CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

EUROPEAN UNION

STRATEGIC TRAINING NEEDS ASSESSMENT

2026 - 2029

CEPOL is an agency
of the European Union

CEPOL's EU Strategic Training Needs Assessment 2026-2029 Report

Table of Contents

TABLE OF FIGURES

ACRONYMS AND ABBREVIATIONS

AI	Artificial intelligence
AMLA	Anti-Money Laundering and Countering the Financing of Terrorism
API	Advance Passenger Information
ARO	Asset Recovery Office
ATM	Automated Teller Machine
B2C	Business-to-Consumer
CaaS	Crime-as-a-Service
CBRN	Chemical, Biological, Radiological and Nuclear
CCH	Cannabis, Cocaine, and Heroin
BEC	Business Email Compromise
CaaS	Crime-as-a-Service
CEO	Chief Executive Officer
CEPOL	European Union Agency for Law Enforcement Training
CIR	Common Identity Repository
CHSG	Common Horizontal Strategic Goal
CISE	Common Information Sharing Environment
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CNP	Card-Not-Present
COSI	Standing Committee on Operational Cooperation on Internal Security
CSDP	Common Security and Defence Policy
CSAM	Child Sexual Abuse Material
CSE	Child Sexual Exploitation
CSIRT	Computer Security Incident Response Team
CT-SIENA	Counter-Terrorism Secure Information Exchange Network Application
DDoS	Distributed Denial of Service
DeFi	Decentralised Finance
DG Home	Directorate-General for Migration and Home Affairs
EaP	Eastern Partnership
EASO	European Asylum Support Office
EAW	European Arrest Warrant
EEAS	European External Action Service
EES	Entry/Exit System
EFE	European Firearms Experts
EIGE	European Institute for Gender Equality
EIO	European Investigation Order
EJTN	European Judicial Training Network
ESDC	European Security and Defence College
EMCS	Excise Movement and Control System
EMPACT	European Multidisciplinary Platform against Criminal Threats
ENAA	European Network on the Administrative Approach to Prevent and Fight Organised Crime
ENFSI	European Network of Forensic Science Institutes

ENPE	European Network of Prosecutors for the Environment
EnviCrimeNet	Network of European law enforcement agencies against environmental crime
EPPO	European Public Prosecutor's Office
ESDC	European Security and Defence College
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EU	European Union
EUAA	European Union Agency for Asylum
EUCPN	European Crime Prevention Network
EUDA	European Union Drugs Agency
EUFJE	European Union Forum of judges for the Environment
EUIPO	European Union Intellectual Property Office
eu-LISA	European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	European Asylum Dactyloscopy Database
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EU-STNA	European Union Strategic Training Needs Assessment
EUTWIX	European Enforcement Support System
FaaS	Fraud-as-a-Service
FIMI	Foreign Information Manipulation and Interference
FIU	Financial Intelligence Unit
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
FTF	Foreign Terrorist Fighter
GBV	Gender-Based Violence
GDPR	General Data Protection Regulation
IAB	Initial Access Broker
iARMS	Illicit Arms Records and tracing Management System
IMI	Internal Market Information System
InterCOP	International Cyber Offender Prevention Network
IOM	International Organization for Migration
IoT	Internet of Things
IMPEL	EU Network for the Implementation and Enforcement of Environmental Law
IP	Intellectual Property
IPEP	IP Enforcement Portal
ISO	International Organisation for Standardisation
IT	Information Technology
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JRC	Joint Research Centre
LBS	Legal Business Structure
LE	Law Enforcement
LEEd	Law Enforcement Education Platform

LETS	Law Enforcement Training Scheme
LGBTQI+	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, and Others
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
LLM	Large Language Model
LR	Likelihood Ratio
MaaS	Malware-as-a-Service
MDA	Maritime Domain Awareness
MDMA	Methylenedioxy-Methylamphetamine (Ecstasy)
MENA	Middle East and North Africa
MID	Multiple-Identity Detector
MLA	Mutual Legal Assistance
MS	Member State
MTIC	Missing trader intra-community
NATO	North Atlantic Treaty Organization
NAVT	European Network of Associations of Victims of Terrorism
NFFP	National Firearms Focal Point
NFT	Non-fungible token
NGO	Non-Governmental Organisation
NPS	New Psychoactive Substances
OCG	Organised Crime Group
OLAF	European Anti-Fraud Office
OSINT	Open-Source Intelligence
OTF	Operational Task Force
P2P	Peer-to-Peer
P/CVE	Preventing and Countering Violent Extremism
PERCI	EU platform on illicit content online
PMF	Privately Made Firearm
PNR	Passenger Name Record
PPP	Public-Private Partnership
ProtectEU	The European Internal Security Strategy
RaaS	Ransomware-as-a-Service
sBMS	Shared Biometric Matching Service
SIENA	Secure Information Exchange Network Application
SIM	Subscriber Identity Module
SIRIUS	Platform for cross-border access to electronic evidence
SIS	Schengen Information System
SGBV	Sexual and Gender-Based Violence
SOCTA	Serious and Organised Crime Threat Assessment
THB	Trafficking in Human Beings
THC	Tetrahydrocannabinol (Cannabis)
UK	United Kingdom
UN	United Nations
VAT	Value Added Tax
vIBAN	Virtual International Bank Account Number
VIS	Visa Information System

VPN	Virtual Private Network
WCO	World Customs Organization

PREFACE

Law enforcement across the European Union is functioning in a rapidly changing environment. Driven by technological advancements, criminal activity is progressively destabilising, increasingly nurtured online, and strongly accelerated by new technologies, making it more digital, cross-border and interconnected than ever before. Serious and organised crime no longer threatens only public safety; it impacts the very foundations of our institutions and society, with criminal networks increasingly operating as proxies for hybrid threat actors. This evolving landscape requires constant adaptation, enhanced cooperation, and an intelligence-led capacity to anticipate and respond effectively to emerging threats.

In this context, CEPOL's EU Strategic Training Needs Assessment (EU-STNA) 2026–2029 provides a comprehensive, evidence-based overview of current and future training requirements.

The findings of this report show that training needs is rarely limited to specific crime or operational domains. Instead, it is characterised by overlapping and interconnected phenomena, in which transversal skills and core capability gaps, for instance about intelligence-led policing or information exchange, are prevalent. The evolving nature of crime is increasingly shaped by developments in the online field. Digital infrastructures are not only enablers, but also part of the environment in which offenders operate. Emerging technologies, including artificial intelligence, are further increasing the complexity and scale of criminal activities, which reinforces the need for specialised skills and continuous upskilling.

These developments are reflected in the training priorities identified by Member States, with strong demand in areas such as drug trafficking, cyber-attacks and counter-terrorism. At the same time, emerging fields such as environmental crime and hybrid threats point to an increasing transnational dimension of crime. This requires cross-sectoral knowledge and cross-border coordination between teams. This new landscape highlights the need for EU-level training to equip law enforcement with both specialised expertise and horizontal competencies to ensure that capabilities are aligned with operational realities and future demands.

Building on the experience of its two previous cycles, CEPOL's EU-STNA 2026–2029 reflects a mature, collective and intelligence-led process. It is based on extensive consultations with Member States, EU institutions, agencies, training providers and expert networks, ensuring that its findings are grounded in operational realities. The assessment identifies nine horizontal capability gaps and a comprehensive set of

thematic training needs, while also highlighting a significant increase in demand for EU-level training. Member States report that more than 170,000 law enforcement officials will require training in priority areas during the next cycle, underlining the urgent need to scale up and coordinate training provision at European level.

Addressing these challenges requires a shift in our approach to training. Training can no longer be seen as a series of isolated interventions designed to tackle individual threats. Instead, it must be seen as a strategic investment in preparedness, resilience and joint operational capacity. This entails enhancing cross-border collaboration, promoting multidisciplinary and experiential learning formats, incorporating digital and data-driven approaches and ensuring that training stays relevant to the current realities of law enforcement.

CEPOL plays a central role in supporting this transformation. As the EU hub for law enforcement training, it contributes to strengthening cooperation, promoting common standards and facilitating knowledge exchange across Member States. CEPOL's EU-STNA directly informs its multiannual learning programming and supports the implementation of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), ensuring coherence between training provision and EU internal security priorities. It also contributes to the objectives of the *ProtectEU* strategy and the broader European preparedness agenda, reinforcing the Union's capacity to respond to complex and evolving threats.

In this context, continued investment in training is essential. The demand for training at the EU-level exceeds the existing offer, and there are significant disparities in capacity and expertise among Member States. To tackle these challenges, we need to improve coordination among training providers, develop scalable learning solutions and gradually establish minimum common standards and sectoral qualification frameworks. Strengthening cooperation with academia, the private sector and international partners will also be critical to ensuring that training remains both innovative and closely aligned with operational needs.

CEPOL's EU-STNA 2026–2029 provides a forward-looking framework to guide EU-level training efforts. By translating identified capability gaps into concrete priorities, the Agency supports a more coherent and effective approach to law enforcement capacity building across the Union. Strengthening skills, cooperation and a common law enforcement culture remain essential to ensuring preparedness for emerging challenges.

This report supports those objectives as a practical tool for decision-making and the implementation of training priorities across the European law enforcement community. Heads, directors and policy advisors of law enforcement training institutions are encouraged to use its findings to inform curricula development, strategic planning and resource allocation; trainers, experts and practitioners may draw on the assessment to design and deliver relevant, high-impact training activities that reflect evolving crime trends and technological advancements; EU decision-makers

can rely on this report to guide policy development, prioritisation and alignment with the Union's internal security frameworks; and EU Justice and Home Affairs agencies and partners may align their portfolios and joint initiatives with its findings to maximise coherence, reach and operational effectiveness. Through its broad uptake and application, CEPOL's EU-STNA 2026–2029 can serve as a shared reference point, strengthening collective capacity and reinforcing a coordinated European response to the current security challenges.

This publication is delivered at a moment of transition for CEPOL. It builds on the solid groundwork established by my predecessors. With this report as a foundation, the Agency is well positioned to build on past achievements and navigate future challenges —a responsibility that I am honoured to take forward as CEPOL's new Executive Director.

Jan Pecháček

CEPOL Executive Director

Executive Summary

The European Union Strategic Training Needs Assessment (EU-STNA) is the Union's collective, multiannual process for identifying and prioritising the law enforcement (LE) training needs that require coordinated action at the European level. Mandated by Regulation (EU) 2015/2219, which assigns the European Union Agency for Law Enforcement Training (CEPOL) responsibility for assessing strategic training needs and developing multiannual learning programmes, the EU-STNA serves as the Union's central mechanism for translating identified capability gaps into coordinated training priorities.

Taking place in a period defined by rapid digital transformation, geopolitical instability, and increasingly hybrid and technology-enabled criminal threats, the 2026–2029 EU-STNA consolidates its role as the strategic analytical framework guiding EU-level training policy and programming. By embedding forward-looking elements such as the operational use of Artificial Intelligence (AI) and emerging technologies in policing, this cycle reinforces the EU-STNA as a key instrument for strengthening LE competence, cooperation, and resilience across the Union.

Drawing on an analysis of policy documents from the previous four years, the EU-STNA synthesises the training requirements of law enforcement agencies, as identified by subject-matter experts during thematic focus group meetings. In these discussions, experts evaluated which capability challenges emerging from the desk research could be addressed through training. The identified training needs were subsequently ranked by Member States, with the prioritisation weighted according to their representation in the European Parliament. The final list therefore reflects the aggregated priorities of the EU Member States.

Key findings

The 2026-2029 EU-STNA identifies nine horizontal capability gaps and 102 related training needs that recur across all thematic areas and therefore constitute the core training priorities for the next cycle. Validated through expert consultation and Member States feedback, these gaps[1] represent the foundational competencies required for a

[1] Core capability gaps are tools or activities that, although not necessarily crimes as such, facilitate the commission of various crimes; aspects relating to the combating and prevention of crime that are common to various crime areas; and societal challenges.

capable, and future-ready European law enforcement community, in the order of frequency of their mentions under thematic areas:

1. Law enforcement cooperation, information exchange and interoperability
2. Follow, catch and seize the proceeds of crime
3. Use of digital tools, AI, and new technologies
4. Forensics
5. Fundamental rights
6. Prevention and administrative approach
7. Barriers to crime, infiltration, and corruption
8. Document fraud
9. The most threatening criminal networks and individuals

Compared to the previous cycle, the new EU-STNA for 2026-2029 demonstrates strong continuity while introducing a sharper strategic focus. EU cooperation mechanisms, such as EMPACT, Europol platforms, and joint operational frameworks, are functioning well but require sustained awareness and practical promotion to ensure their full potential is realised across all Member States. Hence, law enforcement cooperation, information exchange and interoperability remain a key cross-cutting training need. Financial investigation is now positioned as a comprehensive, end-to-end process spanning asset detection, tracing, freezing, and recovery, with an emphasis on strengthening both operational capability and interagency cooperation throughout the asset management lifecycle. In terms of new technologies, AI is at this cycle fully embedded within the digital skills dimension however, its deployment in law enforcement operations is increasingly accentuated as requiring lawful, accountable, and rights- compliant practices, with fundamental rights considerations becoming integral to training and policy design. Resilience against the infiltration of the legal and public sectors also emerges as a new horizontal concern. Beyond these developments, themes of prevention, integrity, and anti-corruption have gained prominence. The administrative approach has gained visibility as a complementary dimension of crime prevention and disruption, reflecting growing interest in multidisciplinary cooperation and the use of non-criminal law tools to prevent and deter organised crime.

Building on this horizontal framework, the EU-STNA 2026-2029 process identified the crime areas and operational domains where EU-level training support is urgently required. The prioritisation confirms the enduring relevance of traditional high-impact areas such as drug trafficking, counterterrorism, and trafficking in human beings, while placing stronger emphasis on cyber-enabled and technologically advanced criminality. Two domains stand out for their expanded or new strategic relevance: environmental

crime, reflecting the security implications of criminal conduct, which causes or is likely to cause damage to the environment and human health, and hybrid threats, capturing the growing intersection of criminal, cyber, and state-aligned activities used to destabilise the EU. Together with the external dimension of internal security, these priorities highlight the need for law enforcement to operate within a broader more interconnected European security ecosystem, bridging traditional crime control, crisis management, and resilience-building.

The EU-STNA identified a total of 213 thematic training needs, organised within 15 thematic categories. For the forthcoming EMPACT cycle, responding Member States have indicated that training is needed for 170,729 law enforcement officials in the ranked thematic priorities across the European Union[2]. This is a 55% percent increase compared to the last 4 years, clearly indicating higher training demand that the available offer on EU level.

Consultation with EU-level training providers confirmed that, while a broad spectrum of crime areas is theoretically covered, the quantity of training delivered at EU level falls significantly short of operational needs. Providers consistently highlighted the importance of enhancing coherence, strengthening coordination mechanisms, and increasing the frequency of training activities. They also noted the relevance of their work to cross-cutting priorities such as fundamental rights, digitalisation, victims' rights, data protection and the use of administrative prevention tools.

Thematic clusters of EU-level training needs, established as priorities for 2026–2029, are as follows:

1. Drug trafficking
2. Cyber-attacks (fastest-growing crimes in the online sphere)
3. Counterterrorism
4. Online fraud schemes (fastest-growing crimes in the online sphere)
5. Migrant smuggling
6. Online child sexual exploitation (fastest-growing crime in the online sphere)
7. Excise and customs fraud (economic and financial crimes)
8. Trafficking in human beings
9. VAT (including MTIC) fraud (economic and financial crimes)
10. Border management and maritime security
11. Environmental crime

[2] This figure excludes training needs on core capability gaps and in thematic areas under the "Other" category and contains the number of officials where Member States completed the respective survey.

12. Firearms and explosive crimes
13. Hybrid threats
14. Intellectual property crime, counterfeiting of goods and currencies (economic and financial crimes)
15. External dimensions of internal security

In addition to the horizontal and thematic training needs already presented, a number of specialised requirements have been classified under an "Other" category. These needs, while narrower in scope, remain operationally significant and reflect critical capacity gaps within specific domains of law enforcement activity. They include training on Core International Crimes, English law enforcement terminology, and joint training for dog handlers. Further priorities relate to enhancing the law enforcement response to kidnapping and extortion, strengthening leadership and management capabilities (including EU funding and project management competencies) and disaster victim identification. Although these needs may not fall within broader thematic clusters, their inclusion underscores the importance of addressing niche operational and managerial skill sets, to ensure a comprehensive approach to capability development across the EU law enforcement community.

Overall, the findings reaffirm that criminal phenomena are increasingly cross-cutting, digital, and transnational, demanding multidisciplinary responses through the use of interoperable IT systems, components and tools. Two structural constraints persist across most domains: fragmented legal and regulatory frameworks that hinder cooperation and prosecution; and resource limitations that affect both the uptake of training and the operational deployment of trained officials. Some regional variations can be observed among training needs, particularly within thematic clusters linked to the EU's external borders, with countries along the Eastern borders being especially affected. Crimes involving a strong cross-border dimension also tend to be more influenced by regional differentiations. The outcomes of the EU-STNA 2026–2029 are closely aligned with the Council's priorities for the next EMPACT cycle and with the key threats identified in Europol's EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025 and the EU Terrorism Situation and Trend report (EU TE-SAT). Both frameworks highlight the accelerating impact of digitalisation and AI on crime, the rise of cyber-attacks, online fraud schemes, and online child sexual exploitation, and the continued prominence of large-scale drug trafficking and migrant smuggling. Furthermore, the EU-STNA 2026–2029 highlights the continued need to sustain investment in counterterrorism-related training and to strengthen law enforcement capabilities to anticipate, prevent and address threats and criminal activities in this area. The EU-STNA also reflects SOCTA's assessment of hybridised threats, where

organised crime networks intersect with state-aligned or politically motivated actors, as well as systemic risks such as corruption, infiltration of legitimate business structures, and environmental crime. In addition, the training of EMPACT actors themselves is emphasised as a cornerstone of operational coordination, ensuring that EMPACT structures remain equipped to translate EU priorities into practical, field-level cooperation.

Forward-looking considerations for EU-level training

The training needs emerging from this assessment point to a clear evolution in the EU-level training landscape. LE requires not only specialised knowledge within each crime area but also transversal competencies that cut across operational domains, including digital investigation, financial and crypto-forensics, intelligence-led analysis, and ethical, rights-based practice. EU-level training should prioritise cross-border, technology-enabled, and intelligence-driven learning approaches that strengthen both operational cooperation and analytical capability. The findings signal a shift from thematic, threat-specific training towards an integrated model that builds cooperative mechanisms, anticipatory capacity, and resilience across the entire European LE community.

Addressing these challenges, alongside the growing impact of AI, data-driven policing, and hybrid threats, will be essential to ensure that EU-level capacity building keeps pace with the evolving threat landscape and continues to strengthen Europe's collective security architecture. The standardisation of competencies through a future Sectoral Qualifications Framework on Policing could help structure training pathways and ensure coherence across this diverse landscape.

The findings further reveal considerable differences among Member States in terms of institutional capacity, access to training, and thematic specialisation. In several areas, such as child sexual exploitation, certain Member States have established dedicated capacities, while others rely on limited individual expertise. Similar regional variations are observed in areas of economic crime, such as VAT and excise fraud, where some regions exhibit strong cross-border cooperation. These disparities underline the need for differentiated, or "two-speed", training provision tailored to varying national levels of preparedness and expertise. In some cases, the reinforcement of basic training, such as on document fraud or firearms, remains essential before advanced or specialised training can be effectively absorbed.

