ANALYTICAL REPORT 03

INTERNAL SECURITY FUND: ANALYSIS OF EU MEMBER STATE PRIORITIES

A report produced by the ENACT Consortium

Main Authors

Dimitra Graikini (VICOM)

David Ríos Morentin (VICOM)

ENACT.
European Network Against Crime and Terrorism

ABOUT ENACT

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

The project aims to satisfy two major ambitions,

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

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

Funded by
the European Union

DISCLAIMER

COPYRIGHT

04

EXECUTIVE SUMMARY

The Internal Security Fund (ISF) is a critical financial instrument that supports EU Member States in preventing and combating serious cross-border crime, cybercrime, and terrorism. The largest share of the fund is dedicated to the National Programmes, which are implemented under a shared management framework between the European Commission and the national authorities of the Member States.

Under this framework, Member States are responsible for selecting projects, allocating funding, and managing day-to-day implementation. The priorities in these programmes align well with the security challenges faced by each EU Member State and their capability and capacity-building needs. In this regard, the ENACT network has produced the present report to extract, structure and analyse the Fight against Crime and Terrorism (FCT) priorities articulated within the initial 2021-2027 National ISF Programmes.

The methodology involved extracting planned actions from the official documents and systematically mapping these priorities to the EU Civil Security (EUCS) Market Taxonomy. This mapping was structured across three core dimensions: Policy, Functions, and Technology. The findings highlight a dominant policy focus on building threat-agnostic infrastructure, while operationally, Member States heavily prioritise data and intelligence management functions. Technologically, we have a strong, unified consensus on investing in secure data storage and exchange systems.

Ultimately, the analysis reveals a clear strategic shift across the European Union towards intelligence-led policing models, characterised by growing investment in data-centric capabilities, digital infrastructure, and the disruption of organised crime. This direction closely aligns with broader European Research and Innovation (R&I) trends.

ACRONYMS

ARAS	Lithuanian Counter Terrorism Unit
BMVI	Border Management and Visa Instrument
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CCI	Common Identification Code
CL3	Cluster 3
DG HOME	Directorate General Migration and Home Affairs
EU	European Union
EUCS	European Union Civil Security (taxonomy)
FCT	Fighting Crime and Terrorism
GNR	Guarda Nacional Republicana (Portugal)
IBMF	Integrated Border Management Fund
ISF	Internal Security Fund
LEA	Law Enforcement Agency
NFI	Netherlands Forensic Institute
NICC	National Institute of Criminalistics and Criminology (Belgium)
PNR	Passenger Number Record
PPE	Personal Protective Equipment
PSP	Policia de Segurança Pública (Portugal)
R&I	Research and Innovation
SEF	Serviço de Extrangeiros e Fronteiras (Portugal)
SIS	Schengen Information System
SO	Specific Objective

06 REPORT OBJECTIVE

This report presents an analysis of the Fight against Crime and Terrorism (FCT) priorities identified in the initial 2021–2027 Internal Security Fund (ISF) National Programmes of EU Member States. It examines the main policy areas, operational functions and technology priorities reflected in these programmes and maps them against the EU Civil Security (EUCS) Taxonomy.

By comparing these findings with broader European research and innovation trends in the FCT domain, the report supports a better understanding of Member State capability needs and strategic priorities. The analysis also provides an evidence base for identifying future research priorities and areas that may require further attention from policymakers, security authorities, technology developers, researchers and civil society.

DISCLAIMER ON THE USE OF AI

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

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

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

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

07 INTRODUCTION

The Internal Security Fund (ISF) is a critical financial instrument established by the European Union to ensure a high level of security within its borders.[1] Its primary purpose is to facilitate the prevention and combat of cross-border, serious, and organised crime, including terrorism and cybercrime, while also supporting and protecting victims of crime and addressing security-related incidents, risks and crises. In the previous programming period (2014-2020), the ISF was divided into two distinct components: ISF Borders and Visa, and ISF Police. In turn, for the current programming period (2021-2027), the structure has been refined. The ISF now operates as a standalone fund with a more cross-cutting approach. At the same time, border management is handled by the separate Integrated Border Management Fund (IBMF) through the Border Management and Visa Instrument (BMVI).

The overall implementation of the Internal Security Fund (ISF) is divided between centrally managed components (implemented under "Direct" or "Indirect Management" by the European Commission) and a "Shared Management" component implemented through the ISF National Programmes. A portion of the budget is administered centrally by the European Commission under "Direct Management", whereby the Commission is responsible for launching calls, selecting projects, awarding funding and overseeing implementation. This component primarily supports Union-wide actions, emergency assistance, and specific transnational projects. In addition, certain activities may be implemented under "Indirect Management", in which the Commission entrusts specific budget implementation tasks to EU agencies (e.g., Europol, eu-LISA), international organisations, or other designated entities, while retaining overall responsibility for the use of Union funds. However, most of the funds operate under a "Shared Management" model, implemented through the ISF National Programmes. Under this arrangement, Member States are responsible for selecting, managing and monitoring projects within the framework of their approved national programmes, whilst the European Commission provides strategic oversight and assurance of compliance with EU rules. These programmes are essential because they provide targeted financial support that complements national budgets, enabling Member States to invest heavily in resource-intensive security infrastructure, advanced technological systems, and specialised capacity-building initiatives.

Since the present analysis examines Member State priorities as articulated in these programmes, it **focuses exclusively on this Shared Management framework**. Under this decentralised approach, Member States manage their allocated resources directly to suit their specific national security landscapes.

[1] https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/internal-security-fund_en

To ensure a harmonised approach to security funding across the EU, all ISF National Programmes follow a standardised eight-section structure. While Section 1 establishes the strategic baseline and Sections 3 through 8 address administrative governance, covering financing plans, fundamental rights compliance, and partnership involvement, the substantive core of the programme resides in **Section 2.**

08

This section defines the actionable measures through three primary **Specific Objectives (SOs)**:

- **SO1 - Information Exchange**: Increasing the flow of data among EU law enforcement, competent authorities, and relevant EU bodies. This includes ensuring the interoperability of large-scale EU information systems and improving overall data quality. The goal is to provide frontline officers and investigators with rapid, secure access to critical intelligence across borders.

- **SO2 - Cross-Border Cooperation**: Intensifying joint operations related to terrorism, serious organised crime, and cybercrime. This objective focuses on facilitating multi-agency efforts, such as Joint Investigation Teams (JITs) and alignment with EU policy cycles like EMPACT. It provides the necessary backing to build trusted networks and coordinate law enforcement responses to threats that span multiple jurisdictions.

- **SO3 - Strengthening Capabilities**: Supporting efforts to combat crime and radicalisation while managing security-related incidents and risks. This covers the practical enhancement of law enforcement toolkits through specialised training and the procurement of advanced technological, physical, and forensic equipment. It also extends to the protection of public spaces, critical infrastructure resilience, and support frameworks for victims of crime.

To translate these strategic goals into measurable outcomes, Section 2 requires Member States to define Output and Result Indicators[2] alongside an Indicative Financial Breakdown[3] that categorises expenditure by "Type of Intervention." This financial categorisation is further refined by various funding modalities designed to align national initiatives with broader EU-wide priorities. Most notably, these include:

- **Regular Actions**: Standard national projects funded under the basic allocation to meet national priorities.

- **Specific Actions**: Transnational projects with high EU added value involving cooperation between multiple Member States.

- **Annex IV Actions**: High-priority Union topics, such as radicalisation and IT interoperability, which are incentivised by an increased 90% co-financing rate.

- **Operating Support & Emergency Assistance**: Funding dedicated to the maintenance of critical systems and the rapid response to unforeseen crises.

[2]Annex VIII of Regulation (EU) 2021/1149 (Core performance indicators, encompassing Output and Result Indicators). Available at: https://eur-lex.europa.eu/eli/reg/2021/1149/oj/eng
[3]Annex VI of Regulation (EU) 2021/1149 (Types of Intervention nomenclature used for the Indicative Financial breakdown). Available at: https://eur-lex.europa.eu/eli/reg/2021/1149/oj/eng

Underpinning these modalities is a uniform list of eleven Intervention Codes (001-011)[4] which dictate the tangible outputs of the programme, ranging from technological infrastructure and data quality to human capital development through training and expert deployment.

09

By leveraging this highly structured framework, the Shared Management model fosters a multi-agency environment.
National law enforcement and specialised security agencies remain the primary beneficiaries of the fund. This broad group may include, depending on the priorities defined in individual National Programmes, traditional bodies like national police forces, border guards and customs administrations (e.g., the Czech Police and Customs Administration, and Portugal's GNR, PSP and SEF). Furthermore, the funding may support highly specialised units, such as Counter-Terrorism Teams (e.g., Lithuania's ARAS Unit and Hungary's Counter-Terrorism Centre), Cybercrime Bureaus, Asset Recovery Offices and Financial Intelligence Units. In addition, forensic, academic and research institutions may also benefit from the fund, as scientific advancements in crime detection are a major ISF focus. Stakeholders in this category may include national forensic science institutes (such as the Netherlands' NFI, Belgium's NICC, and Slovakia's Forensic Institute). Academic and research centres are also active partners, often through Specific Actions,[5] supporting Member State authorities in developing new policing technologies and cybersecurity tools (e.g., Cyprus's KIOS Research and Innovation Centre, and Greece's Foundation for Research and Technology). To manage security incidents and protect critical infrastructure or public spaces, the ISF may also support the involvement of civil protection and emergency responders, including fire and rescue services, civil defence forces, and multidisciplinary coast guards. In addition, the broader criminal justice chain is integrated into the ISF framework to ensure operational cohesion. Notably, this includes Ministries of Justice and penitentiary institutions, which play a crucial role in initiatives aimed at preventing radicalisation within prisons and managing the execution of penalties. Finally, civil society, non-governmental organisations, and regional/local authorities are essential stakeholders for grassroots crime prevention and victim support, while the private and business sectors are engaged due to their expertise in research and development, protecting critical infrastructure and combating cybercrime.

Despite the clear overarching objectives established by the ISF, the National Programmes act primarily as forward-looking projections formulated at the beginning of the funding period. To maintain flexibility in planning and resource allocation, Member States typically rely on broad generalisations rather than providing explicit, granular details regarding their exact technological and functional priorities. Nevertheless, these programmes offer a unique window into the strategic needs and primary capability concerns of EU Law Enforcement Agencies (LEAs). To leverage this resource effectively, it is necessary to extract and structure these generic requirements into a standardised format. Doing so enables robust analysis and allows for meaningful comparisons, whether between different Member States, across objectives, or regarding the alignment between ISF priorities and Research & Innovation (R&I) trends. Ultimately, structuring this data provides a vital evidence base to support decision-making for the future programming of EU funds.

[4] Annex VI, Table 2 ("Codes for the Type of Action dimension") of Regulation (EU) 2021/1149. Available at: https://eur-lex.europa.eu/eli/reg/2021/1149/oj/eng

[5] Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund for the duration of the multiannual financial framework 2021-2027 provides that Member States may receive funding for specific actions in addition to their initial allocation under their respective programmes. Specific actions fund transnational or national projects that bring added value in accordance with the objectives of the Fund/Instrument and the priorities of the Union, as for example, actions focused on innovation uptake.

In this view, this report presents an analysis carried out by ENACT security research experts on the Fight against Crime and Terrorism (FCT) priorities extracted from the initial National ISF Programmes.

The scope of the analysis is to identify the main knowledge areas addressed by these national priorities and map them systematically to the categories of the EU Civil Security (EUCS) Market Taxonomy.[6] This mapping is evaluated across three dimensions: Policy, Functions and Technology.

Therefore, the primary objectives of this report are to:

- Provide structured historical data to the EU FCT stakeholder community in order to understand the national priorities of EU LEAs and support decision-making for future investment and capacity building.

- Establish a common methodological baseline to assist in the future comparison of what was planned in the National Programmes versus what was actually achieved by the end of the 2027 period.

- Support EU policy-makers with quantitative evidence in the evaluation of the investment carried out under the current Multi-Annual Financial Framework and in the decision-making processes for the next one, both in relation to ISF funding and R&I funding.

- Showcase the practical value of the EUCS Taxonomy, developed with the support of the Commission and EU Agencies experts under the EU Security Market Study 2021.

- Provide a foundation for future analyses, including the quantification of FCT priorities, the evolution of these priorities over time and the identification of key blind spots.

[6] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en

11 METHODOLOGY

NATIONAL PROGRAMMES COLLECTION AND VALIDATION

Each National ISF Programme was verified to ensure that the collected documents corresponded to the official and most recent versions published by the competent national authority. Programmes were primarily sourced from the official websites of the managing authorities, as designated by the European Commission, which lists the official Funding Contacts for each Member State, including the authority responsible for the ISF and its publication (European Commission, Funding Contacts[7]). In cases where the authors of this report could not find or had doubts about the latest publicly available version, the managing authority was contacted directly to obtain the document.[8]

Each programme's CCI (Common Identification Code) number was recorded as an official identifier included in the programme documentation and used as a consistency check, ensuring that the document referred to a recognised National ISF Programme for the respective Member State. The structure and content of each document were reviewed and compared with other Member States' programmes to assess completeness and consistency.

The collection and validation process was informed by the programme structure and reporting requirements established under Regulation (EU) 2021/1060 (Common Provisions Regulation), in particular Article 22,[9] and Regulation (EU) 2021/1149 establishing the ISF, in particular Article 3,[10] which served as the reference framework for identifying and verifying the National Programmes.

