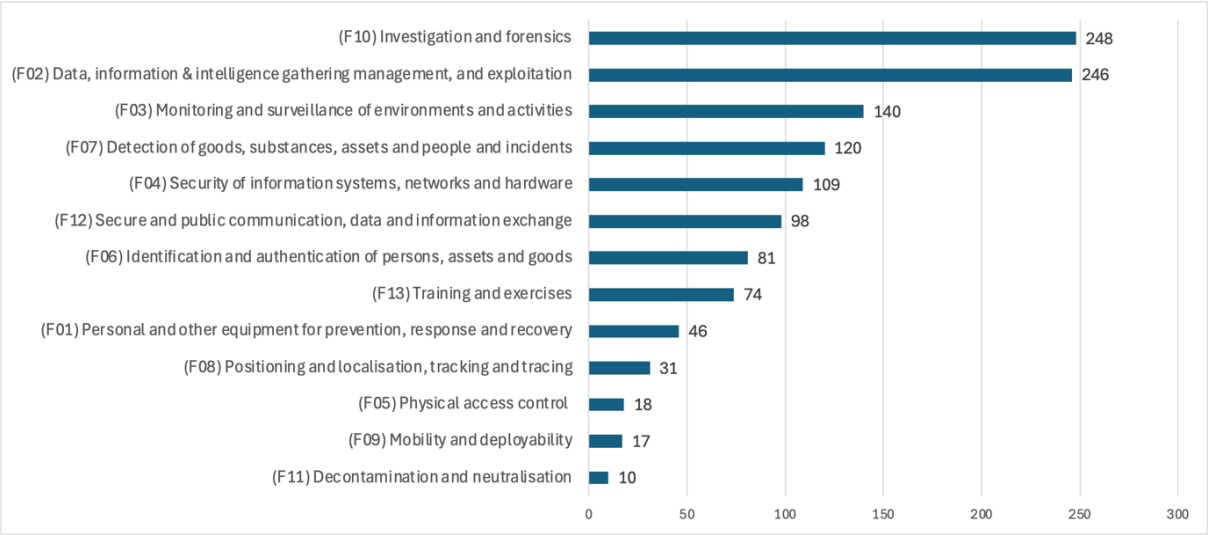


Figure 10 - Mapping of Observations in the functional areas domain, according to the EUCS taxonomy.

Regarding technological areas, **data analytics, Internet-based investigation**, and **digital forensics** are the most prominent. These areas are central to the ENACT's technological strategies and operations, strongly emphasising digital techniques and capabilities. On the other hand, **healthcare/medical equipment** is the least represented technological area, suggesting a more limited role or specific niche application within ENACT's scope.

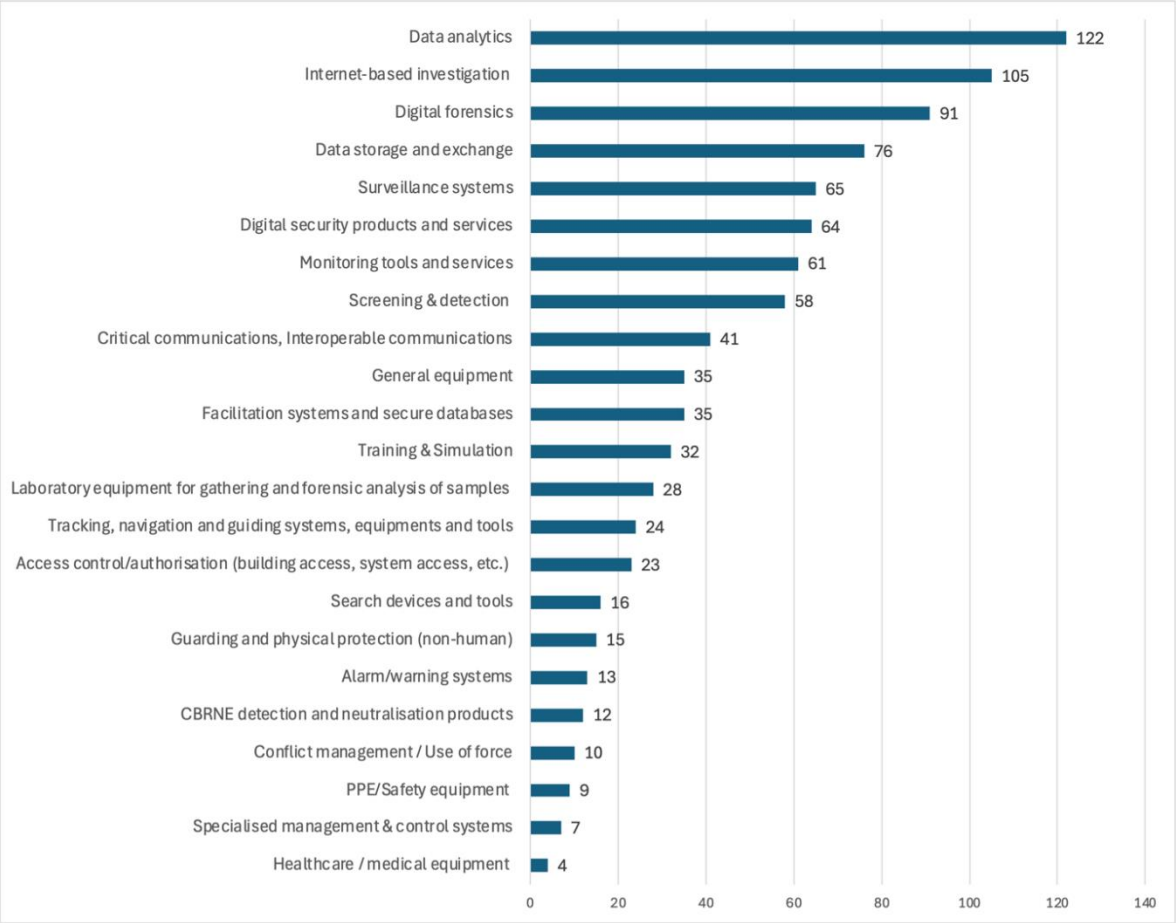


Figure 11 - Mapping of Observations in the technology areas domain, according to the EUCS taxonomy.

In the following sections, we expand on these findings for each observatory, examining their specific focus areas in greater detail.

2.2.1 FCT Capability map

The Capability Observatory is a resource hub managed by ENACT partners, dedicated to monitoring and analysis FCT security threats, police functions, and policy developments. This observatory aims to improve stakeholder effectiveness and efficiency, and to inform policy decision-makers by evaluating current technologies, operational strategies, and ongoing research. To achieve this, the observatory has identified 246 high-relevance observations out of a total of 671 observations related to its focus areas, creating a dynamic and current overview of key trends and issues in FCT threats, policies, and functions. Most of these observations (almost 90%) correspond to news and media, scientific material, practitioner reports, and policy papers and updates (see **Figure 12**).

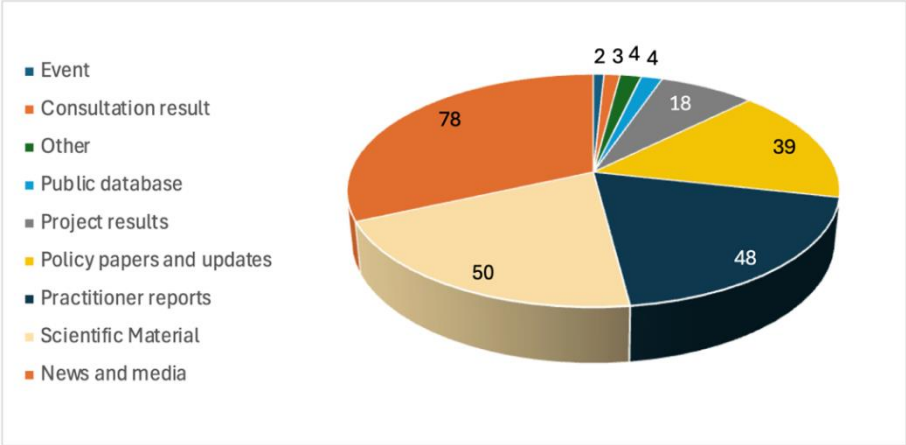


Figure 12 - Distribution of observations highly relevant for the Capability Observatory by category.

Considering the policy domain within EUCS Taxonomy for FCT, **organised crime** stands out with 38% as a domain area of interest, followed by **cybercrime** (31%), **horizontal and societal issues** (17%), and **terrorism and radicalisation** (14%), as shown in **Figure 13**. Within organised crime, **trafficking of humans and goods** is the most represented policy for the Capability Observatory, while in the area of cybercrime, the spotlight falls on **dark net (illegal markets / cryptocurrencies)**.

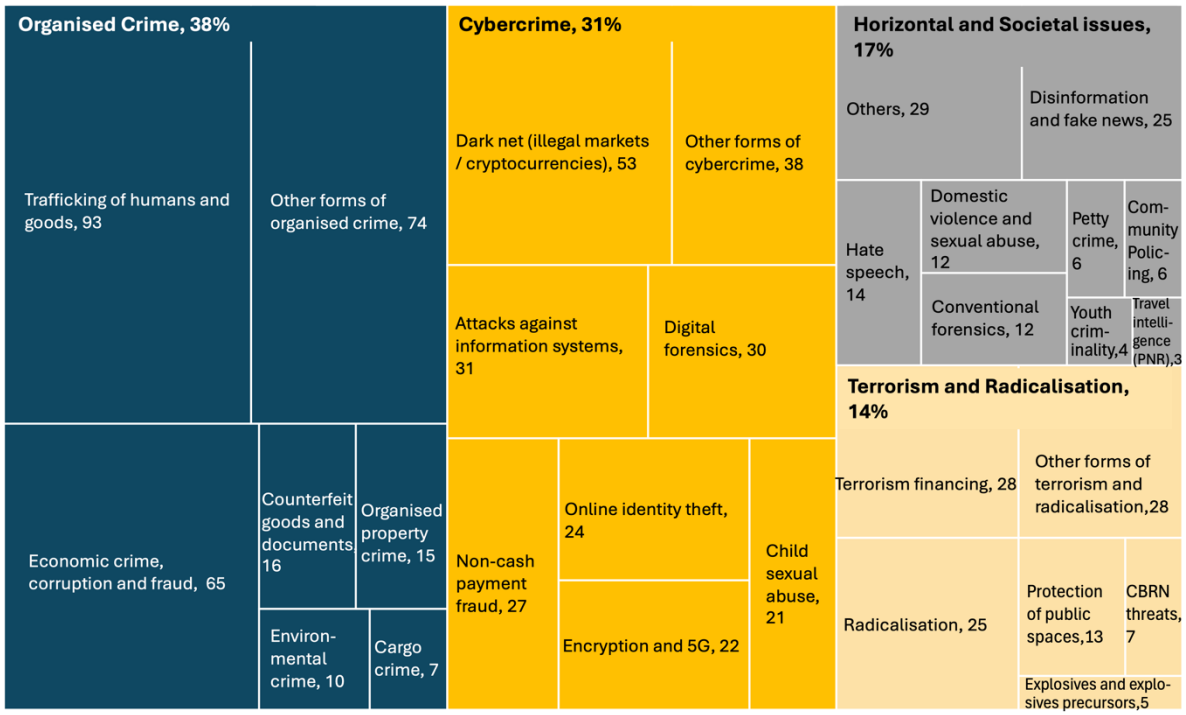


Figure 13 - Distribution of observations with high-relevance for Capability Observatory by EUCS Taxonomy policy domain applied to FCT.

For the functions dimension, the top-3 functional areas are **investigation and forensics** (F10), **data, information & intelligence gathering management, and exploitation** (F02), and **monitoring and surveillance of environments and activities** (F03), while the least represented is (F09) **mobility and deployability** with only one observation (see **Figure 14**).

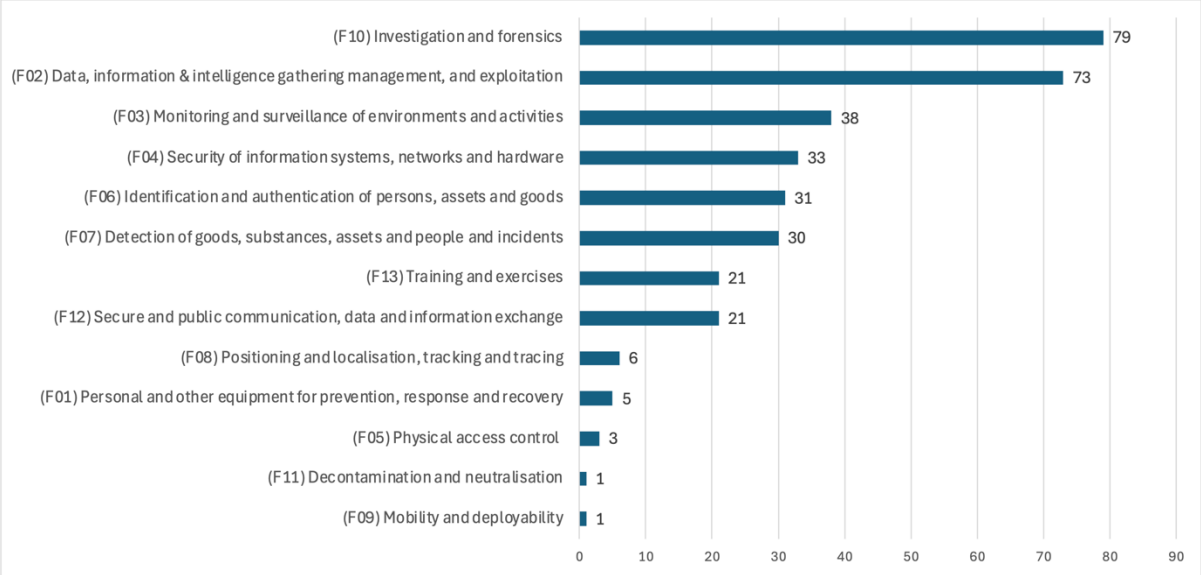


Figure 14 - Distribution of observations with high-relevance for Capability Observatory by EUCS Taxonomy functions dimension applied to FCT.

Data analytics, **internet-based investigations**, and **digital forensics** are the most common areas within the Technology Areas dimension of the EUCS Taxonomy FCT classification (see **Figure 15**).

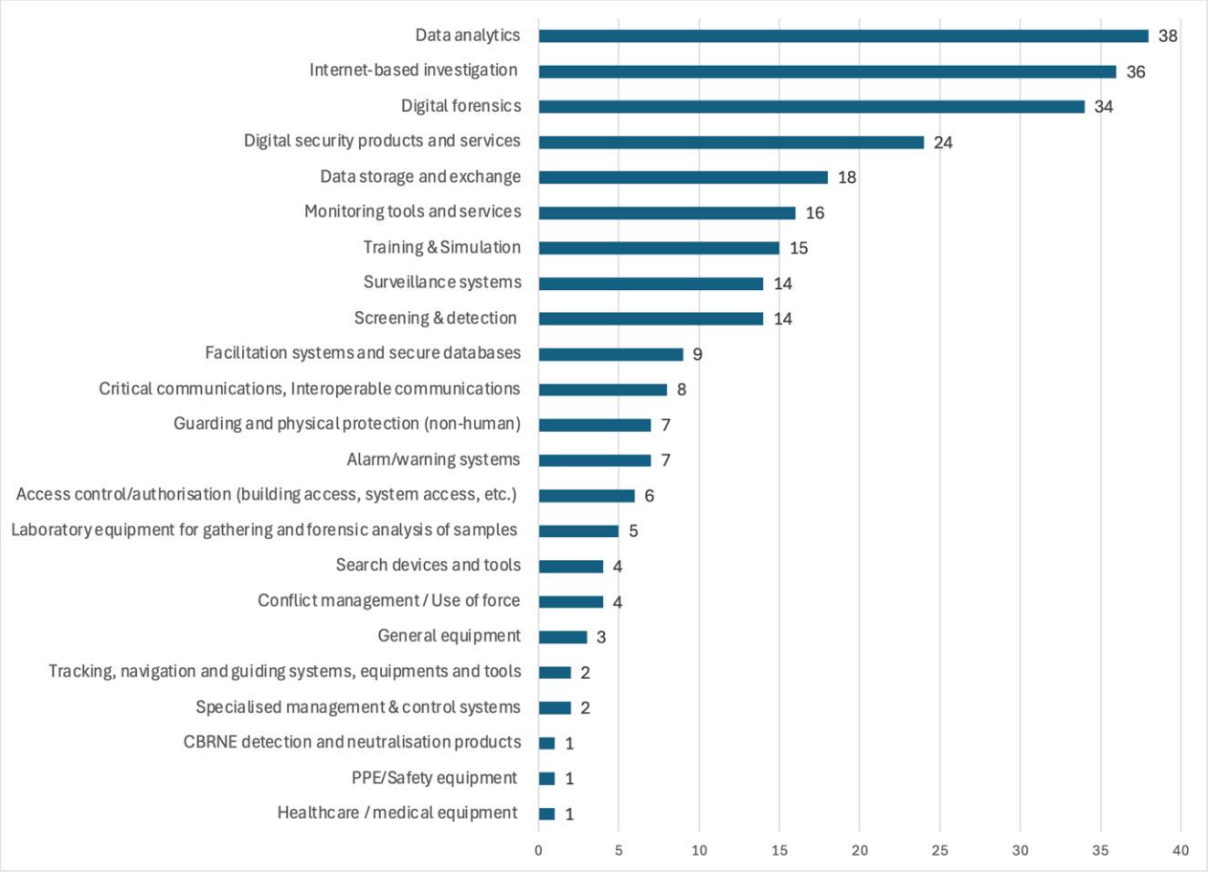


Figure 15 - Distribution of observations with high-relevance for Capability Observatory by EUCS Taxonomy technology areas dimension applied to FCT.

The main trends in news, technologies and science from the Capability Observatory perspective are presented in **Table 1**.