Building on these findings, the EU-STNA 2026–2029 highlights the main directions for EU-level law enforcement training in the coming cycle. Training provision will continue to address the nine horizontal capability gaps identified in this assessment, including

cooperation, interoperability, digital competencies, forensics, prevention, integrity, and rights-based practice, forming the foundation for all thematic areas. EU-level training is expected to further evolve towards joint, multidisciplinary, and practice-oriented formats that reflect the realities of cross-border operations. The integration of advanced technologies, data-driven analysis, and AI into training design and delivery will be essential to ensure operational relevance and resilience. Emerging domains such as hybrid threats, environmental crime, and the external dimensions of internal security point to a wider European security ecosystem that increasingly connects criminal, technological, and geopolitical factors. Addressing these will require maintaining close cooperation among JHA agencies, MS, academia, and private-sector actors.

By translating empirically assessed threats into concrete training priorities, the EU-STNA 2026–2029 ensures that EU-level capacity building directly supports operational cooperation and aligns with the evolving strategic framework for internal security. Its implementation through EMPACT 2026–2029 and CEPOL's multiannual learning programming will maintain coherence between EU-level training provision and the Union's wider security objectives. This contributes to the new ProtectEU - the European Internal Security Strategy and the EU Preparedness Union, with a focus on resilience, interoperability, and preparedness against hybrid, digital, and cross-border threats. Through this forward-looking approach, the EU-STNA 2026-2029 can serve as the Union's strategic roadmap for LE capacity building - driving coherence, operational readiness, and a shared culture of security and professionalism across the MS.

The number of officials who need training in thematic areas ranked is approximately 1.5 times higher than in the previous EMPACT cycle and exceeds the current capacity of training providers. Capacities should be strengthened to deliver specialised training and to enhance support for cross-border investigations. Additionally, as indicated in focus group meetings, awareness-level training across multiple thematic areas would be beneficial to ensure a more consistent level of preparedness among EU law enforcement officials.

To ensure sustainable capability development, training should be approached from a life-long learning perspective, supporting continuous professional growth throughout law enforcement careers. In this regard, the establishment of an accredited training quality assurance framework is essential. Developing a sectoral qualifications framework (SQF) for policing, aligned with the European Qualifications Framework (EQF) and relevant Council recommendations, could serve as a foundational step towards a harmonised, competency-based approach across the EU. As a subsequent step, the certification and accreditation of law enforcement training activities through

micro-credentials[3] could provide a practical foundation for the quality assurance framework.

Overview of the methodology

Implemented by CEPOL in close cooperation with the Member States, the European Commission, and other Justice and Home Affairs agencies, the EU-STNA ensures that EU-level training provision supports the Union's shared internal security objectives and strengthens operational cooperation under the European Multidisciplinary Platform Against Criminal Threats. It serves as a strategic reference framework for law enforcement capacity building under the European Agenda on Security, ProtectEU and the EMPACT policy cycle, while contributing to the implementation of the Law Enforcement Training Scheme (LETS) and align closely with the broader policy context.

Since its pilot in 2017, the EU-STNA has evolved over the 2018–2021 and 2022–2025 cycles into a consistent and well-structured component of the EU's internal security architecture. It provides a systematic, evidence-based, and participatory framework that combines desk research, expert consultation, Member State prioritisation, and coordination with EU-level training providers to ensure that collective efforts remain coherent, complementary, and responsive to operational realities.

The 2026–2029 cycle builds on the foundations laid by the previous assessments, applying lessons learned and introducing further methodological refinements. Conducted by CEPOL, in close cooperation with Member States, EU agencies, and thematic expert networks, it represents the Union's third multiannual process for identifying and prioritising EU-level law enforcement training needs.

The assessment focuses exclusively on the training dimension of internal security and its external aspects. It does not rank or assess crime threats but identifies where EU-level training can most effectively strengthen operational capabilities, cooperation, and interoperability across Member States. The analysis combines a comprehensive review of EU policy and strategy documents with extensive expert consultations, ensuring both policy alignment and operational validation.

A distinction is made between environmental challenges, referring to structural factors that influence law enforcement performance but cannot be resolved through training (e.g., legal fragmentation, resource constraints), and capability challenges, referring to

[3] As per Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02

gaps in knowledge, skills, responsibility, or autonomy that can be addressed through targeted learning interventions.

A structured prioritisation exercise formed one of the key components of the methodology. Member States were invited to rank both the main thematic categories and the individual EU-level training needs through a survey circulated by CEPOL. Each Member State submitted one coordinated national position, reflecting priorities from an EU perspective. The ranking was carried out by assigning numerical values to indicate relative importance, and Member States were also requested to estimate the number of law enforcement officials requiring training in each area during 2026–2029, using a broad definition of law enforcement authorities. In line with previous cycles, non-responses or partial responses were treated using standardised rules to ensure comparability.

Validated through Member State consultation, the results present a prioritised list of EU-level training needs and nine cross-cutting capability gaps that form the strategic framework for the next training cycle. These findings serve as a shared reference point for aligning EU-level and national training provision with CEPOL's multiannual learning programming, the EMPACT 2026–2029 priorities, and the broader objectives of ProtectEU. Building on previous cycles, the EU-STNA 2026–2029 introduces methodological improvements and a forward-looking framework to enhance law enforcement capabilities and cooperation across an increasingly complex security landscape.

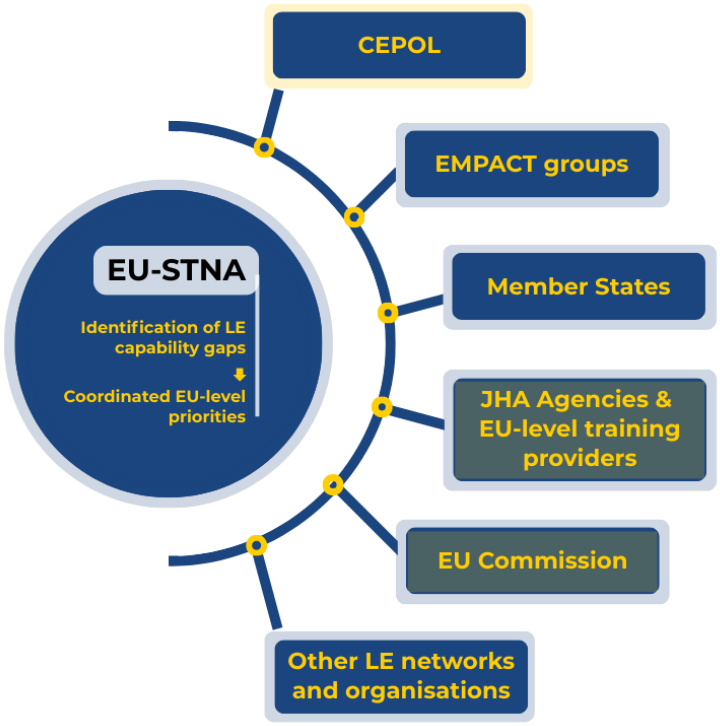
BACKGROUND

The EU-STNA 2026–2029 identifies the strategic and EU-level training needs of LE officials for the next four-year cycle of the EMPACT. It provides a consolidated, evidence-based foundation for guiding EU-level training and capacity-building, ensuring that collective efforts effectively support operational cooperation, interoperability, and policy coherence across the Union.

Established under Regulation (EU) 2015/2219, which mandates CEPOL to assess strategic training needs and deliver multiannual learning programmes, the EU-STNA functions as the Union's central mechanism for identifying law enforcement capability gaps and translating them into coordinated EU-level training priorities. Bringing together the Member States, the European Commission, CEPOL, and other JHA agencies, the EU-STNA ensures that EU-level training provision supports the Union's common internal security objectives and strengthens the professional competence of law enforcement officials across Europe.

The EU-STNA serves as a strategic reference point for EU-level capacity building under the European Agenda on Security, ProtectEU and the EMPACT framework. It also supports the implementation of the LETs, promoting a shared European LE culture and the interoperability of skills. The process is closely aligned with the EU's broader policy landscape, including Council Conclusions on internal security, the use of artificial intelligence in law enforcement, the fight against organised crime, and the response to hybrid and technology-driven threats. By providing a structured and evidence-based mechanism for collective prioritisation, the EU-STNA ensures that European LE training remains coherent, forward-looking, and responsive to evolving security challenges.

Figure 1. EU-STNA governance and actors



In a context where crime evolves faster than institutional adaptation cycles, maintaining up-to-date competencies, ensuring cross-border interoperability, and applying advanced investigative tools have become fundamental to safeguarding European internal security. The EU-STNA process was established to provide a systematic, evidence-based mechanism for identifying the most central EU-level training needs across Member States and for ensuring that training resources are directed where they generate the greatest added value. Launched as a pilot in 2017, the EU-STNA has since evolved through the 2018–2021 and 2022–2025 cycles into a regular, multi-stakeholder exercise combining desk research, expert consultation, Member State prioritisation, and coordination with EU-level training providers. It plays a central role in enhancing complementarity among EU training actors, preventing overlap, and fostering a coherent European law enforcement learning space. The 2026–2029 cycle continues this evolution, applying methodological refinements introduced in earlier cycles and integrating forward-looking elements, consolidating the process as a permanent component of the EU's internal security architecture.

Methodology

The EU-STNA follows a seven-step, multi-annual, and consultative process designed to systematically and transparently identify, validate, and prioritise EU-level LE training needs. Each step builds on the previous one, creating an iterative cycle that links

evidence, expert judgement, political validation, and feedback from implementation. The approach ensures that EU-level training priorities are simultaneously anchored in policy objectives and responsive to operational realities across Member States.

Figure 22. EU-STNA methodological process and validation loop

Step 1 - Desk research. The process begins with a comprehensive desk research phase, which establishes the analytical foundation for all subsequent stages. CEPOL systematically reviews a broad corpus of EU strategic and policy documents, including Council conclusions, Communications, agency threat assessments, evaluations, and legislative texts, provided by the European Commission (DG HOME) and the JHA agencies. The purpose of this stage is to map the current and emerging security threats, horizontal capability challenges, and thematic areas where training has a clear EU-level dimension. The findings are structured and coded into analytical categories that form the initial list of potential training themes to be validated later through expert consultation.

Step 2 - Expert consultations. In the second step, the preliminary findings are evaluated and refined through consultations with operational experts. CEPOL organises focus groups and interviews, involving EMPACT thematic groups, JHA agencies and specialised professional networks. These discussions provide essential

practitioner insight, ensuring that the identified capability gaps and training needs reflect the real conditions and challenges faced by law enforcement authorities in the field. Experts also highlight emerging issues not yet captured in policy documents, helping to distinguish between capability challenges that can be addressed through training and broader environmental or structural constraints.

Step 3 – Member State prioritisation. Once the thematic and horizontal training needs are consolidated, Member States are invited to review and prioritise them. National representatives assess the relative importance of each need at the strategic level and may estimate the indicative number of officials requiring training in each area. Member States shall submit figures via their officially nominated contact points who coordinate the response within their countries. This prioritisation exercise provides a quantitative and qualitative picture of where EU-level training interventions would add the greatest value, helping to define the scope and expected scale of future activities.

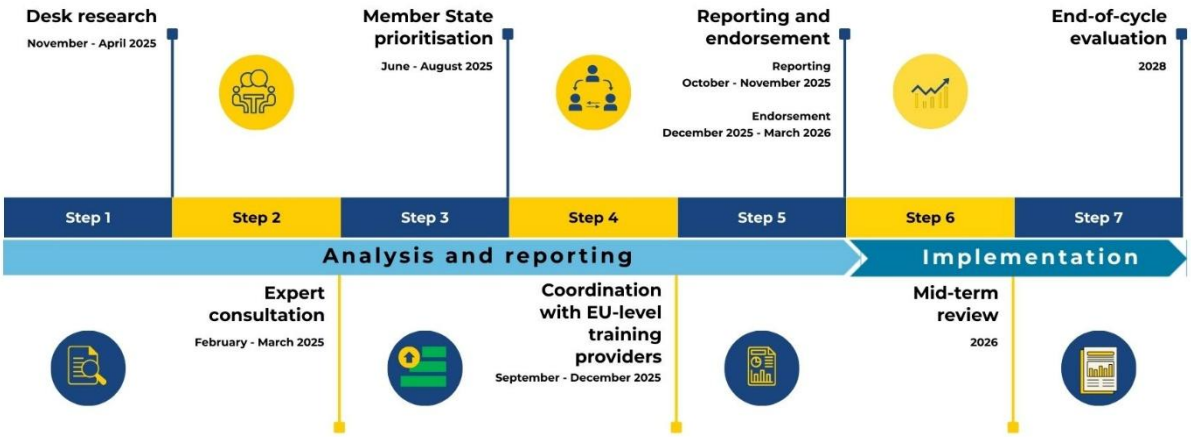
Step 4 – Coordination with EU-level training providers. Following the prioritisation of Member States, the emerging results are circulated among EU-level training providers, including CEPOL, Europol, Frontex, Eurojust, EJTN, ESDC, and other relevant entities, for comments and coordination. This step ensures complementarity between different training portfolios, prevents duplication, and facilitates the strategic allocation of responsibilities among providers. The process also supports the alignment of the EU-STNA priorities with CEPOL's multi-annual learning programme and the training frameworks of other JHA agencies.

Step 5 – Reporting and endorsement. The validated findings are then consolidated into the EU-STNA Report. This document provides the formal list of EU-level training priorities and serves as the strategic reference for the next four-year cycle. The report shall be presented to the Standing Committee on Internal Security (COSI) and to the European Parliament, thereby embedding the EU-STNA within the Union's internal-security governance architecture. This institutional validation guarantees political ownership of the results and ensures their integration into subsequent policy and programming cycles.

Step 6 – Mid-term review. To maintain relevance throughout the four-year period, the EU-STNA methodology includes a mid-term review. Conducted approximately halfway through the cycle, this review examines whether new threats, technological developments, or policy changes have created additional capability gaps that require EU-level training responses. The review allows for course correction and updating of priorities, keeping the overall framework dynamic and forward-looking.

Step 7 – End-of-cycle evaluation. The cycle concludes with an independent evaluation assessing the process and outcomes of the EU-STNA. The evaluation examines the quality of evidence collection, stakeholder engagement, prioritisation methods and practical implementation impact. Lessons learned from this assessment shape the next EU-STNA cycle, ensuring continuous methodological improvement and sustained alignment with the subsequent EMPACT framework.

Figure 33. Timeline and methodology



Analytical scope and focus

To clarify where training can deliver measurable operational improvements, the EU-STNA distinguishes between two types of challenges:

- Environmental challenges, referring to structural factors that affect performance but cannot be solved through training, and
- Capability challenges, referring to gaps in knowledge, skills, responsibility, and autonomy that can be addressed through targeted learning interventions.

Figure 44. Distinction between environmental and capability challenges

This distinction clarifies where training can make a measurable contribution to operational improvement while identifying contextual issues that demand broader policy attention.

The entire process is iterative, combining analytical evidence, expert judgement, and Member State validation. This ensures that EU-level training priorities reflect both policy imperatives and practical operational needs.

Timeline and process

Steps	Stakeholders involved	Outputs
Step 1. Desk research December 2024 - May 2025	• DG Home • JHA agencies • MS	• 264 documents analysed • 1401 capability challenges identified
Step 2-3. Identification of EU-level training needs February - June 2025	• MS • DG Home • JHA agencies • Other LE professional networks via focus group meetings and online consultations	• 22 focus group meetings • 1 online survey • 1 direct consultation with ENFSI • 212 experts consulted • 317 training needs identified
Step 4. Prioritisation June - September 2025	MS	All but one MS provided ranking
Step 5. Reporting and endorsement September 2025 - Q1 2026	• CEPOL • DG Home • JHA agencies • Council of the EU	Report published
Step 6. Mid-term review 2027		
Step 7. Evaluation 2028		

The 2026–2029 EU-STNA process identified a set of nine horizontal capability gaps that span across all thematic areas, as well as fifteen thematic domains and an additional "Other" category where EU-level training intervention is most warranted. All together, these constitute the analytical backbone of this report and provide the basis for structuring both the horizontal and thematic chapters that follow.

The horizontal capability gaps represent the foundational competencies required across all areas of law enforcement cooperation, while the thematic domains reflect the specific operational and crime-related contexts where these competencies must be applied. The combination of both dimensions ensures that EU-level training priorities address not only thematic specialisation but also the transversal skills and capabilities underpinning effective cross-border cooperation.

All Member States, except one, participated in the prioritisation exercise ensuring broad representation of EU perspectives. Horizontal training needs were ranked according to the frequency with which they were identified within each thematic area, providing a systematic basis for EU-level prioritisation. Participating Member States indicated that 170,729 law enforcement officials across the EU will require training during the

upcoming EMPACT cycle, in the thematic areas ranked by them[4], supporting targeted and proportionate capacity-building efforts.

Capability gaps
1. Law enforcement cooperation, information exchange and interoperability
2. Follow, catch and seize the proceeds of crime
3. Use of digital tools, Artificial Intelligence (AI) and new technologies
4. Forensics
5. Fundamental rights
6. Prevention and administrative approach
7. Barriers to crime, infiltration and corruption
8. Document fraud
9. The most threatening criminal networks and individuals

Thematic training areas
1. Drug trafficking
2. Cyber-attacks (fastest-growing crimes in the online sphere)
3. Counterterrorism
4. Online fraud schemes (fastest-growing crimes in the online sphere)
5. Migrant smuggling
6. Online child sexual exploitation (fastest-growing crime in the online sphere)
7. Excise and customs fraud (economic and financial crimes)
8. Trafficking in human beings
9. VAT (including MTIC) fraud (economic and financial crimes)
10. Border management and maritime security
11. Environmental crime
12. Firearms and explosive crimes
13. Hybrid threats
14. Intellectual property crime, counterfeiting of goods and currencies (economic and financial crimes)
15. External dimensions of internal security
16. Other training needs

[4] This figure excludes training needs on core capability gaps and in thematic areas under the "Other" category and contains the number of officials where Member States completed the respective survey.

Structure of the report

These horizontal and thematic priorities provide the framework for the report's analytical structure. The report is organised into four chapters, presented in an order that reflects both the cross-cutting and thematic dimensions of the EU-STNA 2026–2029. Following this introductory chapter, Chapter 2 presents the consolidated findings on the core capability gaps identified across all thematic areas. Chapter 3 examines in detail the thematic training areas, outlining the specific EU-level training priorities as validated and prioritised by the Member States. Chapter 4 presents the results of the consultation with EU-level training providers, conducted to review the existing EU-level training available to law enforcement, identify potential gaps, and reduce overlaps in provision. Chapter 5 brings together the main conclusions and sets out the strategic directions for EU-level law enforcement training in the 2026–2029 cycle.

In Chapter 2, the presentation of core capability gaps is organised based on the frequency with which horizontal training needs were mentioned within each thematic area. The detailed list of training needs is provided in alphabetical order. The order of thematic subchapters in Chapter 3 reflects the prioritisation of training needs established by Member States, rather than the ranking of crime threats. This sequence underscores the areas in which contributors across the Union identify the most significant capability gaps and where EU-level training interventions are deemed most critical for operational effectiveness. The same prioritisation is applied to the detailed list of training needs within each thematic area.

Each thematic subchapter follows a consistent analytical structure. It starts with a brief overview providing general insights into the respective crime area, followed by a presentation of the key challenges influencing the effectiveness and efficiency of law enforcement in that area. These challenges are divided into two categories: environmental challenges, which refer to structural or contextual factors that cannot be addressed through training, and capability challenges, which concern the knowledge, skills, responsibility, and autonomy of law enforcement officials and can be addressed through targeted learning interventions. Each subchapter then summarises the related training needs, including a prioritised list that indicates the areas where EU-level action is most justified.