Finally, the version, publication date and retrieval date were recorded to ensure that the latest available version as of 15 December 2025 was used. A list with all the links to the publicly available ISF programs of each Member State is included in Annex A.

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

[8] The relevant authorities in Finland and Malta were contacted to confirm the most recent versions of their National ISF Programmes. While Finland provided confirmation, no response was received from Malta; consequently, the analysis relies on the latest version publicly available online for Malta.

[9] Outlining the detailed content of the programmes that Member States must submit to the European Commission for approval to access funds.

[10] Establishing the Specific Objectives of the Internal Security Fund for 2021-2027.

EXTRACTION OF PRIORITIES

12

The extraction focused on identifying all text passages in the National ISF Programmes describing planned priorities, actions or areas of focus under the three SOs of the ISF: Exchange of information (SO1), Cross-border cooperation (SO2) and Preventing and combating crime (SO3).

A ***priority*** was operationally defined as any explicit or implicit statement indicating what a Member State intends to support, develop, strengthen, maintain, or implement under one of the SOs. No predefined list of priorities was imposed, and no interpretation was conducted at the extraction stage.

Each National Programme was analysed individually. Two standardised extraction instructions were applied, depending on the language of the programme: a) programmes available in the English language: relevant passages were extracted verbatim, b) programmes available in other languages: relevant passages were identified, translated into English and recorded alongside the original text in the national language. In all cases, page numbers or section references were captured where available. To enhance consistency, extraction decisions were guided by a common set of operational criteria defining what constituted a priority statement. Extracted passages were subsequently reviewed to verify completeness, contextual accuracy and alignment with the extraction criteria. Any ambiguous cases were resolved through expert review. Each extracted priority was recorded as a separate entry in the dataset and assigned a unique identifier combining the Member State, the SO and a sequential number (e.g., BG-SO1-007) to facilitate traceability and subsequent analysis.[11]

NORMALISATION AND CONSOLIDATION OF PRIORITIES

Following the extraction stage, a normalisation step was carried out in order to consolidate semantically equivalent or closely related priorities within each National Programme. As mentioned above, the initial extraction produced a large number of verbatim entries per Member State. These entries reflected the full granularity of the programme texts, notably including repeated references to the same priority formulated in different sections (e.g. in titles, descriptions, implementation measures, or expected results), as well as closely related actions contributing to a common strategic objective. The purpose of the normalisation step was to reduce structural duplication while preserving substantive content. This was necessary to ensure that subsequent quantitative mapping to the EUCS Taxonomy would not artificially inflate the frequency of certain areas due to textual repetition rather than genuine policy emphasis.

Normalisation was conducted through a controlled grouping process based on semantic equivalence and policy coherence. Priorities were grouped where they:

- Referred to the same strategic objective using different wording;
- Described complementary actions forming part of a single operational line;
- Repeated the same thematic focus across different sections of the programme.

Importantly, no new priorities were created, and no content was discarded. Grouped priorities retained all original textual elements, which were stored and considered fully during the subsequent mapping phase. At the end of the normalisation process, the number of priorities reduced from 1147 raw extracted entries to 470 consolidated priorities.

[11] Due to its length, the complete list of priorities is not included in this report. It may be made available upon request for specific Member States or policy objectives at enact@shu.ac.uk.

MAPPING OF PRIORITIES TO THE EUCS TAXONOMY

13

Once the normalisation stage was finished, the consolidated priorities were mapped to the EUCS Taxonomy across the three dimensions analysed, namely Policy, Functions and Technology, using the highest level of aggregation for each dimension where applicable.

The mapping methodology followed the same analytical logic and level of aggregation that was previously applied at the 1st ENACT Analytical Report - FCT R&I: An analysis of EU priorities 2014 - 2024,[12] whereby textual references are reviewed and flagged against the taxonomy elements based on explicit presence and substantive alignment.

The mapping process combined/included:

- Structured keyword identification;
- Contextual reading of the full priority text;
- Expert analytical judgement.

Each consolidated priority was reviewed in its entirety, including all grouped textual components, to ensure that no relevant element was excluded from consideration. This approach ensures that, although structural duplication was removed in the normalisation phase, the qualitative richness of the original text remained fully available for classification.

The mapping itself constituted a quantitative exercise: taxonomy elements were flagged when explicitly addressed within a priority, and aggregate counts were subsequently produced at Member State and EU level. The frequency of references to specific taxonomy elements was therefore used as a proxy indicator of thematic emphasis as per the judgement of ENACT experts.

Importantly, it was considered that the prior normalisation step did not influence the qualitative mapping decision. All underlying text fragments contained within a grouped/normalised priority were taken into account when assigning taxonomy categories. The normalisation affected only the counting unit (i.e. preventing multiple counts of the same substantive priority), not the analytical interpretation of its content.

Overall, the present analysis draws on the initial National Programmes of each Member State, based on their most recent available versions. Any deviations of the final expenditure carried out under their National Programmes by the different Member States have not been considered in this report. Hence, the result of the analysis reflects the priorities of the Member States from a pure operational perspective, and not the actions eventually implemented, which could have been influenced by other factors, such as national budget constraints. Furthermore, because the National Programmes act as forward-looking strategic projections, they typically rely on broad generalisations rather than providing explicit, granular details. This intentional formulation allows Member States to maintain the necessary flexibility in their planning and resource allocation throughout the multi-year funding cycle.

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

USE OF AI-ASSISTED ANALYSIS

14

Given the length, structural heterogeneity and multilingual nature of the National ISF Programmes, AI-assisted analytical tools were used for translation and during the extraction and normalisation phases to ensure systematic processing of large textual volumes. For the extraction of priorities and their subsequent normalisation, NotebookLM was used as the primary analytical tool.

Dedicated prompts were developed to identify relevant priority statements and to group semantically related passages. The extraction and normalisation processes were AI-assisted, with the model applying consistent criteria across all documents. The researchers defined the extraction logic and consolidation principles in advance and supervised the overall process, but the operational identification and grouping of text passages relied on the AI tool. Furthermore, AI tools were used in selected sections of this report to improve the clarity and coherence of the text.

15 RESULTS

PROGRAMMATIC BASELINE: THE ISF SPECIFIC OBJECTIVES

The initial assessment distributed the documented national priorities across the three official SOs of the ISF to establish a clear programmatic baseline. Figure 1 shows the macro-level distribution of the total 470 identified priorities across these three statutory boundaries and across all Member States. Of these, 155 priorities were assigned to SO1, 117 priorities to SO2, and 198 priorities to SO3.

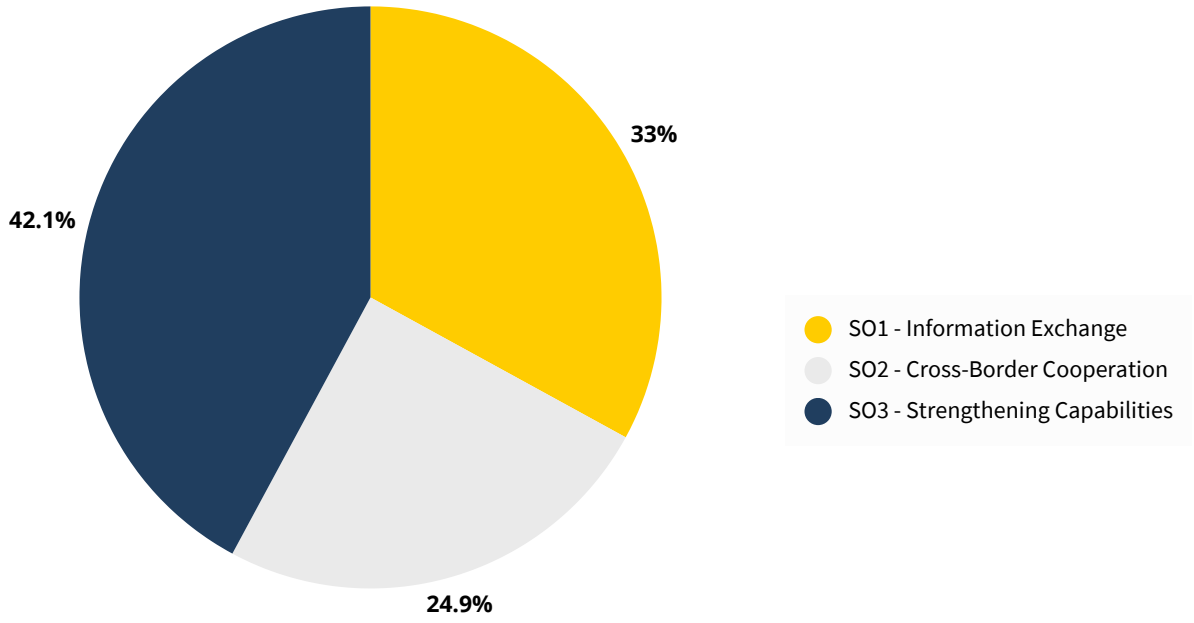


Figure 1 – Macro-distribution of documented National Priorities across the three ISF SOs

This distribution illustrates the relative emphasis placed by Member States on each of the three ISF objectives during the programming phase. However, the primary purpose of this report is not to compare priorities across the ISF objectives themselves, but rather to analyse them using the multi-tiered EUCS Taxonomy across its Policy, Functions and Technology dimensions to provide a more detailed and operationally precise evaluation of the planned actions. Thus, the detailed Member State distribution of priorities across the three SOs is presented in Annex B, while the main body of the report focuses on the taxonomy-based analysis.

For readers interested in the financial execution of the National Programmes, the European Commission's Cohesion Open Data Platform provides an interactive financial analysis of the ISF 2021-2027 funding.[13] It is important to note that the Cohesion platform tracks quantitative budget allocations and expenditure structured strictly around the administrative ISF SOs. Because the present report employs a different analytical approach, that of extracting and mapping textual priorities to the EUCS Taxonomy rather than tracking monetary allocations, a direct numerical comparison between the findings of this analysis and the Cohesion platform is not possible. Furthermore, as the 2021-2027 implementation period is active during the preparation and publication of this report, the expenditure data presented on the platform reflects ongoing, rather than finalised, spending.

POLICY DIMENSION

The policy dimension of the EUCS FCT Taxonomy has a two-level structure, with four main policy categories in Level 2, each with a subset of policy areas in Level 3. The analysis for each level is illustrated in Figure 2.

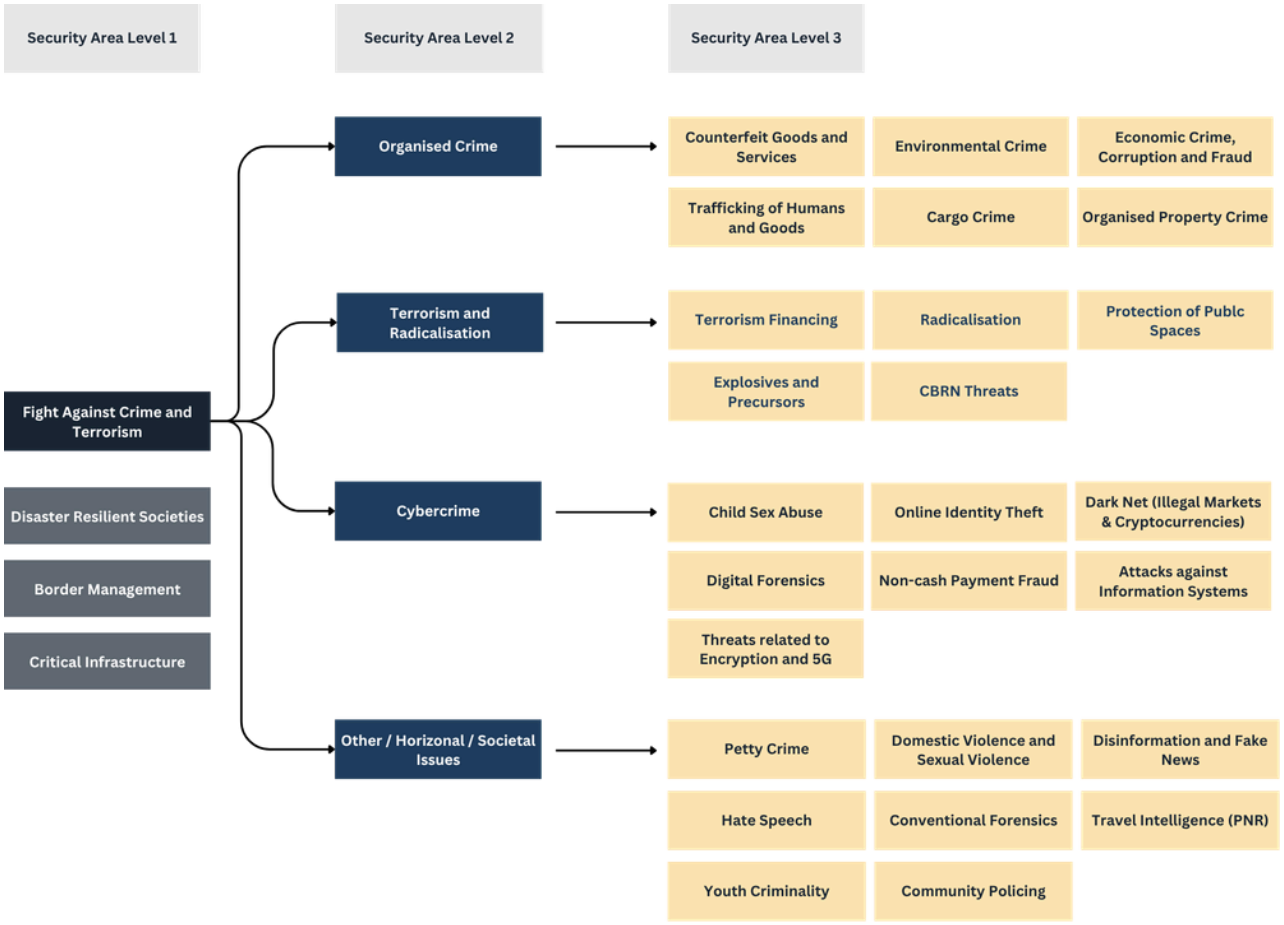


Figure 2 – FCT policy dimension of the EU Civil Security taxonomy policy pillar

POLICY LEVEL 2

17

This section outlines the policy priorities identified across the ISF National Programmes of the EU member states. The analysis categorises the reported national priorities according to the overarching taxonomy, grouping them into four primary Level 2 domains: **Organised Crime**, **Terrorism and Radicalisation**, **Cybercrime**, and **Other/Horizontal Societal Issues**.