Table 1 – The main trending news, technologies and science from the Capability Observatory.

Trending News in the Capability Perspective:
• News and media observations follow the same general trend of capabilities observations, **with organised crime** and **cybercrime** being the ones under most focus. Under these policy areas, **trafficking of humans and goods** and **economic crime, corruption and fraud** when it comes to organised crime, while **darknet (illegal markets/ cryptocurrencies)** and **digital forensics** are the most addressed topics under the cybercrime policy area.
• Almost a third of news regarding economic crime also address **terrorism financing**, showing a clear link between the organised crime and terrorism and radicalisation policy areas.
• 80% of **darknet (illegal markets/ cryptocurrencies)** news observations also relate to economic crime, corruption and fraud, a clear demonstration on how organised crime groups is leveraging new technologies for their illegal activities.
• **Disinformation and fake news** are the most discussed topic under Horizontal Issues, with most new pieces addressing the risks of how disinformation campaigns can have a big political impact, particularly during elections.
• On **darknet**, particularly related to financial crimes, the main technological trends are on the use of cryptocurrencies and phishing attacks[3].
• Technologies addressed in **disinformation and fake news** are mainly the use of deepfakes and the mass distribution of propaganda through social media channels[4].
Trending Tech in the Capability Perspective
• **Data, information & intelligence gathering management, and exploitation** make up for a third of the observations related to technologies. On the functions side, **data analytics** and **internet-based Investigations** are the topics that generated the most observations from news (22% and 11%, respectively).
• **Data, information & intelligence gathering management, and exploitation** is a transversal technology area, addressing in a balanced way the policy areas of **trafficking of humans and goods, economic crime, corruption and fraud**, **darknet** and **disinformation and fake news**.
• Due to the increasingly prevalence of a digital footprint in emerging threats, tools that help law enforcement agencies (LEAs) conduct digital investigations and implementing prevention mechanisms efficiently, are becoming a priority[5].
Trending Sciences in the Capability Perspective
• On the scientific aspects, the trend remains the same, with the policy areas of **trafficking of humans and goods** and **economic crime, corruption and fraud** when it comes to organised crime, **darknet (illegal markets/ cryptocurrencies)** under the cybercrime policy area, and **disinformation and fake news** on horizontal issues policy area. However, on the terrorism focus, the phenomena of **radicalisation** is the one under most focus, instead of financing of terrorism.
• Around one third of the scientific studies and practitioners' reports address the topic of investigation and forensics. This is also true for Functions, with **digital forensics** and **internet-based investigations** taking the top spot (15% each).
• New investigation techniques are being studied and developed rapidly, due to the increasing digital footprint of crimes and also leveraging the use of AI[6].

2.2.2 FCT Technology map

The Technology Observatory monitors products, services, ongoing research, and scientific breakthroughs to enhance operational effectiveness and efficiency for stakeholders across various KHs. Out of 671 observations, 35% are of "High-relevance" for Technology

[3] ¿Qué sectores sufrieron más ataques de phising en 2023? - CyberSecurity News
[4] Disinformation campaigns likely to undermine EU elections, experts say – Euractiv
[5] New network to target migrant smugglers in the digital domain | Europol (europa.eu)
[6] Digital forensics and strong AI: A structured literature review - ScienceDirect

Observatory. Of these 35%, 83% originate from scientific material, project results, and news and media sources (see **Figure 16**).

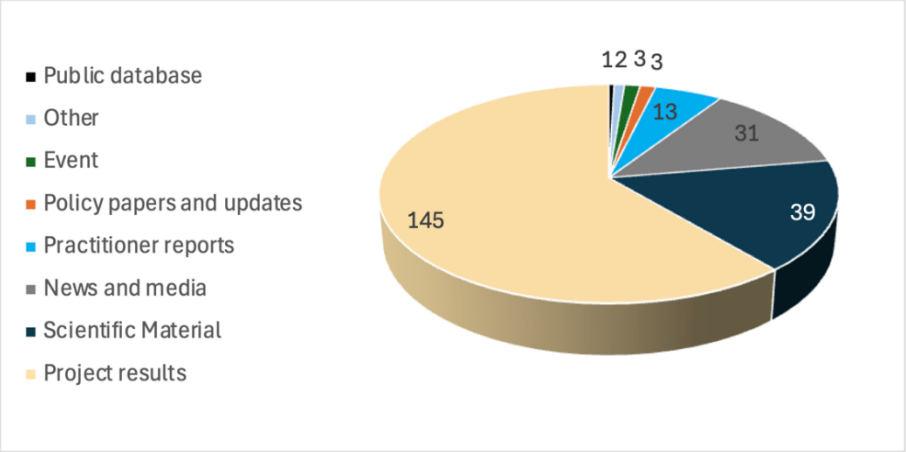


Figure 16 - Distribution of observations highly relevant for the Technology Observatory by category.

Within the Policy dimension of the EUCS Taxonomy FCT classification, 31% of all high-relevance observations for the Technology Observatory pertain mainly to **organised crime** topics, followed by **cybercrime** (27%) (see details in **Figure 17**).

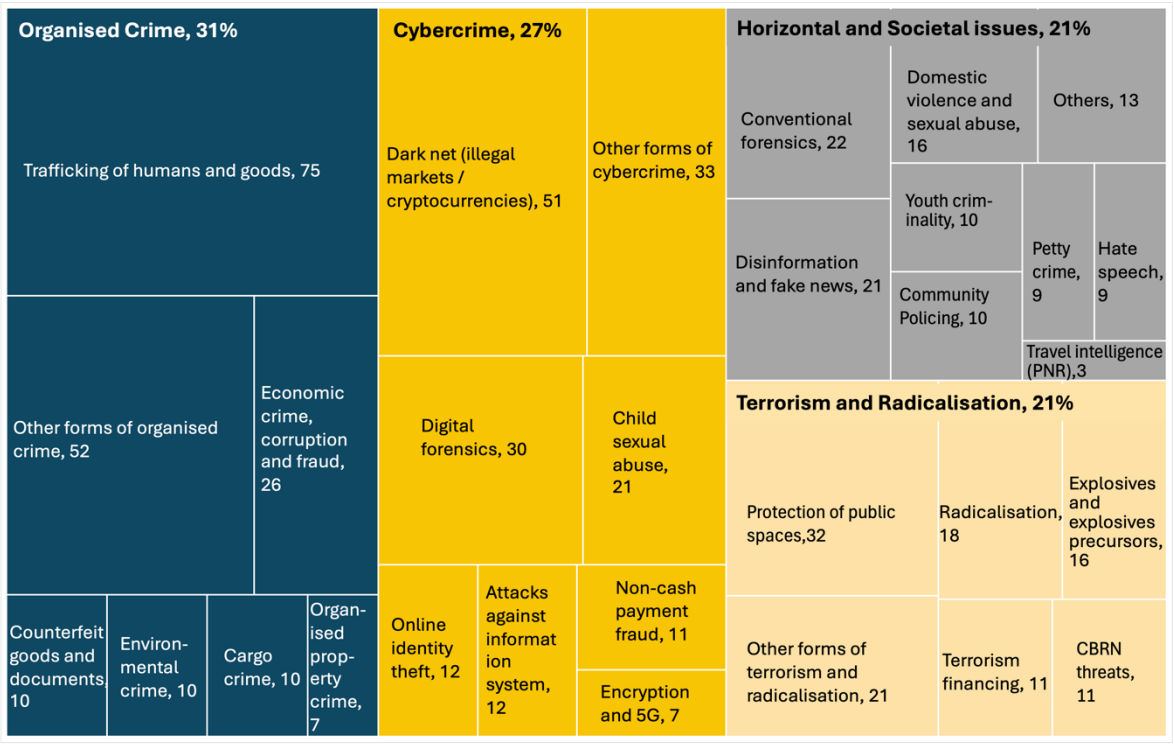


Figure 17 - Distribution of observations with high-relevance for Technology Observatory by EUCS Taxonomy policy domain applied to FCT.

In terms of the EUCS Taxonomy FCT classification, particularly within the Functions dimension, the most prominent areas are **investigation and forensics** (F10), with 125 occurrences; **data, information & intelligence gathering, management, and exploitation** (F02), with 112 occurrences; and **detection of goods, substances, assets, people, and**

incidents (F07), with 67 occurrences. **Mobility and deployability** (F09), with only six occurrences, was the least represented (see **Figure 18**).

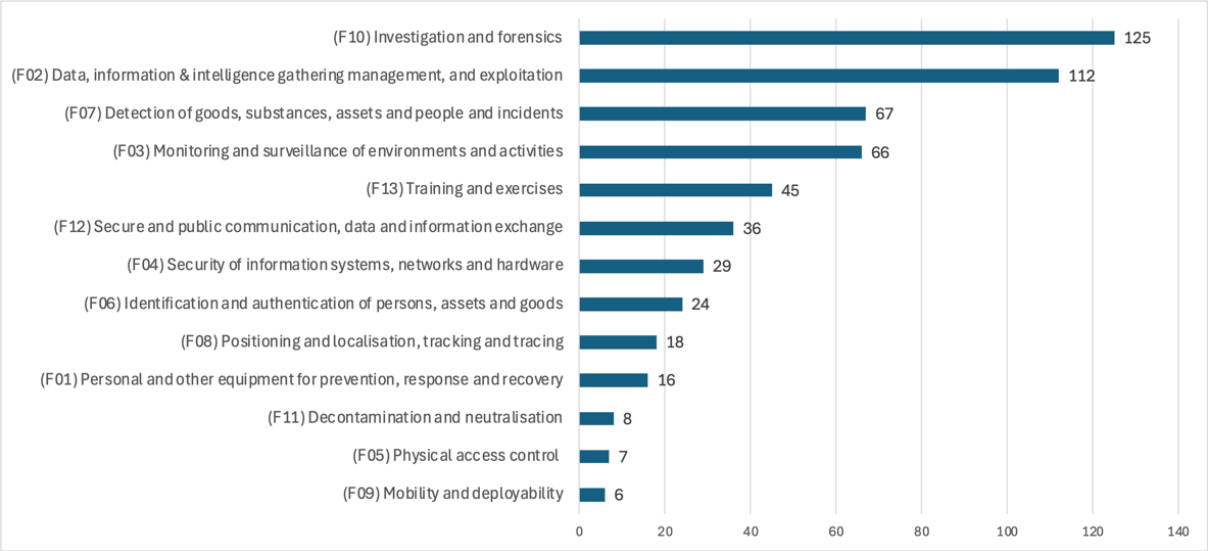


Figure 18 - Distribution of observations with high-relevance for Technology Observatory by EUCS Taxonomy Functional Area dimension applied to FCT.

Figure 19 depicts the distribution of the highly relevant observations for Technology Observatory, according to EUCS taxonomy technology areas dimension, revealing that **data analytics**, **internet-based investigations**, and **digital forensics** are the most emphasised areas. This trend may suggest that these fields are considered critical for the observatory's objectives, possibly due to their increasing relevance in addressing contemporary security challenges and the need for sophisticated investigative tools in a digital environment. In contrast, **guarding and physical protection (non-human)** were absent from high-relevance technology observations. This suggests that the observatory places a higher value on digital and analytical capabilities in its current technological landscape.

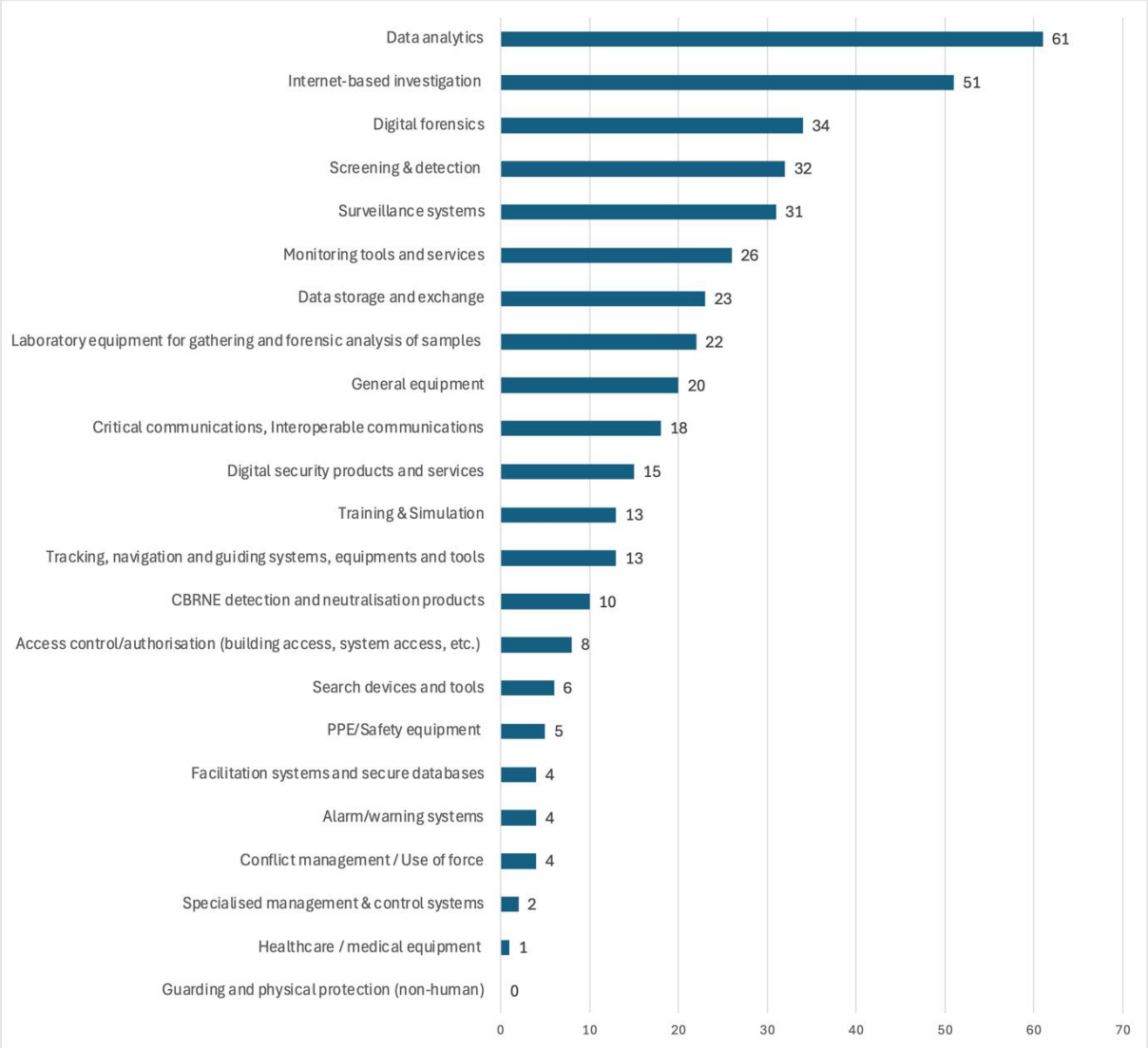


Figure 19 - Distribution of observations with high-relevance for Capability Observatory by EUCS Taxonomy Technology Areas dimension applied to FCT.

The main trending news, technologies and science from the Technology Observatory perspective are presented in **Table 2**.

Table 2 - The main trending news, technologies and science from the Technology Observatory.

Trending News in the Technology Perspective:
• Almost 50% of all news topics are related to cybercrime areas, namely online identity theft, dark markets and cryptocurrencies and digital forensics.
• In **organised crime** and **terrorism and radicalisation,** articles focused on the use of AI and large language models (LLMs), deepfakes and disrupting the dark web, with additional mentions for 3D printed weapons and detection of drugs.
• 60% of news topics concerning horizontal issues related to the topic of **disinformation and fake news** surrounding technologies for deepfake generation and detection.
Trending Tech in the Technology Perspective
• The top functions areas are: ○ **Investigation and forensics** and **data, information & intelligence gathering management, and exploitation** have significant overlap and covers all technologies from conventional forensics to AI, text analysis, encryption and pattern analysis. ○ **Detection of goods, substances, assets and people and incidents** – primarily focused on the development of new sensors. ○ **Monitoring and surveillance of environments and activities** – linked to many of the sensing activities and well as environmental crime monitoring through geospatial intelligence
• In Technology areas, there was an intense focus on **data analytics** technologies particularly for trend and pattern analysis. While **screening and detection** technologies were linked to the development of (mainly drugs) sensors.
Trending Sciences in the Technology Perspective
• 65% of all observations classified as scientific material relate to the area of **organised crime**; only 13% are related to **terrorism and radicalisation**.
• Research into AI, LLMs and AI assistants remain popular, as do various applications for image processing (from video to satellite imagery).
Trending Projects in the Technology Perspective
• Almost half of all active projects contain some form of **cybercrime** element
• Projects relating to **data gathering** (F02); **investigation and forensics** (F10), **training and exercises** (F13) and **detection** (F07) and were the most common functions areas.
• Technology for supporting internet investigations is still the most common technology under development.

2.2.3 FCT Market Map

Observations from events, such as fairs and conferences, represent 80% of observations relevant to the Market Observatory. Together with Policy papers (5%) and news (8%), they represent 93% of relevant observations (see **Figure 20**).

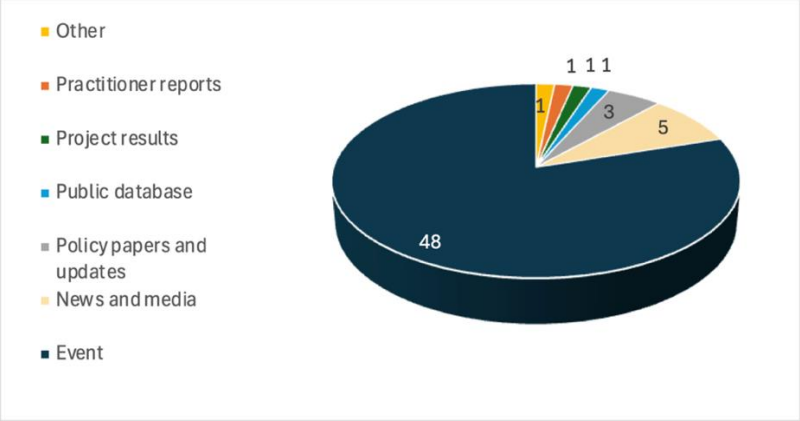


Figure 20 - Distributions of observations highly relevant for the Market Observatory by category.