1. Core capability gaps (Horizontal training priorities)

Core capability gaps are the horizontal, recurring challenges that cut across all crime areas and operational contexts[5]. They are evidenced consistently throughout the EU-STNA 2026-2029 desk review and were validated through expert consultations and Member State feedback. Because they underpin effectiveness in every thematic field, these gaps should be embedded as a baseline in all training for LE practitioners and systematically reflected in EU-level curricula, both in generalist programmes and in specialist courses.

The EU-STNA 2026-2029 process identified nine cross-cutting areas with 104 training needs where strengthening capability through training will have the greatest system-wide impact:

1. Law enforcement cooperation, information exchange and interoperability
2. Follow, catch and seize the proceeds of crime
3. Use of digital tools, AI, and new technologies
4. Forensics
5. Fundamental rights
6. Prevention and administration approach
7. Barriers to crimes, infiltration, and corruption
8. Document fraud
9. The most threatening criminal networks and individuals

These nine areas emerged as the central capability challenges confirmed through document analysis, expert consultations, and Member State validation. They are presented in the order of their frequency across thematic areas rather than by priority level. Together, they define the core domains where capacity building should be prioritised through EU-level training during the 2026-2029 cycle.

In general, there is a strong element of continuity with the 2022-2025 cycle, reinforcing the need for sustained investment to ensure that LE capacity keeps pace with an increasingly complex and rapidly evolving security environment. AI is now explicitly integrated into the broader digital capability challenge. A theme of *"follow, catch and seize the proceeds of crime"* reframes financial investigation around end-to-end asset recovery, and administrative and regulatory measures are positioned alongside

[5] Core capability gaps are tools or activities that, although not necessarily crimes as such, facilitate the commission of various crimes; aspects relating to the combating and prevention of crime that are common to various crime areas; and societal challenges.

preventive approaches to crime. A new area, namely "*barriers to crime, infiltration and corruption*", has been added to reflect the growing threat that organised crime poses to the integrity of legal business structures, public administration, and state institutions.

The prioritisation of *law enforcement cooperation, information exchange and interoperability* as the leading horizontal challenge marks an important shift in focus. It reflects the expanding scale, speed and cross-border character of contemporary criminality and highlights the operational imperative of cooperation, secure information exchange and technological interoperability as the foundation for effective joint responses across jurisdictions, and disciplines.

Many of these core challenges are also being addressed through Horizon Europe, particularly under the "Fighting Crime and Terrorism" cluster, which develops innovative tools, training materials and operational methodologies for practitioners. Continued coordination between EU-level training providers and such research initiatives is essential to maximise synergies, enhance impact and avoid duplication of effort.

The following sections present each of the nine core capability challenges in detail, outlining their defining features and the specific training needs identified under each.

1.1 Law enforcement cooperation, information exchange and interoperability

The EU-STNA 2026–2029 identifies law enforcement cooperation, information exchange and interoperability as the foremost horizontal challenge to address through training. It underpins the effectiveness of all operational cooperation within the Union and remains a precondition for a coherent European law enforcement area. Meeting this challenge requires a shared operational culture across agencies and borders, consistent proficiency with existing cooperation mechanisms, and the effective use of large-scale IT systems supporting information exchange and of interoperability components and tools. The reinforcement of the EMPACT framework as the backbone of law enforcement cooperation requires continuous training of all EMPACT actors. On the same model, the creation of a training curriculum aimed at practitioners from Police Custom Cooperation Centres would be highly beneficial.

A key priority is strengthening a common EU law enforcement culture that fosters cooperation among international and national police bodies, customs agencies, and public–private partners, particularly in areas such as cyber-enabled criminality. This shared culture supports a more unified and effective response to cross-border threats.

Training must therefore raise awareness and operational proficiency in the practical use of EU cooperation tools and mechanisms, including Eurojust coordination, Secure Information Exchange Network Application (SIENA), Joint Investigation Teams (JITs), the European Arrest Warrant (EAW), the Prüm Convention, rules for information exchange established under Directive 2023/977, and operational practices such as cross-border surveillance. Consistent interpretation of relevant Court of Justice rulings and consistent procedures for verifying high-risk individuals at borders are equally essential to ensure legal and operational coherence. While enhancing law enforcement culture is primarily an EU-level priority, complementary initiatives at the regional level can further reinforce its effectiveness.

The increasing emphasis on interoperability brings new requirements for the quality, integrity, and technical standards of biometric and other data exchanged across systems, as well as for awareness of potential vulnerabilities and data security. Training should strengthen user competence in the collection, handling, and lawful processing of such data, in full respect of data protection principles and access rights.

Training should enhance practitioners' ability to operate and interconnect large-scale systems covered by Regulations (EU) 2019/817 and (EU) 2019/818, including the Schengen Information System (SIS), Visa Information System (VIS), the European Dactyloscopy Database (Eurodac), and the European Travel Information and Authorisation System (ETIAS). It is important to reinforce the use of interoperable EU systems for risk assessment in visa and border-management processes, ensuring consistent application of security procedures across Member States. Additionally, the Advanced Passenger Information (API) and Passenger Name Record (PNR) are key electronic data interchange systems that require appropriate operational use by law enforcement authorities.

The EU-STNA 2026-2029 process highlights the critical importance of end-user readiness to leverage interoperability components and tools such as the European Search Portal (ESP), the shared Biometric Matching Service (sBMS), the Common Identity Repository (CIR) and the Multiple-Identity Detector (MID) for effective identity resolution and detection of identity fraud.

List of detailed training needs

- Awareness of EU interoperability components and tools, and their added value in facilitating secure and streamlined access to information necessary for the

performance of law enforcement and border management tasks, including the detection of identity misuse.
- Ensuring quality and integrity of biometric data in EU information exchange systems: standards, vulnerabilities, and best practices.
- Large-scale EU IT information systems, and main interoperability components and tools (e.g. Multiple-Identity Detector (MID), European Search Portal (ESP), Common Identity Repository (CIR), the Central Repository for Reporting and Statistics (CRRS)).
- Lawful data collection, handling, and processing in EU information exchange systems, including data protection principles and access rights.
- Operational use of Advanced Passenger Information and Passenger Name Record data in border security and law enforcement, including integration, accuracy, and legal frameworks
- Preparing end users to effectively access and use existing EU security and migration databases.
- Risk assessment procedures using ETIAS, VIS, and other interoperable EU systems to identify potential security threats in visa and ETIAS application processes.
- Technical training on operational use and functionalities of large-scale EU information systems (e.g., SIS, VIS, Eurodac, ETIAS).

1.2 Follow, catch and seize the proceeds of crime

Strengthening the capability to trace, restrain and recover criminal assets constitutes the second core horizontal priority identified by the EU-STNA 2026-2029 process. It spans technological, investigative, legal, and international cooperation dimensions and requires extensive, practice-oriented training.

Evolving financial ecosystems, encompassing non-fungible tokens (NFTs), decentralised finance (DeFi), virtual international bank account numbers (vIBAN), peer-to-peer platforms and AI-driven money laundering schemes, are transforming the landscape of criminal finance. Addressing these developments demands advanced skills in tracing cryptocurrencies and pseudonymous tokens, conducting blockchain crypto-forensic analysis, and performing deep- and dark-web investigations using enhanced open-source intelligence (OSINT). The digital nature of financial evidence further necessitates specialised competence in the lawful cross-border exchange and

preservation of electronic evidence, including awareness of relevant legislation and admissibility requirements.

From an operational perspective, LE practitioners must understand and investigate complex criminal structures and techniques. Training should cover enablers and crime-as-a-service models, the use and layering of shell companies, and money-mule recruitment methods increasingly deployed on social media. Key skills include identifying early red flags, employing disruption techniques, and dismantling physical cash-courier networks operating across borders.

Effective asset recovery depends equally on the confident application of legal instruments and multi-agency coordination. Training must therefore strengthen knowledge of existing international cooperation frameworks and mutual recognition mechanisms, such as the use of Article 31 of the European Public Prosecutor's Office (EPPO) Regulation, to overcome procedural and jurisdictional barriers. Understanding and applying complex regulatory concepts, including "beneficial ownership" and the mutual recognition of freezing and confiscation orders, is essential to ensure that criminal proceeds can be systematically traced and recovered across the Union. Specialised modules should also enhance practitioner competence in identifying cross-chain laundering typologies and applying forensic techniques across decentralised financial systems.

List of detailed training needs

- Asset recovery techniques, tools, legal channels, and cross-border cooperation, multi-agency approach.
- Cross-border cooperation tools and techniques, as outlined in Article 31 of the EPPO Regulation.
- Cross-border exchange of electronic evidence along with preservation of e-evidence and related legislation.
- Deep and dark web investigative techniques, advanced OSINT.
- Detecting and disrupting cross-border cash courier networks used to move illicit funds physically requires cross-border cooperation.
- Early detection techniques, including identifying red flags and indicators of relevant transfers, revenue or EU expenditure fraud, as well as disruption techniques.
- Emerging technologies, including non-financial tokens, peer-to-peer platforms, and pseudonymous tokens.

- Enablers and crime-as-a-service; typologies, investigative techniques related to parallel financial systems; operation of shell companies.
- Financial and cryptocurrency forensics, including: blockchain analysis, cryptocurrency tracing, cross-chain laundering detection, and forensic investigation of DeFi systems.
- Overview of DeFi and money laundering implications.
- Regulatory issues: mutual recognition of freezing and confiscation orders; interpretation of "beneficial ownership" and "commercial scale".
- Techniques for money mule recruitment include monitoring social media and other online platforms.
- Tracing cryptocurrencies (including crypto basics such as typology, crypto forensics for specialists in the financial crime area.

1.3 The use of digital tools, AI, and new technologies

Digitalisation and emerging technologies are transforming both the methods of crime and the operational landscape of law enforcement. Criminal actors increasingly exploit encrypted platforms, anonymisation tools and Crime-as-a-Service (CaaS) markets, reducing investigative visibility and complicating cross-border cooperation. The rapid evolution of AI misuse, enabling the creation of deepfakes, adaptive malware and synthetic identities, further accelerates harm and outpaces the development of detection and investigative tools. These developments create far-reaching capability challenges, from tracing fraud involving cryptocurrencies and NTFs to investigating modern vehicle-related digital crime or obtaining admissible electronic evidence from encrypted or AI-altered sources.

Law enforcement must be prepared to anticipate and counter emerging hybrid threats, including drone-based attacks. Addressing these challenges requires capability development that combines technical depth, strategic foresight, and strong ethical and legal safeguards, while ensuring transparency, accountability, and respect for fundamental rights in the operational use of AI and digital tools. Training must also foster awareness of the broader legal and regulatory ecosystem, including the Artificial Intelligence Act, Digital Services Act, General Data Protection Regulation (GDPR), and emerging domains such as big data and quantum technologies that are increasingly relevant for law enforcement operations and oversight.

Training should therefore prioritise a balanced set of technical, investigative and ethical competencies. Key areas include lawful decryption methodologies, advanced digital forensics, analysis of anonymised and darknet content, and specialised investigation of cyber-enabled fraud involving digital assets such as cryptocurrencies and NFTs. These training priorities are closely linked to the EU's ongoing efforts under the ProtectEU package and the Roadmap on Lawful and Effective Access to Data for law enforcement.

A baseline of AI literacy for all practitioners is essential, covering the identification of criminally used AI, awareness of the Artificial Intelligence Act and other relevant regulatory frameworks, and the responsible use of AI-assisted tools for investigation and analysis. Specific attention should also be given to AI-based techniques used in sanction evasion, document fraud and synthetic identity creation, as well as to the organisational use of AI in decision-making and personnel management.

Training should also strengthen awareness of emerging technologies with operational relevance, such as connected and smart vehicles, counter-drone detection systems, and predictive or real-time analytics tools, ensuring that their use remains both lawful and effective. Finally, familiarity with cross-border intelligence-sharing platforms and secure communication mechanisms should be mainstreamed to support coordinated digital investigations and a more integrated EU LE response to technology-driven crime.

List of detailed training needs

Artificial Intelligence

- AI-related risks that impact fundamental rights, discriminatory profiling, surveillance, and data handling.
- Application and operational use of AI-assisted capabilities developed for or used by law enforcement agencies.
- Identification and investigative response to AI-based techniques used in sanction evasion, document fraud, and synthetic identity creation.
- Implications and risks of AI use in organisational decision-making and personnel management in law enforcement.
- Deployment in offline and online environments of custom trained AI tools for detecting, analysing and investigating crimes in offline and online environments.

Applied digital forensic

- Awareness for first responders on emerging technologies (e.g., connected vehicles, smart systems) and their forensic relevance in digital crime scenes.
- Digital investigative techniques and forensic tools related to vehicle theft, including the latest offender methods.
- Drone-based threats, operational response frameworks, and counter-drone detection and mitigation systems.
- Digital forensic investigative methodologies; technical knowledge on search, collection, and seizure of admissible evidence from next-gen digital infrastructures, forensics in investigating piracy networks; AI-assisted digital forensics (real-time filtering, triage, prioritisation) tools.

Digital investigations

- Investigating cyber-enabled fraud and theft involving digital assets, including cryptocurrencies, non-financial tokens, vIBANs, and decentralised financial systems.
- Investigative frameworks and available tools to address online-facilitated crimes, including cybercrime-as-a-service.
- OSINT techniques for digital investigations and situational awareness.
- Techniques for identifying, accessing, and analysing content on anonymised websites and darknet platforms.
- Lawful decryption techniques and advanced threat intelligence analysis, including handling encrypted communications and devices, digital decryption tools and procedures, legal aspects of decryption in investigations and threats enhanced by AI.

Others

- Legal and ethical frameworks (Artificial Intelligence Act, Digital Services Act, GDPR) and the use of AI, restrictions on high-risk or prohibited uses of AI in law enforcement and justice contexts, big data, and quantum technologies by law enforcement and criminals.
- Cross-border intelligence exchange platforms, coordination mechanisms, and secure communication tools.
- Use of satellite surveillance, predictive modelling, and real-time analytics to identify and respond to evolving security risks.

1.4 Forensics

Forensic capabilities are fundamental to investigations across nearly all crime areas, yet are increasingly challenged in the digital, chemical and ballistic domains. A primary challenge concerns the lawful acquisition and admissible analysis of electronic evidence, often encrypted, decentralised or AI-altered, which complicates investigations ranging from child sexual exploitation to intellectual property theft. To respond to it, advanced digital forensics should include lawful decryption, the acquisition and preservation of admissible electronic evidence from complex digital environments, and the use of AI-assisted tools for data filtering, triage, and analysis. These efforts should align with EU initiatives on lawful data access that promote secure and proportionate access to digital evidence by law enforcement authorities. Training should also address synthetic media and AI-generated content forensics, including the detection and interpretation of deepfakes and AI-driven manipulation.

Law enforcement agencies frequently lack the advanced digital forensic tools and expertise required to trace illicit financial flows across cryptocurrencies, NFTs and DeFi platforms, impeding investigations into money laundering, VAT fraud and terrorism financing. Crypto forensics should equip investigators to trace illicit financial transactions across blockchains and DeFi systems.

In drug trafficking, forensic and toxicological capacity must evolve rapidly to analyse new psychoactive substances (NPS), monitor the increasing potency of synthetic drugs, and detect adulteration with substances. Therefore, drug-related forensics training should cover innovative analytical and toxicological techniques for emerging synthetics and NPS, drawing on advanced methods such as chemometrics and data science.

Firearms investigations likewise require modernised forensic infrastructure and expertise. This includes the ability to conduct timely ballistic analysis and trace weapons produced through 3D printing, conversion, or fraudulent sourcing, in line with international standards such as ISO 21043. Ballistic information exchange should also be reinforced.

In addition, awareness training for first responders should address the forensic implications of new technologies, such as smart and connected vehicles, ensuring proper evidence preservation at digital and hybrid crime scenes. Modern crime scene forensics, including digital trace detection and scene reconstruction using technology-enabled tools, should be integrated into basic and advanced training curricula.

Finally, foundational improvements, covering method validation, accreditation, risk management and audit processes for laboratories, certification of forensic professionals, and reporting standards such as the expression of results and use of likelihood ratios are essential to maintain the reliability, comparability, and courtroom readiness of forensic results across Member States. The responsible use of AI tools in forensic workflows, for example, in report writing, anonymisation, simulated case generation and cross-case data comparison, should also be incorporated to strengthen analytical consistency and efficiency.

List of detailed training needs

- Applications of chemometrics on forensic data.
- Audit and risk management for forensic laboratories.
- Basic digital forensics, including mobile device forensics, chain of custody and lawful evidence handling, acquisition, analysis, and reporting of digital evidence, and courtroom presentation of forensic findings.
- Expression of results, understanding, and application of Likelihood Ratio to forensic evidence.
- Innovative tools and technologies for forensic practices across multiple disciplines.
- Introduction to Data Science.
- ISO 21043 parts 1, 2, 3, 4 and 5.
- Synthetic media and AI-generated content forensics, including: deepfake detection, AI-generated evidence analysis, adversarial AI techniques used in fraud and impersonation, and real-time monitoring of AI-driven cyberattacks.
- Updated crime scene forensics, including digital trace detection, scene reconstruction using tech-enabled tools.
- Use of AI in forensics and investigations (e.g., analysis, legal compliance, generation of evidence and documentation).

1.5 Fundamental rights

Safeguarding fundamental rights is integral to effective and legitimate policing. Law enforcement agencies face persistent challenges in ensuring rights-based practice while addressing increasingly complex criminal threats. A key challenge concerns the protection of victims, particularly in cases of trafficking in human beings (THB), child sexual exploitation and terrorism, where the absence of trauma-informed, victim-centred approaches, risks re-victimisation. Victims may also face legal jeopardy due to insufficient safeguards against prosecution for offences committed under coercion.

Securing testimony often proves difficult due to fear, trauma, and inadequate witness protection mechanisms.

Further challenges arise in cross-border contexts. The rights of foreign victims of terrorism or trafficking are frequently undermined by unclear legal status, language barriers and fragmented systems of assistance across Member States. Allegations of fundamental rights violations at borders, such as pushbacks or ill-treatment, require consistent, independent investigative pathways. The growing operational use of AI in policing is another emerging concern, with ethical and transparency safeguards often lagging technological deployment. Equally, intelligence surveillance and cross-border information exchange call for robust legal and operational safeguards to ensure proportionality and accountability in data handling.

Gaps also persist in the monitoring, investigation, and prosecution of hate crimes, where difficulties in recognising biased motivation and moderating extremist or discriminatory content online hinder effective enforcement. Cooperation with online platforms is essential to balance the removal of hate speech and disinformation with the protection of freedom of expression. Developing counter-narratives to tackle fake news and online radicalisation should form part of rights-based policing. These issues call for strengthened institutional awareness, analytical capacity, and inter-agency cooperation to ensure that fundamental rights remain central to law enforcement operations.

Training must therefore embed rights-based practice systematically across all operational areas. Priorities include trauma-informed and victim-centred investigative techniques, identification of vulnerable persons, interviewing methods, and understanding complex dual victim-perpetrator dynamics, particularly among youth. In border management, training should build competence in conducting vulnerability assessments and applying child-sensitive and gender-responsive safeguards in contexts such as migrant smuggling. Training should also draw on EU-level guidance for identifying and addressing discriminatory motives in law enforcement operations and incorporate case-based learning on hate crime investigations involving marginalised groups and misogynistic or discriminatory content.