To provide a comparative view of the strategic focus across the EU, the findings are presented as percentages of the total identified priorities of each National Programme rather than absolute numerical counts.

As shown in Figure 3, **Other/Horizontal Societal Issues** represent the most significant policy area of focus across Member States, accounting for **41.28%** of all documented priorities across the Member States. This is followed by **Organised Crime**, which constitutes 26,36% of the strategic initiatives. Cybercrime makes up **17.02%** of the identified priorities, while **Terrorism and Radicalisation** represent the smallest share at **15.34%**. It is important to note that a significant number of priorities outlined by Member States did not make explicit reference to a single, concrete policy area (such as Cybercrime or Terrorism and radicalisation). Thus, cross-cutting capabilities, such as general information exchange systems, broad forensic laboratory upgrades or passenger data processing, were mapped in the **Other/ Horizontal Societal Issues** category. Consequently, the high percentage of priorities in this domain reflects the strategic focus of Member States on building threat or policy-agnostic infrastructure and cooperation frameworks that support the fight against multiple crime areas simultaneously.

This pattern reflects the legal requirements of the ISF Regulation, which mandates that Member States align their national funding with overarching EU security goals. Specifically, the heavy focus on the Horizontal pillar answers the EU's call to build a shared, interconnected security ecosystem. By keeping more than half of these priorities broad, countries are investing in threat-agnostic infrastructure, such as interoperable data exchange networks and multi-purpose forensic labs, which are needed to support all law enforcement actions simultaneously.

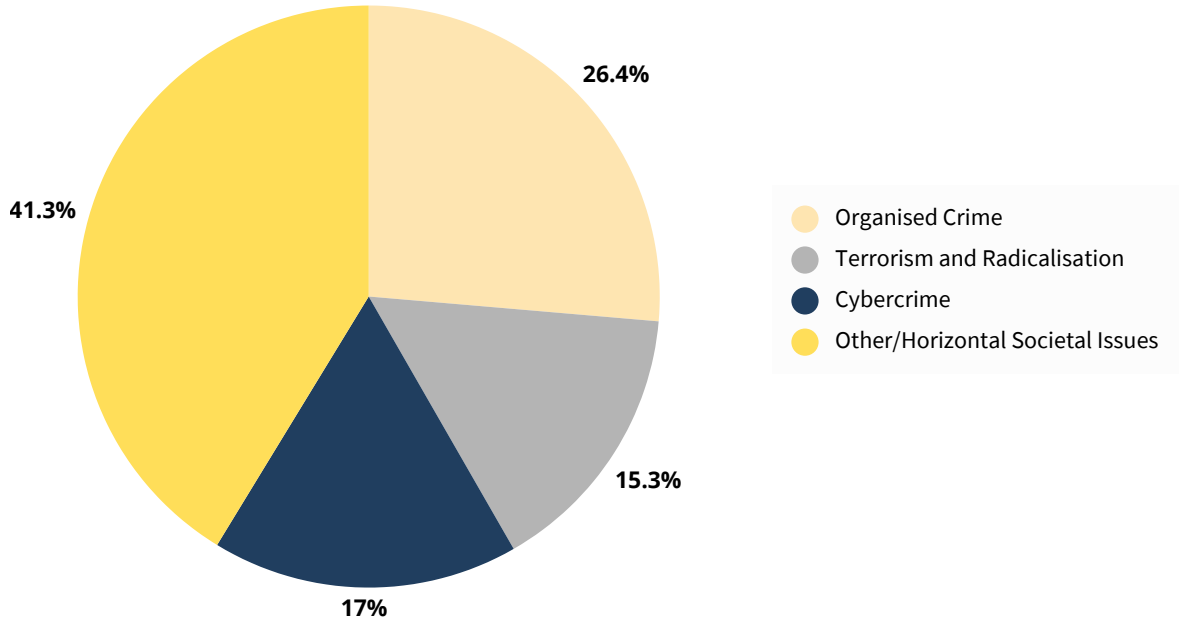


Figure 3 – Overall distribution of ISF priorities by Policy Level 2 categories (%)

MEMBER STATE VARIATIONS - LEVEL 2

While the aggregated data provides a clear picture of overall priorities at a European level, an analysis at the national level reveals distinct variations in how Member States allocate their strategic focus across the four primary domains. Figure 4 illustrates the relative distribution of these Level 2 priorities for each country.

The country-by-country mapping reveals that although cross-cutting structural development remains a shared baseline, individual National Programmes heavily shift their allocations to align with specific geographic, economic and security realities.

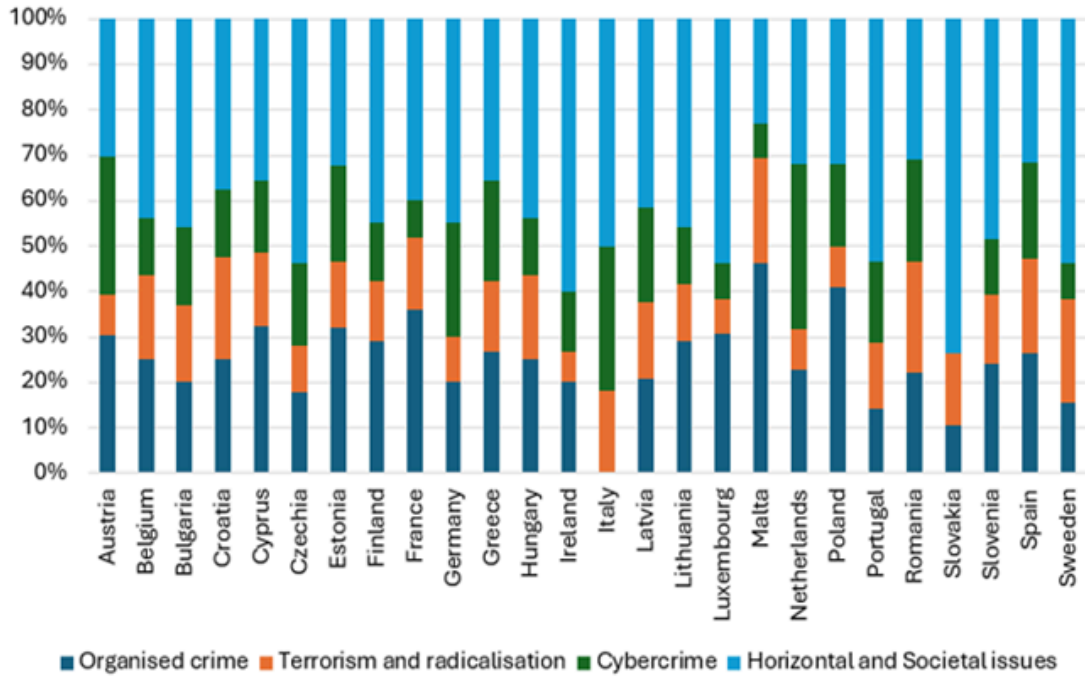


Figure 4 – Distribution of ISF Level 2 Policy priorities by Member State (%)

Reflecting the macro-level trend, a substantial majority of Member States dedicate the largest single portion of their National Programme priorities to the **Other/Horizontal Societal Issues** domain. This emphasis on threat-agnostic capacity building is most pronounced in Slovakia, which leads the Union by dedicating 73.68% of its total priorities to this category. Similarly elevated levels are visible in Ireland (60%), as well as in the Czech Republic, Luxembourg, Sweden and Portugal, all of which allocate over 53% of their strategic initiatives toward cross-cutting institutional infrastructure and common security frameworks.

Organised crime represents a major focus area for Malta, which leads this category with 46.15% of its documented priorities toward dismantling criminal networks. This operational prioritisation is closely mirrored in Poland (40.91%), followed by France (36,00%) and Estonia (32.14%), signalling a concerted investment in tackling trafficking, smuggling, and cross-border illicit activities.

The focus on digital threats varies a lot across the EU. It is highest in strongly digital countries that invest heavily in online defence. The Netherlands puts the largest emphasis on **Cybercrime**, making it its top individual priority at 36.36%. This focus is also clear in Austria and Italy, where **Cybercrime** ties for first place as their highest category at 30.43% for both Member States.

Finally, although **Terrorism and radicalisation** have the smallest overall share across Europe, local threat levels drive higher funding in specific countries. The highest focus is found in Romania (24.44%), Sweden and Malta (23.08%) and Croatia (22.50%). This distribution suggests a risk-driven approach, focusing on areas like protecting public spaces, countering explosives, and preventing radicalisation where local needs require a stronger response.

POLICY LEVEL 3

Before analysing the sub-categories of the Policy dimension, it is important to note the classification logic applied to the priorities in the National Programmes. To ensure analytical accuracy and avoid over-representing certain sub-categories, a conservative mapping approach was applied using the following rules:

- Priorities at the Level 3 Policy tier were considered and counted only when they were explicitly mentioned. Therefore, when a priority aligned with a general policy area but lacked an explicit mention of a specific Level 3 element, it was mapped exclusively at the Level 2 tier to avoid speculative classification. As a direct result of this conservative approach, not all priorities advanced to the Level 3 tier. Table 1 outlines the Level 3 mapping rate, showing the percentage and absolute volume of national priorities within each pillar that contained sufficient operational detail to be mapped at Level 3.

Table 1 – Mapping depth of ISF priorities within the Policy dimension levels

Policy category (Level 2)	Priorities mapped to Level 3
Organised Crime	70.90% (134 out of 189)
Terrorism and Radicalisation	76.36% (84 out of 110)
Cybercrime	74.59% (91 out of 122)
Other/Horizontal Societal Issues	45.27% (134 out of 296)
Total Framework	**61.78% (443 out of 717)**

In addition, to fully capture the strategic nuances of the Member States, the specific threat priorities (Policy Level 3) are analysed through two distinct quantitative lenses in this report:

- Intra-category distribution: In the immediate sub-sections below, Level 3 priorities are analysed within their parent Level 2 categories (Figures 4-7). For example, the percentage of specific cyber threats relative only to the total Cybercrime priorities is considered. This illustrates the internal strategic composition of each broad crime area.

- Global distribution: Following the intra-category breakdown, a consolidated macro-analysis evaluates all Level 3 priorities against the total pool of specific threats combined (Figure 9). This global perspective strips away the Level 2 silos to reveal the absolute, overarching threat priorities across the European Union.

ORGANISED CRIME SUB-TAXONOMY

Within the domain of **Organised Crime**, the distribution of priorities reveals a highly concentrated focus on two specific areas of illicit activity, as shown in Figure 5.

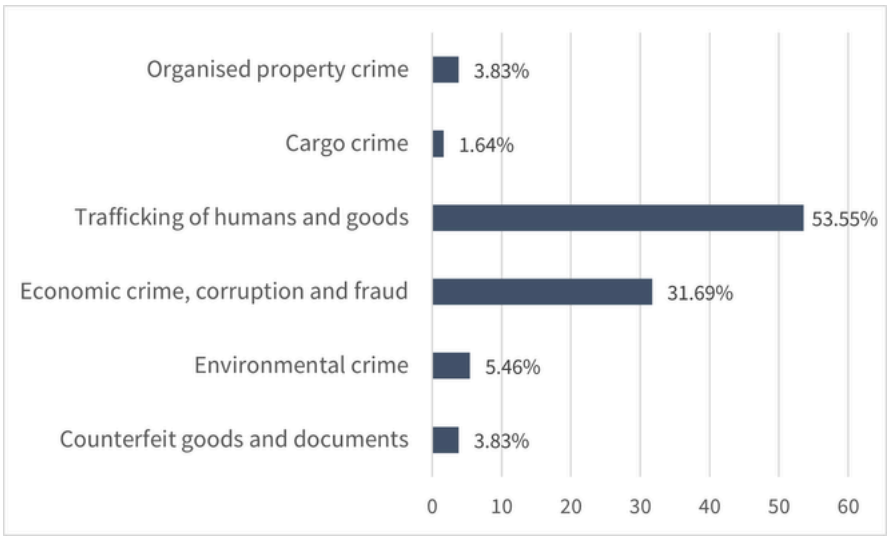


Figure 5 – Percentage of priorities addressing Organised crime Level 3 elements

The overwhelming majority of national priorities in this category target the **Trafficking of humans and goods**, which accounts for **53.55%** of all Organised crime priorities. This highlights a clear consensus among Member States regarding the severity of cross-border smuggling and human exploitation networks. The second most prominent area is **Economic crime, corruption and fraud**, representing 31.69% of the focus within this domain.