For the Market Observatory, the overall distribution regarding the EUCS Taxonomy level 2 classification is **cybercrime** at 39%, **terrorism and radicalisation** at 28%, **horizontal and**

societal issues at 24% and **organised crime** at 8%. In cybercrime, **attacks against information systems** are the most represented with more than 50% of cybercrime (see **Figure 21**).

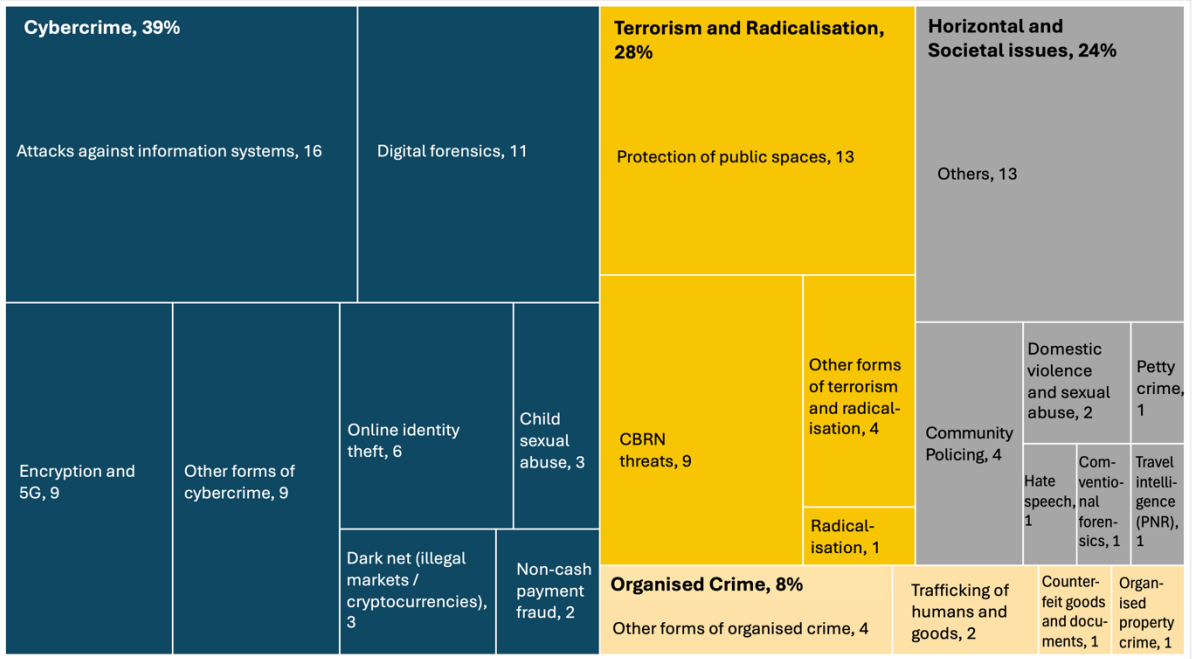


Figure 21 - Distribution of observations with high-relevance for Market Observatory by EUCS Taxonomy policy domain applied to FCT.

The Functions dimension reveals a strong focus on the **security of information systems, networks, and hardware** (F04); **personal and other equipment for prevention, response, and recovery** (F01); and **data, information & intelligence gathering, management, and exploitation** (F02). In contrast, **positioning and localisation, tracking, and tracing** (F08) and **decontamination and neutralisation** (F11) have only a single occurrence, reflecting a market trend where digital security and data management are considered more urgent or impactful than traditional tracking and tracing functions (see

Figure 22).

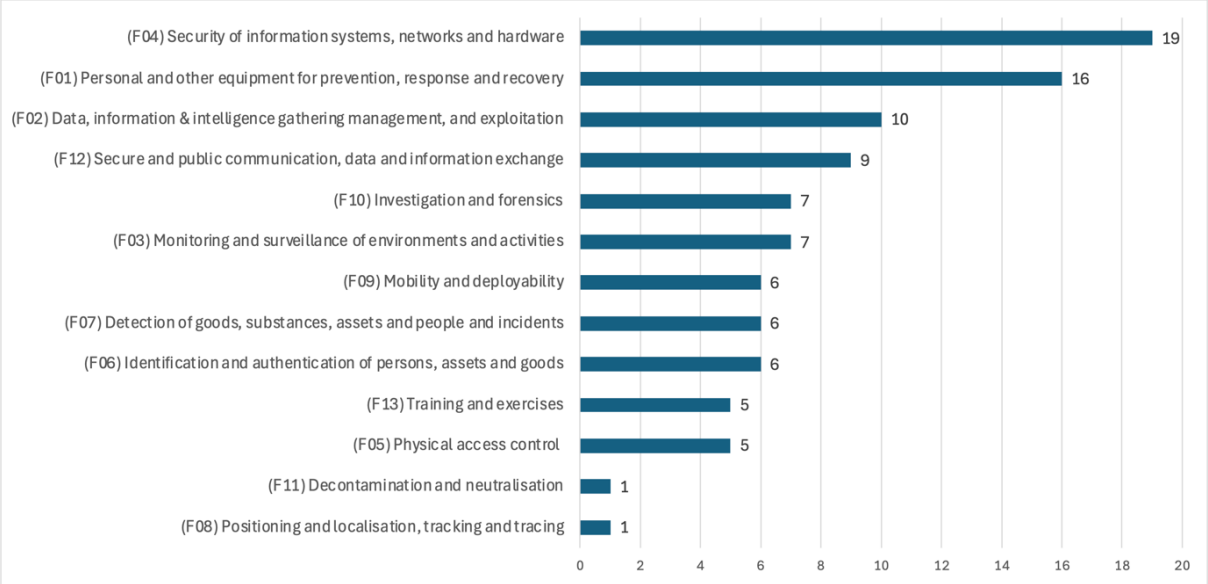


Figure 22 - Distribution of observations with high-relevance for Market Observatory by EUCS Taxonomy Functional Area dimension applied to FCT.

Within the Technology Areas dimension, **digital security products and services**, **surveillance systems**, and **digital forensics** are the most prevalent categories (see

Figure 23), while **personal protective equipment (PPE) and safety equipment** has no occurrences recorded. This lack of representation might indicate that the market currently places less emphasis on traditional safety measures, potentially prioritising more sophisticated digital and technological solutions instead. It could also reflect a market trend where investment and innovation are more concentrated on digital security rather than physical safety equipment.

Figure 23 - Distribution of observations with high-relevance for Market Observatory by EUCS Taxonomy Technology Areas dimension applied to FCT.

The main trending news, technologies and science from the Market Observatory perspective are presented in **Table 3.**

Table 3 - The main trending news, technologies and science from the Market Observatory.

Trending News in the Market Perspective:
• The news related to the Market Observatory mainly revolved around the announcement of police forces launching public calls for equipment procurement.
• 40% of the observations were regarding funding towards equipment for increasing border security and border management.
• Technologies mentioned included portable body scanners, radar and thermal devices, open source-software and databases.
Trending Tech in the Market Perspective
• The most represented technologies in observations relevant to the Market Observatory are related to **digital security**, **digital forensics**, **data analytics**, **storage and secure database**, amounting for over 37% of observations.
• None of the observations touches upon **PPE and Safety equipment**.
• Observations on managing conflicts and use of force focus on ammunitions and anti-drone capabilities.
• Drones are also a major topic for discussion under surveillance systems, either as a mean for surveillance or for technologies to identify and counter drones.
Trending Innovation and Procurement in the Market Perspective
• Observations at both national and European level stress the importance of innovation to mitigate security challenges. These observations stress the need to accelerate innovation and facilitate market uptake.
• However, these observations do not refer to a specific technological field.
• Procurement on ammunitions, software and investigation scientific tools.
• Funding for upgrades and modernisation allocated to digital forensics and border management.

2.2.4 FCT Ethical, Legal & Societal Map

The ELS Observatory focuses on monitoring ethical, legal and societal issues. Of the total of observations, 19% are considered as high-relevance ELS Observatory, with policy papers and updates representing more than half of the observations (see **Figure 24**).

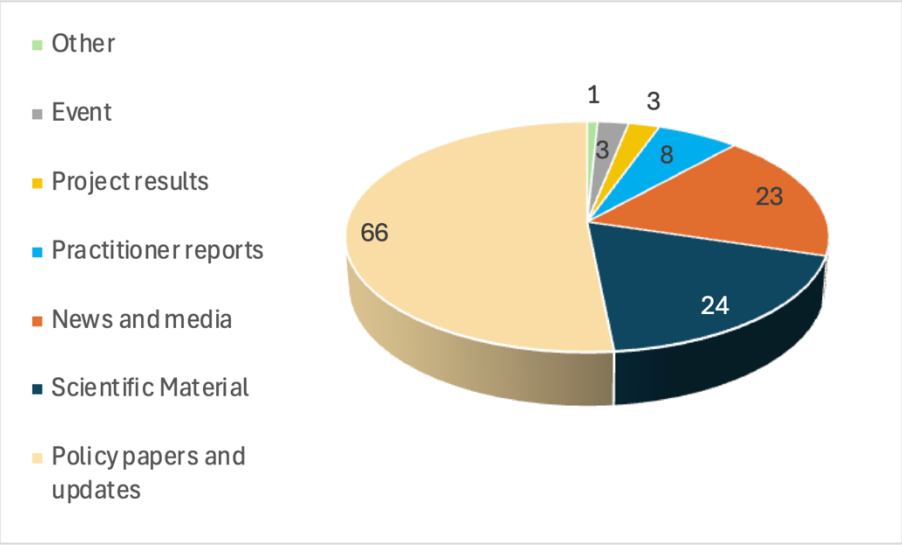


Figure 24 - Distributions of observations highly relevant for the ELS Observatory by category.

The ELS Observatory tree-map summarises the high relevance level observations classification related to EUCS Taxonomy. The dominant elements are **cybersecurity** at 30% and **horizontal and societal issues** at 29%. **Other forms of cybercrime** and **digital forensics** are the most prominent categories for cybersecurity. In contrast, **terrorism and radicalisation**, with 19%, is a less dominant element, and its sub-area **explosives and explosives precursors** are the element with a smaller number of observations in terrorism and radicalisation (see details in **Figure 25**).

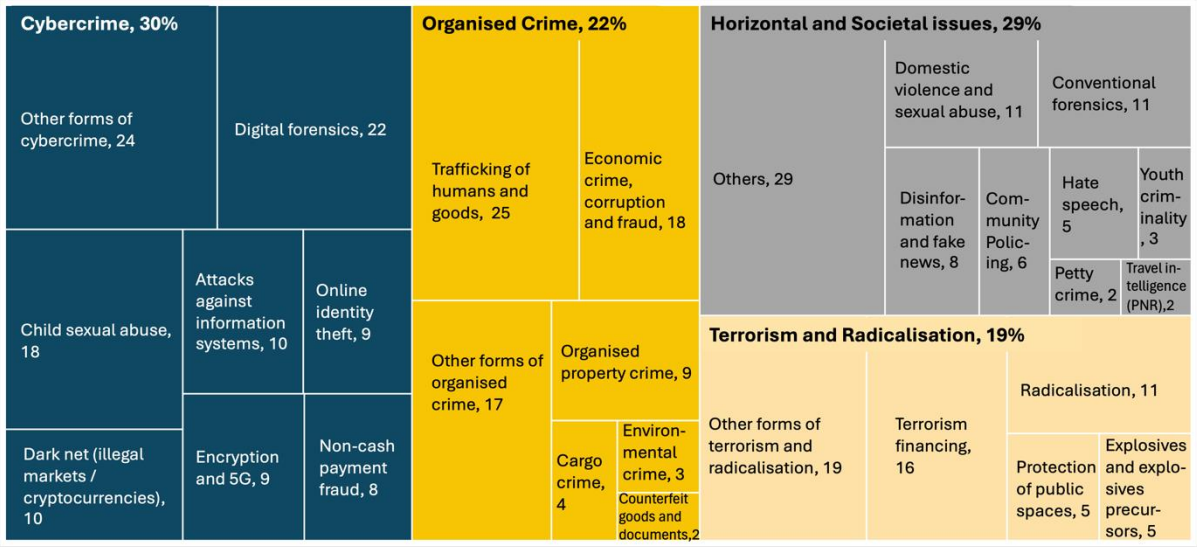


Figure 25 - Distribution of observations with high-relevance for ELS Observatory by EUCS Taxonomy policy domain applied to FCT.

As observed in **Figure 26**, **data, information & intelligence gathering, management, and exploitation** (F02), **investigation and forensics** (F10); and **secure and public communication, data, and information exchange** (F12) stand out as the most observed functional areas. On the contrary, **decontamination and neutralisation** (F11) has no representation.

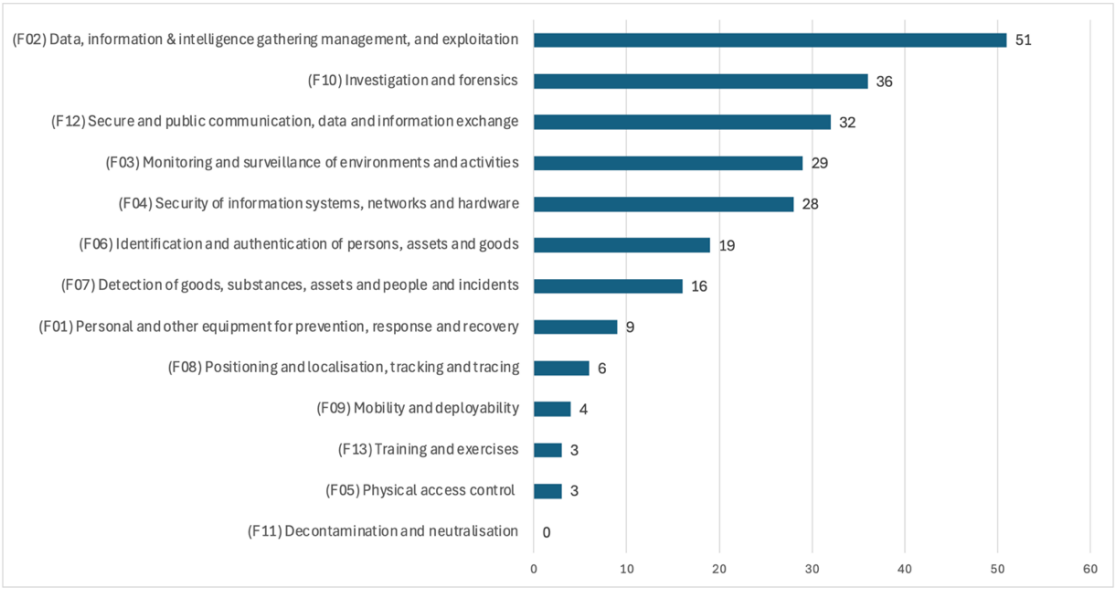


Figure 26 - Distribution of observations with high-relevance for ELS Observatory by EUCS Taxonomy Functional Area dimension applied to FCT.

Within the Technology Areas dimension, **data storage and exchange**, **monitoring tools and services**, and **facilitation systems and secure databases** are the most frequently represented categories (see **Figure 27**). It suggests that these areas are central to the observatory's technological focus, likely due to their critical role in ensuring secure data management, effective monitoring, and reliable information facilitation. In contrast, several categories, including **chemical, biological, radiological, nuclear, and explosive** (**CBRNE) detection and neutralisation products**, **laboratory equipment for gathering and forensic analysis of samples**, **healthcare/medical equipment**, and **conflict management/use of force**, show no occurrences. The absence of these areas indicates that the ELS Observatory places minimal emphasis on these more specialised or traditional technologies, possibly reflecting a strategic focus on digital and data-driven solutions over physical or medical technologies.

Figure 27 - Distribution of observations with high-relevance for Technology Observatory by EUCS Taxonomy Technology Areas dimension applied to FCT

The main trending news, technologies and science from the Technology Observatory perspective are presented in **Table 4**.

Table 4 - The main trending news, technologies and science from the ELS Observatory.

Trending News in the ELS issues Perspective:
• Media follows new uses of technology in law enforcement context and shares international contexts to combat crime
• **Child sexual abuse**; **digital forensics**; **trafficking of humans and goods**.
• EU has stronger rules to combat **trafficking of human and goods**, with international partnerships.
• EU is exploring the use of AI technologies in investigating and combating **child sexual abuse**.
• Use of technologies in law enforcement should walk hand in hand with rules regarding safe use of e-evidence.

Trending Tech in the ELS issues Perspective
• A lot of new technologies and forms of **data exchange** are being explored, while fundamental rights are enforced via civil society and policies.
• **Data, information & intelligence gathering, management, and exploitation**; **surveillance systems**; **security of information systems**, networks and hardware.
• International **data exchange**, involving biometric information – especially in borders.
• Facial and behaviour recognition in public spaces – and the challenges of this application.
Trending Sciences in the ELS issues Perspective
• **Trafficking of humans and goods**; **terrorism financing**; **conventional forensics**; **organised property crime**.
• Research focused on understanding how drug trafficking impact society.
• Scientific material exploring EU policy on countertrafficking with preventing forms of radicalisation speech online and financing – including via cryptocurrencies.
• International contexts and agreements are a common focus of research activities.