Another focus area is the effective prevention, investigation, and prosecution of domestic violence to upholding human rights, ensuring public safety, and promoting gender equality. Domestic violence is not an isolated phenomenon but a widespread violation that disproportionately affects women and girls. Addressing it robustly demonstrates our commitment to the principles of equality before the law, non-discrimination, and human dignity. Training law enforcement officials is a cornerstone

of an effective response. Frontline officials are often the first institutional contact for victims. Their capacity to recognise indicators of domestic violence, assess risk, and respond sensitively and lawfully can determine whether a victim receives protection or remains at risk.

Awareness of the human rights implications of new technologies, including the ethical use of AI and data-driven policing, should be integrated into all training programmes. Finally, personnel deployed in Common Security and Defence Policy (CSDP) missions should receive targeted instruction on human rights, gender mainstreaming and civilian protection to ensure compliance with international standards and the EU's fundamental rights framework. Training on the Victims' Rights Directive and other EU instruments for victim protection, particularly regarding migration-related vulnerabilities, should also be included to strengthen cross-sectoral cooperation and assistance.

List of detailed training needs

- Cooperation with online platforms to address hate speech while balancing freedom of expression and legal obligations.
- Disinformation and fake news: developing counter-narratives to combat online disinformation.
- EU-level practices on investigations and prosecutions of hate crime: identifying motivations, sharing good practices at the EU level, case studies, victim support, marginalised groups, special needs of victims, misogynism, discriminatory content targeting children and marginalised groups, basic awareness to sensitise the public, and recognition of biased motivation.
- Fundamental Rights and Data Protection: transparency and accountability in data retention, processing, and use but also compliance during surveillance practices.
- Identifying and investigating hate crimes and hate speech online, including detection, removal, and the right to be forgotten.
- Safeguards in intelligence surveillance and cross-border information exchange: legal and operational perspectives.
- Training on EU-level guidance for identifying and addressing discriminatory motives in law enforcement operations.
- Victim protection through EU instruments and cross-sectoral cooperation, with emphasis on migration-related vulnerabilities and the new Victims' Rights Directive.
- Victims of domestic violence, GBV, trafficking, and terrorism through the lens of Fundamental Rights

1.6 Prevention and administrative approach

Effective crime prevention depends on early detection, proactive capability and the systematic use of administrative and regulatory tools alongside criminal enforcement. The EU-STNA 2026-2029 process highlights that law enforcement agencies continue to face challenges in detecting lone-actor trajectories, anticipating emerging drug threats, including diversion of precursor chemicals, and tracking evolving firearms trafficking routes influenced by geopolitical instability. Strategic foresight remains limited, with few tools available to identify early-stage radicalisation or to anticipate the criminal exploitation of new technologies.

Law enforcement is not yet systematically integrated into the preventive design of public spaces or the protection of critical infrastructure while structured engagement with local communities and civil actors remains underutilised as a means of early prevention. At the same time, administrative and regulatory measures are underused as tools to close legal loopholes that enable trafficking in NPS, firearms and environmental offences. Enhancing the coherence and consistency of national legal frameworks is crucial to preventing criminals from exploiting divergences between administrative and criminal enforcement regimes. Administrative approaches should be systematically applied in the fight against organised crime, using licensing, compliance, and sanction mechanisms to create upstream barriers to criminal infiltration and illicit market activity.

Training should therefore strengthen both preventive and administrative capacities across law enforcement and partner agencies. Key areas include the effective application of administrative measures and licensing controls to prevent the diversion of precursor chemicals, as well as strategic communication skills to support early prevention and counter radicalisation. Training on risk and vulnerability assessments for critical infrastructure should be prioritised to ensure coordinated, foresight-based protection planning.

For environmental crime, practitioners require a clear understanding of the new EU Directive and the distinction between administrative and criminal enforcement mechanisms. More broadly, training should promote knowledge of relevant EU sectoral environmental legislation such as those on pollution, waste management and trafficking in wildlife species, helping to harmonise enforcement practices and improve cooperation between administrative and criminal authorities within and across Member States. Programmes should also facilitate multi-disciplinary cooperation and the sharing of best practices between administrative, regulatory and criminal law

enforcement bodies, ensuring that the preventive potential of the administrative approach is fully realised across the Union.

Through this integrated approach, combining administrative, regulatory, and criminal dimensions, law enforcement can create upstream barriers to crime, close enforcement gaps and contribute more effectively to prevention across the EU security landscape.

List of detailed training needs

- Application of administrative and regulatory measures to prevent and disrupt organised crime, including licensing, compliance, permit systems, and the use of sanctions, procurement, and business-authorisation regimes.
- Asset tracing, and recovery competencies, including financial oversight, use of legal channels for confiscation, and coordination with administrative controls.
- Comprehensive administrative and judicial investigations through coordinated EPPO – OLAF investigations
- Community-based and strategic communication approaches to prevention, including cooperation with local authorities and civil society, and targeted awareness-raising and counter-radicalisation initiatives.
- Cross-border and judicial cooperation skills, including the use of EU platforms (SIENA, P2P, CISE), mutual legal assistance procedures, and an understanding of different judicial systems for the admissibility of evidence.
- Integration of administrative and criminal investigations, ensuring coherent workflows and effective intelligence-sharing between regulatory and law enforcement authorities.
- Integrity and anti-corruption safeguards in regulatory, licensing, and inspection functions to prevent misuse or infiltration of public authority.
- Multi-agency coordination and information exchange, covering cooperation models between administrative, regulatory, and criminal enforcement bodies, including joint investigations, task forces, and environmental enforcement cooperation.
- Risk and vulnerability assessment methods for early detection of emerging threats, protection of critical and public infrastructure, and integration of foresight and hybrid-threat preparedness.
- Risk-based inspection, due diligence, and trade-monitoring techniques to detect criminal infiltration of legal business structures, supply chains, and high-risk sectors such as excise goods, chemicals, firearms, and waste.

1.7 Barriers to crime, infiltration, and corruption

The EU-STNA 2026-2029 process highlights the significant challenges law enforcement faces in creating robust barriers to organised crime infiltration and corruption. These challenges are systemic, operational, and technological in nature, stemming from fragmented legal frameworks, inconsistent data collection, and uneven investigative capacity across Member States. Limited availability of harmonised and real-time data constrains trend analysis, risk identification and the admissibility of evidence in cross-border cases. Addressing these issues requires greater use of structured analytical and risk-assessment tools to map corruption trends, enablers, and sectoral vulnerabilities.

Vulnerabilities are particularly acute in high-risk sectors such as public procurement, defence, ports, and waste management, areas where organised crime seeks to infiltrate legitimate markets and institutions. Financial and digital investigations are increasingly complex, as criminal networks exploit multi-jurisdictional money-laundering schemes, opaque beneficial ownership structures, and emerging value-transfer technologies such as cryptocurrencies and decentralised finance platforms. The uneven capacity to deploy advanced analytical and digital-forensic tools, coupled with insufficient use of cooperation instruments, such as Joint Investigation Teams, further weakens collective resilience. Corruption risks are also expanding into emerging digital environments, including online marketplaces, virtual-asset ecosystems and metaverse platforms, where oversight and transparency mechanisms remain underdeveloped.

Addressing these challenges requires stronger multi-agency cooperation, enhanced information exchange between administrative, financial, and law-enforcement authorities, and coordinated oversight mechanisms. Training should therefore promote familiarity with EU intelligence exchange tools such as Secure Information Exchange Network Application (SIENA) and P2P platforms and build competence in using them to coordinate corruption and financial crime investigations across jurisdictions. Training should also focus on developing advanced financial investigation skills for corruption and money-laundering cases, particularly the tracing of proceeds through cryptocurrencies, virtual assets, and other emerging financial technologies. It should also focus on fostering effective cooperation with the European Anti-Money Laundering Authority (AMLA) and international partners.

Equally, practitioners should strengthen expertise in corruption risk assessment and the detection of red flags in high-risk sectors, including EU-funded projects, infrastructure and defence procurement, and areas exposed to hybrid threats or sanctions evasion. Training should promote awareness of political and institutional corruption, including

internal integrity risks within law enforcement, as well as corruption linked to sport and governance. Specific modules should address the misuse of cultural goods in corruption-linked money-laundering schemes and the development of specialised investigative techniques for corruption in sectors such as agriculture, construction, healthcare, education, and energy.

Sharing operational good practice across these domains could help raise investigative standards and harmonise responses. Finally, to reinforce cross-border coherence, personnel should receive training on the legal framework of the new EU Anti-Corruption Directive and the effective use of cooperation tools such as JITs, SIENA, and Article 31 of the EPPO Regulation, including understanding the EPPO mandate where applicable. Specifically, Ukrainian officials would particularly benefit from these trainings, as well as for officials from other non-EU countries such as Belarus in the area of anti-corruption. Together, these efforts will support a more coordinated and integrity-based European approach to countering infiltration and corruption.

List of detailed training needs

- Analysing corruption trends, enablers, and risk patterns in organised crime, using structured analytical and risk assessment tools.
- Awareness of using SIENA and P2P platforms for intelligence exchange in corruption and financial crime investigations.
- Best practices in detecting and investigating corruption across crime types, including drug trafficking, firearms trafficking, waste crime, revenue and EU expenditure fraud.
- Corruption risk assessments in EU-funded projects involve detecting red flags and identifying sector-specific vulnerabilities.
- Detecting, analysing, and investigating corruption in sport, including match-fixing, illegal betting, and governance-related risks.
- Financial investigation techniques linked to corruption cases; detection and investigation of the use of emerging financial technologies, such as cryptocurrencies and alternative value transfer methods.
- Systems in corruption cases, information exchange with non-EU countries, and cooperation with AMLA.
- Internal corruption risks and investigative practices within law enforcement institutions.
- Legal and investigative methods for detecting and investigating political corruption, including campaign financing, undue influence, and conflicts of interest.

- Legal framework and the new anti-corruption Directive.
- Specialised investigative techniques for corruption in high-risk sectors and administrative procedures.
- Sharing of corruption detection and investigation best practices in agriculture, infrastructure, healthcare, public procurement, education, construction, and energy sectors.
- The use of cultural goods in corruption-linked money laundering schemes.
- Use of Joint Investigation Teams and other EU cooperation instruments, use of art. 31 of EPPO Reg. when the EPPO is competent and participating MSs involved, understanding EPPO mandate.

1.8 Document fraud

Document fraud is a major and complex challenge for law enforcement, acting as a key enabler of a wide range of criminal activities, from migrant smuggling and human trafficking to financial crime and sanctions evasion. Its scale and sophistication are amplified by decentralised crime-as-a-service markets and the growing criminal use of AI to generate deepfakes and synthetic identities that bypass verification systems. Fraudulent practices also extend to residence-related schemes such as sham marriages, which require specialised detection and investigative skills. These developments erode the reliability of identification and border-control procedures, exploiting systemic weaknesses in both administrative and criminal frameworks.

Addressing document fraud requires a coherent and joined-up approach across the EU, combining consistent legal frameworks, resilient verification processes, robust anti-corruption safeguards and modern investigative tools. Improved cross-border cooperation and enhanced data-sharing mechanisms are essential to detect and dismantle networks engaged in large-scale forgery and identity fraud. Administrative oversight also needs to be strengthened to prevent infiltration of public bodies and the abuse of legitimate documentation channels.

Training should therefore reinforce practical skills and awareness across several dimensions. Core priorities include recognising forgery techniques, performing identity and document verification, and using investigative databases effectively. Practitioners should also receive specialised training on AI-enabled counterfeiting and complex CaaS structures, supported by operational exercises on detecting deepfakes and tracing financial flows linked to fraudulent documents. Training should develop the capacity of trainers and multipliers in identity verification, including the application of facial comparison and other biometric techniques. Enhanced competence in OSINT

and financial fraud investigations could further improve the capacity to uncover document-fraud networks and their enablers.

Finally, strengthening risk analysis, visa verification, and integrated border-management skills could raise the preventive threshold and ensure more consistent standards across Member States. Through these combined efforts, law enforcement can more effectively counter document fraud as a systemic facilitator of transnational crime and corruption.

List of detailed training needs

- Awareness of the use of fraudulent documents to travel and stay in the EU. Detecting counterfeit and forged documents across countries, sharing information, and developing suitable investigative techniques to tackle forgery. CaaS operations.
- Common forgery techniques, document specifications, and verification methods.
- Document verification, integrating techniques and the use of different databases.
- Effective use of data sharing systems, investigative tools, and awareness of developments in the criminal landscape.
- Investigating document fraud networks.
- OSINT and financial fraud techniques.
- Risk analysis.
- Stakeholder engagement, including communication with third parties.
- Train the Trainers or multiplier course on identity verification procedures and facial comparison.
- Understanding AI technologies and their use in counterfeiting documents.
- Visa verification techniques, including security features, and visa counterfeiting modus operandi.

1.9 The most threatening criminal networks and individuals

The EU-STNA 2026–2029 process underlines the ongoing challenge of tracking and disrupting the most threatening criminal networks, transnational, highly adaptive structures that operate seamlessly across physical and digital environments. These networks combine durable social bonds, such as kinship or diaspora links, with agile, technology-enabled operations that blur traditional investigative boundaries. Their use

of encrypted communications, anonymised platforms and decentralised command structures makes penetration increasingly difficult. Many such groups also maintain resilient, remote, or prison-based leadership models, ensuring continuity even when key members are detained.

The expansion of the CaaS model further complicates disruption efforts. By outsourcing core criminal functions such as violence, money laundering, document fraud and cyberattacks, networks obscure hierarchies and expand their operational reach. In this regard, awareness training focused on enablers and CaaS providers, and adapted to the targeted region, could be beneficial to investigators and prosecutors. Violence and intimidation remain strategic instruments used to assert territorial control, protect markets, and enforce internal discipline, requiring targeted analytical and tactical responses. At the same time, criminals exploit emerging technologies, including artificial intelligence and deepfakes, for fraud, impersonation and deception, outpacing law-enforcement detection capabilities. Training must also address the early detection of grooming and recruitment tactics, particularly those targeting minors through online platforms and gaming environments.

A recent trend indicates that organised criminal groups increasingly target young people for recruitment and exploitation in various forms of criminal activity. These recruitment efforts are often conducted via social media platforms, leveraging their anonymity features. Law enforcement authorities must be equipped to detect and disrupt such recruitment tactics and to prevent the online manipulation of vulnerable young individuals.

These networks increasingly infiltrate legitimate economic and political systems, using shell companies, public procurement mechanisms and other business structures to conceal profits and launder proceeds, often facilitated by corruption or insider assistance. The EPPO plays a growing role in investigating related offences; therefore, practitioners should be familiar with its mandate and the application of Article 31 of the EPPO Regulation in cross-border financial investigations. Criminal networks also exploit geostrategic and post-conflict vulnerabilities, where demobilised combatants or displaced individuals may be drawn into organised crime or private militias. Understanding the impact of geopolitical instability on recruitment and expansion dynamics is increasingly vital for strategic analysis and prevention.

Responding to these challenges requires strengthened analytical, investigative and intelligence capacities. Law-enforcement agencies must be able to map complex, multi-layered criminal ecosystems, anticipate operational shifts and coordinate disruption efforts across borders. This demands enhanced structural intelligence

analysis, improved cross-border information sharing and the systematic use of EU cooperation instruments. Advanced digital investigation skills are essential for operations conducted entirely in online environments, including decryption, digital forensics, OSINT, and cryptocurrency tracing—covering assets such as cryptocurrencies and NTFs. Training should also promote awareness of emerging digital environments and AI-enabled automation within organised crime operations, ensuring that investigators can identify synthetic identities, deepfakes and automated criminal processes.

List of detailed training needs

- Criminal misuse of AI, including detection of synthetic identities, deepfakes, and automation in criminal operations.
- Digital forensics and investigative approaches to encrypted platforms, including decryption strategies and lawful evidence gathering with special regards to the recruitment of your perpetrators.
- Emerging platforms and tools employed for recruitment, with a focus on monitoring and the early identification of criminal grooming tactics aimed at young people.
- Enablers and crime-as-a-service ecosystems, including document fraud, logistics, and laundering services.
- Exploitation of legal businesses and political structures, including the role of EPPO and the application of Article 31 of the EPPO Regulation.
- Financial crime investigations linked to the most threatening criminal networks and individuals, including shell companies, cryptocurrency tracing, money laundering techniques, insider facilitation, and typologies of illicit financial flows.
- Impact of geopolitical instability and post-conflict dynamics on the evolution, expansion, and recruitment strategies of the most threatening criminal networks.
- Investigative best practices and modus operandi of resilient criminal groups, including remote and prison-based leadership models.
- OSINT, investigation techniques for encrypted channels and the dark web.
- Structural intelligence analysis and cross-border intelligence sharing for mapping and dismantling the most threatening criminal networks.
- Structures of criminal groups and reasons for using violence (analysis of different structures, operations of organised crime groups).

2. THEMATIC TRAINING PRIORITIES

2.1 The production, trafficking, and distribution of illicit drugs

Drug trafficking remains a major threat to public safety and governance across Europe. The trade in cannabis, cocaine, heroin, synthetic drugs, and new psychoactive substances (NPS) generates vast criminal profits, driving violence, corruption, and institutional instability. In particular, the use of intimidation and violence to control drug markets, while exploiting minors and vulnerable youth, including through online platforms, deepens insecurity in communities and reinforces cycles of crime.

Unprecedented cocaine production, diversified trafficking routes and intensified competition between criminal networks are driving increased criminal violence. Cannabis markets continue to expand, with high supply, rising potency and blurred legal–illegal boundaries. Heroin supply uncertainty has reinforced the EU's role as a production hub for synthetic drugs and NPS. As a result, increasingly potent opioids are spreading across Europe, contributing to higher poisoning and overdose deaths. The EU now acts both as a main entry point for cocaine and a global production centre for synthetic drugs, while trafficking routes diversify, encrypted online platforms facilitate distribution and synthetic drug manufacturing generates growing environmental harm.

Environmental challenges

Law enforcement efforts are constrained by a continuously evolving drug market featuring rapidly emerging formulations and highly potent synthetic substances (e.g., nitazenes, fentanyl derivatives), which consistently outpace regulatory classification and adaptation. Fragmented legal frameworks across Member States and regulatory gaps enable uncontrolled production, trafficking, and diversion of NPS, making harmonised judicial action difficult.

Environmental damage caused by illicit drug production presents further challenges beyond the immediate scope of training. Cannabis cultivation contributes to deforestation, chemical waste, and the excessive exploitation of water and energy resources. Synthetic drug and cocaine production generate hazardous waste through industrial-scale processes, aggravated by inadequate regulatory measures and limited resources to manage chemical contamination.

Broader systemic constraints include limited law enforcement and forensic resources, insufficient international cooperation, and cross-agency coordination (customs, border, environmental bodies, health authorities), weak engagement between public health and law enforcement sectors, and inadequate intelligence sharing mechanisms. These factors hinder coordinated cross-border action, slow early warning responses to emerging substances and limit the capacity for effective strategic intervention.

Challenges concerning knowledge, skills, responsibility and autonomy, and related training needs

Challenges

Law enforcement requires enhanced capabilities to detect, investigate and prohibit illicit drugs and NPS across all stages of production, trafficking, and distribution. Officers need advanced skills in tracking and detection, particularly in identifying concealment methods used in legitimate trade shipments (e.g., foodstuffs, textiles, construction materials).