In contrast, other sub-categories, such as **Environmental crime**, **Organised property crime**, and **Counterfeit goods and documents**, receive notably less strategic emphasis in the ISF National Programmes, each constituting a marginal fraction of the overall efforts in this group.

TERRORISM AND RADICALISATION SUB-TAXONOMY

Although **Terrorism and radicalisation** represent the smallest of the four main domains (15.34% in Level 2), the distribution of priorities within this category is notably diverse and relatively evenly distributed, reflecting a multifaceted approach to counterterrorism.

As seen in Figure 6, the most pressing concern for member states is the **Protection of public spaces,** which leads the category at **33.03%**. Preventive measures are also heavily prioritised, with initiatives aimed at countering **Radicalisation** making up exactly 25% of the domain. Finally, regulating and monitoring dangerous materials remains a consistent focus, with **Explosives and explosive precursors** representing 17.86% and **CBRNE** (**Chemical, Biological, Radiological, Nuclear and Explosive**) threats accounting for 15.18% of the counterterrorism priorities.

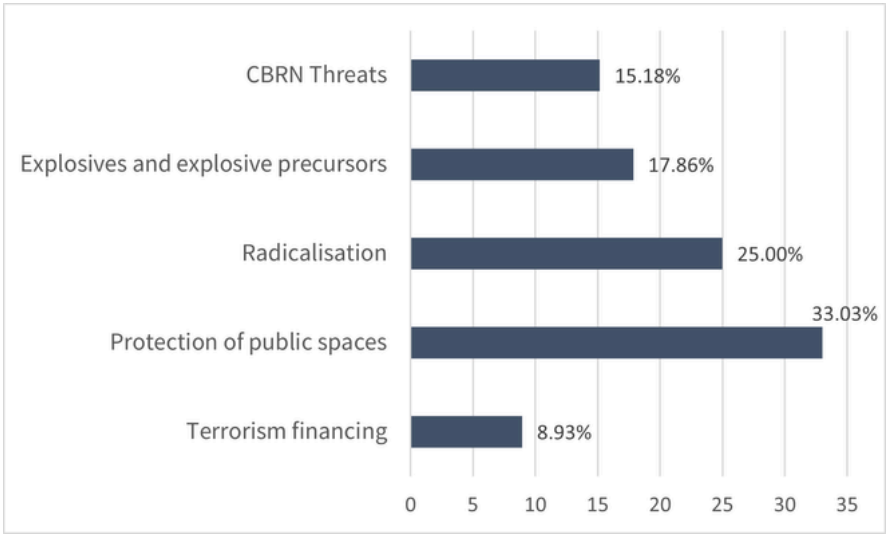


Figure 6 – Percentage of priorities addressing Terrorism and radicalisation Level 3 elements

CYBERCRIME SUB-TAXONOMY

As digital threats continue to evolve, Member States have allocated nearly a quarter of their total priorities to addressing **Cybercrime**. Figure 7 breaks down the strategic focus within this domain.

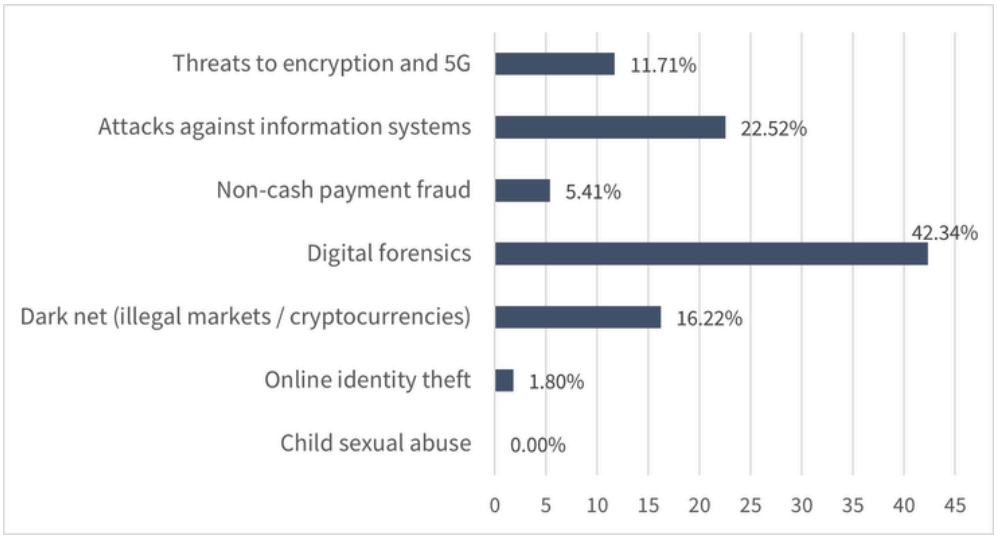


Figure 7 – Percentage (%) of priorities addressing Cybercrime Level 3 elements

The area of **Digital Forensics** is the undisputed priority, making up **34.56%** of all cyber-related initiatives. This points to a widespread need to improve digital evidence recovery and analysis capabilities. Additionally, **Child Sexual Abuse** and **Attacks against information systems** jointly constitute the second most frequently identified priorities, each representing 18.38% of the cybercrime-related initiatives, followed by efforts to monitor and disrupt operations of the **Dark Net (Illegal Markets/Cryptocurrencies)**, which account for 13.24% of the focus.

OTHER/HORIZONTAL SOCIETAL ISSUES SUB-TAXONOMY

The **Other Horizontal Societal Issues** category captures cross-cutting priorities that support broader law enforcement and security operations. The majority of the priorities classified under this L2 category referred to generic capabilities without a concrete policy focus. However, there were some priorities allocated to some concrete L3 items in the Horizontal and Societal issues category. Figure 8 details such specific allocations.

The enhancement of investigative capabilities is a primary concern, with **Conventional Forensics** taking the lead at 34.42%. The processing and analysis of passenger data also remain highly relevant, as **Travel Intelligence (PNR)** accounts for 29.22% of the initiatives.

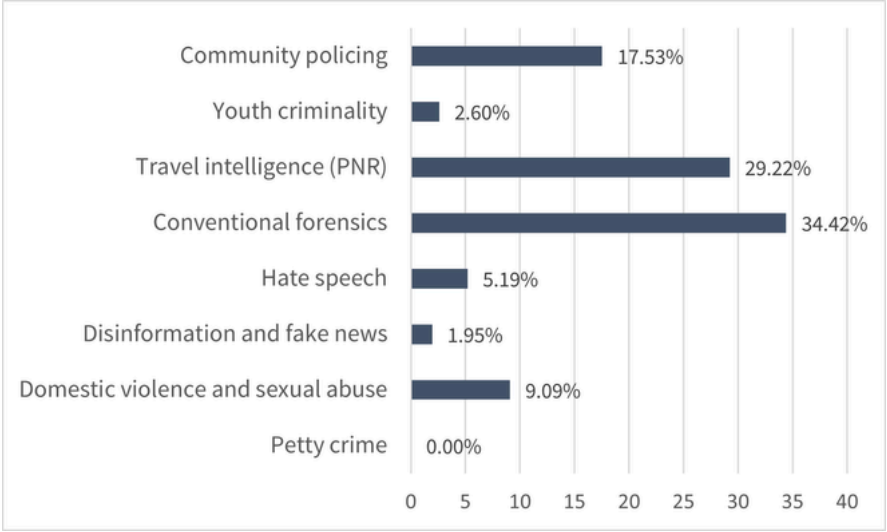


Figure 8 – Percentage (%) of priorities addressing Horizontal and Societal issues Level 3 elements

The country-by-country mapping reveals that although cross-cutting structural development remains a shared baseline, individual National Programmes heavily shift their allocations to align with specific geographic, economic and security realities.

OVERALL DISTRIBUTION OF SPECIFIC THREATS - LEVEL 3 MACRO-VIEW

Looking beyond the broad crime categories, this section reviews all specific Level 3 threat priorities together (Figure 9). By combining these areas into a single overview, the most frequently referenced specific policy priorities and operational focus areas across the European Union can be observed.

Traditional cross-border illicit activities and core investigative infrastructure are most frequently referenced in the National Programmes, indicating they are the primary operational focus. Within this bracket, the **Trafficking of Humans and Goods** stands as the most frequently referenced specific threat priority across the EU at **16.76%**. This is followed by **Economic Crime, Corruption, and Fraud**, which represents **9.91%** of the global share. Systemic capacity building is heavily driven by a massive collective commitment to forensics, split between **Conventional Forensics** at **9.06%** and **Digital Forensics** at **8.03%**. When viewed together, forensic infrastructure outpaces nearly every other threat area, signalling a continent-wide shift toward modernisation and robust evidence gathering that works alongside **Travel Intelligence (PNR)** processing systems at **7.69%**.

Beneath the front-running categories, a stable core of mid-range priorities emerged within the 3% to 7% range. **Protection of Public Spaces** led this tier at **6.32%**, while prevention-oriented priorities were closely balanced between **Radicalisation** (**4.79%**) and **Community Policing** (**4.62%**). In the digital domain, **Attacks Against Information Systems** and **online Child Sexual Abuse** each accounted for a **4.27%** share. This operational block was rounded out by targeted actions against **Explosives and Explosive Precursors** at **3.42%** and **Dark Net Monitoring** at **3.08%**.

In short, while the ISF addresses a wide range of security issues, Member States are clearly prioritising an intelligence-led policing model, meaning resources are heavily directed toward disrupting cross-border organised crime and building the digital, forensic, and data tools needed for modern investigations.

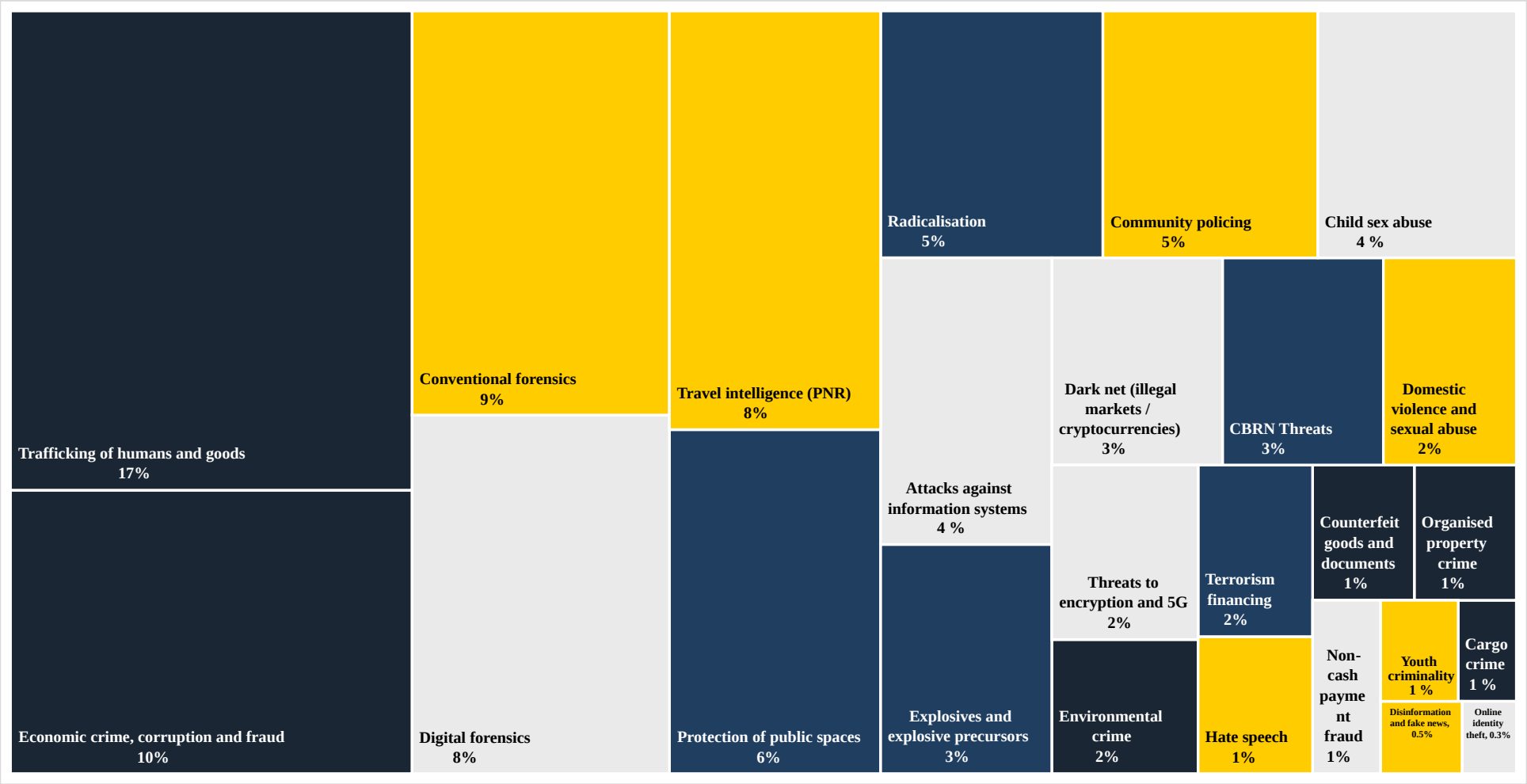


Figure 9 – Macro-view of overall Level 3 threat distribution (%)

MEMBER STATES VARIATIONS - LEVEL 3

When examining the specific Level 3 priorities, the data shows a strong, unified consensus across the EU Member States. **Trafficking of Humans and Goods** is widely recognised as a critical threat, ranking within the top three priorities for 21 of the 26 analysed Member States. Similarly, capabilities targeting **Economic Crime, Corruption and Fraud**, as well as the development of **Conventional Forensics** and **Digital Forensics**, heavily dominate the top national rankings across the board.