2.3 Flash Knowledge Reports (KER3)

The **Flash Knowledge Reports (KER3)** are short and quick reports built either on demand or on initiative. These reports generally focus on one policy, threat, event, function or technology (i.e., the driver). They connect it with the other dimensions monitored by the observatories, building on the information readily available in the SKB. In essence, the Flash Reports are a documented outcome of an expert search in the ENACT knowledge base. A summary of each Flash Report is provided below.

2.3.1 Flash Report #1 - Security Market Overview: Trends & Insights from the SICUR Exhibition

The **Flash Report # 1** consolidates the SICUR Exhibition. **SICUR**[7] is the international reference fair for security market in Spain. It brings together, in Madrid, companies, associations, professionals, and users of global security in the public and private spheres in Madrid every two years.

Innovation and technological development are the main protagonists of this professional meeting, which addresses comprehensive security from five areas: security, cybersecurity, fire and emergency safety, occupational safety, and health at work. SICUR's agenda is firmly rooted in advancing societal well-being and developmental progress, serving as a catalyst for exchanging knowledge and the proliferation of cutting-edge technologies. SICUR 2024 explicitly addressed the Innovation theme, which also serves as a proxy measure of the themes of interest for the security community.

SICUR had 654 exhibitors, showing a comprehensive display of the latest in security equipment and technology. The areas addressed include intrusion security, fire prevention, occupational health, traffic protection, cybersecurity, defence, and insights from the technical press and associations, illustrating the event's broad coverage of security concerns.

A meticulous analysis of SICUR's exhibitor's portfolio revealed a total of 113 exhibiting companies with offerings considered relevant for the FCT domain. ENACT collected 113 observations referring to 113 exhibitors, 28 referring to conferences and 7 referring to the innovation gallery. Apart from the exhibiting companies, there was also a large exhibition area dedicated to Spanish LEAs. The analysis of the exhibitors showed a high offer in technologies

[7] **SICUR event website:** https://www.ifema.es/sicur

contributing to police functions such as physical access control, monitoring and surveillance and personal protection. A parallel analysis on the conferences held during the event also show a notable interest on cybersecurity (protection of information technology – IT – infrastructure) and protection against chemical, biological, radiological, and nuclear (CBRN) incidents.

2.3.2 Flash Report #2 - Security Market Overview: TECNOSEC & DRONExpo

The **Flash Report # 2** presents the security market overview of TECNOSEC & DRONExpo. TECNOSEC has evolved into the premier professional forum for police, intelligence, and security technologies since its inception. Held annually in Madrid, this event, sponsored by Telefónica, Indra, Bluenest, Zebra, and Ineco, provides a centralised platform for the most significant business opportunities among a growing array of specialised technological solutions.

The 3rd edition of **TECNOSEC[8] & DRONExpo[9]** featured over 100 exhibitors, welcomed more than 4000 professional visitors, hosted over 80 speakers across various panel discussions and commercial presentations. ENACT collected 81 observations referring to exhibiting companies, 11 referring to conferences and 13 referring to Conferences & Policy.

As part of the “Brokerage Event” organised by the Enterprise Europe Network and Madri+d, more than 150 meetings were held, fostering valuable networking opportunities and collaboration within the industry. Several Spanish authorities attended the event to witness the latest technologies showcased by sector companies, designed for diverse security applications and intended for use by security forces, intelligence agencies, and the Armed Forces, among others.

To provide a thorough analysis of the showcased technologies and their significance within the broader context of security market trends and needs, this report systematically correlates exhibitor profiles and conference themes with the EUCS Taxonomy. This analysis shows that monitoring and surveillance of environments and activities function stands out as the most addressed police function addressed by the exhibitors. Exhibitors also prominently featured functions related to **data, information & intelligence gathering, and exploitation**, **mobility and deployability**, and **secure and public communication, data and information exchange.** This coverage, in comparison with the R&I topics typically addressed in the EU-funded FCT research work programmes, make TECNOSEC a good market reference for the FCT R&I ecosystem, and a potential window to the market for innovative FCT technologies.

2.3.3 Flash Report #3 - Countering Drug Production and Distribution

The third ENACT Flash Report was commissioned by the EMCDDA (European Monitoring Centre for Drugs and Drug Addiction), now formalised as an EU agency – **EUDA (European Union Drugs Agency)[10]**, in an effort to catalogue and analyse all relevant technological advancements done in the past few years when it comes to the fight against drugs. The focus

[8] **TECNOSEC 2024 event website:** https://www.tecnosec.es/en/
[9] **DRONExpo 2024 event website:** https://www.dronexpo.es/en/
[10] **EUDA website:** https://www.euda.europa.eu/index_en

for this report is to assess the developments in EU Horizon 2020 and Horizon Europe research projects in relation to drug production, drug distribution and drug forensics. This report will entail emerging threats and current gaps from LEA's side, technologies under development on the projects, which of these innovative solutions reached the market and an analysis of ELS issues that may arise during the development of the project. This effort will prove to crucial in aiding EUDA having a holistic view of the innovation landscape when it comes to the criminal panorama revolving trafficking of drugs.

The data for the assessment was extracted from the SKB based on the data collected on all projects funded under Horizon programmes under the calls related to the FCT. In addition, relevant projects also funded under the Border Management theme and a search of CORDIS for projects mentioning "illegal/illicit substances" or "drugs" were used to identify further projects. Projects not related to illicit drugs or concerning health programmes were excluded from the scope. Overall, 34 projects were identified and categorised according to the EUCS taxonomy, furthermore, they were also classified according to whether they address drugs production, distribution, or forensics. A distinction for those projects concerning distribution but linked to border/customs-oriented projects were also made.

The analysis identified that the majority (76%) of all drugs related projects concern **organised crime** and specifically trafficking, with the functions addressed focused on the **detection of goods, substances, assets people and incidents**, followed by **investigation and forensics**, and **data, information, & intelligence gathering management and exploitation**. Thus, covering the conventional forensics and digital aspects. In terms of technology, **screening and detection** technologies were more prevalent with additional categorisations relating to **surveillance systems** and **monitoring tools and services**.

Utilising the information published through CORDIS for each project (including the fact sheet, results in brief, reporting and documents, where available) a deeper dive into the technological developments was carried out. These technologies primarily concern the development of new sensors – for environmental monitoring and on-the-sport monitoring for various illicit substances, as well as new lab-based techniques. For those projects focused on the detection of trafficking in online spaces, data acquisition and analytical technologies were prioritised, while those combined with the border management area introduced new scanning techniques for the detection of drugs on cargo, packages and people.

This Flash Report is currently under development.

2.3.4 Flash Report #4 - EUROSATORY 2024

The Flash Report # 4 consolidates the **EUROSATORY exhibition**[11]. EUROSATORY is the largest international exhibition dedicated to the defence and security industry. Since 1967, it is held in Paris, France, every two years for industries, research centres, associations and ministries to present their products, services and needs, and to discuss and conclude partnerships.

The last edition (2024) was 5 days long and welcomed more than 62000 visitors from 150 countries in front of 2000 exhibitors, 48 national pavilions and 120 conferences. It revolved around 12 technology clusters aiming to foster cooperation and ease visitors targeting relevant

[11] **EUROSATORY event:** https://www.eurosatory.com/

exhibitors: Drones and Robotics, Embedded Electronics, Training and Simulation, Engineering and Manufacturing, Non-Conventional Threat CBRNE, Research, Tests and Measurement, Intelligence, Cyber, Civil Security and Firefighting, Technologies for infrastructure security, Medical Cluster, and Human support and logistics.

To extract actionable insights and identify technological and innovation trends, the ENACT Consortium is almost concluding the characterization of exhibitors at EUROSATORY 2024 according to the EUCS taxonomy, based on the full list of **EUROSATORY 2024 exhibitors**[12].

Some of the key-results already found[13] are:

- EUROSATORY is a major event not only for the defence players but also for security and LEAs with 69% of exhibitors and 65% of conferences relevant to both of them;
- Most of exhibitors are manufacturers or provider of general equipment related to **mobility and deployment** (58%), **protective equipment** (47%) or **training and simulation** (45%);
- Regarding law enforcements missions, some are well represented such as **monitoring and surveillance** (25%) and **protection of public spaces** (13%).

This Flash Report is currently under development.

2.3.5 Flash Report #5 - Real-time and Post Biometric Identification

Biometric identification is a topic of interest in the FCT community, being the object of study of different R&I initiatives. Nonetheless, the risks to fundamental rights and freedoms involved in the use of biometric identification are also a very relevant theme in the debate of using said technologies in the FCT. In the last years, the topic has also occupied a central place in the legislative debate involving the regulation of AI. So, the relevance of this report is illustrated by the relation of the topic with the different ENACT observatories:

- **Capabilities:** it is crucial to understand the level of understanding and training of LEAs for the use of biometric identification technologies, while presenting the levels of accuracy and errors.
- **Technology:** technologies are being developed for guaranteeing the development and deployment of biometric identification instruments.
- **Market, funding and standardization:** considering the risks and opportunities, it is crucial to understand if the market requires biometric identification technologies, how funding is being placed for the development of said instruments, and if any standards are in place to guarantee the legal use of the equipment.
- **ELS:** with the new regulations in place in EU, it is crucial to understand what the ethical and legal limits are put for the use of biometric identification, establishing the difference between real-time and post identification, while exploring if projects are considering these aspects and the societal acceptance of these new tools.

The topic is also connected to different categories of the EUCS Taxonomy, but the following have a close relationship with the use of biometric identification:

- Trafficking of humans and goods

[12] **EUROSATORY 2024 exhibitors:** https://www.eurosatory.com/en/trends/exhibitors-2024/
[13] **Note:** Statistic pending confirmation, only the data from the Flash Report will be consolidated.

- Terrorism and Radicalisation
- Online identity theft
- Disinformation and fake news
- Travel intelligence (Passenger Name Record - PNR)
- Data, information & intelligence gathering, management, and exploitation
- Monitoring and surveillance of environments and activities
- Identification and authentication of persons, assets and goods
- Detection of goods, substances, assets and people and incidents
- Access control/authorization (building access, system access, etc.)
- Monitoring tools and services
- Screening & detection
- Surveillance systems

552/671 observations are related to at least one of the categories listed above. However, fewer than half of the annotation are directly linked to biometric identification. Also, considering the approved text of the **AI Act**[14], the ELS Observatory noted that there is need for more focused research on observations about the difference between real-time and post biometric identification. Thus, the ELS KO leader is working on adding at least 30 new observations on this regard, being the majority of those scientific material, policy papers and updates, and news and media. With these inputs, it is possible to define in a more concrete way how the topic of this flash report is affecting the FCT domain.

This Flash Report is currently under development.

2.4 Advanced Expert Reports (KER4)

The observatories also generate **Analytical Reports (KER4)** to provide deeper insights into topics that necessitate further examination beyond the scope of KER3, either upon request or as proposed by the observatories. Utilising the data from the SKB and input from relevant key stakeholders, the observatories have recommended a range of analytical reports for future development, already producing one report. ENACT plans to engage a pool of external experts to generate on-demand reports in response to specific requests.

2.4.1 Analytical Report #1 - FCT R&I: An Analysis of EU Priorities 2014-2024

The **Analytical Report #1** prepared by ENACT Consortium presents an analytical exercise carried out on the R&I priorities set by the EC for the FCT between 2014 and 2024. These priorities have been identified by classifying the focus of 76 FCT research topics and subtopics according to the EU Security Taxonomy developed by the Commission under the EU Security Market Study released in 2021 (see **Appendix A**).

The analysis has been conducted from a Work Programme perspective. It therefore reflects the priorities and ambitions of the Commission when the Work Programmes were adopted, and not the matters addressed, and the results achieved by the projects that were eventually funded after each topic. This report presents the analysis results for the different taxonomy

[14] **AI Act:** https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

dimensions and covers 76 different topics/sub-topics, spanning over ten years of FCT research.

The objective is to provide structured historical data to policymakers to support them in the decision-making process for setting the FCT R&I priorities for the remaining Horizon Europe work programmes and the strategic priorities of the next EU-funded R&I Framework Programme (FP 10). In addition, this analysis aims to: showcase the value of the taxonomy developed with the support of the Commission and EU Agencies experts under the EU Security Market Study 2021.

The findings show an unequal distribution of research priorities within the policy and functional dimensions. In the policy dimension, the Commission has prioritised research against economic crime, corruption, and fraud, particularly emphasising the trafficking of humans and goods and illegal markets in the dark web. In the functional dimension, the most common research needs are investigation & forensics and data, information & intelligence gathering, management, and exploitation.

Regarding technology, even though EU-funded security research doesn't specify the types of technologies to be used, Internet-based investigation technologies and data analytics technologies have emerged as the most frequently referenced.

The report is a foundational reference for the ENACT network's upcoming work and provides crucial data for the FCT R&I community to support future decision-making and research programming. The data highlights trends in research priorities over the past decade, identifying the most addressed areas and those with significant funding gaps. This information is valuable for the EC to detect and rectify any imbalances in funding distribution in future work programs under Horizon Europe or in the strategic planning of the next EU-funded R&I framework program, FP10.

2.5 FCT State-of-Play Policy Report (KER5)

The present SoP FCT Policy Report offers a concise and targeted overview of recent developments, latest insights, and recommendations from various ENACT activities from March to July 2024. The 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 of CERIS (Community of European Research and Innovation for Security) 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. 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.

2.5.1 Policy View

The current policy landscape in the FCT is significantly 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. **Cybercrime** is closely

followed, capturing 31% of 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.

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 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** 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.

2.5.2 Technology View

2.5.2.1 Summary of Technology View

Technology continues to play a key role in the FCT. As criminal actors leverage on technological tools, it is essential that Police Authorities and Security Practitioners are also equipped with technology that can support the prevention, response and mitigation of crime and terrorism. Technology can be in various stages of development – the most mature is that already on the market through commercial and operational providers, the next is that being developed in applied research projects (such as those in Horizon programmes) and finally those that are more closely aligned with basic research which can be found in scientific publications. Technology does not standalone and is *usually* designed to address a specific function or respond to a specific challenge. In the SKB, there are four functions areas that are each addressed by at least one-third of the observations present (and categorised as highly relevant for the Technology Observatory):

- Data, information & intelligence gathering management, and exploitation;
- Monitoring and surveillance of environments and activities;
- Detection of goods, substances, assets and people and incidents;

- Investigation and forensics.

2.5.2.2 Commercial and Operational Products View

ENACT produced two Flash Reports from international exhibitions that highlight the technology market for the security sector, particularly for crime and terrorism. These reports, derived from the TECNOSEC and SICUR exhibitions, identified 95 and 113 companies, respectively, as significant contributors to the FCT domain.

Through this analysis, the key technologies showcased at SICUR focused on **access control/authorisation systems** and **surveillance systems**. The report was able to narrow this down to **video surveillance systems** (closed-circuit television - CCTV - systems, cameras and sensors, video analytics) as the most common. Within **surveillance systems**, technology included **small tactical drones** and **autonomous ground vehicles;** while **access control** included control gates, biometric identification/authentication, smart locks. PPE and safety equipment. Meanwhile, in TECNOSEC, **surveillance systems** were most common, followed by **data analytics** and **critical communications, interoperable communications** and **digital security products and services**.

Based on these reports its clear that technologies related to **surveillance systems** are the most prevalent on the safety and security market, while in events that are more oriented towards Law Enforcement (such as TECNOSEC), **data analytics and communications technologies** emerge compared to those in the wider security sector (such as at SICUR).

2.5.2.3 Projects View (EU & Member States, R&I and Development)

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 **training 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 significantly skewed towards projects related to drugs (due to the preparation for the EUDA report) 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 the Seventh Framework Programme for Research and Technological Development (FP7) or Horizon 2020 (H2020) and the technologies are no longer under active development within the project context.

2.5.3 Market View

2.5.3.1 Summary of Market View

The Market Observatory complements the insights provided by the Technology and Capability Observatories by offering a detailed analysis of both demand and supply, as well as the evolving ecosystem. 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 Framework Programmes, examining the types of actions funded and the distribution of both public and private funding.

Further analysis explores the market size through procurement activities and spending patterns across EU countries. To provide a comprehensive view of the FCT R&I market, the analysis also details market actors (from the ENACT Stakeholders Directory) and their profiles according to the Horizon Framework Programmes glossary and taxonomy. This examination is divided into two parts: the first focuses on participants in FCT R&I projects, expanding on observations from the FCT R&I stakeholders' map; the second reviews solution providers, including insights from the TECNOSEC and SICUR exhibitions and their alignment with the EUCS taxonomy function areas.

The review covers available EU R&I and procurement funding programmes relevant to the FCT sector. A summary table outlines the various programmes, their objectives, and their scope, including aspects such as joint procurement, support for pilots and testing, and research and innovation.

2.5.3.2 Market Size

The evolution of FCT R&I investment in EU programmes is analysed, with a particular focus on the Horizon 2020 and Horizon Europe Framework Programmes. An analysis of FCT R&I priorities from 2014 to 2024 is already available on the ENACT website in the **Analytical Report #1**.

According to the data collected on **Horizon Dashboard**[15], the total EU funding granted to the participants of the selected projects was €367.4 million 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 €380.0 million. This results in a difference of €12.5 million between the total cost and the total EU contribution, meaning that, out of the nearly €380 million in Horizon 2020 FCT R&I Investment between 2014 and 2020, EU fund have covered nearly 97% of the total cost. Under Horizon Europe, we considered only the Horizon Europe FCT calls from 2021 and 2022, with a total net EU contribution of €81.6 million. The share of private investment in the selected grants represents 10% of the total cost (€90.5 million).

Figure 28 shows the distribution of signed grants between 2014 and 2023. A total of 70 projects have been funded under the 23 identified calls, with the average total cost of a FCT R&I project under the Horizon 2020 Framework Programme being €5.43 million, while the average EU contribution per project is €5.25 million. Indeed, the grants Horizon 2020 successful proposals in 2020 were signed in 2021. The figure shows a continuous interest in supporting FCT R&I with a minimum of 7 grants and an average of 10 grants signed per year throughout the Framework Programme.