Specialised expertise is needed to dismantle high-tech indoor cannabis operations involving hydroponics and energy theft but also to monitor and investigate synthetic stimulants production in laboratories (e.g., methamphetamine, amphetamine, synthetic cathinones, MDMA), illicit opioid processing sites, and the extraction of cocaine from carrier materials. This includes a strong understanding of complex chemical production techniques, identification of evolving methods, and the ability to track diversion of precursor and pre-precursor chemicals within legitimate supply chains.

Forensic and toxicological expertise require enhancement to keep pace with new synthetic drugs and increasingly potent substances. This includes improved capabilities for analysing THC variability in cannabinoids, detecting heroin adulteration, identifying synthetic compounds, and supporting rapid risk assessment procedures. Strengthening forensic monitoring systems and laboratory competence is essential.

In the online domain, strengthened digital investigation competencies are required to counter the increasing exploitation of encrypted communication networks, online marketplaces, and social media platforms for drug distribution. Improved skills in cyber intelligence collection, covert online monitoring and digital tracing are critical.

There is an essential need to develop intelligence-gathering and analytical skills, especially regarding synthetic stimulant use among high-risk populations, drug market trends, drug-related corruption in port operations, evolving maritime trafficking routes

and air transport, and the role of the EU as an export hub. Officers must be trained to contribute effectively to structured intelligence systems and cross-border intelligence-sharing mechanisms.

In complex environments such as ports and supply chains, enhanced cooperation with the private sector is essential, as private operators hold critical operational knowledge, data, and risk insights that are indispensable for understanding criminal modus operandi and for effective responses.

Finally, training should reinforce operational autonomy and decision-making in complex investigations, including responsibility for raiding and dismantling large-scale drug production operations, coordinating multi-agency actions and intelligence sharing mechanisms, and managing high-stakes operations involving dangerous substances. Officers must be able to independently assess threats, initiate specialised backtracking investigative measures, tracking criminal activities towards the identification and dismantling of criminal organisation networks, and contribute effectively to joint international operations.

Training needs

Summary

Comprehensive and specialised training is required to effectively address the diverse and evolving challenges posed by both traditional drugs like cannabis, cocaine, and heroin as well as synthetic drugs and new psychoactive substances (NPS).

Countering the increasing sophistication of drug production, trafficking and distribution highlights several training needs. A key priority is enhancing digital investigative skills, including training on cyber investigations, darknet markets, encrypted platforms, social media, and alternative digital payment methods used for drug distribution.

Law enforcement agencies need targeted training to respond to the growing violence associated with drug trafficking, including intimidation, firearms use and spill-over into public spaces. Training should strengthen the ability to identify early warning signs of violence, manage high-risk operations safely, and apply intelligence-led and preventive approaches to disrupt violent criminal networks.

Dedicated training is required to address the increasing recruitment of minors and vulnerable young people by drug trafficking networks, including through online platforms. Law enforcement should be equipped to detect recruitment patterns, with preventive and multi-agency responses in cooperation with social and youth services,

to disrupt recruitment pipelines, and contribute to breaking the cycle between drug trafficking, violence and youth exploitation.

Furthermore, training is needed to improve intelligence gathering and sharing. This includes developing skills to gather and share structured intelligence on criminal networks, evolving routes, and market shifts, as well as strengthening cross-border intelligence mechanisms. In this regard, regional programmes taking into account the specificities of trafficking routes could be envisaged. Training should also focus on improving engagement and coordination between law enforcement and public health authorities to facilitate early warning responses and to develop strategic drug policy.

Law enforcement also requires training in financial investigations, including those related to cryptocurrencies, financial flows, and asset recovery, to disrupt the economic underpinnings of drug trafficking.

Lastly, an understanding of different judicial systems and legal frameworks across jurisdictions is essential for effective cross-border enforcement and the application of administrative approaches in conjunction with criminal justice approaches. Given the varying pace among Member States in adopting administrative approaches, countries that are more advanced would benefit from different training than those that have yet to implement them.

Further details

Training needs specifically identified within the EMPACT priority Cannabis, Cocaine, Heroin (CCH):

For CCH, training is essential to understand and respond to specific production methods, trafficking routes, and environmental impacts. Regarding cannabis, training is required to gather and share structured intelligence related to its smuggling through various routes (e.g., North America, North Africa, Italy, and Türkiye) and on production and emerging product trends of cannabinoids. LE also needs training on modus operandi and responses to smuggling via postal parcels and express courier services. A distinct need is training to recognise waste from cannabis cultivation sites, including energy theft, deforestation as part of significant deterioration of protected habitats, and exploitation of water infrastructure, to ensure these offences often linked to environmental crime, are prosecuted, which requires coordination between drug and environmental crime investigators. Specific trainings designed to address this challenge could be especially impactful in Benelux countries, Spain, Portugal, Greece, and France.

For cocaine, training should address the detection of cocaine and its intermediate products (including chemically concealed forms of cocaine hydrochloride and cocaine base), as well as the processing and production laboratories. Training should focus on following the entire cocaine crime script. For heroin, LE requires training in gathering and sharing intelligence on trafficking, including tracking, and detecting heroin and its acetic anhydride, and monitoring market shifts and trafficking through alternative smuggling corridors. Expertise in identifying criminal infiltration and the misuse of legal business structures is also specified.

Training needs specifically identified within the EMPACT priority Synthetic drugs/NPS:

NPS present unique challenges due to its novelty and rapid evolution, demanding specialised training. LE needs training to enhance its capacity to detect new synthetic stimulant precursors and pre-precursors and evolving production methods, allowing it to counter the rapid adaptation of criminal networks. This includes training on monitoring the emergence and re-emergence of highly potent synthetic opioids, such as fentanyl derivatives, nitazenes, as well as other NPS.

Training is crucial for improving online and postal interdiction capabilities, specifically in monitoring online platforms, social media, darknet markets, and encrypted communications, to detect ultra-potent synthetic drugs trafficked in small quantities via postal and express delivery services.

Regarding production and (pre-)precursor control, LE requires training to track the diversion of (pre-)precursor chemicals, strengthen control over these chemicals, and dismantle industrial-scale synthetic drug production sites, particularly in established EU hubs. This also involves training to detect new (pre-)precursor chemicals and understand related regulatory controls.

In the environmental domain, training is needed to address weak regulatory frameworks for the disposal of synthetic stimulant production waste, to better manage hazardous waste and environmental impacts, and to investigate and dismantle illicit waste disposal, particularly from large-scale production sites. This training need is especially pronounced in the Benelux countries.

Finally, forensic, and public health monitoring requires training to close gaps in forensic and toxicological monitoring of emerging synthetic substances, enhance capacity to analyse new synthetic drugs, and monitor synthetic stimulant adulteration trends. LE also needs training to effectively monitor and respond to rising trends in administering synthetic drugs, such as methamphetamine and synthetic cathinone injection, which are linked to significant public health risks. Given the inherent dangers, specific training

on risks and safety protocols for law enforcement operating in the context of synthetic drugs and NPS trafficking, trade, and production is also essential.

List of detailed training needs

Member States indicated that 27 276 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat the production, trafficking and distribution of illicit drugs.

The production, trafficking and distribution of cannabis, cocaine, and heroin (EMPACT CCH)

1. Following the crime script, cocaine address detection of cocaine and its intermediate products (chemically concealed cocaine, as well as cocaine base) and the processing and production laboratories.
2. Financial investigations linked to drug production and trafficking, including tracking proceeds through cryptocurrencies and decentralised platforms.
3. Gathering and sharing of intelligence on heroin trafficking; tracking and detecting heroin, heroin precursor chemicals; monitoring heroin market shifts and trafficking through alternative smuggling corridors.
4. Gather and share structured intelligence related to smuggling cannabis through different routes (North America, North Africa Western Balkans, Italy, Türkiye, Northern and Eastern Europe).
5. Criminal infiltration into and misuse of legal business structures, the potential role of legal business structures in every stage of the crime script.
6. Investigation of poly-drug trafficking routes, including the use of drugs as currency in exchanges between organised crime groups.
7. Application of administrative measures and licensing controls to prevent diversion of precursors and legal substances to illicit drug production, in conjunction with a criminal justice approach.
8. Share modi operandi as well as responses to smuggling cannabinoids via postal services/parcels.
9. Gather and share structured intelligence related to production and emerging product trends of cannabinoids.
10. Undercover cyber investigations, including social media platforms, darknet and encrypted communication, operation of cyber patrolling teams, and collection of digital evidence.
11. Countering drug-related violence and youth recruitment by organised crime groups

12. Recognition of waste coming from illegal drug laboratories and plantations, energy theft, deforestation as part of significant deterioration of protected habitats, and exploitation of water infrastructure has a negative impact on the environment; they should be prosecuted. Coordination between drug and environmental crime investigators is necessary.

The production, trafficking and distribution of synthetic drugs and new psychoactive substances (EMPACT NPS/Synthetic Drugs)

1. Diversion and trafficking of drugs and precursors, both wholesale and retail, via postal parcels and courier services, courier walls, cooperation between police and customs and the private sector.
2. Financial investigations linked to drug production and trafficking, including tracking proceeds through cryptocurrencies and decentralised platforms.
3. Detecting and interdicting illicit synthetic drugs and NPS shipments, including concealment in postal parcels, cargo, and commercial supply chains.
4. Investigating and dismantling the synthetic drug and NPS production and distribution infrastructure, including labs, transport routes, and waste dump sites
5. Awareness and use of EU information-sharing platforms and cooperation tools in synthetic drug investigations.
6. Investigating poly-drug trafficking networks and overlapping smuggling routes involving synthetic drugs.
7. Import, production, diversion, export of licit medicine, to the illicit drug market, e.g., ketamine, tramadol, fentanyl and etomidate, use of legal business structures.
8. Identifying and reporting on precursor chemical misuse, including regulatory updates and techniques to detect mislabelled substances.
9. Forensic analysis and interpretation of drug samples; application of innovative tools and technologies for drugs and toxicological analysis and profiling.
10. Application of administrative measures and licensing controls to prevent diversion of precursors and legal substances to illicit synthetic drug production, in conjunction with a criminal justice approach.
11. Undercover cyber investigations, including social media platforms, darknet and encrypted communication, operation of cyber patrolling teams, and collection of digital evidence.
12. Risks and law enforcement response strategies for synthetic opioids and high-potency stimulants.
13. Identifying and addressing environmental harms from synthetic drug production: coordination between drug and environmental crime investigators.

14. Understanding different judicial systems and legal frameworks regarding drug trafficking.

2.2 Cyber-attacks

Cyber-attacks demonstrate rapidly evolving sophistication of tactics and tools, where emerging technologies, such as Artificial Intelligence, blockchain, and quantum computing provide criminal networks with new capabilities to expand the speed, scale, and sophistication of their operations. Cyber-attacks increasingly target critical infrastructure, governments, businesses, and private citizens, and increasingly demonstrate a hybrid structure combining profit motives with ideological or state-aligned objectives.

Environmental challenges

Addressing these attacks poses significant environmental challenges, particularly across borders. A primary issue is the lack of real-time access to cyber threat intelligence feeds and the persistent difficulty in sharing timely, actionable intelligence among Member States and with private sector partners. This is compounded by the challenge of cooperation and operational information sharing in cross-border cybercrime investigations, along with coordination gaps among law enforcement and cybersecurity agencies, Computer Security Incident Response Teams (CSIRTs), and private companies.

Investigative capabilities are challenged by the capacity to manage and analyse large volumes of digital evidence, as well as by challenges in harmonising investigative approaches and admissibility standards for digital evidence. The evolving nature of threats introduces specific difficulties, such as tracking fragmented dark web markets, encrypted private forums, and peer-to-peer illicit networks. There is also limited capability to investigate quantum-secured criminal communications and the potential development of quantum-assisted cybercrime, as well as insufficient means to dismantle sophisticated operations, such as Ransomware-as-a-Service (RaaS), DDoS-for-hire services, and initial access brokers (IABs).

Protecting critical infrastructures against ransomware and hybrid threat-linked disruptive cyber-attacks remains a key challenge. This includes weak capabilities in early detection of supply-chain attacks through compromised third-party service providers. A major operational challenge is the attribution of cyber-attacks, which is further complicated by the increasing fragmentation and short lifespans of

cybercriminal groups, and by the complex scenarios in which state-sponsored, hybrid, or ideologically motivated actors blend into CaaS environments.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Law enforcement faces significant challenges in combating cyberattacks due to interconnected gaps in expertise, operational capabilities, and decision-making autonomy. Officers must keep pace with a rapidly evolving threat landscape, where cyberattacks are increasingly driven by hybrid threat actors and state-aligned networks rather than purely profit-motivated criminals. Understanding the significant role of data theft in ransomware operations, anticipating AI-enabled and future quantum-supported attacks, and recognising the convergence between cybercrime and other strategic threats are essential but currently limited areas of knowledge. In addition, there is a lack of awareness regarding relevant legislative frameworks such as the NIS2 Directive.

Operationally, insufficient expertise in investigating complex models such as Ransomware-as-a-Service and Malware-as-a-Service, neutralising zero-day exploits and misconfigurations, and tracing stolen data through multi-layered extortion schemes undermines investigative effectiveness. Skills gaps are widening in countering AI-driven automation, managing digital ransom negotiations, and preparing for quantum-secured criminal communications.

In terms of responsibility, the increasing pressure to protect critical infrastructure from disruptive and hybrid threat-linked cyberattacks, necessitates stronger capabilities in crisis management, incident response coordination, victim support mechanisms, and the strategic capacity to respond to persistent hybrid cyber threats that combine cyber-attacks, data theft, disinformation, and infrastructure destabilisation. Furthermore, offender prevention approaches remain underdeveloped, limiting proactive interventions.

Autonomy is hampered by fragmented coordination mechanisms and insufficient cross-border operational information sharing. Jurisdictional and technical barriers restrict investigations into attacks originating beyond EU borders, while delayed readiness for post-quantum cryptography exposes operational security to future risks.

Training needs

Summary

Training needs focus on strengthening both awareness-level and practical competencies to address the rapidly evolving cyber threat environment. Awareness training should equip law enforcement officers with an understanding of hybrid threats and the increasingly complex motivations behind cyberattacks, which are not limited to profit-driven crime but also include state-aligned and ideologically motivated actions. This is especially relevant for cyber investigators and CSIRTs from Eastern Europe and Baltic States. This foundational perspective must be complemented by knowledge of emerging technologies such as artificial intelligence, blockchain, the Internet of Things, quantum computing, as well as decentralised platforms and deep and dark web environments, including the metaverse. Furthermore, officers need to be familiar with the dynamics of Crime-as-a-Service models and shifting modus operandi employed by cybercriminal networks.

In addition to awareness-level training, practical and skills-based training is essential to strengthen investigative capabilities, particularly in malware and cryptocurrency investigations. This includes developing proficiency in advanced decryption techniques and identifying or dismantling anonymised criminal infrastructure, as well as monitoring and investigating communication channels on the deep and dark web. Capacity building must also support technological adaptation and the deployment of advanced detection tools. Joint training activities with Computer Security Incident Response Teams, and service providers are essential to enhance interoperability and real-time collaboration.

Finally, offender prevention training—incorporating models such as the cybercriminal pathway and the InterCOP 4D approach—should form part of a holistic strategy. Across all areas, training should reinforce the ability to collaborate with policymakers, other enforcement agencies and the technology sector to enhance both operational readiness and coordinated response to cyber threats.

Further details

Awareness-level training is fundamental to understanding the evolving cyber threat landscape, including hybrid threats and state-aligned or ideologically motivated attacks. Officers must be familiar with emerging technologies such as AI, blockchain, quantum computing, IoT, malware trends and malware analysis, the deep and dark web, and decentralised online environments, including the metaverse.

Practical training should focus on enhancing forensic and investigative capabilities for malware and cryptocurrency cases. This includes developing expertise in advanced

decryption, identifying anonymised criminal infrastructure and investigating AI-driven automated attacks. The capacity to monitor and analyse encrypted communications and dark web forums, which serve as channels for recruitment and coordination is essential.

A collaborative training approach is necessary. Joint exercises with CSIRTs and service providers can enhance interoperability and operational readiness. Training should also target offender prevention, applying approaches such as the cybercriminal pathway model and InterCOP's 4D method.

Finally, training must support improved coordination and operational integration between law enforcement, cybersecurity stakeholders and policymakers, enabling more effective response to transnational cyber threats and alignment with future technological developments.

List of detailed training needs

Member States indicated that 7 387 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat cyber-attacks:

1. Advanced cybercrime forensics, including ransomware forensics, malware analysis, dark web investigations, phishing attack analysis, forensic imaging, and device acquisition.
2. Emerging cyber threats, including AI-driven attacks, Internet of Things vulnerabilities, decentralised platforms, and quantum-related risks.
3. Joint training for law enforcement and Computer Security Incident Response Teams on malware investigations, supply-chain attacks, and incident response coordination, involving public–private partnerships.
4. Hybrid threat-linked cyber-attacks.
5. Tracing cryptocurrency transactions and financial flows linked to ransomware, extortion, and hybrid threat-driven cyber-attacks.
6. Monitoring and investigating cybercriminal recruitment and operational communications on encrypted, anonymised, deep and dark web platforms.
7. Training to enhance awareness of emerging technologies exploited in cybercrime, including blockchain, Artificial Intelligence, quantum computing, malware trends, Internet of Things, deep and dark web, and the metaverse.
8. Forensic investigation of online legal business structure (LBS) abuse, including identification of digital criminal activity via LBS, evidence collection

from online commercial platforms, integration of forensic practices in LBS-related investigations.
9. Training on cyber offender prevention strategies, including behavioural pathways to cybercrime and early intervention models such as InterCOP's 4D approach advanced decryption.
10. Enhance awareness of relevant legislative frameworks such as the NIS2 Directive.

2.3 Counterterrorism

The EU faces a persistent, evolving, and diversifying terrorist and extremist threat, with jihadist actors continuing to pose the greatest risk. Geopolitical conflicts, notably in the Middle East, are intensifying radicalisation and social division. Violent extremist ecosystems, such as No Lives Matter, Order of Nine Angles or 764, also represent a challenge. Online platforms and gaming ecosystems are increasingly exploited to target minors and exploit emerging technologies, including AI, for propaganda and recruitment. Threat actors are seeking access to 3D-printed weapons and exploiting virtual assets for terrorism financing, while migratory routes to enter Europe remain a potential entry path for foreign terrorist fighters and terrorist suspects.

Environmental challenges

Challenges in confronting terrorism and violent extremism are multifaceted. These include the increasing importance of online recruitment and manipulation of vulnerable young persons, including children, groomed by violent online communities on social media and gaming platforms to commit violent acts. The nexus with organised crime, especially child sexual exploitation and sextortion, is becoming more significant, even if opportunistic, where terrorists leverage criminal networks for financial gain, logistical support, and access to illicit firearms, explosives, and fraudulent identity documents. Geopolitical instability, particularly the Russian war of aggression against Ukraine, exacerbates the availability of illicit firearms and ammunition, while advancing technologies, such as 3D printing and AI, increase the sophistication of privately manufactured weapons.

In this context, Preventing and Countering Violent Extremism (P/CVE) initiatives require a greater capacity to assess escalation risks between opposing extremist groups and anticipate inter-group violence, together with sustainable resources, dedicated staffing, and long-term coordination structures.

Responding to radicalisation and countering terrorism, requires addressing legal and operational limitations hindering lawful access to encrypted communications, Virtual Private Network (VPN) traffic, and dark web activity. Stronger analytical tools are

essential to process coded, multilingual, or meme-based extremist content online. Legal barriers impeding the return of individuals posing a threat to public policy, public security or national security need to be addressed, and the recast of EU Return Directive is underway, while appropriate operational frameworks are required to support the investigation of encrypted extremist abuse networks targeting minors, managing individuals returning from conflict zones, or monitoring supporters of terrorist organisations.