Because of this strong consensus, variations at the sub-taxonomy level are rare but highly indicative of specific regional or national security challenges. Notable outliers among the Member States' top priorities include:

- Croatia uniquely identifies **Explosives and Explosive Precursors** as its number one strategic priority, the only Member State to place this in its top three.
- Finland is the only Member State to elevate **Environmental Crime** into its top three law enforcement priorities.
- Malta places a distinct emphasis on **Terrorism Financing**, ranking it among its most critical focus areas.
- France is the sole country to feature **Counterfeit Goods and Documents** within its top three strategic initiatives.

FUNCTIONS DIMENSION

This section focuses on the EUCS Taxonomy Functions (Figure 10) prioritised within the ISF National Programmes, essentially the operational *how* of the security initiatives planned under each programme. Unlike the policy area, which defines *what* is being fought, the Functions dimension describes the activities and capabilities addressed under the programme and candidates for funding during the implementation period.

As mentioned in the previous section regarding the mapping of the priorities in the Policy dimension, to standardise the classification of operational Functions across varying national priorities, the following mapping rules were consistently applied:

- Information Systems and identification: Any priority referring to large-scale law enforcement databases and information systems containing personal information or traceable assets (e.g., SIS, PRÜM, PNR) was systematically mapped to **Data, Information & Intelligence Gathering Management, and Exploitation** and **Identification and Authentication of Persons, Assets and Goods**.

- Broad definition of Training: The **Training and Exercises** function was utilised as a comprehensive category for human capital and capacity building. Consequently, all priorities referring to cross-border collaboration, police cooperation, networking, deployment of liaison officers, joint operations, exchange of best practices, awareness campaigns and victim/witness support were consolidated under this function. Furthermore, priorities specifically involving joint or operational teams also triggered the **Investigation and Forensics** function.

- Cybersecurity delineation: The Security of information systems, networks and hardware functions was strictly reserved for initiatives explicitly targeting cybersecurity or defending against cyberattacks, separating it from general IT infrastructure maintenance.

Following the analysis, as shown in Figure 11, there is a clear and dominant emphasis on the management of data. **Data, Information & Intelligence Gathering Management, and Exploitation** is the most significant of the functions, accounting for **23.13%** of the total. This is followed closely by **Training and Exercises** (**20.20%**) and then by **Secure and Public Communication and Data Exchange** (**12.92%**) and **Investigation and Forensics** (**12.37%**).

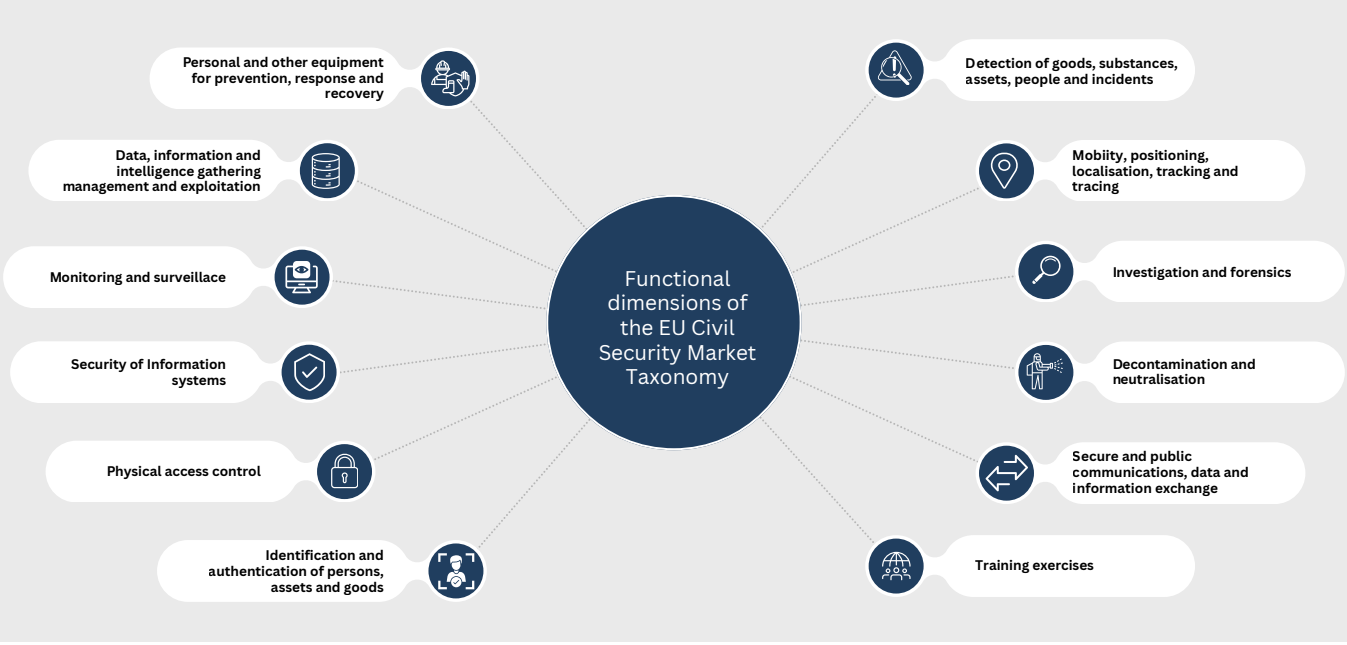


Figure 10 – Functions dimension of the EU Civil Security market taxonomy

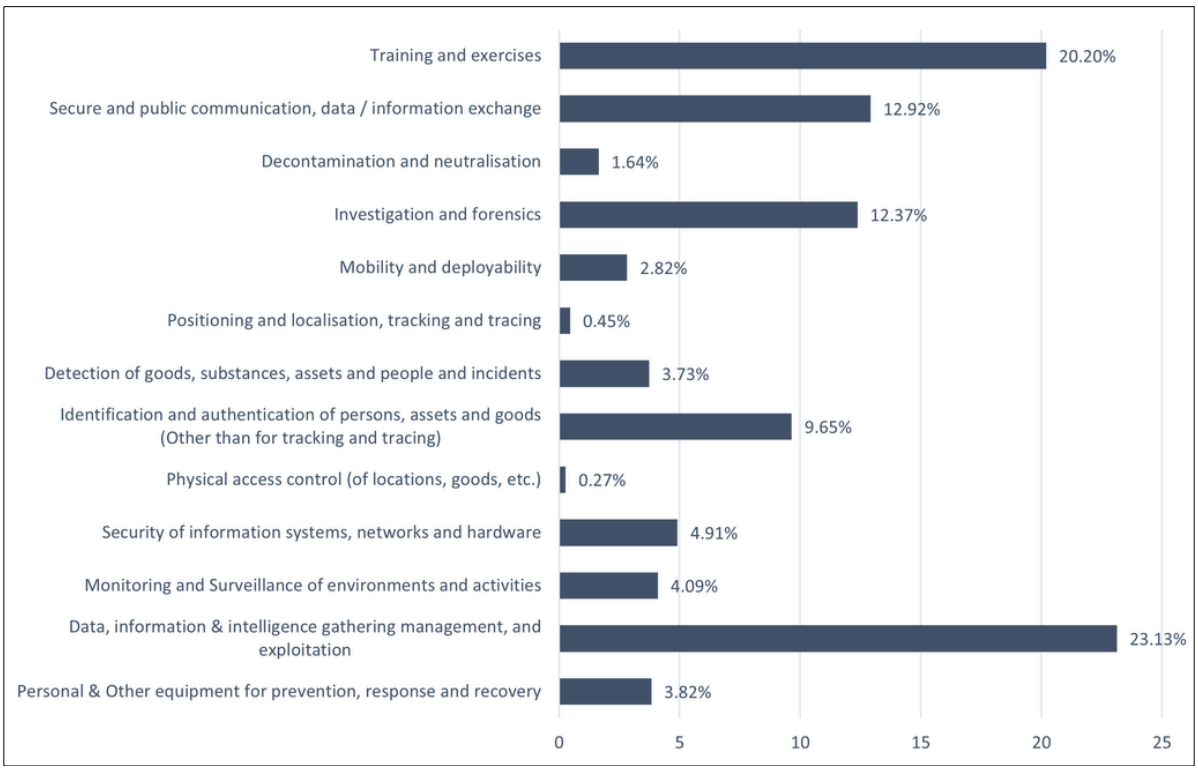


Figure 11 – Overall distribution of ISF priorities by Functions categories (%)

MEMBER STATES VARIATIONS

29

When analysing the distribution by Member State (Figure 12), a higher degree of uniformity is observed compared to the Policy dimension. This suggests that across the EU, the operational "toolkit" required by law enforcement is largely consistent.

Notably, **Data and Intelligence Management** is a universal priority, appearing in the "Top 3" for every single analysed Member State. Similarly, **Training and Exercises** are a top-three priority for 21 of the 26 analysed Member States.

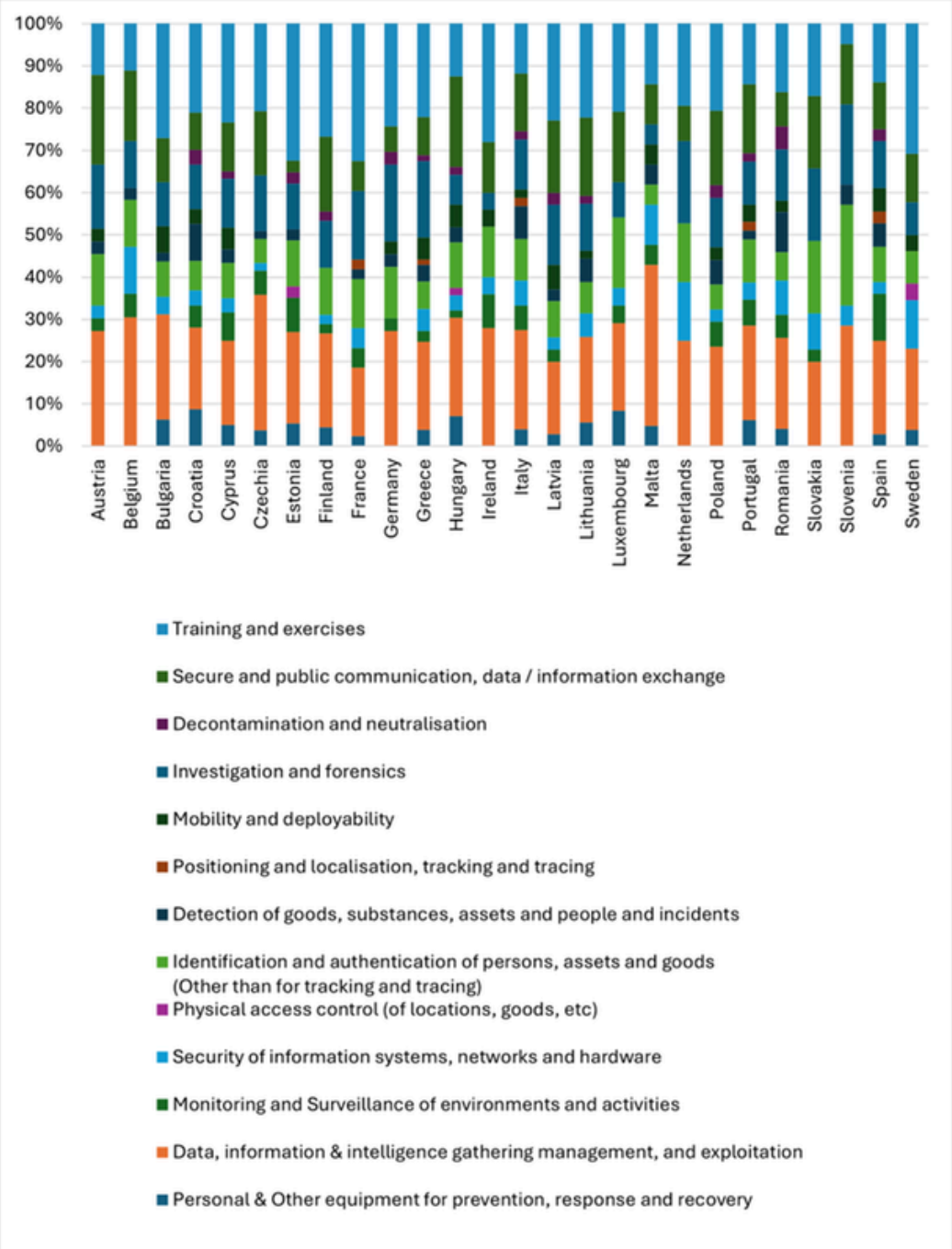
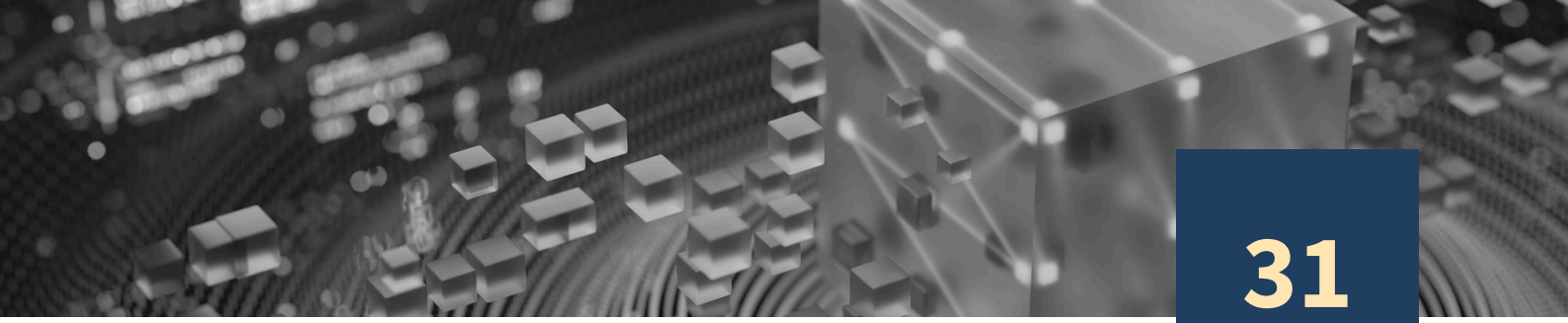