[15] **Horizon Dashboard:** https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard

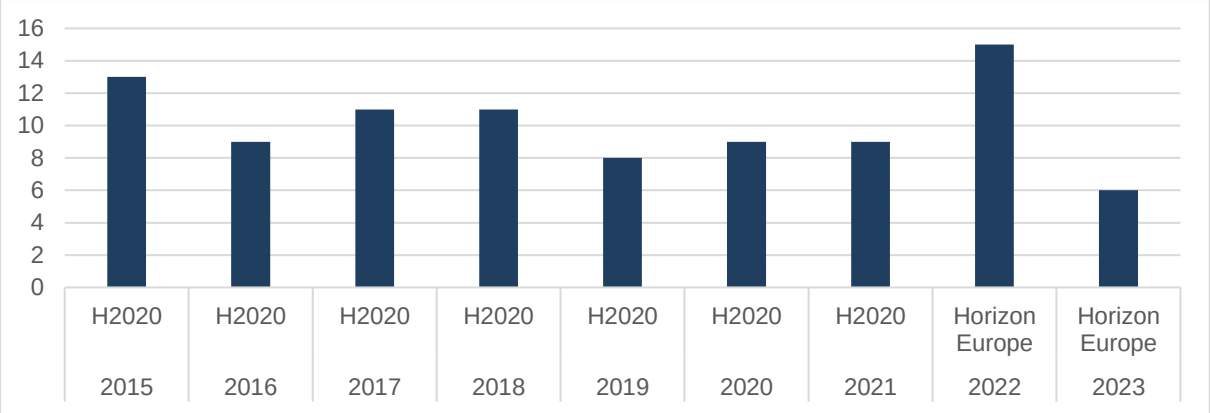


Figure 28 - Number of FCT signed grants per year under Horizon 2020 and Horizon Europe Framework Programmes.

As showed in the **Figure 29**Erro! A origem da referência não foi encontrada.**,** when looking at the type of action and funding scheme used to support FCT R&I under Horizon 2020, 80% of the signed grants were research and innovation action (RIA). Call for coordination and support action (CSA) and innovation action (IA) represent 2% of the total grants, and pre-commercial procurement (PCP) represents 18%. In comparison, we observe an increase in terms of share of IA, which covers 70% of the eligible costs of the action, under the Horizon Europe Framework Programme.

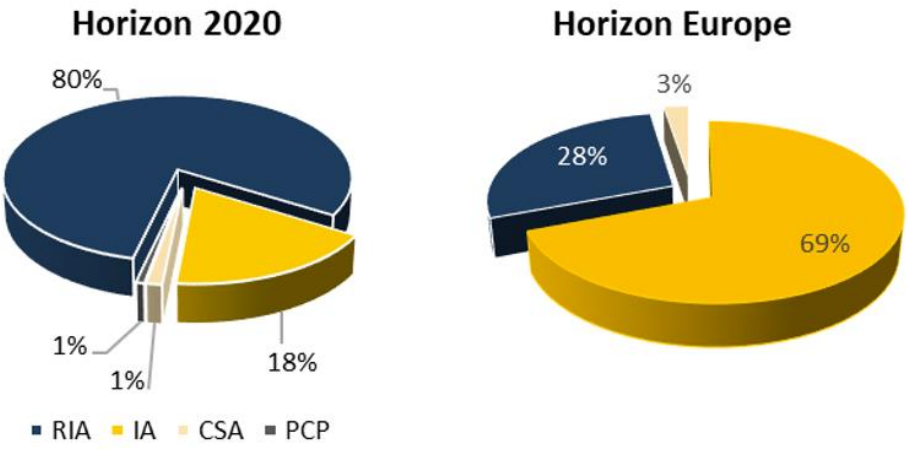


Figure 29 - Share of Horizon 2020 and Horizon Europe FCT funded projects by type of action.

The comparison between the Horizon 2020 Framework Programme (2014-2020) and the first two years of the Horizon Europe framework Programme (2021-2022), allows to make two observations. Firstly, the total budget allocated to FCT R&I is decreasing. Secondly, the share of IA has increased under Horizon Europe. This trend could be explained by either the fact that the solutions developed to address FCT issues are closer to the market, thus requiring more Innovation Action (IA); or by the decreased budget allocated to FCT R&I, which may have prompted a focus on more market-ready solutions.

When analysing the spending of Member States on FCT, one could be tempted to have a broad approach. As shown in **Figure 30,** data from 2015 to 2020 reveals that France has spent almost three times more than the other countries in FCT, with more than €2 billion compared to Spain €800 million, Germany's 700 or Italy's 600. While it is clear that France

has allocated significantly more budget to FCT than its neighbours, a more thorough analyse gives us a better understanding of the context in which the money was allocated.

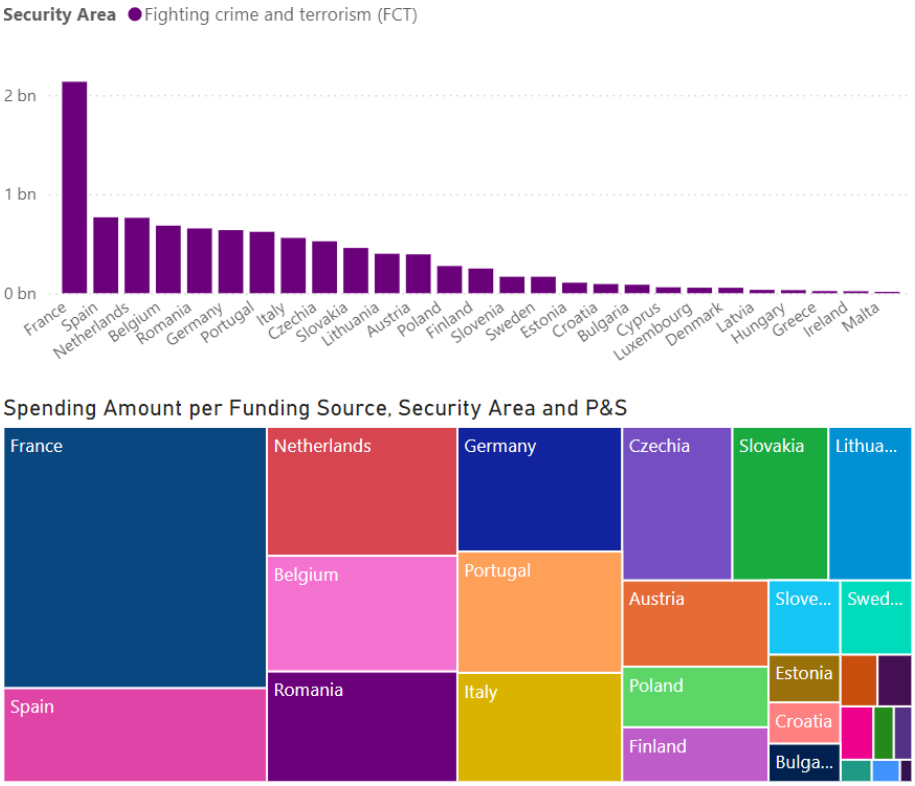


Figure 30 - Countries spending from 2015 to 2020 (note: data obtained from EUCS market segmentation model source[16]).

To further analyse the variations in spending during this timeframe, we selected 8 member states where notable changes occurred.

[16] **EU civil security market segmentation model database:** 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

Table 5 summarises the variation of spending (in € billion) for each country and year. These variations are to be interrogated through the prism of the security context of the country. From this table, a graph can be created (**Figure 31**) that visually summarises the trends for these 8 countries from 2015 to 2020.

Table 5. Spending variation from 2015 to 2020 for a sample of members countries.

	2015	2016		2017		2018		2019		2020	
	Rank	Rank	Variation	Rank	Variation	Rank	Variation	Rank	Variation	Rank	Variation
France	1	4	↘	1	↗↗	1	↗↗	4	↘	4	↘↘
Lithuania	4	1	↗	10	↘	13	=	20	=	16	=
Germany	10	2	↗	4	=	6	↘	8	=	18	↘↘
Romania	11	3	↗	2	↗	12	↘	11	=	1	=
Netherland	7	17	=	3	↗	15	↘	1	↗↗	12	↘↘
Italy	14	16	=	16	↗	11	=	2	↗↗	14	↘↘
Portugal	18	19	=	6	↗	7	↘	3	↗	8	↘↘
Austria	5	11	↘	12	=	21	↘	5	↗↗	7	↘↘

Examining the data reveals that 2020 cannot be compared to previous years due to the impact of the COVID-19 crisis. The pandemic led countries to redirect their budgets to address the crisis, which distorted the results. Additionally, during this period the policy priorities in terms of public investment/procurement shifted to address the COVID crisis, hence relegating investment in FCT to a lower priority.

Starting our analysis in 2015 is logical, as Europe, particularly France, was significantly affected by terrorism following the Paris attacks, which resulted in over 100 casualties. This drama and the ones that followed had a great impact on FCT spending in Europe as one can observe that France's spending boomed in 2017 and 2018. However, we should not reduce our analysis to this single influence. Indeed, those variation can also be explained by national context such as:

- France's spending climb, apart from the numerous attacks that harmed the country, can be explained by the adoption of a law aiming to fight organised crime, terrorism and their funding in 2016.
- Lithuania is the country that invested the most in 2016 as they were implementing a plan to develop public security and developing a new system to process data and early detection of terrorist and severe crimes.
- Romania's higher spending compared to France in the same period was likely due to the enforcement of a new Penal Code designed to fight corruption while taking chair of the Organisation for Security and Co-operation in Europe.
- Italy's budget for FCT remained relatively low until 2019, shortly after a new government administration took office.
- Between 2018 and 2019, Netherland's spending on FCT is multiplied by four, right after a national newspaper was the target of a major attack by a drug lord, and as drug was a major security problem in the country.

Moreover, the impact of the context varies across countries. For example, Germany follows steady path with very insignificant ups and downs, keeping its FCT spending between €0.12 and €0.18 billion for four years.

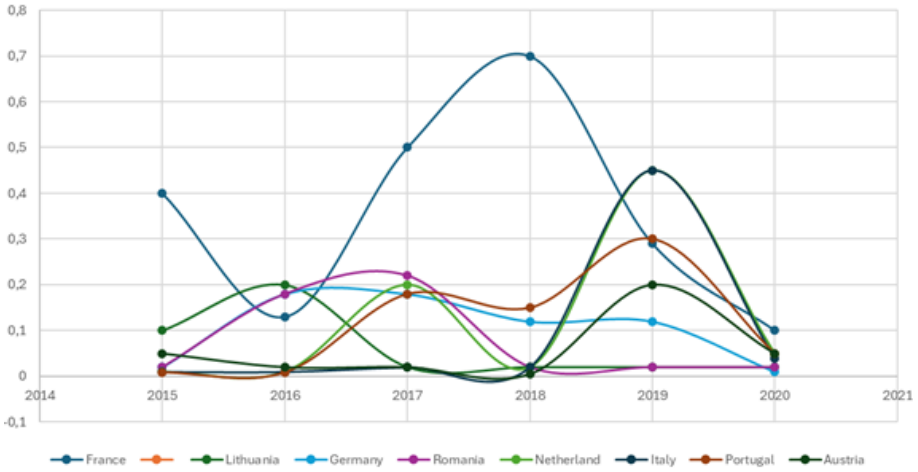


Figure 31 - Curve chart of the evolution of spending from 2015 to 2020 for eight selected member states.

Apart from the raw variations that one can observe, we can go further on our analysis by studying the costs items (**Figure 32**). On the six studied years, the repartition is the one opposite. For all countries combined, **general equipment and vehicles** – only to transport people – arrives first with €2.5 billion spent, closely followed by **surveillance systems** with €2.3 billion. The following categories are **PPE and safety equipment**, **digital security products and services**, **guarding and physical protection**, **equipment for deterrence/prevention**, **critical interoperable communications**, **specialised management & control systems**, **training & simulation**, and finally **monitoring tools and services**.

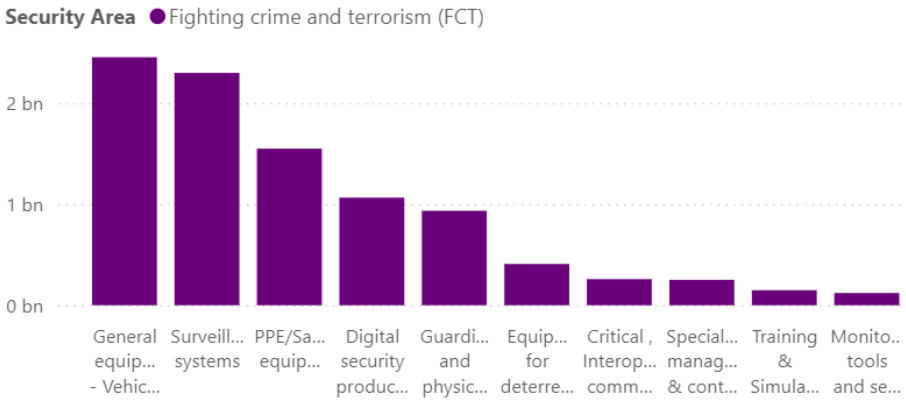


Figure 32 - Security area spending for top 10 product and services categories from 2015 to 2020.

This repartition is to be nuanced given that it varies from a country and a year from another. If we take our spending's champion France (**Figure 33**), the repartition is quite different with more importance given to **surveillance systems**.

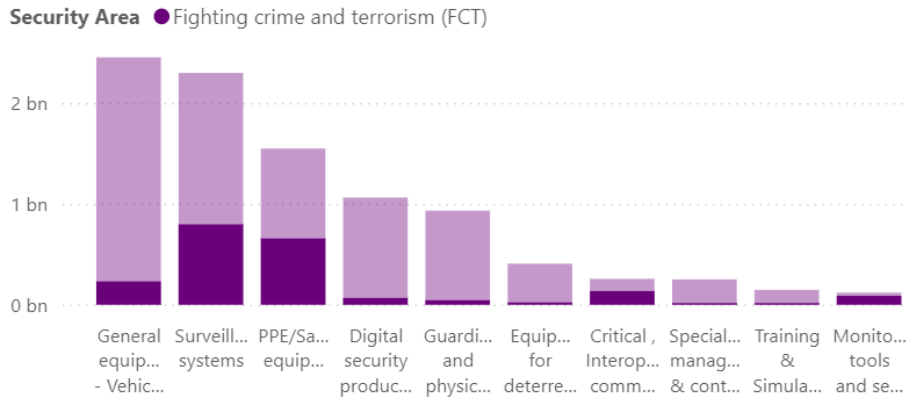


Figure 33 - France's security area spending for top 10 product and services categories over 5 years (2015-2020).

However, if we take a sample of eastern countries general equipment comes out first and surveillance systems are relegated in fifth place after **PPE/safety products**, **digital security** and **guarding and physical protection** (see **Appendix B**). In southern countries, even without considering France, **surveillance systems** is the biggest item cost, far from general equipment (see **Appendix C**).

The explanation of this breakdown is due to the regularity of spending for some items. **Figure 34** highlights the most important spending categories, while the whole variation breakdown is summarised **Appendix D**. The graph below illustrates that some categories experience more variability than others. Notably, **general equipment and vehicles** seems to be a very steady item cost. On the other hand, surveillance systems boomed in 2018 and 2019, but it showed significant fluctuations over the following years. The year 2020 evidences a clear downtrend due to the impact of the COVID-19 crisis.

Figure 34 - Curve graph of costs item variation per year (2015-2020).

We can also observe and put in perspective the yearly spending for FCT (**Figure 35**) in relation to the number of contracts closed per year (**Figure 36**). Comparing these two graphs, one can observe a correlation with a one-year gap. From a low number of contracts and a poor contract amount in 2015, 2016 is a weak year for spending in the security area. Meanwhile, 2018 was a very strong year for deals, with approximately 5000 projects/ contracts closed for almost €9 billion, which is reflected on 2019 with more than €2.5 billion spent in FCT area. Furthermore,

despite a relatively stable number of projects from 2016 to 2019, the amount of funding allocated grew to peak in 2018 before diminishing, yet staying above of the previous standards, in 2019, mirroring the importance given to this sector.

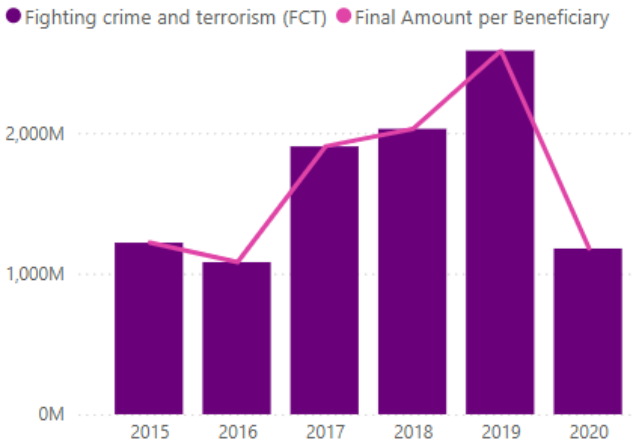
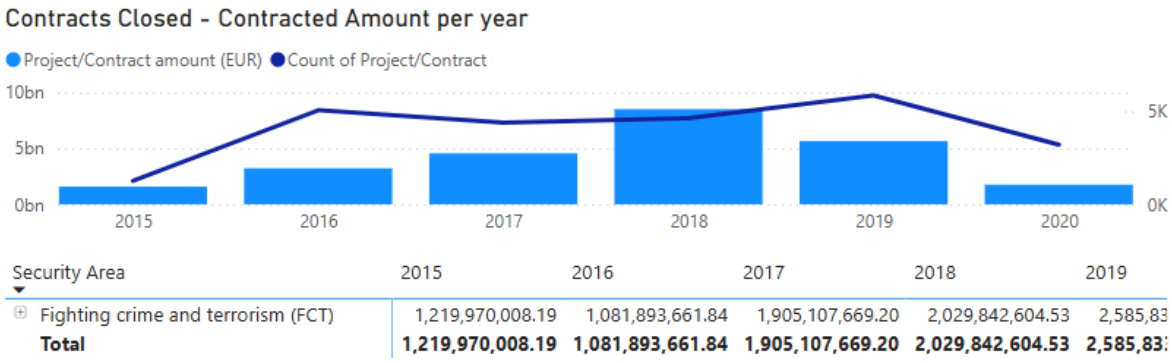


Figure 35 – Histogram of yearly spending per security area from 2015 to 2020.