Appropriate tools are necessary to respond to the growth of 3D weapons and to counter the threat posed by non-cooperative drones. There is indeed an increased concern due to the daily performance gains and innovations in drone systems in terms of flight speed and duration, payload capability, integration with AI for autonomy and swarming capabilities, alongside additive manufacturing (3D printing). Furthermore, the broad range of threat actors exploring their potential, ranging from terrorists and extremists to criminal networks, and state actors or state-sponsored proxies and the current limits of countermeasures to detect, track, identify, mitigate or neutralise drones as appropriate from technical, operational, governance and regulatory perspectives.

Ongoing priority measures are, notably, assessing the harmonisation of Member States' laws and procedures for the use of counter-drone systems, upgrading the existing JRC living lab into a Counter-Drone Centre of Excellence, continuing the delivery of counter drone training for law enforcement that has been organised by the ISF funded High Risk Security Network (HRSN). Furthermore, adopting full standards for C-UAS testing methodology and voluntary performance requirements, developed by the EU-funded COURAGEOUS2 and further upgrading the digital platform containing information on drone incidents, currently accessible to the law enforcement representative's member of the EC Chaired C-UAS Working Group.

While the EU has strengthened the legislative framework regarding the protection of critical infrastructure, both from a physical and cyber resilience perspective, ProtectEU stresses the importance of timely transposition and correct implementation of these Directives.

Operational coordination, multi-agency cooperation, and information exchange are key to ensuring appropriate takedown mechanisms aimed to counter terrorist threats. Such cooperation would also ensure the coordination between internal and external counter-terrorism law enforcement actors required for a unified response.

Law enforcement capability to support foreign victims of terrorism across jurisdictions requires harmonised procedures across Member States for victim interviews and evidence collection, which can otherwise lead to secondary victimisation. Additionally, an EU-wide framework is needed to enable cross-border witness protection for foreign victims.

Legal, institutional, and strategic frameworks require shared EU-wide threat analysis criteria and standards for classifying terrorism-related risks, including emerging terrorist financing methods, while consistent legal thresholds could allow more effective cross-border investigations. Gaps in national legal frameworks currently limit law enforcement capacity to prevent, investigate, and prosecute terrorism, as well as to contribute to strategy development. Barriers also exist in using battlefield or third-country evidence in domestic proceedings.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Challenges posed by terrorism and violent extremism are complex and require enhanced prevention, early detection, technological adaptation, and cross-border cooperation. Identifying lone actors and radicalised individuals—particularly those from outside the EU using irregular migration routes—remains difficult, while law enforcement needs stronger mechanisms for community engagement and better capacity to counter online manipulation and early-stage radicalisation among youth. In correctional settings, intelligence coordination must be strengthened to manage radicalisation in prisons and support transitions post-release, including for individuals returning from conflict zones.

Law enforcement requires improved understanding of ideologies that are prone to violent mobilisation, such as anarchism, and fluid extremist threats, including those linked to mental health vulnerabilities. Technological advances necessitate stronger capabilities to detect and counter new, easily sourced weapons such as 3D-printed or autonomous systems, alongside improved preparedness for CBRN threats. In addition, increased capacity is needed to investigate the misuse of charitable organisations and informal value transfer systems in terrorist financing.

Managing returning foreign terrorist fighters continues to demand better coordination across law enforcement, intelligence and judicial actors, and improved detection at external borders.

Interdependencies between physical and digital infrastructure, highlight the need for enhanced risk assessment and response to cascading or systemic threats, including those targeting emerging digital vulnerabilities.

Operational challenges include insufficient use of secure information-sharing tools, limited multi-agency coordination and weak alignment between law enforcement and judicial bodies, particularly in cross-border victim support. This is combined with a general lack of awareness in the justice system. Greater capacity is crucial to safeguard victims of terrorism and improve information-sharing to prevent opportunistic collaboration between terrorist and criminal networks. Upholding a fundamental rights-based approach to victim support requires clarifying the procedural status of foreign victims, harmonising victim interview and evidence procedures and establishing a coherent EU framework for compensation and witness protection to ensure equal access to justice and encourage victim participation.

Key challenges in the field of terrorist financing include both the lack of sufficient human and technical resources and the lack of awareness of the financing aspect of terrorism when it comes to financing methods. Since it is very difficult to follow the money related to terrorism, the capacity of law enforcement to detect, investigate and combat the financing of terrorism should be continuously strengthened.

Training needs

Summary

Training is central to effectively addressing the evolving challenges of terrorism and violent extremism.

A key priority is strengthening prevention and early detection. This encompasses training in identifying common risk indicators, in advanced detection of document fraud, and in effective strategic communication for radicalisation prevention through multi-stakeholder cooperation.

Combating online radicalisation is a critical training area. Priorities include strengthening proficiency in digital tools, including AI, for monitoring online trends, structuring Member State monitoring, and sharing evidence-based practices. Specialised training is necessary to counter online gamification of violent extremism, identify key actors in the gaming ecosystem, and understand psychological manipulation tactics. Training to increase the capacity to identify lone actors and early-stage radicalisation is mandated.

In correctional settings and border security, training priorities include contributing to the creation and application of risk assessment tools. It also includes training to manage the transition and reintegration of terrorism offenders and in working with cross-border monitoring and coordination mechanisms, such as information systems and databases, police and judicial cooperation and border control tools to detect returning foreign terrorist fighters (FTFs).

Emerging technologies and complex threats demand substantial training. This includes detection, risk assessment, and response to AI, drones, and 3D weapons. Enhanced and virtual realities, digital twins and their potential misuse and preventive application could also be covered. Capabilities to address hybrid threats, disinformation, and to manage CBRN-e threats and incidents are high-priority areas.

In financial investigations, training must focus on cryptocurrencies and crypto assets in general, detecting informal value transfer systems, such as crypto-Hawala, facilitating best-practice exchanges between Financial Intelligence Units (FIUs) and terrorism financing investigators, and building Public-private partnerships (PPPs). Multidisciplinary training is required in cross-border critical infrastructure protection, with threat, risk, and vulnerability assessments and PPPs. This capacity is vital for responding to emerging threats and coordinating EU-level crises.

Finally, protection and support of victims of terrorism, understanding international mechanisms, and cooperation with victim associations are key training needs. Addressing mental health vulnerabilities through enhanced coordination between law enforcement and the health sector is a priority.

Further details

Training should strengthen the prevention and detection of radicalisation and terrorism by improving understanding of gender-specific dynamics, including the role of women as enablers or perpetrators. It should also enhance the ability to identify radicalisation trends among vulnerable groups, particularly teenagers. In the online environment, training needs to cover the investigation and dismantling of encrypted extremist networks targeting minors, as well as the assessment of the real-world impact of radicalising content to support evidence-based prioritisation.

To improve the detention management of returning foreign fighters and their family members, as well as the rehabilitation, reintegration and resocialisation of returnees, training should support the monitoring and risk assessment of women and children held in conflict-zone camps and reinforce the capacity of prison and probation staff to identify and manage radicalisation. In relation to tactical and technological threats,

training should develop capabilities to analyse large volumes of drone-related surveillance data and enhance preparedness, detection, and response protocols for CBRN threats. Skills gaps in counter-drone operations across law enforcement and relevant private-sector actors also require targeted training, both at regional and EU-level.

List of detailed training needs

Member States indicated that 8 726 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat terrorism:

1. Online radicalisation: digital tools to monitor and assess trends, use of AI by law enforcement, how to structure a monitoring tool in MS, application of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, sharing of evidence-based practices, countering the online gamification of violent extremism, identification of gaming platforms and psychological manipulation tactics for radicalisation.
2. Counterterrorism risk assessment and response to emerging technologies, including Artificial Intelligence, drones, and 3D-printed weapons.
3. Detection and early risk assessment of lone actors and small autonomous cells, including behavioural indicators.
4. Financial investigation techniques in terrorism cases, including crypto-based and informal value transfer systems, the abuse of non-profit organisations, exchange of best practices between Financial Intelligence Units, and building Public Private Partnerships
5. Forensic readiness for terrorism, including digital evidence collection in terrorism cases, cross-border online intelligence gathering, and coordination with cyber threat intelligence efforts.
6. Cross-border critical infrastructure protection, public-private partnerships, threat assessment, risk assessment, vulnerability assessment, and emerging threats to critical infrastructure
7. Cross-border monitoring and coordination mechanisms to detect returning foreign fighters and persons involved in terrorist activities, and to build appropriate operational partnerships.
8. Detection, containment, and incident management of Chemical, Biological, Radiological and Nuclear e-threats in counterterrorism contexts

9. Coordination mechanisms for managing the transition of terrorism offenders and radicalised individuals, best practices on the coordination of reintegration.
10. Assessment tools for detecting radicalisation in detention centres and prisons, including staff awareness and the use of evidence-based models.
11. EU-level coordination mechanisms and protocols for response to terrorism-related crises
12. Strategic communication on the prevention of radicalisation, law enforcement, and multi-stakeholder cooperation
13. Operational use of EU counterterrorism cooperation and information exchange tools, including EU information systems (e.g., SIS) and interoperable components, Europol's information exchange and analytical systems (e.g., SIENA, EIS and PERCI), protocols, reporting standards, and platform engagement (e.g., Internal Referral Units) and Eurojust frameworks (e.g., Counter-Terrorism Register).
14. Protection and support of victims of terrorism, international victim support mechanisms, cooperation with the European Network of Associations of Victims of Terrorism (NAVT)
15. Law enforcement coordination with health services to identify and manage radicalisation linked to mental health vulnerabilities

2.4 Online fraud schemes

Online fraud is the fastest-growing form of organised crime in Europe, marked by increasing scale and sophistication. It includes crypto-based investment scams and Business Email Compromise, targeting individuals, businesses, and public institutions. Artificial Intelligence accelerates its impact through deepfakes, spoofing, and automation. These schemes generate substantial illicit profits and exploit financial systems, contributing to economic destabilisation across national and EU levels. Victims suffer significant financial and psychological harm, often compounded by subsequent re-victimisation. The rapid evolution of these threats poses serious challenges to digital security and public trust in financial and communication infrastructures.

Environmental challenges

Law enforcement agencies face significant and escalating challenges in effectively combating online fraud, the most rapidly expanding and sophisticated sector in organised crime. Online fraud is increasingly driven by advances in automation and Artificial Intelligence, enabling criminals to craft extremely realistic narratives and often leveraging current societal trends to enhance the schemes' convincing nature.

A central issue is the pervasive use of cryptocurrency, serving as both a payment method for illicit gains and a primary product in investment fraud. Key fraud types, such as investment fraud, Business Email Compromise (BEC), and romance fraud, are particularly prolific, with AI, machine learning, deepfakes, and large language models (LLMs) increasing their credibility and reach. These technologies facilitate convincing impersonations and social engineering, leading to severe financial and psychological harm for often re-victimised individuals. Fraud against payment systems is also evolving, shifting towards digital exploitation.

A primary challenge confronting law enforcement is that investigative frameworks are not adequately equipped for AI-enhanced fraud, deepfake scams, and synthetic identity fraud. The rise of generative AI tools, such as WormGPT and FraudGPT makes it difficult to anticipate and counter the highly realistic narratives and convincing impersonations criminals can now create. This is compounded by delays in obtaining crucial digital evidence due to complex jurisdictional barriers and limited cooperation from financial institutions and tech providers. Online fraud is often not prioritised, leading to insufficient access to specialised investigative tools typically reserved for more serious organised crime. Looking ahead, law enforcement must also contend with

the anticipated threat from quantum computing, which could undermine current encrypted data protections in fraud contexts.

Another critical challenge is the inability to disrupt re-victimisation cycles. Stolen credentials are frequently resold, leading to individuals being targeted repeatedly. Furthermore, gaps in online reporting systems make it difficult for victims to report fraud and identity theft quickly and easily, necessitating better infrastructure and a focus on avoiding victim-blaming.

Addressing the transnational nature of online fraud also presents substantial hurdles. There are weaknesses in tackling fraud schemes operated from outside the EU and especially those that involve the laundering of illicit proceeds through foreign financial networks. This global complexity is exacerbated by delays in responding to cross-border requests for operational assistance or information, highlighting a critical need for 24/7 points of contact and faster Mutual Legal Assistance (MLA) procedures. Lastly, insufficient cooperation mechanisms with financial institutions and payment service providers hinder the timely reporting of suspected fraud or major security incidents, severely impacting law enforcement's ability to proactively disrupt these criminal enterprises.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Law enforcement agencies face rapidly evolving challenges in combating online fraud, necessitating urgent adaptations in capabilities, investigative methods, and cooperation frameworks.

In terms of investigative and forensic capabilities, law enforcement faces significant challenges in identifying and investigating persistent fraud operations that mimic legitimate businesses and complex mixed-method fraud schemes, such as those combining investment and romance fraud. A major hurdle is tracing stolen funds through layered crypto-based laundering, gambling platforms, and money mule networks, as well as the difficulty of disrupting the laundering mechanisms behind Chief Executive Officer (CEO) fraud and fake investment platforms. Investigating advanced payment fraud methods, such as SIM swapping, card-not-present attacks, and compromised identities, remains a challenge. Detecting and investigating fraud targeting payment systems, digital skimming, tokenised methods, and CNP transactions is challenging, combined with difficulties with transaction tracing, blockchain analysis, and real-time crypto asset freezing. Furthermore, there is limited

digital forensic and cyber investigation capacity to track online fraud, ransomware, and illicit activity on the dark web.

Emerging and disruptive technologies are significant enablers of online fraud, with fraud schemes enhanced by AI, automation, and crime-as-a-service tools. The growing complexity of Fraud-as-a-Service (FaaS) ecosystems enables low-skilled actors to execute advanced scams, challenging efforts to detect and disrupt phishing kits, fake trading platforms, malware, and automated scam tools. Law enforcement faces a challenge to keep pace with industrialised fraud operations using bots, call centres, chatbots, and spoofed websites, combined with limited preparedness for new fraud vectors linked to fintech, tokenisation, mobile payments, and platform automation. A significant challenge is the lack of tools to identify and investigate AI-powered scams, involving deepfake voices, synthetic identities, and CEO impersonation. Law enforcement capacity is outpaced by AI-driven social engineering and emotion-manipulation techniques.

A further challenge is the capacity to provide practical guidance and support to fraud victims, particularly small businesses, and identity theft victims, including financial, legal, and psychological recovery pathways. There is difficulty detecting fraud schemes that exploit emotional vulnerability, such as fake humanitarian appeals or emergency requests. Limited law enforcement intelligence due to underreporting of online fraud, especially by businesses, is a significant challenge. Furthermore, a re-victimisation risk exists due to the limited capacity to track or block further misuse of stolen credentials.

Investigating cross-border fraud campaigns that exploit call centres, automated messaging, and virtual infrastructures remains a challenge. There are gaps in coordination against globally operating fraud networks that exploit the virtual, borderless space. Fragmented cooperation and slow Mutual Legal Assistance processes, limit access to digital evidence and hinder disruption efforts. Finally, there are gaps in the systematic sharing of reports from payment providers and digital service operators with law enforcement when crimes are suspected, and delays in freezing assets due to cross-jurisdictional laundering and the speed of financial operations.

Training needs

Summary

Law enforcement agencies require comprehensive training to effectively combat the evolving and sophisticated landscape of online fraud. These training needs aim to address the technical, analytical, and cooperative dimensions of modern fraud.

One critical area requiring attention is understanding and investigating fraud enabled by AI and other emerging technologies. This includes examining how AI, deepfake technology, and Crime-as-a-Service tools are revolutionising online fraud, facilitating identity spoofing and scalable scams. Training must also explore new attack surfaces related to fintech innovations, platform automation, and mobile payments, enabling personnel to understand how criminals exploit these ecosystems.

Training is required to strengthen advanced financial and digital forensics capacity for tracing illicit assets and identities. This includes training in tracing cryptocurrency transactions, identifying complex money laundering patterns, and seizing illicit digital assets used in fraud and underground economies.

Awareness raising on relevant legislation also represents a necessity that should be addressed.

Finally, strengthening cross-border cooperation and understanding offender tactics is essential. This involves training on techniques and legal instruments for identifying, tracking, and dismantling platforms used by cybercriminals and fraud networks.

Further details

Training needs to increase knowledge and understanding of investment fraud, including fake trading platforms, Ponzi schemes, and social media-based scams, with emphasis on the psychological tactics and digital traces involved in human-targeted fraud schemes.

Awareness-level training on the ethical and legal implications of AI in fraud detection is also crucial, ensuring a balance between innovation, privacy, and fundamental rights. This includes understanding behavioural patterns, manipulation techniques, and crime scripts commonly used in online fraud, enabling better detection and prevention strategies.

Training in advanced financial and digital forensics must include investigating how criminals exploit gambling and investment platforms for money laundering, and how to disrupt these mechanisms through financial and operational analysis.

Personnel must learn to investigate fraud schemes targeting digital payment systems, including card-not-present (CNP) fraud, skimming, mobile wallets, and token-based platforms.

Advanced techniques for unmasking digital identities and conducting lawful decryption to access critical evidence in encrypted environments are also necessary for effective online investigations.

Strengthening cross-border cooperation requires training to improve investigative capacity to address transnational fraud operations exploiting call centres, virtual infrastructures, and global messaging, which is crucial and emphasises inter-agency and cross-border collaboration.

Law enforcement must also master the tools and procedures for accessing electronic evidence across borders, understanding legal frameworks, such as European Investigation Orders, Mutual Legal Assistance, and voluntary disclosures.

Training on analysing socio-economic trends and disinformation helps identify emerging fraud themes and influence scam evolution and victim behaviour.

List of detailed training needs

Member States indicated that 13 805 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat online fraud schemes:

1. AI-Enhanced Fraud and Crime-as-a-Service Schemes - Examine how artificial intelligence, deepfake technology, and CaaS tools are revolutionising online fraud, including identity spoofing and scalable scams.
2. Cryptocurrency tracing and countering money laundering techniques - methods for tracing crypto transactions, identifying laundering patterns, and seizing illicit digital assets used in fraud and underground economies.
3. Deanonymisation and lawful decryption in online investigations - advanced techniques for unmasking digital identities and conducting lawful decryption to access critical evidence in encrypted environments.
4. Electronic Evidence and Jurisdiction in Cross-Border Investigations - tools and procedures for accessing electronic evidence across borders, including legal frameworks, such as European Investigation Order, Mutual Legal Assistance, and voluntary disclosures.
5. Cross-border fraud campaigns and international cooperation: investigation of transnational fraud operations exploiting call centres, virtual infrastructure, and global messaging, with an emphasis on inter-agency and cross-border collaboration.
6. Artificial Intelligence and Fundamental Rights: the ethical and legal implications of AI in fraud detection, balancing innovation with privacy and fundamental rights.