Figure 12 – Distribution of ISF Functions priorities by Member State (%)

Beyond this consensus, national strategies diverge to address specific domestic needs. In Czechia, Greece and Romania, data exploitation is the primary centre of gravity, while Belgium and Slovakia show a higher relative commitment to human capital development through training. Distinct functional clusters are also evident: Nordic and Western nations like the Netherlands and Sweden prioritise information system security to protect digital infrastructure, whereas Mediterranean and Balkan states, such as Croatia and Bulgaria, focus more on modernising physical response equipment.

Geographic factors further drive unique outliers. Portugal and the Baltic states (Estonia and Latvia) place a specialised emphasis on identification and authentication, likely tied to managing expansive external borders. Meanwhile, Spain and Poland prioritise situational awareness through monitoring and surveillance. These variations demonstrate that while the EU moves toward a standardised intelligence-led model, Member States continue to leverage the ISF to address specific national operational gaps.



TECHNOLOGY DIMENSION

The Technology dimension identifies the specific tools, products and technical solutions Member States intend to acquire, develop or deploy, and maps them to the categories of the Technology pillar of the EUCS Taxonomy. This section bridges the strategic gap between the Policy objectives (what is being fought) and the Functional requirements (how it is being fought) by detailing the technical means of implementation.

The Technology dimension of the EUCS Taxonomy has different levels of aggregation, but for the scope of this analysis, only the highest level has been addressed (Figure 13).

Technology areas	
Access control/authorisation (building access, system access, etc.)	Labroratory equipment for gathering and forensic analysis of samples
Alarm/warning systems	Healthcare/medical equipment
Data analytics	Monitoring tools and services
CBRNE detection and neutralisation products	PPE/safety equipment
Data storage and exchange	Screening and detection
Digital forensics	Search devices and tools
Digital security products and services	Specialised management and control systems
Faciliation systems and secure databases	Surveillance systems
General equipment	Tracking, navigation and guiding systems, equiment and tools
Guarding and physical protection (non-human)	Training and simulation
Internet-based investigation	Conflict management / use of force
	Critical communication, interoperable communications

Figure 13 – Technology dimension of the EU Civil Security market taxonomy

Before examining the distribution of specific technological categories, it is important to clarify the overall footprint of Technology within the National Programmes. A significant amount of the stated ISF priorities do not entail any type of investment in technology, or at least not in security-specific technology, focusing instead on organisational measures, legal and collaboration frameworks or purely procedural enhancements. According to the analysis, **73.56% of the identified priorities have explicit or implicit technology associated with them**. The subsequent distribution analysis focuses specifically on this technologically active subset.

Within this scope, an analysis of the overall distribution reveals a strong, unified preference for digital and data-oriented infrastructure. As shown in Figure 14, the Technology dimension landscape is predominantly led by **Data Storage and Exchange**, which accounts for **16.92%** of the total national priorities. This is followed by significant priorities regarding **Data Analytics** (**11.64%**) and **Facilitation Systems and Secure Databases** (**10.34%**). Conversely, traditional technologies such as police vehicles (considered under the General equipment category) or Communications, are in the mid-tier of the ranking, and others like **Guarding and Physical Protection** and **Alarm/Warning Systems** represent a marginal fraction of the overall European technological focus under the ISF National Programmes.

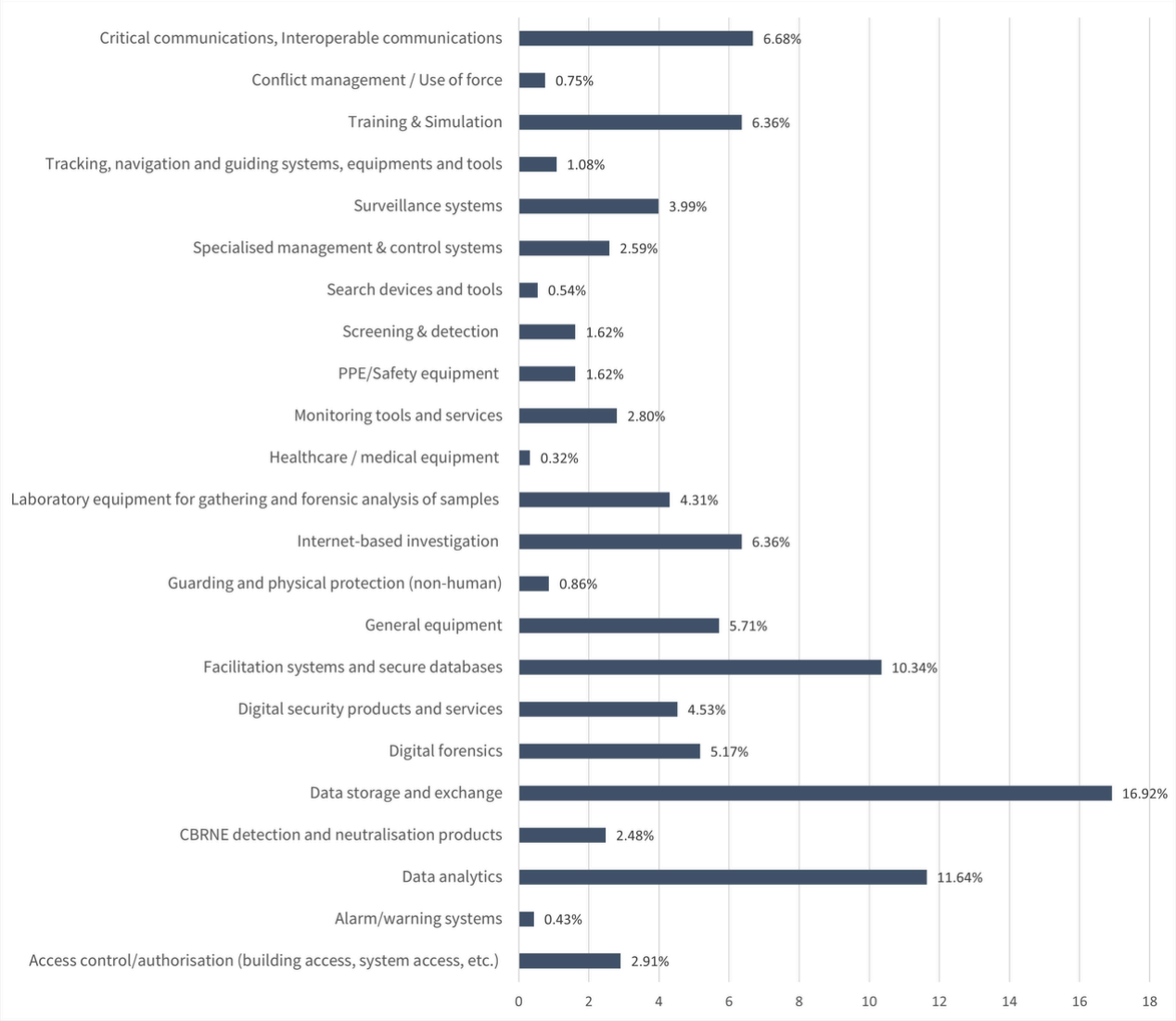


Figure 14 – Overall distribution of ISF priorities by Technology Level 1 categories (%)

MEMBER STATES VARIATIONS

The aggregate data indicate a continent-wide technological shift toward digital infrastructure; however, by examining the distribution at the Member State level (Figure 15), critical nuances and strategic specialisations are revealed.

The procurement and enhancement of **Data Storage and Exchange** serves as a universal baseline, appearing in the top three technological priorities for **25 out of the 26 analysed Member States**. This overwhelming consensus indicates a shared fundamental requirement for interoperable and secure law enforcement databases across the Union. **Data Analytics** also acts as a core capability, ranking in the **top three for 19 Member States**.

However, beyond this shared digital foundation, national technological strategies diverge to address specific operational environments:

- **Forensic laboratory infrastructure**: While software dominates globally, countries such as Belgium, Czechia and Slovakia place a distinct emphasis on physical evidence, ranking Laboratory equipment for gathering and forensic analysis of samples within their top three technological investments.

- **Cyber & digital security**: Consistent with its functional priorities identified earlier, Sweden is highly specialised in protecting its digital networks, uniquely ranking Digital security products and services among its primary technological acquisitions.

- **Surveillance & physical controls**: In contrast to the heavy intelligence focus of other nations, Spain shows a distinct strategic requirement for situational awareness, placing Surveillance systems in its top three priorities. Similarly, France uniquely prioritises Access control and authorisation systems.

Ultimately, the distribution of priorities in the Technology dimension confirms that the EU is moving collectively toward a digitally interoperable and analytical security framework, but that individual Member States continue to calibrate their ISF technological investments to mitigate their most pressing geographic, forensic and jurisdictional vulnerabilities.

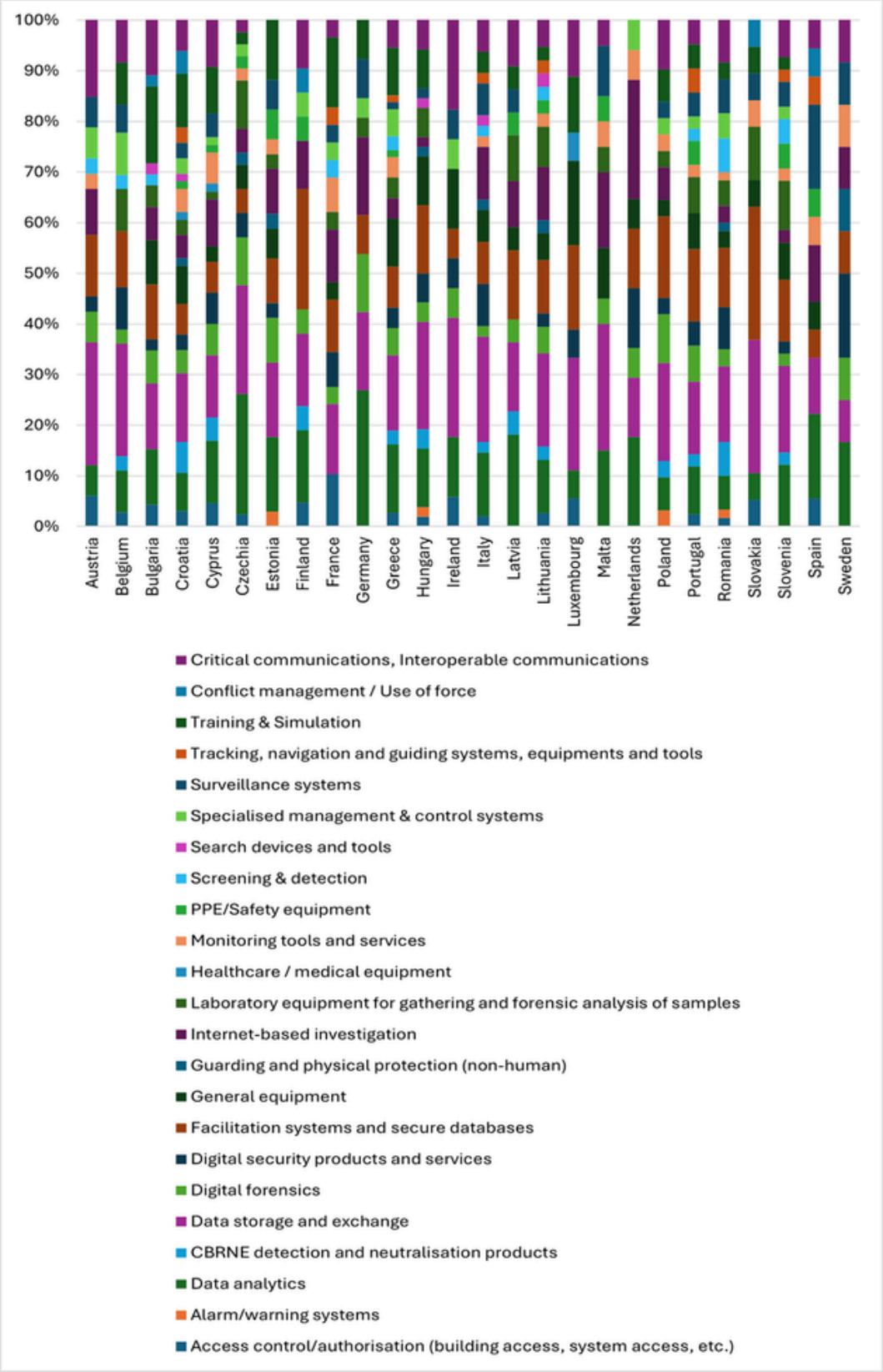


Figure 15 – Distribution of ISF Technology priorities by Member State (%)

ALIGNMENT WITH EUROPEAN RESEARCH AND INNOVATION TRENDS

When evaluating the strategic focus of the ISF National Programmes, it is highly instructive to compare these operational implementation priorities with the broader European R&I landscape. An analysis of the FCT topics under the Horizon 2020 and Horizon Europe Framework Programmes (2014-2024), conducted by the ENACT network,[14] reveals a correlation between the operational plans of Member States and the forward-looking priorities of EU security research across all three taxonomy dimensions (Figure 16).