Security Area	2015	2016	2017	2018	2019
Fighting crime and terrorism (FCT)	1,219,970,008.19	1,081,893,661.84	1,905,107,669.20	2,029,842,604.53	2,585,83
Total	**1,219,970,008.19**	**1,081,893,661.84**	**1,905,107,669.20**	**2,029,842,604.53**	**2,585,83**

Figure 36 - Histogram of contract amount and curve graph of contract amount.

2.5.3.3 Relevant Market Actors

The profiles of FCT R&I stakeholders and market actors are also presented, beginning with an analysis of participants in both the Horizon 2020 and Horizon Europe Framework Programmes. The focus then shifts to other market actors, particularly the exhibitors featured at the SICUR 2024 and TECNOSEC fairs. The geographical distribution of FCT R&I stakeholders across Europe and third countries is also examined.

Figure 37 shows the distribution of both Framework Programmes beneficiaries by organisation types, according to the EC Horizon 2020 and Europe beneficiary taxonomy.

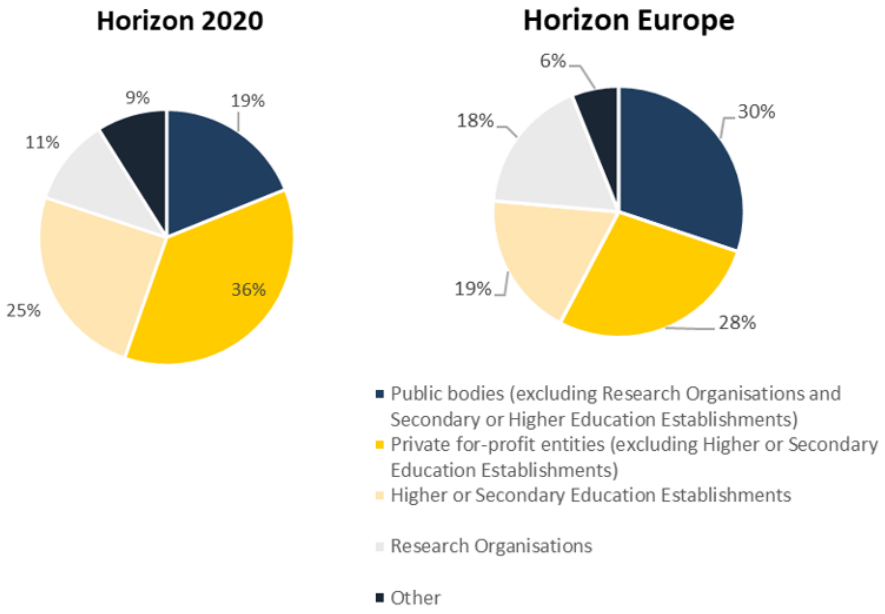


Figure 37 - Share of FCT Horizon 2020 and Horizon Europe beneficiaries by organisation types.

Figure 38 presents the evolution of the share of beneficiaries' organisation type between Horizon 2020 and the first two years of the Horizon Europe Programme. The share of public bodies, according to the Horizon glossary, has significantly increased under Horizon Europe. In the contrary, the share of both private for-profit organisations and higher or secondary education establishments has decreased.

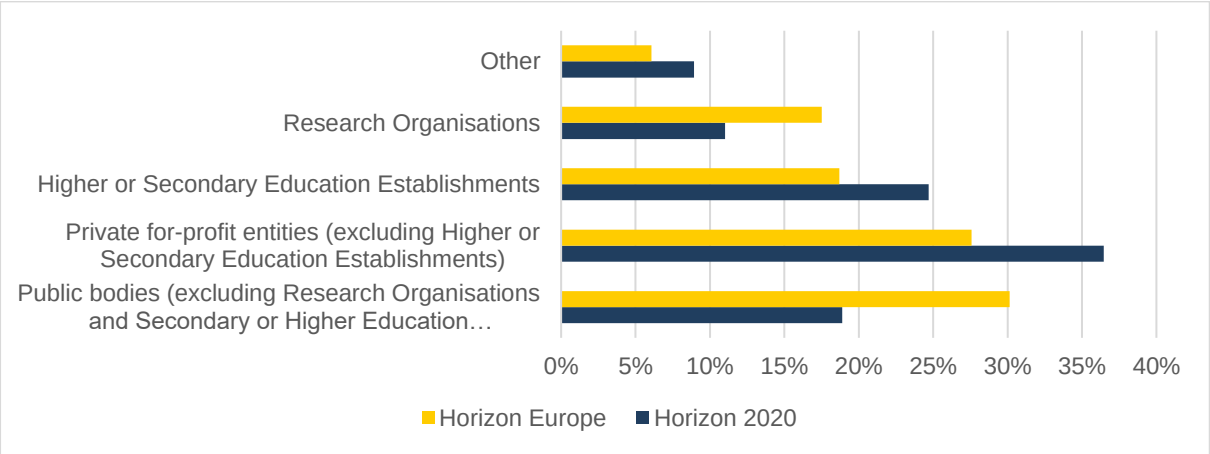


Figure 38 - Horizon 2020 and Horizon Europe beneficiaries' type of organisation comparison.

Furthermore, ENACT Consortium performed a meticulously analysis of the stakeholders participating in two fairs (SICUR and TECNOC & DRONExpo), which was converted into two flash reports (see section **2.3**). The distribution of SICUR and TECNOSEC exhibitors across functional areas, as classified by the EUCS taxonomy (see **Figure 39**), is analysed by focusing on exhibitors at these security fairs exclusively. Security fairs and exhibitions provide a valuable opportunity to bring together solution providers, such as industrial companies, and end-users. The technologies and functions showcased at these events reflect the solution providers' understanding of end-users' needs. A total of 192 exhibitors participated in the TECNOSEC and SICUR fairs, representing EU Member States, the United States, New Zealand, and China.

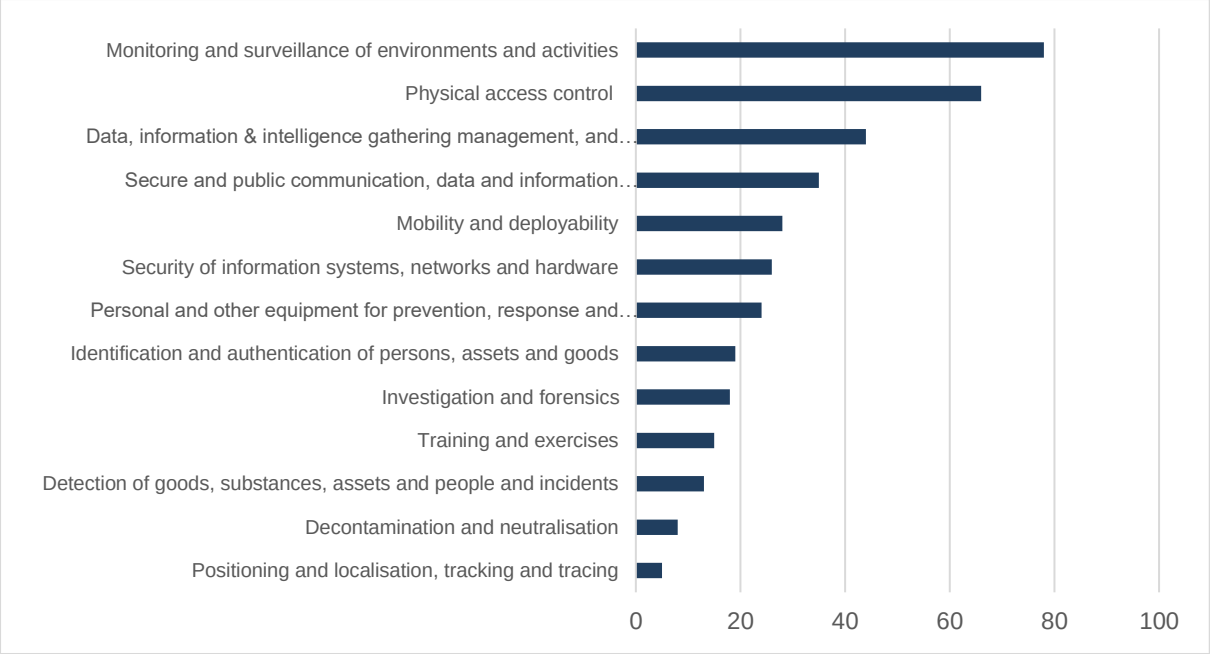


Figure 39 - Mapping of SICUR and TECNOSEC exhibitors' interest areas in the functional areas' domain, according to the EUCS taxonomy.

As regard to the functional areas, a significant number of exhibitors are interested in **monitoring and surveillance of environments and activities**. During the TECNOSEC event, the DRONExpo event was also hosted, which explains the high interest in the drones related function areas, such as **data, information & intelligence gathering management, and exploitation**, **secure and public communication, data and information exchange** and **security of information systems, networks and hardware**. The complementarity between these functions are key enablers for operating drones. The **positioning and localisation, tracking and tracing** function surprisingly shows a substantial lower interest by exhibitors, suggesting drones could be operated in a known area, such as for critical infrastructure or sensible sites protection.

2.5.3.4 Review of Relevant Funding Opportunities

The EU provides several FCT R&I funding opportunities designed to support both end-users and solution providers. The available funding options can be used to facilitate research, development and innovation activities, as well as additional pilots, testing, or procurement of innovative solutions, either individually or in combination.

Table 6 shows the available funding programmes and their respective objectives, identified by combining information from the Funding & Tenders portal with the EUCS Market Segmentation model. These funding opportunities cover a wide range of actions, involving various stakeholders. The funds and mechanisms are managed and allocated in different ways, with three distinct management types:

- **Direct management:** the funding is directly managed by the EC and/or its implementing bodies (Executive Agencies) through a delegated act. For example, the Horizon Europe Programme is under the EC direct management.

- **Shared management:** both the EC and national authorities manage the fund. This management can result in specific calls, managed by the EC, and other by the national authorities. By example, the Internal Security Fund is under shared management.
- **Indirect management:** programmes or parts of programmes fully implemented by national authorities, international organisations or de-centralised agencies.

Table 6 - Other EU funds addressing R&I and procurement in the FCT domain.

Programmes	Details	Scope
Horizon Europe	• A dedicated FCT destination is under the Cluster 3. • Other destination from the Cluster 3, such Border Management, Resilient Infrastructure, Increased Cybersecurity among others, can also contribute to FCT. • Other Cluster, such the Cluster 4 (Digital, Industry and Space) can also include calls relevant to FCT.	R&I
Internal Security Fund	• It aims at increasing the exchange of information between EU law enforcement authorities and enhancing co-operation and cross border operations. • It fosters cross-border cooperation via intensifying cross-border joint operations. • It contributes to the fight against crime via strengthening capabilities to combat and prevent crime and reinforcing protection against terrorism, organised crime and cybercrime.	R&I, procurement and training
Digital Europe	• The Programme is fine-tuned to fill the gap between the research of digital technologies and their deployment, and to bring the results of research to the market. • Among other priorities, the fund aims at support cybersecurity, AI and a wider use of digital technologies.	Bringing innovation to market
Connecting Europe Facility	• This Programme supports the deployment of digital networks, i.e. sustainable and high-capacity projects such as 5G coverage of trans-European corridors and submarine cables. • From the FCT perspective, Digital Europe funds Digital security products and services.	Deployment and financial support to procurement
Border Management and Visa Instrument	• The Fund contributes to securing strong EU external borders, which in turn will allow the EU to maintain a Schengen area without internal border controls. • It aims at strengthening EU capacity for borders and security controls. • It ensures the EU's visa policy continues to evolve and modernise, whilst strengthening security and mitigating irregular migration risks. • It is implementing the new mandate of the European Border and Coast Guard.	Defining priorities and needs, public contracts opportunities
Customs Control Equipment Instrument	• This Programme specifically provides financial support to the customs authorities of the European Union Member States for the transparent purchase, maintenance and upgrade of customs control equipment, including innovative detection technology equipment, such as x-ray scanners, automated number plate detection systems and other non-intrusive soft detection equipment for border crossing points, inland customs offices and mobile customs units as well as a variety of customs laboratory equipment for goods analysis	Procurement and testing
Customs Programme	• It targets primarily the EU and the EU enlargement countries' national customs administrations as beneficiaries. • It provides funding for workshops, collaboration, IT capacity-building, trainings.	Procurement and pilots and prototyping

Programmes	Details	Scope
	• It also provides support to innovation activities, in particular proof-of-concepts, pilot projects, prototyping initiatives, smart data mining and collaboration among systems;	
EU Anti-fraud programme	• The programme promotes activities against fraud, corruption and any other illegal activities affecting the financial interests of the EU through action grants. • It encourages the reinforcement of investigative capability and capacity of Member States, including their digitalisation, in view of stepping up the fight against fraud, corruption and any other illegal activity. • It includes support for specialised training and research activities.	Training and research
Programme for the Protection of the Euro against Counterfeiting	• The programme aims at preventing and combating counterfeiting and related fraud, thus enhancing the competitiveness of the Union's economy. • It targets law enforcement and judicial authorities, banks and others involved in combating euro counterfeiting. • The programme funds staff exchanges, seminars, training courses, studies and the purchase of equipment for third countries.	Training and joint procurement
Union of Civil Protection Mechanism	• The mechanism supports efforts of Member States and additional Participating States to protect primarily people, but also the environment and property against man-made hazards, including the consequences of acts of terrorism, technological, radiological or environmental disasters, among others. • It enables a rapid response, and promotes an effective and coherent approach to prevention of and preparedness for disasters	Knowledge exchange and training, joint procurement

2.5.4 Ethical, Legal, Societal view

2.5.4.1 Summary of ELS View

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. So, one can see that since the design phase of new activities or instruments, ethical and societal concerns are considered, because of regulations already in place or being discussed, or because of scientific results published and largely disseminated in events and in the media.

In the FCT domain, fundamental rights, values and freedoms are constantly in dispute, which leads to a debate marked by continuous assessments of impacts on individuals and groups. With the digitalisation of several practices, the search for a proportional approach when conducting activities in the FCT gains more relevance and urgency, with new interpretations of concepts and consequences, and with a further need for engagement with different stakeholders. ELS applications are now part of any stakeholder involved in the FCT domain. 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.

This conclusion can also be exemplified by the development of the ELS Observatory: at the beginning of the project, the ELS Observatory did not have a lot of high-relevance observations; but with more debates about topics of interest and understanding which topics are relevant to the ELS observatory, in the FCR R&I domain, more observations were added,

reaching 126 high-relevance observations. These annotations have more focused contents and translate topics that could be interesting to the partners and external stakeholders who connected to the project. So, this shows the importance of ethical and legal experts being involved in projects and activities, to guarantee that the concerns related to the impacts on society are part of the daily vocabulary of agents in the FCT domain while developing solutions in compliance to the regulatory framework.

2.5.4.2 Critical Ethical and Societal Issues

Following a tendency already observed in previous years, data exchange still occupies a relevant position in the FCT domain. On the possibilities of data exchange, international cooperation has taken a central role on the possibilities and necessities for investigating and preventing crime, especially **organised crime** and **cybercrime**. Since various illegal actions and organisations are transnational, global cooperation is essential for law enforcement activities. This scenario, however, still faces several challenges, such as guaranteeing the level of protection of human rights in different jurisdictions, lack of trust in new data-based technologies, and observing the necessity of processing data for each purpose. Also, as a global phenomenon, but with different local consequences and understandings, disinformation has been a topic vastly brought to the discussion of societal issues in the FCT domain.

Societal engagement has been brought up as a way of guaranteeing civil representation and safeguarding the interests of different sector of society. From this understanding, forms of evaluating the societal impact of a new procedure or technology is a recurring topic in research material and project results (e.g., human rights impact assessment, societal impact assessment). Practitioners' reports, representing more than half of the high-relevance observations for ELS Observatory, in the other hand, do mention societal impacts periodically. These reports are usually more related to actions and results of operations, technologies and forms of investigation. So, the ELS Observatory is still lacking on more material on how to apply, in practice, forms of assessing societal impacts and guarantee social engagement.

FCT events do tackle ethical, societal and legal topics, but in a more lateral and generalized manner. For the best development of good practices in the FCT domain, it is crucial that more events involving different actors, including ethics and legal specialists and law enforcement agents, are hosted. This conclusion also adds value to the ENACT annual events that aim to be a place of exchange of knowledge and opportunity between various stakeholders.

2.5.4.3 EU and Member States Legal Framework

In the last six months, the AI Act legislative process, including its approval and publishing, should be pointed out as a major development in the EU legal framework. By establishing horizontal rules for different types of AI technologies, the novel regulation brought decisive rules for the use of AI in the FCT domain. Taking into account the relevance of the topic, the AI regulation and use by law enforcement can be found in most of the categories of observation added into the ENACT knowledge hub (policy papers and updates, project results, scientific material, news and media, and others). 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. All in all, considering the prohibitions set by the AI Act, biometric identification and use of biometric data in AI technologies are central themes in the FCT with AI. On this, discussions around prohibited AI practices are of extreme importance to the FCT Community. Understanding limits and

possibilities of different AI solutions and their acceptable and unacceptable uses and risks is part of the interpretation of the AI Act alongside other norms.