7. Detecting payment fraud in digital and tokenised environments – investigation of fraud schemes targeting digital payment systems, including card-not-present fraud, skimming, mobile wallets, and token-based platforms.
8. Investigating investment fraud, including fake trading platforms, Ponzi schemes, and social media-based scams - human-targeted fraud schemes involving impersonation, spoofing, and manipulation, with emphasis on psychological tactics and digital traces.
9. Emerging Fraud Vectors in Fintech and Automated Platforms - new attack surfaces related to fintech innovations, platform automation, mobile payments, and how criminals exploit these ecosystems.
10. Investigating Gambling and Investment Platforms Used for Laundering – understanding of how criminals exploit gambling and investment platforms to launder money, and how to disrupt these mechanisms through financial and operational analysis.
11. Social Engineering Tactics and Fraud Crime Scripts - behavioural patterns, manipulation techniques, and crime scripts commonly used in online fraud, enabling better detection and prevention strategies.
12. Monitoring Online Threat Actors and Disrupting Illicit Platforms - techniques and legal instruments for identifying, tracking, and dismantling platforms used by cybercriminals and fraud networks.
13. Socio-Economic Trends and Fraud Narrative Analysis - Identify emerging fraud themes by analysing societal trends, disinformation, and economic shifts that influence scam evolution and victim behaviour.

2.5 Migrant smuggling

Migrant smuggling remains a highly lucrative and resilient criminal enterprise, impacting all EU Member States as regions of transit, or destination. Its scope is extensive, encompassing illegal entry, secondary internal movements, exit strategies, and the fraudulent legalisation of residence. These activities are frequently facilitated through a crime-as-a-service model, with networks adapting routes and leveraging digital technologies for marketing, recruitment, coordination, and communication. Such journeys are often marked by recklessness and fatalities. The growing instrumentalisation of irregular migration by hybrid threat actors – exacerbated by geopolitical instability – further expands the demand for these illicit services, placing significant pressure on border management systems and contributing to the broader destabilisation of EU societies.

Environmental challenges

The EU-SOCTA underscores how migrant smuggling is shaped by its profitability, adaptability, and connections to digital tools and to geopolitical instability.

A primary concern is the high loss of life and violence. Criminal networks treat migrants as commodities, showing disregard for human dignity, evident in the dangerous overcrowding of sea vessels and vehicles. Violence also targets rival criminals, law enforcement, and migrants themselves.

The instrumentalisation of irregular migration by hybrid threat actors is a growing and visible factor, exploiting the situation to destabilise the EU and its Member States, with the effect of creating more business for smugglers and potentially destabilising societies.

Digitalisation significantly nurtures and accelerates migrant smuggling. Criminal networks extensively use online platforms for marketing, recruiting, communication, and money transfers. They employ professional social media advertising strategies to promote successful crossings.

These criminal networks are highly adaptable and resilient, quickly changing routes and methods in response to opportunities, demand, or obstacles, which makes them difficult to counter. This activity places immense strain on border management systems and demands substantial resources from law enforcement.

Disruption of smuggling networks and associated criminal infrastructure requires greater capacity to trace and dismantle high-level networks where leaders operate remotely. This necessitates improved operational and legal capacities to dismantle complex, transnational networks effectively. Law enforcement requires specialised capacity to disrupt the modular "crime-as-a-service" networks involved in journey planning, document fraud, or maritime logistics.

Challenges concerning knowledge, skills, responsibility and autonomy, and related training needs

Challenges

Law enforcement faces the challenge of investigating and responding to overlapping criminal structures involving smuggling, trafficking, and other organised crime. There is a need for preparedness to counter poly-criminal networks and to address gaps in maritime smuggling disruption capabilities, including networks supplying equipment for

sea crossings. Enhanced skills are needed to detect, analyse, and dismantle smuggling networks operating via social media and encrypted communication platforms. Achieving this depends on advanced digital investigative tools and forensics, alongside more effective digital case management and cross-border data-sharing capabilities. Law enforcement must also develop the capacity to detect and investigate fraudulent schemes to legalise stay and persistent document and identity fraud.

Informal value-transfer systems (e.g., hawala) are not inherently illegal, but they are frequently exploited to move criminal proceeds. Persistent tracing challenges – together with the rise of crypto-asset and digital transfer payments linked to smuggling– require enhanced investigative capacity. Building this expertise will help follow the money, preserve lawful use, and target organisers of illicit flows.

Law enforcement has limited capacity to conduct effective vulnerability assessment and smuggling-risk screening at borders. Operational flexibility is crucial to adapt to rapid shifts in smuggling routes or political manipulation. Staff need enhanced frontline risk assessment competencies during border checks and improved cross-border coordination to track individuals and investigate criminal networks.

Protection of vulnerable individuals in migrant smuggling contexts requires greater safeguards for children and vulnerable persons. Law enforcement needs improved early identification and protection capabilities for those subjected to high-risk smuggling methods. Crucially, there is a need for comprehensive staff training in trauma-informed approaches and in identifying vulnerabilities such as LGBTQI+ needs and THB, including labour exploitation. Robust identification and improved referral mechanisms for victims of trafficking, torture, or sexual and gender-based violence (SGBV) are essential.

Gaps in inter-agency and cross-border cooperation hinder operational response. Incomplete coordination between various actors and a lack of legal frameworks to address politically motivated or state-enabled smuggling present significant challenges. Developing strategic coordination, early warning systems, and operational mechanisms to prevent the abuse of asylum procedures is crucial.

Politically instrumentalised and state-facilitated smuggling is a hybrid threat that requires effective early warning systems and intelligence integration across migration, border control, hybrid threats, and national security domains to detect orchestrated flows. Law enforcement requires enhanced capacity to detect and respond to such threats, including the capacity for planning for mass arrivals due to deliberate migration instrumentalisation.

Training needs

Summary
Law enforcement across the European Union requires comprehensive training to effectively combat migrant smuggling, particularly in several key areas:

Firstly, significant training is needed in digital investigations to counter the increasing online operations of smuggling networks. This includes developing expertise in Open Source Intelligence, leveraging social media platforms, and utilising AI in detecting online content related to irregular migration dynamics and in dismantling smuggling networks. Related training needs to be primarily centred on analysts, investigators, the judiciary and first line officers working at the external borders of Poland, the Baltic countries, and Finland. Furthermore, training in digital forensic tools, securing data and evidence, creating digital forensic reports, and ensuring judicial cooperation for evidence acceptance is crucial to address smuggling in the digital domain. In terms of bi- or trilateral judicial cooperation, countries such as Egypt, Bulgaria, Greece, Poland, or Latvia are likely to be the primary parties concerned, depending on the specific case involved.

Secondly, financial investigations demand specialised training. This encompasses the investigation of migrant smuggling cases involving informal value transfer systems like hawala and cryptocurrencies. There is also a need for training on how to dismantle "brotherhoods" – networks of public officials or respected individuals – that serve as legal organisations to cover the activity of organised criminal groups.

Thirdly, training should focus on the diverse facets of "crime-as-a-service" offered by smugglers and the instrumentalisation of migration. This includes investigating maritime logistics (including small boats, supply chains, and rental companies) and the supply of vehicles to smuggling networks. In this regard, regional dimensions are particularly pronounced, with the English Channel and the Mediterranean identified as primary zones of concern for maritime logistics, while Member States such as Greece and Latvia are more prominently involved in issues related to vehicle supply. Law enforcement also requires training on sources of information and intelligence exchange on smuggling flows, and on fostering judicial cooperation against state actors involved in the instrumentalisation of migrant smuggling. This is especially relevant to implement in relation to Poland and the Eastern Partnership (EaP) countries. Cooperation with other intelligence services (defence, intelligence, security) is also a key training area. Additionally, training in document and identity fraud investigations, 'breeder documents', forensics, and securing evidence is vital.

Lastly, vulnerability assessment and protection of individuals are critical training areas. This involves smuggling risk assessment, behavioural analysis, and document screening, with a specific focus on vulnerable persons, including minors. Law enforcement personnel need to be proficient in interviewing techniques. Training should cover vulnerability risk assessment, identification, and management of vulnerable persons, utilising a trauma-informed approach. Understanding the exploitation of migrants and the link to human trafficking is also essential. Furthermore, it is necessary to provide training on EU cooperation tools, mechanisms, and databases such as Joint Investigation Teams, Operational Task Forces, SIENA, and report creation, as well as training involving service providers, banks, and accommodation services. Furthermore, the development of an integrated border management system terminology in English is also needed.

Further details

Several further areas underline the scope of the capabilities required of law enforcement officials.

Another specific requirement is training focused on how to treat vulnerable persons while collecting biometric data. This emphasises a sensitive and ethical approach to interacting with vulnerable individuals, such as minors, while simultaneously performing the technical task of biometric data collection. It underscores the importance of balancing operational objectives with humanitarian considerations in this specific context.

Further training concerns return operations, specifically addressing scenarios such as refusal of entry and repatriation. Law enforcement involvement in these processes requires specialised knowledge and procedures related to the legal, logistical, and humanitarian aspects of migrant departures.

Furthermore, training is required to monitor secondary movements of migrants. This points to the need for developing capabilities to track and analyse the onward journeys of migrants after their initial arrival or detection, which is crucial for understanding migration dynamics and dismantling smuggling networks effectively.

Lastly, building networking opportunities with third countries is identified as a unique training priority. This goes beyond formal judicial or intelligence cooperation, focusing on fostering broader strategic relationships and partnerships with non-EU countries to enhance long-term collaborative efforts against migrant smuggling.

Together, these training needs emphasise a comprehensive approach that includes personal security, ethical handling of sensitive data and individuals, managing post-

entry operational phases, advanced intelligence gathering, and proactive international relationship building.

List of detailed training needs

Member States indicated that 9 909 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat migrant smuggling:

1. Digital investigations, including Open-source intelligence, AI, and social media monitoring, to detect smuggling-related content and dismantle online migrant smuggling networks.
2. Financial investigation techniques in migrant smuggling cases, including tracking informal transfer systems such as hawala and cryptocurrency flows.
3. Detecting and investigating document and identity fraud linked to migrant smuggling, including but not limited to breeder documents, forensics, securing admissible evidence and creating forensic reports.
4. Digital forensic tools and procedures, including data security, forensic reporting, and judicial cooperation to ensure the admissibility of evidence.
5. Operational use of EU cooperation tools and databases (e.g., Joint Investigation Teams, Operational Task Forces, SIENA) to support joint investigations and intelligence exchange in migrant smuggling cases.
6. Investigative methods to detect and dismantle institutionalised or socially embedded support networks (brotherhoods) enabling migrant smuggling and serving as legal organisations to cover organised crime groups.
7. Migrant smuggling risk assessment, behavioural analysis, document screening with focus on vulnerable persons, including but not limited to minors, interviewing techniques.
8. Indicators and investigative linkages between migrant smuggling and trafficking in human beings.
9. Techniques, tools, and investigative approaches to detect and counter migrant smuggling conducted through digital platforms and encrypted communication channels.
10. Instrumentalisation of migration: sources of information and intelligence exchange on smuggling flows; judicial cooperation against state actors involved in the instrumentalisation of migrant smuggling; cooperation with other intelligence services (defence, intelligence, security).

11. Public-private cooperation in migrant smuggling prevention and detection, including engagement with banks, accommodation providers, and other relevant sectors.
12. English law enforcement terminology related to migrant smuggling domain.
13. Vulnerability risk assessment, identification and management of vulnerable persons, use of trauma-informed approach.
14. Various types of crime as a service: maritime logistics, including but not limited to small boats, chain of supply, rental companies; supplying vehicles to smuggling networks, chain of supply, rental companies.

2.6 Online child sexual exploitation

Online Child Sexual Exploitation (CSE) is a serious crime with profound psychological and physical impacts. The incidence of this crime is growing, associated with the increasing presence of children, including very young children, accessing the internet through mobile phones. Offenders are increasingly technologically aware, operating across both the dark and clear web, using encrypted platforms and closed groups to facilitate grooming, abuse, and to evade detection. The rise of generative AI has accelerated the creation of synthetic child sexual abuse material (CSAM), complicating identification and response efforts. Victims are subjected to coercion, extortion, and enduring trauma, underlining the fundamental importance of trauma-informed, child-centred approaches to avoid further harm and re-victimisation.

Environmental challenges

Child sexual exploitation is increasingly driven by technological advancements, leading to rapid growth in online offences and the volume of child sexual abuse material. Mobile devices, social media, digital platforms, and normalised online sexual behaviours facilitate grooming, sexual extortion, and the widespread exchange of abusive content. Generative AI introduces new risks by producing and manipulating CSAM, further complicating identification and multiplying the volume of harmful material online. Offenders exploit encrypted apps, the dark web, and cross-platform ecosystems, often using sophisticated countermeasures to evade detection. Livestreamed abuse, AI-generated content, and instructional "paedophile handbooks" amplify the threat, while disparities in legal and procedural frameworks across Member States hinder coordinated investigations, prosecutions, and victim protection. While underlining the importance of undercover and proactive investigations, it is worth noting that in some Member States, legislation does not permit them.

Fragmented national cybercrime capacities create strategic gaps, and delays in real-time data exchange and mutual legal assistance undermine transnational responses.

Long-term protection, psychological support, and follow-up for child victims remain insufficient, particularly for those affected by coercion, grooming, and manipulation within extremist or violent online communities. Law enforcement also faces structural challenges in collaboration and resource allocation, including uneven cross-border cooperation, inconsistent victim identification and referral protocols, and limited operational engagement with private sector actors and non-governmental organisations (NGOs) specialising in CSE-related intelligence and victim support.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Effectively addressing CSE requires enhanced expertise and operational capabilities. Law enforcement must improve detection and analysis of offender networks operating across multiple digital platforms, encrypted apps, and gaming environments, and better understand grooming methods and radicalising content. Officers need advanced skills in digital forensics, case management, and cross-border data sharing, as well as the ability to assess the real-world impact of online radicalisation and abuse material to inform prioritisation.

Capacity building is also essential in managing victims and preventing recidivism. This includes strengthening monitoring and risk assessment in detention and conflict-zone camps, improving protection and follow-up mechanisms, and equipping prison and probation staff to address radicalisation among offenders. Investigators must remain current on emerging technologies and AI-enabled threats, as well as new distribution methods such as subscription services, livestreamed abuse, and decentralised content ecosystems.

Autonomy is constrained by fragmented structures, limited personnel, and low national capacities, which impede effective cross-border coordination, deployment of automated detection tools, and integration with private sector partners. Harmonising investigative approaches, victim support protocols, and legal procedures across Member States is critical to ensure consistent, effective responses, while strengthening international cooperation and interoperable intelligence systems is essential to track offenders and identify victims efficiently.

Training needs

Summary

To respond to the complex challenges of child sexual exploitation, training must span several critical areas to address the increasingly digital and sophisticated nature of this crime.

Training is essential for offender management, offender risk assessment, risk management, and offender behavioural analysis. This includes understanding the tech-savviness of CSE offenders, who are highly aware of security measures and adept at developing sophisticated countermeasures to evade investigations.

Regarding detection and investigation, there is a pressing need for training on understanding legislation related to the implementation and use of AI and new digital tools in CSE. This is critical as generative AI is increasingly used to produce and manipulate child sexual abuse material, including creating new content, making adults appear younger, or "nudifying" non-explicit images.

Training in financial investigations related to CSE is essential, specifically concerning cryptocurrencies and informal value transfer systems. This includes developing expertise in blockchain analysis to trace financial transactions, given that cryptocurrencies, decentralised finance platforms, and AI-driven automation can obscure illicit transactions. Understanding complex schemes, such as chain hopping used to obfuscate the origin of funds, is also crucial.

Law enforcement requires training in victim identification, including minors involved in self-generated material. This is particularly challenging given the proliferation of self-generated sexual material due to normalised online sexual behaviours, such sexting, and the growing threat of sexual extortion. Furthermore, training in a trauma-informed and victim-centred approach is crucial, recognising that CSE involves severe physical and psychological violence that profoundly impacts child victims for prolonged durations.

Training on international cooperation, information exchange frameworks and mechanisms, including Mutual Legal Assistance, is vital. The cross-border nature of CSE offences, with offenders leveraging end-to-end encrypted communication applications to create international networks, necessitates robust international collaboration.

Further details

For the behavioural analysis of offenders, law enforcement requires specialised training in undercover and proactive investigations, particularly to navigate international online

offender communities on both the dark and clear web, where abuse, grooming techniques, and operational security tips are exchanged. This training must address how to effectively respond to the dynamic behaviour and adaptability of organised, transnational CSE offenders. This capacity currently varies significantly across the Member States.

For detection and investigation, training is required for new investigative tools relevant to online CSE, especially for analysing high volumes of AI-generated CSAM to identify victims and offenders. This is particularly applicable to Member States with less resources dedicated to CSE. Regarding the use of AI tools in digital investigations of CSE, a European AI tool repository is being developed at Europol.

Law enforcement needs greater training on strategies to overcome barriers posed by end-to-end encryption in communication applications, which facilitate cross-border networking among offenders.

Given the importance of trauma-informed and victim-centred approaches, law enforcement could benefit from providers of such training, such as Barnahus. An example of trauma-informed principles applied to interviewing is 'social interviewing', and this capacity should be included in training.

Regarding cooperation, training is needed on mechanisms for working with the private sector and providers, such as SIRIUS, to engage with legitimate platforms used by criminals and navigate legal frameworks for investigations.

List of detailed training needs

Member States indicated that 6 948 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat online child sexual exploitation:

1. AI-assisted and digital forensic tools for detecting, analysing, and disrupting online child sexual exploitation, including synthetic child-sexual abuse material and livestreamed abuse.
2. Emerging child sexual exploitation trends and new investigative technologies, including AI-generated child-sexual abuse material, deepfakes, and grooming in virtual environments.
3. Forensic approaches to child sexual exploitation (child sexual exploitation), including detection of AI-generated child-sexual abuse material, forensic investigation of live-streamed abuse, online behavioural analysis, trauma-

informed handling of digital evidence, and undercover operations in online environments.
4. Cooperation mechanisms with private sector providers and the use of platforms, such as SIRIUS, for intelligence sharing and joint operations.
5. Financial investigations in child sexual exploitation cases, including tracing payments through cryptocurrencies, symbolic transfers, and informal value transfer systems.
6. Blockchain analytics for tracing digital financial transactions linked to the production, purchase, or distribution of child-sexual abuse material.
7. Legal and technical investigative tools to detect grooming and exploitation in gaming platforms, social apps, and immersive digital spaces.
8. Undercover and proactive investigative methods, including operations in encrypted and dark web environments used for child sexual exploitation.
9. International cooperation tools and procedures, including Mutual Legal Assistance, for cross-border investigations and real-time data exchange in child sexual exploitation cases.
10. Victim identification techniques, including tools for analysing anonymised or self-generated child-sexual abuse material and identifying minors.
11. Offender profiling, risk assessment, and behavioural analysis to support early intervention and targeted child sexual exploitation offender management.
12. Trauma-informed, victim-centred law enforcement practices to reduce re-victimisation and support child protection.
13. Legal frameworks and ethical standards for AI use in child sexual exploitation investigations, including data protection and evidentiary admissibility.

2.7 Excise and customs fraud (Economic and financial crimes)

Excise and customs import fraud significantly undermine EU financial integrity by exploiting public funds through adaptive transnational schemes. Customs fraud leverages e-commerce growth, employing undervaluation and false origin declarations, often enabled by document manipulation and misuse of legal entities. Excise fraud is driven by tax disparities and high duties, evident in the illicit production of counterfeit tobacco products. Criminal networks are expanding into counterfeit vaping and biofuels, using skilled technicians and artificial intelligence to generate fraudulent documentation. These activities are further facilitated by the abuse of duty

suspension systems, notably the Excise Movement and Control System (EMCS), and exploit geopolitical instability, sustaining a dynamic illicit market across borders.

Environmental challenges

Law enforcement faces significant challenges in combating excise fraud due to a combination of inconsistent resources, legislative gaps, and the adaptability of criminal networks. A primary issue is the lack of consistent resources to identify and remove from the market counterfeit or illicit excise products, including e-cigarettes and waterpipe tobacco. Operational tools designed to interdict the illicit movement of these products, particularly through the misuse of legal frameworks such as the Excise Movement and Control System, need to be taken up systematically across Member States.