POLICY DIMENSION: THEMATIC OVERLAPS AND OPERATIONAL REALITIES

At the overarching Level 2 policy tier, **both the R&I Topic analysis and the ISF National Programmes display a distinct distribution of focus**. Most notably, **Other/Horizontal Societal Issues** represent the largest area of investment under the ISF, accounting for nearly half of all operational priorities at 41.28%. However, as mentioned in the Policy dimension analysis section, this high percentage reflects the strategic focus of Member States on building threat-agnostic infrastructure and cooperation frameworks that support multiple crime areas simultaneously. Meanwhile, traditional crime-fighting vectors show varying distributions across both landscapes. **Organised Crime** constitutes a significant and balanced focus in both analyses, representing 21.15% of R&I topics and accounting for 26.36% of the ISF priorities. Conversely, while **Cybercrime** was the most prominent strategic priority in the R&I research landscape at 33.65%, it normalises to 17.02% when applied to the operational realities of the ISF national programmes.

When examining the Policy Level 3 sub-categories, the alignment between theoretical research and operational needs becomes highly evident, alongside a few notable divergences reflecting ground-level realities:

- **Organised Crime**: Both analyses identify **Economic Crime, Corruption and Fraud** and **Trafficking of Humans and Goods** as the two leading categories. In the R&I topic analysis, they are equally ranked at 31.82% each, while in the ISF priorities, **Economic Crime, Corruption and Fraud** lead at 53.55%, followed by **Trafficking of Humans and Goods** at 31.69%.

- **Terrorism and Radicalisation**: Both analyses highlight the **Protection of Public Spaces** as the leading category, accounting for 26.09% in the R&I topic analysis and increasing to 33.03% in the ISF priorities.

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

- **Cybercrime**: This is the only category where the leading sub-category differs between the two analyses. In the R&I topic analysis, **Dark Net (Illegal Markets/Cryptocurrencies)** ranks highest at 28.57%, while in the ISF priorities, **Digital Forensics** is the leading sub-category at 34.56%.

- **Other/Horizontal Societal Issues**: Both analyses identify **Conventional Forensics** as the leading category, representing 22.92% in the R&I topic analysis and increasing to 34.42% in the ISF priorities.

Overall, these variations highlight a clear shift from forward-looking research to practical, ground-level application. While the R&I topics focus heavily on exploring emerging digital landscapes and complex cyber-threats, the ISF National Programmes prioritise operational execution. This is achieved by investing heavily in broad, threat-agnostic infrastructure to support cross-border cooperation, while maintaining a strong practical focus on immediate enforcement priorities such as economic crime, trafficking, and everyday forensic capabilities.

FUNCTIONS DIMENSION: SHIFT TOWARD DIGITISED CAPABILITIES

Under the Functions dimension, the R&I topic analysis shows that the most represented categories are **Investigation and Forensics** (24.56%), followed closely by **Data, Information & Intelligence Gathering Management and Exploitation** (23.13%). In comparison, the ISF priorities analysis highlights **Data, Information & Intelligence Gathering Management and Exploitation**, also as the leading category (23.13%), followed by **Training and Exercises** (20.20%).

Overall, both analyses share a strong emphasis on data, information and intelligence-related functions, indicating a consistent priority on information handling and exploitation across both perspectives. However, **the R&I topic analysis** shows greater relative weight on **investigative and forensic activities**, while **the ISF priorities** shift attention towards **capability development through Training and Exercises**. This divergence indicates that the two frameworks, while aligned on data-centric functions, operationalise them differently, with R&I focused on generating analytical insights and ISF priorities centred on enhancing preparedness through training and cooperation.

TECHNOLOGY DIMENSION: EQUIPPING THE INTELLIGENCE-LED MODEL

Under the Technology dimension, the R&I topic analysis identifies **Internet-based Investigation** (16.79%) as the most prominent category, followed closely by **Data Analytics** (14.60%). In comparison, the ISF priorities analysis places greater emphasis on **Data Storage and Exchange** (16.92%), with **Data Analytics** also appearing as a secondary category (11.64%).

Overall, both frameworks converge on the **importance of data analytics**, although with different levels of emphasis, indicating a shared recognition of its cross-cutting relevance. At the same time, the **R&I topic** analysis shows a stronger orientation toward **investigative use cases** enabled by digital environments, whereas the **ISF priorities** reflect a focus on the **infrastructure and operational backbone** required for secure data handling and exchange. This suggests a differentiation in technological orientation, with R&I topics prioritising digital tools for investigative exploitation, while ISF priorities focus on enabling secure, scalable and interoperable information systems.

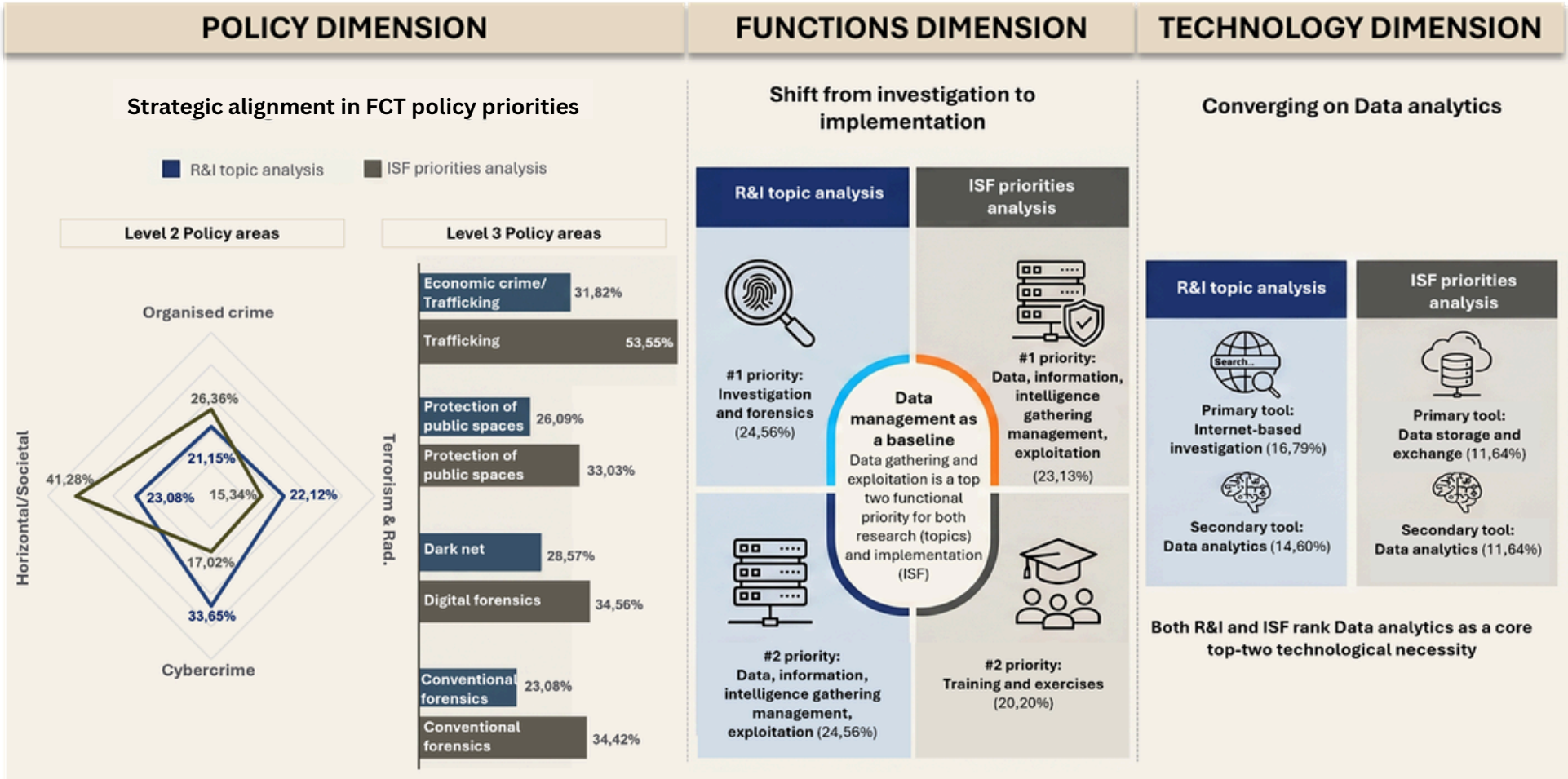
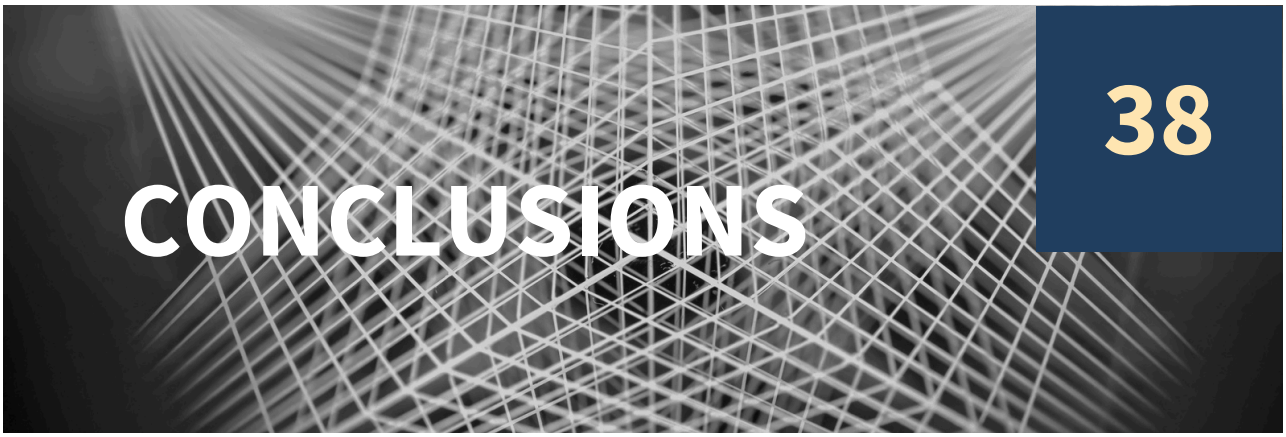


Figure 16 – Strategic alignment and comparative distribution of FCT topics under the Horizon 2020 and Horizon Europe Framework Programmes (2014-2024) and FCT priorities of the ISF National Programmes across the Policy, Functions and Technology dimensions



38 CONCLUSIONS

The mapping of the ISF National Programmes against the EUCS Taxonomy reveals a Member State landscape that is characterised by broad strategic convergence, operationally consistent and technologically focused. The analysis underscores a collective transition toward a more **integrated, data-driven security architecture** across the EU.

Regarding the Policy dimension, the findings demonstrate that **Other/Horizontal Societal Issues** represent the absolutely dominant area of focus across the EU. This shows a profound consensus among Member States to prioritise **threat-agnostic infrastructure**, common **information exchange** channels, and broad **institutional cooperation** frameworks that reinforce the security ecosystem. Within specific crime-fighting domains, **Organised Crime** remains the leading explicit priority vector, driven by an operational urgency to combat **Economic Crime, Corruption and Fraud** and **Human Trafficking**. This is closely supported by tailored investments in **Cybercrime** and **Terrorism and Radicalisation**, where country-by-country variations reflect localised digital vulnerabilities and geographic threat landscapes.