Data use, re-use and exchange is a persistent topic in the EU framework, with various novel acts put into place in the last years, particularly with the new developments of the EU Data Strategy[17]. Closely linked to the some of the ethical issues mentioned above, one can notice how current regulations are addressing modern concerns and opportunities, providing ongoing adjustments to the system for the public interest in a broad manner. While regulations still cannot follow the same speed as the development of technologies, regulatory frameworks, in the EU but also globally, are trying to address specific topics with general considerations to protect ex ante certain values. Additionally, it is also possible to verify that regulations not directly focused on law enforcement but do impact the uses, limits and possibilities of equipments, technologies, information exchange, among other practices, thus affecting the daily activities in this domain.

Another relevant regulatory development followed in the last months was the proposal for a Regulation in the EU to establish rules to prevent and combat child sexual abuse. In connection to the relevance of cybercrimes, which are being broadly studied and reported by media and practitioners, the protection of children is of utmost relevance. Nonetheless, once other values and rights could be heavily affected by some of the rules established by the Regulation, media and academic results report risks of possible surveillance mechanisms allowed by this new regulation. Even though the topic in focus is narrow to some extent, it illustrates very well the high concerns related to surveillance mechanisms used in the FCT, but that affect a large group of people.

Organised crimes, tax fraud and money laundry are significant topics, notably by the wider use of cryptocurrencies. Thus, regulatory and international bodies have been working on guides and other normative developments to ensure the security of digital currencies, alongside procedures and instruments to guarantee the legal use of these assets. Here, once again, several rights and interests are considered by possible regulatory developments, particularly the limits to privacy when designing surveillance measures into the digital currencies, and the efficiencies brought to the digitalisation of payments with trustworthy and security embedded in the solutions.

2.5.5 EUCS Taxonomy for ENACT Content Classification

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

[17] **European Data Strategy:** https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

reference taxonomy chosen by ENACT for this purpose is the one elaborated under the **EU Security Market Study**[18] 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 EUCS Taxonomy. Some additional material related to the EUCS Taxonomy was also made available by DG HOME through the CERIS website, including an **EUCS market segmentation model**[19] and an **EUCS taxonomy and taxonomy explorer**[20]. 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, as presented in **Appendix A**.

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.

2.5.6 Highlights

This section provides a roundup of the most recent news, covering developments from the past month, along with a preview of relevant events scheduled for the upcoming month. It also offers a concise overview of the latest updates and opportunities in the near future.

2.5.6.1 Capability Observatory

On 22nd July 2024, Europol released its **Internet Organised Crime Threat Assessment (IOCTA)**[21] report, 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 significantly more challenging. A key finding is the interconnected nature of various criminal activities, such as organised crime,

[18] **EU Security Market Study:** https://op.europa.eu/en/publication-detail/-/publication/db2efbc8-070a-11ed-acce-01aa75ed71a1
[19] **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
[20] **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
[21] **IOCTA 2024:** https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024#downloads

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**[22] 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 of threats underlines the critical need for international cooperation in addressing the evolving 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.

2.5.6.2 Technology Observatory

As the use of AI and machine learning in crime prevention continues to expand, the complexity of combating criminal activities has also increased. AI enables LEAs 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**[23] 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 lLEAs 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 dual 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 FCT.

[22] **FBI's Internet Crime Report 2023:** https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
[23] **Project CT-Tech:** https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech

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**[24], 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**[25] which focuses on highlighting current best practices in digital forensics, the on-going **CYCLOPES** [26] 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**[27] and **CINTiA 2024 ("Criminal Intelligence – New Trends in Analysis Conference 2024)**[28]**.** All of these events highlight a significant emphasis towards digital forensics and analytics.

2.5.6.3 Market Observatory

As listed in **Table 7**, 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.

Table 7 – List of upcoming relevant events within the FCT area.

Event	Date (2024)	Location	Description
SANS Brussels	September 2-7	Brussels	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	September 9-10	London	Drawing on knowledge gained from major Homeland Security experts from key United Kingdom (UK), European and International security organisations, governments, military, police and industry, Counter Unmanned Aerial Systems (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	September 11	Brussels	The Public Security Exhibition (PSE) is co-organised by the Aerospace, Defence, Security & Space (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

[24] **First Report on Encryption:** https://www.europol.europa.eu/publications-events/publications/first-report-encryption
[25] **Forensic Experts Forum 2024 Conference:** https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference
[26] **CYCLOPES project:** https://www.cyclopes-project.eu/events/workshop-enhancing-digital-forensic-investigations-using-osint-cyber-intelligence
[27] **SPIE conference:** https://spie.org/ESI24D/conferencedetails/artificial-intelligence-security-defence
[28] **CINTiA 2024:** https://ppbw.pl/en/cintia-2024-we-are-opening-registration-for-companies/

Event	Date (2024)	Location	Description
			Brussels through Government-to-Government (G2G), EU and North Atlantic Treaty Organisation (NATO) engagements in the security and resilience sector.
Security Essen 2024	September 17-20	Essen	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	September 19-20	Linter	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**[29] community.
International Cyber Expo	September 24-25	London	International Cyber Expo bursts with networking and business opportunities with a highly sophisticated visitor base.
International Security Expo	September 24-25	London	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 fighting crime and terrorism	September 24-25	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.

2.5.6.4 ELS Observatory

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 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.

[29] Hackers are “persons who delight in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.” People who engage in illegal activities like unauthorized entry into computer systems are called crackers and do not have anything to do with hacking. BruCON does not promote any illegal activities and behaviour. Many hackers today are employed by the security industry and test security software and systems to improve the security of our networks and applications. In addition, for the younger generations, BruCON wants to create some awareness and interest in IT students to learn more about IT Security.

3 Assessment of ENACT Product by FCT community

The FCT community's evaluation of the ENACT product provides valuable insights into its effectiveness and relevance. **Table 8** presents feedback from the FCT community regarding ENACT products, capturing evaluations from two respondents for the Analytical Report#1 “FCT R&I: An analysis of EU priorities 2014 – 2024”: one representing a LEA and the other from a policy organisation. In this evaluation, a score of 1 indicates that the report did not address or contribute to the specific topic, while a score of 5 signifies that the report fully addressed or made an excellent contribution to the topic.

The report received the highest ratings for its quality, timeliness, and structure, indicating a solid satisfaction with these elements. However, there was a slightly lower score regarding the report's value to individual organisations and roles, suggesting that while the report is well-received, its direct impact or applicability to specific organisational needs could be improved. These aspects should continue to be prioritised in future reports. The lower scores in perceived value suggest an opportunity to refine the report's content to better meet its audience's specific needs.

Table 8 – Feedback from the FCT community on ENACT products.

Questions	Respondent 1	Respondent 2
Which type of knowledge hub does your organisation belong to?	LEA	Policy Organisation
What is your role within your organisation?	Stakeholder engagement and policy support	Area Coordinator in EC
The quality of the report	5	4
The reliability of the information within the report	5	3
The timeliness of the report	5	4
The format and structure of the report	5	4
The value of the report to your organisation and role	4	3
The value of the report to the FCT security community overall	5	3

One respondent provided insightful feedback on the report, highlighting areas for potential improvement, which will serve as guide for the preparation of future ENACT products:

"The brief has a very comprehensive approach and concrete analysis from time to time in specific capability area.

However, in future analysis some aspects might be addressed differently to ensure the excellent result of the report. In detail:

- *The report is currently using the policy taxonomy as developed under the EU Security Market study which was concluded some time ago. Would you plan in ENACT to update the Policy Taxonomy and take into account latest developments is several areas?*
- *Secondly, the analysis is not able to produce objective view of the EC investments in particular areas, and thus research priorities, as the methodology used states clearly that*

is only looking at the keywords in the text of the call, without putting any weight to it, thus variation in languages such as must, have to, should, may play no importance in the analysis. Would you plan to include such aspect and level of variation in future analysis?

- *Thirdly the analysis is not taking into account whether the problem was solved (addressed by a successful proposal) or not, thus reappearance of the problem in the next call might lead to wrong messages if projects are not taken into account. Any views on including results of the work of existing projects in those dedicated areas?"*

Based on this feedback, we will consider updating the policy taxonomy to reflect recent developments, incorporate variations in language from EC calls to provide a more objective view of investments, and include information on the outcomes of existing projects to offer a more comprehensive analysis.

Moreover, further feedback with a larger sample size would be beneficial to validate these initial findings and guide future improvements. To obtain more reliable validation of ENACT products, we will enhance our liaison activities to gather additional feedback from the FCT community on the prepared products.

4 Looking Ahead: ENACT Directions and Impact

The ENACT is engaged in the broader FCT through knowledge communication, dissemination and exploitation, contributing to larger societal goals of this theme. The ENACT products developed, rigorously evaluated, and refined during this phase have effectively provided actionable insights and strengthened connections within the European FCT ecosystem, supported by systematic methodologies and collaborative engagement.

Currently, the Consortium is finalising three additional flash reports on different thematic, and working on disseminating the stakeholder map, periodic FCT map, and the first annual SoP policy report, which we done using the working templates design and leveraging ENACT communication channels. All the outputs will be presented at the ENACT Annual Event 2024, held hybrid in Lisbon on September 20th and online.

Moving forward, the feedback gathered during this first batch of network outputs will be crucial in guiding the following batch of network outputs. Furthermore, the inputs from the assessment of ENACT products by the FCT community highlight the importance of tailoring future reports to better meet the specific needs of various stakeholders, ensuring that the content is not only informative but also directly applicable to their unique challenges. As done during the test implementation cycle, feedback from the stakeholders on the quality, usefulness and timeliness of the delivered products will continue to be gathered during the full implementation cycles. Based on the feedback received, the methods, processes and tools employed will be adapted as needed in order to maximise the relevance of ENACT outcomes.

By addressing these areas for improvement, the ENACT Network will continue to grow as an essential resource, further advancing the EU's efforts in combating crime and terrorism, and making a significant contribution to the broader security landscape.

Appendix A – EUCS Taxonomy

The EUCS Taxonomy aims to create a common language or harmonised terminology, as well as a comprehensive categorisation, for security products and services. The taxonomy provides a comprehensive and detailed reference built around three dimensions: the four **security areas** (Level 1) with their respective sub-areas (Level 2 and Level 3), the **security functions** that a given product or service enables or supports (i.e., functional areas) and the list of over 500 **products and services** grouped in technology areas in three levels aggregation. The Level 1 of security area is fixed in FCT. The following tables show the FCT policy dimension (Level 2 and Level3), the functions dimension and the high-level areas of the technology dimension.

A.1 FCT Taxonomy – Policy Dimension

FCT Policy Sub-area (Level 2)	FCT Policy Sub-area (Level 3)
Organised Crime	Counterfeit goods and documents
	Environmental crime
	Economic crime, corruption and fraud
	Trafficking of humans and goods
	Cargo crime
	Organised property crime
Terrorism and radicalisation	Terrorism financing
	Protection of public spaces
	Radicalisation
	Explosives and explosive precursors
	CBRN Threats
Cybercrime	Child sex abuse
	Online identity theft
	Dark net (cryptocurrency)
	Digital forensics
	Non-cash payment fraud
	Attacks to information systems
	Threats to encryption and 5G
Horizontal and societal issues	Petty crime
	Domestic violence and sexual violence
	Disinformation and fake news
	Hate speech
	Conventional forensics
	Travel intelligence (PNR)
	Youth criminality
	Community policing

A.2 FCT Taxonomy – Function Dimension

High Level Security Functions	Description
Personal & Other equipment for prevention, response and recovery	PPE vehicles, platforms and other equipment for: • first responders during incident response and recovery. Includes special land vehicles, such as armored vehicles, water cannon systems, etc.; aircraft (planes, helicopters) and unmanned flight vehicle systems (UAVs); ships and boats for use by coast guards; emergency equipment such as power generation, temporary shelters, specialist search and rescue equipment (other than for positioning and localisation of persons) (see 'decontamination, and neutralisation for more) • regular security operations (police patrolling, civil protection operations border management), including equipment for deterrence / prevention, e.g. non-lethal weapons, guns, etc.), • Emergency medical support, psycho-social support services.
Data, information & intelligence gathering management, and exploitation	Collection, processing, analysis, management, exploitation and dissemination of data, information and intelligence (e.g. Data fusion techniques including mining, trend detection and optimization analysis) to support, inter alia: • Information analysis for intelligence functions, such as counter-terrorism and criminal intelligence (includes systems that enable / support pre-processing of large amounts of data for law enforcement purposes); intelligence for facilitation of travel at border crossing points, i.e. traveller / passenger facilitation, customs risk management systems; • Information management for command & control to facilitate common operational picture between different security actors (within and between departments, regions, nations); • _Information support for situational awareness and (intelligent) decision making including through planning and risk assessment, e.g. forecasting, vulnerability and risk and cascading effects assessments, etc.; • _Digital forensics, including to track and trace criminal actions in information networks; • IT security incident management
Monitoring and Surveillance of environments and activities	Large/wide area surveillance of people and vehicles in specific environments (e.g. marine / maritime, air, land/rail borders). Includes monitoring and surveillance of: • Large and small fast boats and underwater vehicles at blue borders; • Manned and unmanned vehicles (air surveillance), e.g. UAVs, light aircraft (linked to ATM systems); • Movement of people and land-based vehicles at regulated and unregulated land borders; • Remote detection of shipping containers Localised / small area surveillance of people, equipment and vehicles in controlled areas such as facilities, critical infrastructure, urban areas, transport and logistic hubs, seaports and harbours, airports and other specified locations. Includes video and other observation and surveillance systems, such as CCTV and video analytics, etc. • Seismic, meteorological, biological and epidemiological monitoring to predict and detect geological hazards, weather-related hazards, dangerous pandemics, etc. CBRN monitoring in Seveso sites. Also includes monitoring of air / water, etc for early detection of CBRN contaminants.
Security of information systems, networks and hardware	Digital systems / Information and Communications Technology (ICT) hardware, systems and networks, software and hardware security engineering. Includes products for: certification, electronic seals, cryptography, data security and privacy, data loss prevention, data recovery solutions, security of AI systems; use of AI systems to get access to information (security of data mining technologies); infrastructure for secure data storage. Anomaly detection systems, intrusion detection systems; network monitoring systems; malware detection. If we discuss e-access control here, biometrics are missing.

High Level Security Functions	Description
Physical access control (of locations, goods, etc.)	Mechanical access control, barriers, enclosures and physical resilience systems and devices. Includes locks and locking systems, safe, strong boxes, armoured and fire-resistant doors, mechanical seals (and electronic seals without tracking), physical perimeter barriers (e.g. fencing and other security barriers), blast proofing, CCTV systems, etc.
Identification and authentication of persons, assets and goods (Other than for tracking and tracing)	Identification, authentication and verification of: • persons for protection against identity theft and fraud, identity management, passenger travel security and verification (e.g. smart cards, biometrics, PIN and chip cards, identity cards, passport systems etc.), • persons for secured access control to buildings and other designated secure areas (sites and places) such as airports and seaports. • persons in crowded spaces (i.e. identification of searched individuals in crowds); • goods and documents to protect against forgery and counterfeiting. • dangerous or illicit materials and substances (drugs, explosives, CBRN) [Note: Distinction with CBRN / dangerous substance detection: identification occurs after a broad substance type has been detected for early warning, a more precise check is done to identify substance type, source: ESRAB]. • assets (ships, aircraft) for transport tracking and facilitation in support of sea, land, and air surveillance (includes e.g. automated number plate / container number recognition systems for vehicles / cargo).
Detection of goods, substances, assets and people and incidents	Detection and screening for dangerous/hazardous or illicit goods and substances: • Detection of weapons, explosives, drugs, contraband, Radiation and nuclear materials), including screening of passengers, luggage, cargoes, post and parcels, vehicles etc. • Detection of hidden/concealed persons and substances hidden within persons. • Specialised detection for CBRN substances and agents. Detection of vehicle movements, personnel, abnormal behaviour and other potential threats in specific environments (e.g. marine / maritime, air, land/rail border, critical infrastructures, public spaces, crowds, etc.); • Detection of large and small fast boats, underwater vehicles, swimmers in ports and harbours and wider maritime environment; • Detection of manned and unmanned vehicles, e.g. UAVs, light aircraft • Detection of people trying to enter [the EU territory] illegally • Intruder detection / illicit access to buildings (detection of unwanted entities in close proximity to critical infrastructures) • Detection of abnormal behaviour patterns of individuals or groups of individuals (terrorist, criminal behaviour) • Detection of abnormal behaviour patterns of vehicles and goods (in terms of their trajectory on the outside of critical infrastructures). • Intruder detection / illicit access to buildings (detection of unwanted entities in close proximity to critical infrastructures) • Detection of water contamination • Remote detection of illicit access to pipelines • Detection of people and contaminated environments in case of a crisis or security incident. Includes, inter alia: • Detection of people (wounded, injured, buried alive, etc.) • Detection of ill and/or infectious persons • Detection of contaminated environments • Detection of contaminants in supply networks (e.g. water system contamination) Detection of security / crisis incidents for early warning (e.g. Incident detection systems for fire, gas leaks, smoke alarms, etc.)
Positioning and localisation,	Positioning, localisation and tracking of platforms, goods, cargo containers, vehicles (including ships, aircraft), people and inventories:

High Level Security Functions	Description
tracking and tracing	• Localisation and tracking of goods, containers and vehicles in an area (e.g. bar codes, applications that secure integrity of cargo containers such as electronic seals with tracking/positioning such as GPS, RFID…) • Tracking of containers and goods in wide open areas • Tracking and tracing of hazardous substances (and components for substances) and devices (e.g. weapons, explosives, CBRN agents such as radioactive materials, hazardous chemicals) • Control of property change of chemicals to preclude misuse [source: ESRAB] • Positioning, localisation and tracking of persons (personnel movements), emergency services, inventories and aid relief in crisis situations • Observation and localisation of individuals through sub-terrain, debris, fixed structures (walls, metal, etc.). Includes detection and localisation of victims (wounded, buried alive, etc.) in a crisis incident.
Mobility and deployability	Mobility and deployability of people, assets, equipment for / in: • regular security operations (border management, customs, law enforcement / police patrolling, civil protection, etc.). • security incidents / crisis events (i.e. incident response), including management of resources and distribution logistics.
Investigation and forensics	Tools, forensic equipment and systems, etc. to investigate a security threat event (e.g. to develop 'post event' intelligence to identify perpetrators and collect information for eventual legal proceedings etc., the origin of natural disasters, industrial accidents, etc. (Excluding for digital forensics; see 'Data, information & intelligence gathering management, and exploitation').
Decontamination and neutralisation	Decontamination of ill / contaminated persons and environments (large areas and sites), reagents. Neutralisation of perpetrators and devices (including explosives, CBRN and firearms) and effects of a security / crisis incident: • Containment (limitation) of impacts/effects of terrorist device on the environment by isolation shielding material, handcuffs, explosive neutralisation, etc., • Removal of threats (e.g. extinguishers, specialised robots, …), etc., • Restoration and recovery of basic services (e.g. water, communication, energy, etc.), including service/business security (see also cyber – data recovery).
Secure and public communication, data / information exchange	Secure and interoperable communication and information systems for use in • crisis situations (e.g. by police, customs, emergency responders, private security services, etc.), • tactical communications • regular security operations (border surveillance, police patrolling, civil protection operations). Communication equipment and systems for public information management and situation alert (e.g. public information broadcasting, specialised apps, sirens, …)
Training and exercises	Training, virtual reality, emergent reality, workshops, exercises and drills. Includes training platforms and facilities with use of scenario and situation modelling, computer aided training, simulation systems, etc. Cybersecurity education and training (e.g. on how to use tools, human aspects, security management and governance, trust management and accountability)

A.3 FCT Taxonomy – Technology Dimension

Technology area L1	Definition	Technology area L2
Access control/authorisation	Access control systems ensure that access to assets [or places] is authorised and restricted or limited to	Access control/authorisation (building access, system access, etc.)