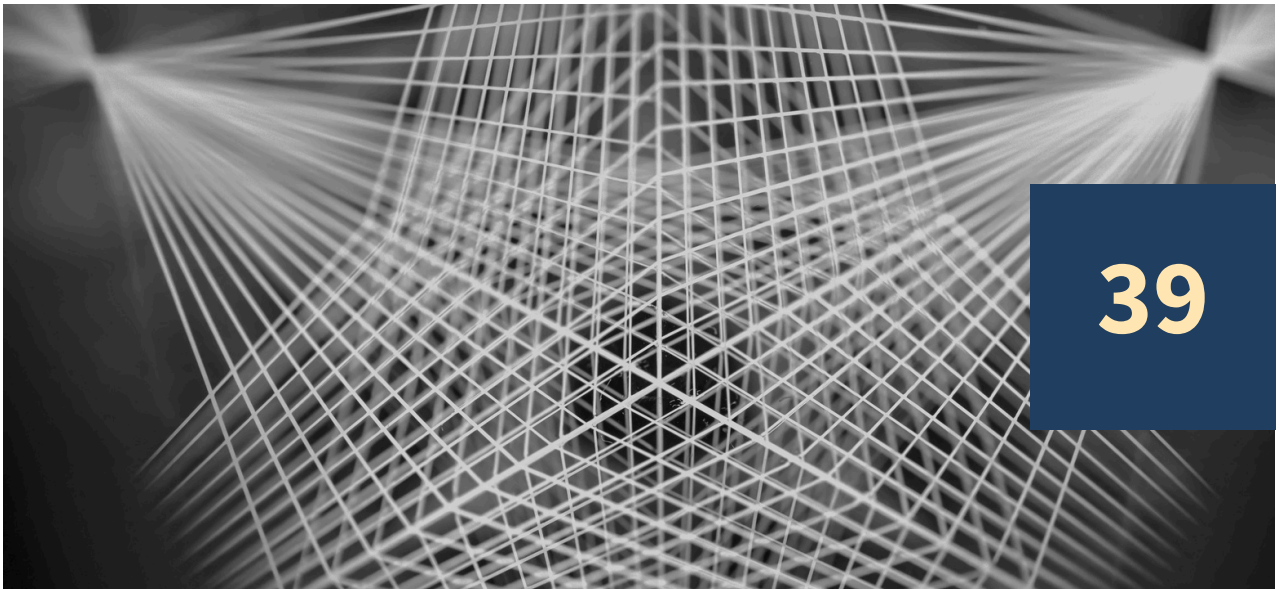
On the Functions dimension, **Data, Information & Intelligence Gathering, Management, and Exploitation** is the most significant capability development need, followed by **Training and Exercises** (which comprises mainly police cooperation), **Secure Communications and Data Exchange** and **Investigation and Forensics**. This “operational toolkit” for law enforcement is largely consistent across Member States.

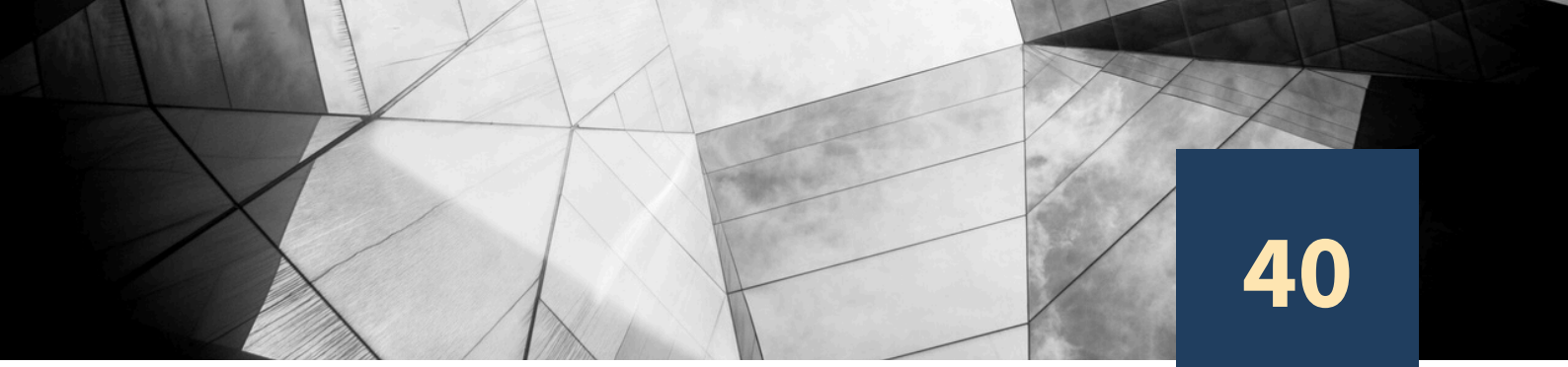
On the Technology pillar, it is worth noting that only 73.56% of the identified priorities have explicit or implicit technology associated with them, showing how technology acts as a strategic capability enabler for modern law enforcement. Among these, there is a strong, unified preference for **digital and data-oriented infrastructure**. In this regard, the analysis shows consensus among Member States on **Data Storage and Exchange** technologies, but while the EU seems to be moving collectively toward a digitally interoperable and analytical security framework, individual Member States continue to calibrate their ISF technological investments to mitigate their most pressing geographic, forensic, and jurisdictional vulnerabilities.

While the current findings provide a robust snapshot of strategic intent, they represent the operational planning phase rather than the final implementation. To ensure that future ISF cycles are both efficient and impactful, the following steps are recommended:

- **Expenditure validation**: Further research is required to cross-reference the qualitative priorities identified in this report with actual, finalised financial expenditure. Utilising tools such as the European Commission's Cohesion Data platform once the 2021-2027 programming period concludes, future studies should conduct a comparative analysis between the initial strategic prioritisation (what was planned) and the financial reality (how much it cost and what was executed). This would help determine whether the national budget constraints, administrative hurdles, or shifting operational realities diverted funds away from the initial strategic priorities.

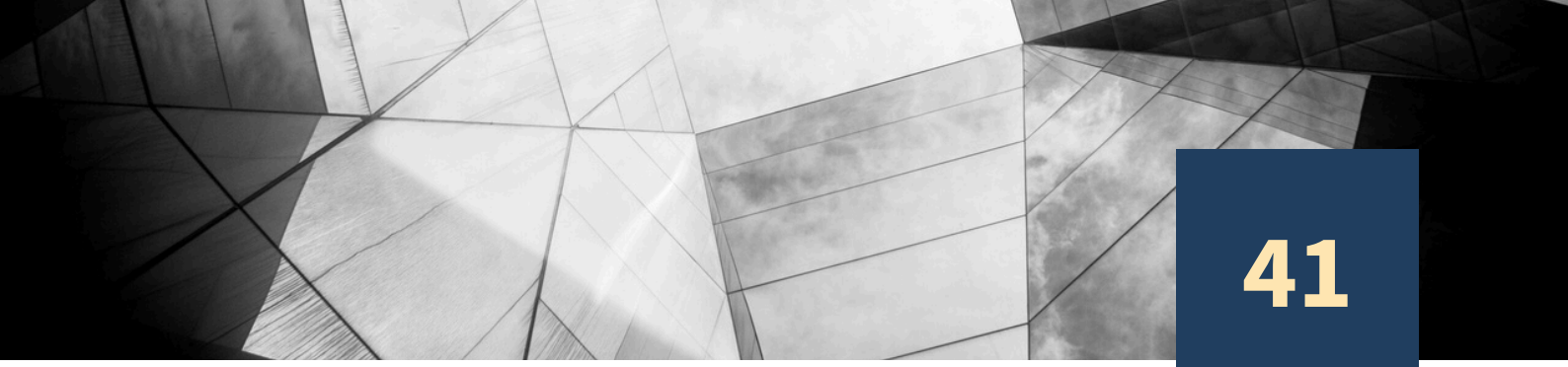
- **Strategic feedback loops**: The insights gained from this taxonomy mapping should serve as a foundation for the planning of future programmes. By applying this evidence-based approach, the EU can help ensure that funding instruments remain responsive to both the common needs of the Union and the specific, evolving vulnerabilities of individual Member States.





ANNEX A: LIST OF PUBLICLY AVAILABLE ISF NATIONAL PROGRAMMES

MEMBER STATE	MANAGING AUTHORITY	SOURCE
Austria	Bundesministerium für Inneres (BMI), Abteilung V/A/4	https://www.bmi.gv.at/107/EU_Foerderungen/Finanzrahmen_2021_2027/Fonds_fuer_die_innere_Sicherheit/start.aspx
Belgium	Federal Public Service Home Affairs - European Funds Unit	https://amif-isf.be/fr/programmation-2021-2027
Bulgaria	International Project Directorate - Ministry of Interior	https://www.mvr.bg/dmp/en/activities/financial-period-2021-2027/internal-security-fund-2021-2027/programming-documents
Croatia	Ministarstvo unutarnjih poslova, Uprava za europske poslove	https://eufondovi.mup.hr/financijski-instrumenti-eu-82/financijski-okvir-2021-2027/489
Cyprus	European Funds Unit, Ministry of Interior	https://www.moi.gov.cy/MOI/eufundsunit.nsf/2127nationalpisf_en/2127nationalpisf_en?OpenDocument
Czechia	Ministerstvo vnitra - odbor fondů EU v oblasti vnitřních věcí	At the date of this report, this information is not publicly available.
Estonia	Estonian Ministry of the Interior	https://dokumendiregistrid.karlerss.com/dokumendid/4235/submission-of-the-internal-security-fund-programme-2021-2027-for-estonia
Finland	Sisäministeriö	At the date of this report, this information is not publicly available.
France	Ministère de l'intérieur - Direction générale des étrangers en France	https://www.interieur.gouv.fr/documentation/programmes-appels-a-projets/programme-national-fsi-2021-2027.html
Germany	Verwaltungsbehörde ISF	https://innerersicherheitsfonds.de/foerderperiode-2021-2027
Greece	Special Service for the Coordination and Management for Migration and Home Affairs Funds	https://migration.gov.gr/programmatiki-periodos-2021-27/
Hungary	Széchenyi Terv Plusz	http://belugyialapok.hu/alapok/programok-2021-2027
Ireland	An Garda Síochána	https://www.garda.ie/en/about-us/our-departments/finance-services/internal-security-fund-isf-2021-2027-national-programming-period.html



MEMBER STATE	MANAGING AUTHORITY	SOURCE
Italy	Ministero dell'Interno - Dipartimento della Pubblica Sicurezza	https://fondieuropeisicurezza.interno.gov.it/isf/it/contents/programma
Latvia	Ministry of the Interior	https://www.iem.gov.lv/en/internal-security-fund-2021-2027-planning-period
Lithuania	Ministry of the Interior	https://vsfsvvp.lt/bendra-informacija/vidaus-saugumo-fondo-programa/vsf-programa/106
Luxembourg	Ministère de la Sécurité intérieure - Police Grand-Ducale	https://fonds-europeens.public.lu/fr/programmes/isf.html
Malta	Funds and Programmes Division	https://fondi.eu/wp-content/uploads/2024/10/QSC-FDP.pdf
Netherlands	Bureau Verantwoordelijke Autoriteit, Ministerie van Justitie en Veiligheid	https://www.uitvoeringvanbeleidszw.nl/subsidies-en-regelingen/algemene-informatie/emvf-2021-2027/isf
Poland	Departament Funduszy Europejskich, MSWiA	Linkhttps://www.gov.pl/web/dfe-mswia/program-funduszu-bezpieczenstwa-wewnetrznego-2021-2027
Portugal	Secretaria-Geral do Ministério da Administração Interna (SG MAI)	Linkhttps://www.sg.mai.gov.pt/FundosComunitarios/QFP20212027/Paginas/default.aspx
Romania	Ministerul Afacerilor Interne - Directia Fonduri Externe Nerambursabile	https://fed.mai.gov.ro/3023/programul-national-2021-2027-securitate-interna-v1-4-aprobat-de-comisia-europeana/
Slovakia	Ministry of Interior of the Slovak Republic	https://www.minv.sk/?o-fonde-isf
Slovenia	Ministrstvo za notranje zadeve	https://evropskasredstva.si/nacionalni-program-sklada-za-notranjo-varnost/
Spain	Ministerio del Interior	https://fondoseuropeos.gob.es/es-es/fondosprogramas/paginas/fsi.aspx
Sweden	Polismyndigheten (Swedish Police Authority)	https://polisen.se/om-polisen/internationell-verksamhet/verksamhet-inom-eu/bmviisf/fonden-for-inre-sakerhet-2021-2027/

ANNEX B: MEMBER STATE BREAKDOWN OF PRIORITIES ACROSS ISF SPECIFIC OBJECTIVES

MEMBER STATE	SO1: INFORMATION EXCHANGE	SO2: OPERATIONAL COOPERATION	SO3: CAPABILITIES AND CRISIS MANAGEMENT
AUSTRIA	5	8	1
BELGIUM	8	4	5
BULGARIA	7	7	11
CROATIA	6	2	13
CYPRUS	6	3	12
CZECHIA	8	4	16
ESTONIA	5	5	7
FINLAND	10	7	9
FRANCE	4	6	10
GERMANY	5	3	5
GREECE	8	5	14
HUNGARY	7	5	6
IRELAND	3	4	6
ITALY	7	5	9
LATVIA	5	3	5
LITHUANIA	7	6	7
LUXEMBURG	4	3	3
MALTA	4	1	4
NETHERLANDS	4	6	5
POLAND	6	5	6
PORTUGAL	7	6	6
ROMANIA	8	4	10
SLOVAKIA	5	3	7
SLOVENIA	8	6	13
SPAIN	5	2	4
SWEDEN	3	4	4
TOTAL	**155**	**117**	**198**

ENACT.
European Network Against Crime and Terrorism

@enact-network

enact-eu.net

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

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