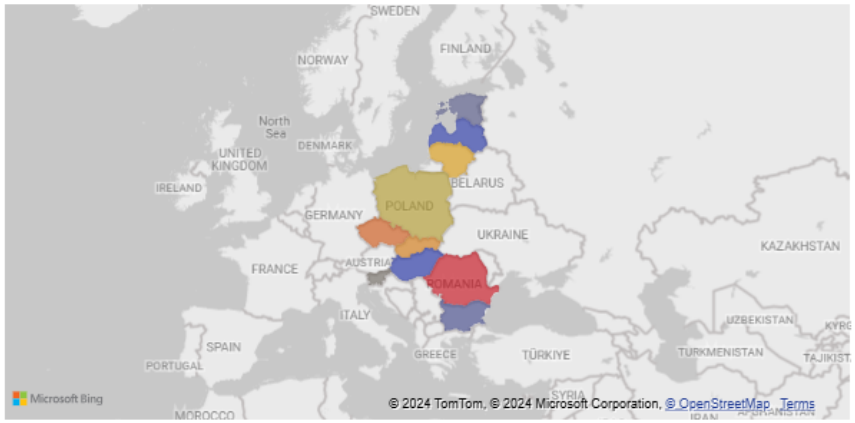
Technology area L1	Definition	Technology area L2
(building access, system access, etc.)	identified and verified persons or vehicles only, based on business and security requirements. Authentication systems provide assurance that a claimed characteristic of an entity is correct.	Identification and authentication of persons
		Identification and authentication of documents and objects
Alarm/warning systems	System to detect and indicate the presence of a [person/object/element] or occurrence of an event [disaster/emergency situation] to an alarm zone and giving signals for appropriate action, including alarms/ warning systems for disasters/ natural hazards.	Alarm/warning systems
		Alarm/warning systems
		(Perimeter) Intrusion detection/alarm systems
		Other uses
Data analytics	Data analytics is used to understand objects represented by data (3.1.5), to make predictions for a given situation, and to recommend on steps to achieve objectives. The insights obtained from analytics are used for various purposes such as decision-making, research, sustainable development, design, planning, etc	Data analytics
CBRNE detection and neutralisation products	Tools/products/technology with the ability to detect the presence or use of chemical, biological, radiological, nuclear and explosive (CBRNE) materials at points of manufacture, transportation, and use	CBRNE detection and neutralisation products
		Containment equipment (to prevent unintentional exposure to pathogens, toxins)
		Neutralisation/decontamination solutions
		Detection (Radiation survey meters, dosimeters, etc.)
Data storage and exchange	Systems and tools related to the organisation and exchange of data.	Data storage and exchange
Digital forensics	Scientific tasks, techniques, and practices used in the investigation of stored or transmitted binary information or data for legal purposes	Digital forensics
Digital security products and services	Resources and tools used to secure and protect online identity, data, and other digital assets and technologies	Digital security products and services
		Integrated product security functions
		Code/malware detection and analysis
Facilitation systems and secure databases	Services and facilities related to easing/facilitating the process of a traveller from their point of origin to the destination in a secure way.	Facilitation systems and secure databases
General equipment	Equipment used to support the operations of personnel in civil security.	General equipment
		Vehicles (excl. UAVs, only including vehicles which transport people)
		Logistics & utilities
		Energy

Technology area L1	Definition	Technology area L2
Guarding and physical protection (non-human)	Intended to delay, stop, or guide people, or to provide protection against hazards.	Guarding and physical protection (non-human)
Internet-based investigation	Tools and methods used for online investigations	Internet-based investigation
		Online investigation tools
		Online search tools
		OSINT tools
Laboratory equipment for gathering and forensic analysis of samples	Tools and equipment used by scientists who work in a laboratory	Laboratory equipment for gathering and forensic analysis of samples
Healthcare / medical equipment	Equipment used for health and medical diagnosis and treatment following disease or injury	Healthcare / medical equipment
Monitoring tools and services	System/tools that constantly check/survey people, places and objects which may also provide alerts or alarms and collect data for evaluation	Monitoring tools and services
		Health / Diseases and epidemiological monitoring systems and tools
		Weather/meteorological monitoring systems
		Land/environment/geography
PPE/Safety equipment	Device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards	PPE/Safety equipment
		Protective clothing (protective garments, protective footwear, hand protection)
		Protective equipment (head, face, eye, respiratory)
		Physiological monitoring
Screening & detection	Tools and devices used to screen and detect risks and threats related to people or objects	Screening & detection
Search devices and tools	Tools and devices used to search [for] people or objects	Search devices and tools
Specialised management & control systems	Specialised management & control systems	Specialised management & control systems
		Management systems
		Decision support/forecasting
		Operating systems
		Command and control
Surveillance systems	System consisting of (camera/video/sensing) equipment, monitoring and associated equipment for transmission and controlling purposes, which may be necessary for the surveillance of a protected area	Surveillance systems
		Unmanned systems (platforms, vehicles)
Tracking, navigation and guiding systems, equipment and tools	Systems / technologies which enable the collection of geospatial data regarding a specific individual, object or area to determine the exact place of a person or entity. Tracking systems / technologies monitor the physical location of a person or entity; tracking technologies can also be used for determining who was in a geographic area [...] at a particular time". Note:	Tracking, navigation and guiding systems, equipment and tools

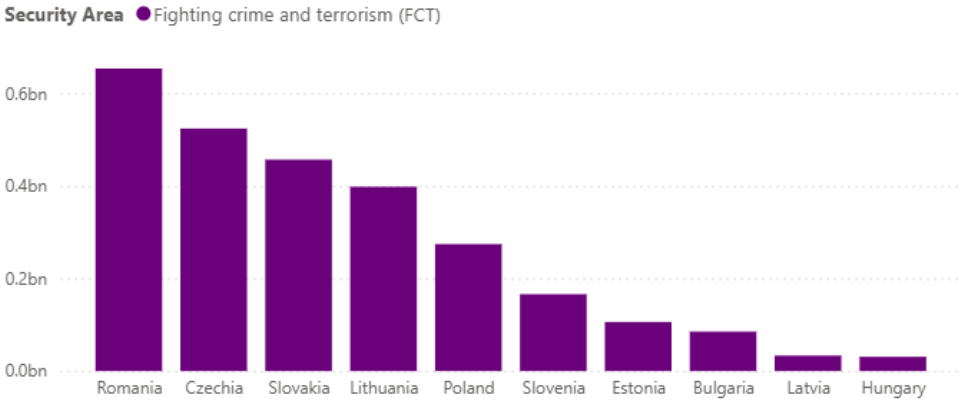
Technology area L1	Definition	Technology area L2
	overlaps with surveillance and monitoring.	
Training & Simulation	Tools and service	Training & Simulation
		Training platforms and systems
		Simulation tools
		Thematic training
Conflict management / Use of force	Objects or devices designed or that can be used for inflicting bodily harm or physical damage.	Conflict management / Use of force
		Lethal weapons
		Non-lethal weapons
Critical communications, Interoperable communications	Systems and technologies that ensure the ability to maintain communications, information sharing and diffusion across diverse systems and organisations (public safety actors, emergency / first responders, etc.) and wit the public in any environmental condition. with responders in any environmental conditions.	Critical communications, Interoperable communications
		Communications systems and networks
		Communications devices (radio-based, wireless)

Appendix B – Eastern countries item costs for the 2015 to 2020 period

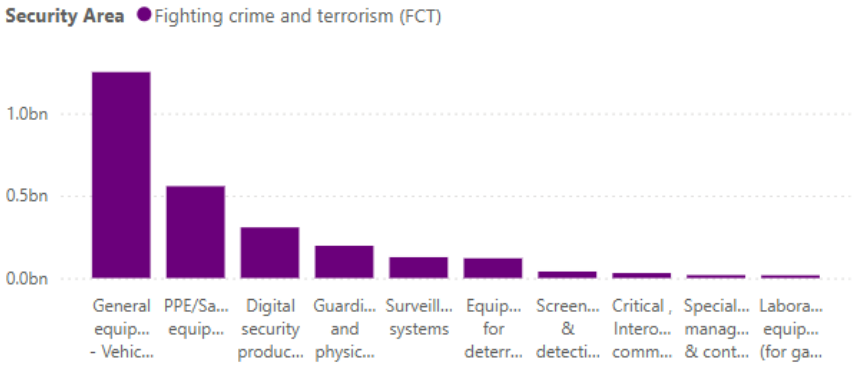
European Countries where money is spent on civil security



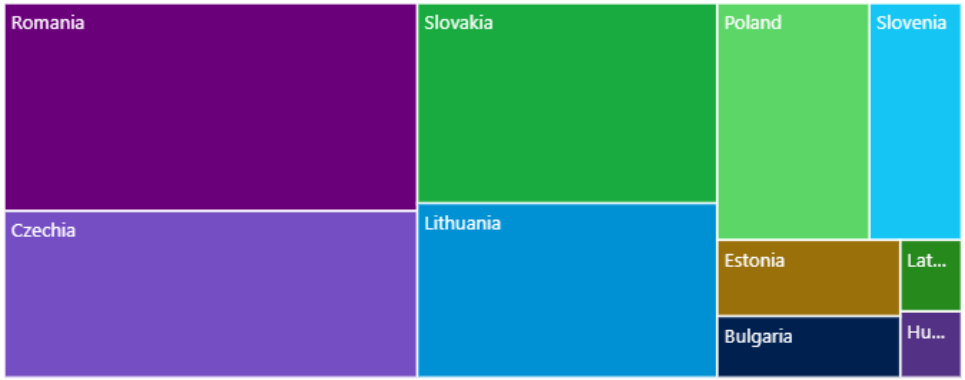
Security Area Spending per Funding Source



Security Area Spending for top 10 P&S categories

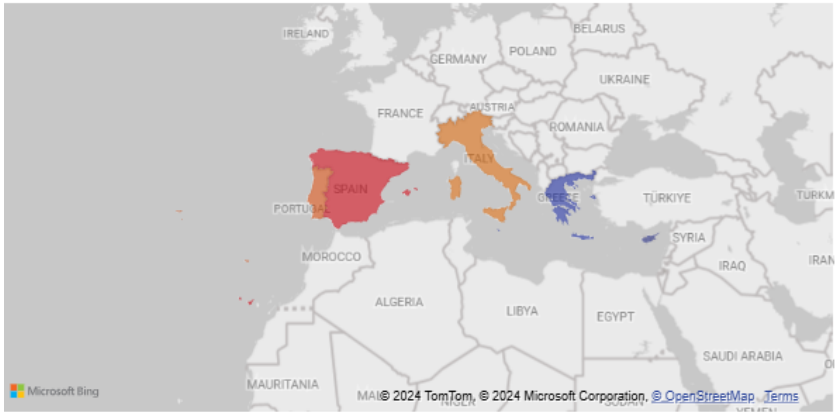


Spending Amount per Funding Source, Security Area and P&S

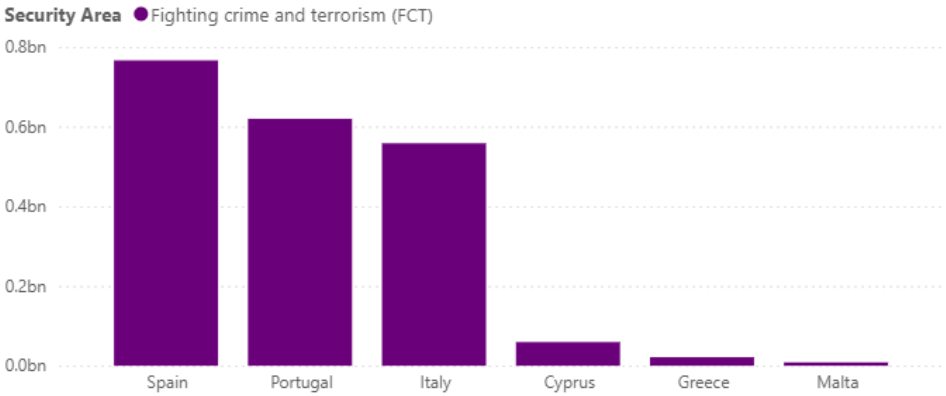


Appendix C – Southern countries item costs for the 2015 to 2020 period

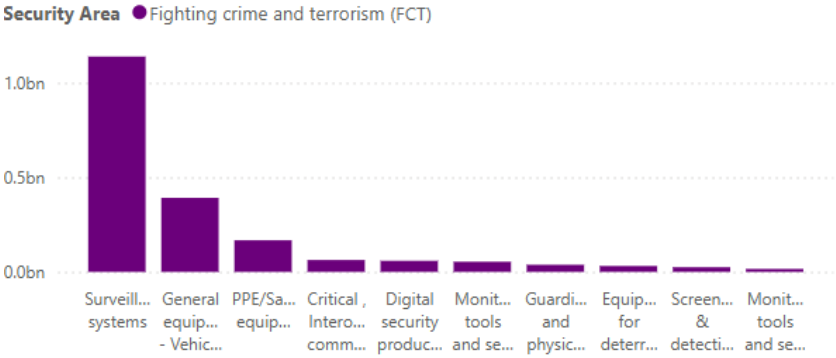
European Countries where money is spent on civil security



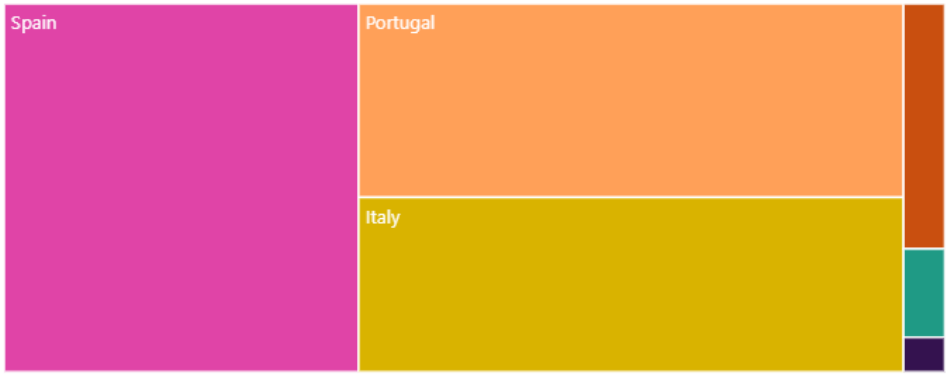
Security Area Spending per Funding Source



Security Area Spending for top 10 P&S categories



Spending Amount per Funding Source, Security Area and P&S



Appendix D – Summarising table of the variation per costs items from 2015 to 2020

	Total	2015		2016			2017			2018			2019			2020		
		Spent	Rank	Spent	Rank	Variation	Spent	Rank	Variation	Spent	Rank	Variation	Spent	Rank	Variation	Spent	Rank	Variation
General equipment and vehicles	2.47	0.25	3	0.22	3	↘	0.64	1	↗↗↗	0.5	2	↘	0.48	2	↘	0.38	1	↘
Surveillance systems	2.303	0.36	1	0.083	4	↘↘	0.14	5	↗↗	0.58	1	↗↗↗	0.96	1	↗↗	0.18	2	↘↘↘
PPE/Safety equipments	1.55	0.32	2	0.26	2	↘	0.57	2	↗↗	0.17	4	↘↘	0.12	5	↘	0.11	4	↘
Digital security products and services	1.01	0.024	8	0.39	1	↗↗	0.15	4	↘↘	0.135	6	↘	0.24	4	↗	0.071	5	↘↘
Guarding and physical protection	1.373	0.49	6	0.053	5	↘↘	0.18	3	↗↗	0.14	5	↘	0.39	3	↗↗	0.12	3	↘↘
Equipment for deterrence/ prevention	0.869	0.52	5	0.033	6	↘↘	0.10	6	↗↗	0.067	8	↘	0.11	6	↗	0.039	6	↘↘