The absence of harmonised EU legislation on raw tobacco, biofuels, new products, and precursors creates opportunities for criminals to engage in fraud, especially fuel fraud, by exploiting significant price differences for excisable goods across countries. Criminal networks are highly adaptive, rapidly shifting to a broader range of products, such as counterfeit vapes and e-cigarettes, and engaging in illicit production of counterfeit tobacco within the EU, often relying on experienced technicians and document fraud.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Law enforcement agencies face significant challenges in combating excise and customs fraud, including limited capabilities, inadequate financial crime response, limited adaptation to evolving threats, and cross-border cooperation.

Greater specialised capabilities are required to identify and dismantle illicit production sites, including those producing tobacco, alcohol, and designer fuels, as well as to address multi-layered, poly-criminal networks that operate across jurisdictions and adapt rapidly. Improved consistency of tools and methods for investigating document fraud across Member States could significantly increase cross-border enforcement effectiveness. Investigations into fuel fraud require increased access to technical expertise and analytical facilities. New smuggling routes and modi operandi need to be consistently integrated into real-time situational awareness. Digital investigative capabilities need to be adapted to online-enabled excise fraud. Operational capacities for detecting and investigating the production and smuggling of excise goods require greater scope and scalability. Mechanisms to monitor raw tobacco and precursors

require more uniform implementation, and excise fraud necessitates greater consistent prioritisation across Member States.

Expertise and operational capacity to address professional money laundering facilitators linked to excise fraud are essential across jurisdictions, with financial intelligence and digital forensics fully integrated into investigations. Tools for tracing and disrupting the laundering of proceeds from excise fraud need to be uniformly implemented.

Preparedness to address excise fraud risks in emerging markets, such as those posed by biofuels and novel nicotine products, needs to be strengthened. Law enforcement capabilities to monitor and disrupt online platforms for illicit goods require further development. Practices for identifying misuse of legal business structures need to be consistently embedded, and structural limitations hindering efforts to investigate infiltration of the legal economy need to be addressed and overcome. Mechanisms for real-time monitoring and traceability of excise goods need to be fully optimised.

Coordination across Member States and neighbouring countries demands a greater structured focus on dismantling criminal networks. Greater integration is necessary to improve effective data sharing and joint operational frameworks among customs, tax, and law enforcement agencies. Overall, strategic and operational collaboration requires greater integration, together with greater alignment and implementation of mechanisms for cross-border cooperation in multinational excise and customs fraud cases.

Training needs

Summary

A comprehensive training program is needed to address the multifaceted challenges of cross-border excise and customs fraud, focusing on key areas to enhance the capabilities of law enforcement and tax authorities.

A primary need is advanced training in specialised investigative techniques to detect and investigate transnational criminal groups. This includes surveillance, covert operations, Open-Source Intelligence, and cyber-patrolling, and it is primarily needed in the Baltic States, Poland, Belgium, the Netherlands, France, and Central European countries. The training must also cover digital investigations.

Another critical area is tackling the financial dimension of these crimes. Training is required on the specific methods of money laundering used in excise fraud and on subsequent asset recovery.

Training must also address the need for effective international cooperation. This includes the practical application of EU instruments and tools, such as the EPPO Regulation, European Investigation Orders, Joint Investigation Teams, Europol, and Eurojust.

Finally, the programme must be adaptive, addressing emerging threats and evolving criminal trends. This includes understanding the misuse of legal business structures, new smuggling routes that arise from global disruptions, and changing modus operandi, including those concerning new products, such as vapes and e-cigarettes. Training initiatives in this area would be particularly relevant for Member States from Eastern Europe and EaP countries.

Further details

Training in digital investigations needs to strengthen skills in using digital tools, data analysis and visualisation, and the presentation of digital evidence in court. This training also needs to address cryptocurrencies, cloud storage, and the use of AI, predictive analytics, and machine learning for intelligence purposes. Addressing money laundering and asset recovery requires improving proficiency in cross-border financial tracking tools to trace illicit proceeds laundered through real estate, offshore investments, and luxury assets.

A significant focus should be on improving the legal and procedural aspects of intelligence analysis and sharing between tax authorities, Financial Intelligence Units, and law enforcement, ensuring compliance with data protection regulations.

Cooperation with non-EU countries, including the UK, and international organisations, such as Interpol and the World Customs Organisation (WCO) presents unique challenges that require dedicated training.

Tackling poly-criminal networks that engage in excise and customs fraud alongside other crimes is also a key training objective, as is a harmonised methodology for customs laboratories to ensure consistent analysis across the EU. This is particularly relevant with regard to the Baltic States, Poland, Belgium, the Netherlands, France, and Central European countries.

List of detailed training needs

Member States indicated that 13 151 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat excise and customs fraud:

1. Analysis and sharing of intelligence between tax authorities, Financial Intelligence Units, and law enforcement: legal and procedural aspects, compliance with data protection regulations and use of new technologies and tools such as Artificial Intelligence, predictive analytics and machine learning.
2. Cooperation tools and instruments with non-EU countries, international organisations, Interpol, World Customs Organisation; cooperation with the UK, the exchange of information that can be used as evidence in the UK; challenges in obtaining financial intelligence and forensic evidence.
3. Available tools for cross-border financial tracking and detection and sharing best practices of using them: trade monitoring, financial oversight, tracking of Excise and customs fraud proceeds laundered through real estate, offshore investment schemes and luxury assets.
4. Emerging crime patterns and the misuse of legal business structures in excise and customs fraud, including crisis-driven adaptations and sanctions circumvention.
5. Cross-border special investigation techniques for excise and customs fraud, including surveillance, covert operations, Open-source intelligence, cyber patrolling, and digital monitoring tools.
6. Emerging excise and customs fraud modi operandi, including trends in vapes, novel nicotine products, and designer fuels.
7. Money laundering typologies and asset recovery strategies linked to excise and customs fraud, with a focus on cross-border financial flows.
8. Digital investigations: digital tools available, Open-source intelligence, analysis and visualisation of data, presentation of digital evidence in court, cryptocurrencies, cloud storage, Virtual Private Network services, use of Artificial Intelligence.
9. EU instruments and tools for cross-border cooperation, intelligence sharing and investigations, and their practical application: Art. 31 of the EPPO Regulation, European Investigation Order, Operational Task Forces, Joint Investigation Teams, Anti-Money Laundering Authority, Europol, Eurojust, European Public Prosecutor`s Office, Naples II Convention.
10. Awareness raising on the exiting EU framework to tackle evasion of EU sanctions.

11. Poly-criminal networks engaged in excise and customs fraud, with a focus on cross-border structures, operations, and disruption strategies.
12. Tools and methods for tracking and tracing smuggled excisable goods across the EU, the Excise Movement and Control System (EMCS)
13. Training on harmonised customs laboratory methodologies for detecting excise and customs fraud, with EU-level experience sharing and analytical techniques.

2.8 Trafficking in human beings

Trafficking in human beings is a serious crime, sustaining sexual exploitation, the provision of forced and illegal labour, coercion into activity, the trafficking of minors, exploitation of forced marriage, of surrogacy and of illegal adoption. It is globally interconnected with other serious and organised crime areas such as migrant smuggling, child sexual abuse, etc. Traffickers increasingly use modi operandi to evade attention and create the appearance of legitimacy. Trafficking increasingly leverages digital platforms for all stages of its operations; it increasingly makes use of sophisticated psychological manipulation of victims and often disguises itself through legal business structures. The criminal networks involved are highly adaptable and increasingly coordinate remotely to evade detection.

Environmental challenges

Addressing trafficking in human beings requires a concerted and multifaceted response to overcome significant challenges across several key areas, which can be categorised into five critical domains.

First, the challenge is to harmonise and strengthen legal frameworks. This involves addressing variations in labour laws and enforcement, implementing stronger legal safeguards to prevent victims from being prosecuted for coerced crimes, and updating obsolete provisions for freezing and confiscating the proceeds of crime. This also requires fully integrating human rights protections into legal responses, standardising content regulation to track material promoting trafficking and re-evaluating restrictive asylum and migration policies that inadvertently increase vulnerability.

Second, it is crucial to enhance and integrate mechanisms for cooperation and information sharing. This means overcoming judicial cooperation difficulties, improving coordination between refugee reception systems and law enforcement, and strengthening intelligence-sharing and international cooperation to tackle transnational exploitation. Strengthening the integration of NGOs and victim support

services into anti-trafficking response frameworks, harmonising statistical frameworks for consistent reporting, and fostering robust public-private sector cooperation are also vital challenges to address.

Third is the necessity to bolster investigative capacities and ensure full criminal accountability for traffickers. This involves addressing disparities in prosecution and sentencing, increasing the use of financial intelligence tools, and developing an integrated law enforcement strategy to disrupt trafficking activities across digital platforms, including social media, dark web, and encrypted networks. It is important to strengthen the capacity to identify victims of human trafficking concealed in large scale movements of refugees. Ensuring clear prosecution mechanisms for full accountability, harmonising EU-wide standards for handling cases, and enhancing digital forensic resources central to this.

Fourthly, there is a need to ensure comprehensive, standardised, and accessible victim protection measures. This requires ensuring broader access to legal aid, developing targeted measures to address intersectional discrimination, and implementing more effective prevention efforts for vulnerable populations.

Finally, there is a need to fortify institutional frameworks and address limitations in law enforcement capacity. This includes establishing a centralised EU-wide tracking system for victims and traffickers and mitigating risks where increased border security inadvertently pushes migrants towards traffickers. It is important that Europol's High-Value Target initiative prioritises major trafficking figures, and that appropriate resources and personnel are available for investigations and support. It also includes ensuring appropriate accountability to address law enforcement corruption.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Strengthening effective EU cooperation requires greater knowledge of existing tools and instruments and legal frameworks, including those addressing the gender dimension of trafficking. This underlines the importance of building capacity for collaborative investigations, intelligence-sharing, and multi-agency responses and to strengthen capacity for information-sharing and victim-centred judicial strategies between Eurojust, law enforcement officials, and victim support agencies. Furthermore, building the knowledge necessary to strengthen cooperation with technology companies and integrating NGOs and victim support in anti-trafficking frameworks presents an ongoing challenge.

To bolster investigation and prosecution, a core challenge is to keep pace with the rapidly evolving digital modus operandi of criminal networks. This demands strengthening knowledge of the online domain's central role, including remote victim identification, cryptocurrencies, and identity fraud. Law enforcement must strengthen specialised digital investigation skills to track digital footprints, trace cryptocurrency transactions, profile online activity, identify traffickers' use of encryption and anonymity, and leverage AI as an investigative tool. Responding to the extent that traffickers increasingly exploit humanitarian settings requires the capacity to distinguish between legitimate volunteers and criminal actors in complex environments.

The capacity to identify and address the intricate links between migrant smuggling and human trafficking is of critical importance. This requires knowledge to effectively identify victims hidden in large-scale movements of refugees and to understand emerging forms of trafficking linked to forced criminality.

For victim protection, a key challenge is overcoming difficulties in identifying victims, as psychological manipulation and additional constraints often prevents victims from self-identifying. This requires knowledge of the manipulation tactics involved and specialised skills in trauma-informed support, victim-centred interventions, and effective interviewing techniques. A fundamental challenge is to implement stronger legal safeguards within European Arrest Warrant proceedings to prevent victims from being prosecuted for coerced crimes and to fully integrate human rights protections into legal responses. This demands that all relevant actors build knowledge of these safeguards and their application, with clear responsibility for upholding human rights.

Training needs

Summary

Addressing the multifaceted challenges in combating trafficking in human beings requires comprehensive training, particularly in the areas of cooperation, investigations, and victim protection.

Cooperation and information exchange are vital and require training on EU cooperation tools and instruments, as well as on intelligence-sharing and investigative coordination across jurisdictions. Training should also cover the legal framework concerning the gender dimension of trafficking. Training to enhance cooperation with private companies is crucial, focusing on leveraging their available technological tools in investigations, sharing best practices, and addressing data-collection concerns. Improved coordination among national authorities, to tackle all forms of exploitation, including labour exploitation, through EU-level guidance and the exchange of best

practices, is essential. Furthermore, a significant training need exists in detecting and preventing the links between migrant smuggling and human trafficking.

In the area of investigations and prosecutions, training must address the different forms of trafficking, including sexual exploitation, child trafficking, labour exploitation, exploitation of forced marriages, of surrogacy and of illegal adoption, and trafficking for organ trafficking, alongside the effective use of Open-Source Intelligence. Digital forensics is a key area that encompasses techniques for tracking digital footprints and employing behavioural analysis to identify victims. Training should also address the application of Artificial Intelligence in investigations and methods for detecting and investigating traffickers' use of encrypted communication platforms and deep web marketplaces. Financial investigations need to expand into emerging areas, such as cryptocurrencies, collaboration with Asset Recovery Offices, and forensic financial investigations targeting informal economic flows associated with trafficking. Additionally, training should acknowledge the emerging trend for trafficking in human beings such as forced criminality.

For the protection of victims, training is needed on trauma-informed support, victim-centred interventions, and specific support for child victims and other vulnerable groups. Best practices in interviewing victims, collaborative workshops, and effective victim identification processes are also critical components, supported by ensuring all law enforcement personnel have training to identify possible trafficking in human beings.

Further details

Training aimed at supporting a harmonised implementation of new legislation in the Member States should be developed to support law enforcement collaboration with technology companies. This is especially relevant to human trafficking and should be complemented by awareness sessions for transport companies to recognise trafficking indicators.

Training should be provided to all law enforcement personnel – not only specialised units – covering the various forms of trafficking, including sexual exploitation, child trafficking, labour exploitation, exploitation of forced marriages, of surrogacy and of illegal adoption, and trafficking for organ trafficking. Effective detection requires strengthening digital forensics and behavioural analysis capabilities, with involvement from IT companies and cascading initiatives to the national level. AI applications to address trafficking should also be integrated nationally.

Addressing traffickers' use of encrypted communications and deep web marketplaces is crucial, although some countries lack a legal basis for such monitoring. Forensic financial investigation capabilities should be expanded to multiply national capacities. Training should foster multi-stakeholder engagement to detect and prevent links between migrant smuggling and human trafficking. Finally, emerging trends such as trafficking linked to forced criminality demand, enhanced capacity to identify trafficking within other criminal contexts.

List of detailed training needs

Member States indicated that 7 077 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat trafficking in human beings:

1. Detecting and investigating traffickers' use of encrypted communication platforms, the dark web, and hidden online marketplaces
2. Investigations and prosecutions of all forms of THB (sexual exploitation, child trafficking, labour exploitation, exploitation of forced marriages, of surrogacy and of illegal adoption, and trafficking for organ trafficking, etc.), with emphasis on Open-source intelligence use and crime-type specific approaches,
3. The use of AI tools in THB detection, monitoring, and investigative strategies while addressing risks and safeguards.
4. Coordination between national authorities on all forms of exploitation through the exchange of operational best practices.
5. Emerging forms of THB forced criminality: legal, investigative, and victim protection perspectives.
6. EU cooperation tools and instruments, intelligence-sharing and investigative coordination across jurisdictions.
7. Cooperation with technology and private sector actors in THB investigations: tools, data sharing, and privacy safeguards.
8. Digital forensic techniques, including behavioural analysis and footprint tracking, to detect and identify THB victims.
9. Identifying and disrupting operational links between migrant smuggling and human trafficking in investigative and preventive efforts.
10. Financial investigations within THB: emerging areas, such as cryptocurrencies, work with Asset Recovery Offices; forensic financial investigations targeting informal THB-related economic flows.
11. Victim identification.

12. Protection of victims: trauma-informed support, victim-centred intervention, child victims, support vulnerable groups, interviewing victims, exchange of best practices, collaborative workshops.

2.9 VAT (incl. MTIC) fraud (Economic and financial crimes)

VAT fraud – particularly Missing Trader Intra-Community (MTIC) fraud – poses a persistent and sophisticated threat to the financial integrity of the EU and its Member States, resulting in annual losses of tens of billions of euros. These schemes involve intricate networks of companies designed to obscure the identities and roles of participants. Criminal actors exploit weaknesses in trade monitoring, financial oversight, and VAT compliance, often misusing legal business structures as shell and buffer companies to manipulate cross-border VAT systems. The threat is compounded by the expertise of fraudsters who rapidly adapt to legislative changes and market conditions. The potential misuse of digital content transactions to evade VAT obligations is an increasing cause of concern.

Environmental challenges

The primary challenge stems from complex criminal schemes in which goods are repeatedly traded across borders to illegally claim VAT refunds on taxes that were never actually paid. An even more complex emerging method is the "contra-trading scheme," which adds extra layers of companies to make the fraud harder to detect.

Through the systematic misuse of legal business structures, criminal networks establish or infiltrate hundreds of shell and buffer companies to exploit cross-border VAT systems, with operations conducted by professionals with extensive knowledge of finance, tax law, and technology, who can adapt quickly to legislative changes and law enforcement actions. Criminals typically target high-value goods, such as electronic products, IT accessories, and luxury cars, while precious metals are increasingly being targeted as well.

Challenges in combating VAT fraud stem from significant systemic weaknesses across legal, enforcement, and technological domains.

A core challenge is the inconsistent and weak legal framework among EU Member States. This fragmentation creates loopholes that criminals exploit, particularly in Free Trade Zones, data-sharing restrictions, anti-money laundering laws, and differing classifications of intangible goods. Compounding this problem is the weak oversight of professional "enablers"—such as lawyers, accountants, and financial service providers—and inadequate controls over shell companies and offshore investment schemes.

On the enforcement side, inconsistent priorities across Member States create procedural barriers and slow the execution of crucial tools, such as European Investigation Orders. Internal challenges, including corruption within tax and financial institutions and weak VAT de-registration processes, further undermine the response to fraud.

Critically, authorities face technological and data-related limitations. Law enforcement has limited digital forensic capacity and faces fragmented access to structured digital evidence and transaction-level VAT data. The lack of centralised tracking systems for high-risk goods and financial transactions, combined with limited access to advanced analytical tools and financial intelligence, significantly hinders the ability to detect and investigate these complex crimes effectively.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Addressing the complex threat of VAT fraud requires addressing significant challenges across legal, enforcement, and technological domains.

A primary challenge is to institutionalise cross-border cooperation mechanisms to address the fragmented investigations and uncoordinated enforcement in the current landscape. This involves enhancing collaboration between national law enforcement, customs authorities, tax agencies, and Financial Intelligence Units to close critical enforcement gaps. Additionally, a key task is to strengthen cooperation with non-EU countries, as weak coordination creates significant difficulties in obtaining essential financial intelligence and evidence from jurisdictions with low regulatory oversight.

In terms of intelligence sharing, the central challenge is to establish structured mechanisms among tax authorities, FIUs, and law enforcement, to enhance fraud detection capabilities. This requires increasing the spontaneous exchange of financial intelligence to enable early intervention and addressing the poor integration of VAT compliance data across Member States, which currently creates enforcement blind spots and fragmented risk assessments.

It is important to improve tracking, monitoring and detection to gain real-time access to VAT fraud intelligence. A critical need is to close gaps in cross-border financial tracking, as criminals exploit these to transfer proceeds to non-EU jurisdictions, making asset recovery difficult. This also involves improving the ability to track funds laundered through real estate and offshore schemes, strengthening detection in business-to-

consumer (B2C) commerce, e-commerce, and systematically monitoring companies that disappear from the VAT register.

A major challenge is strengthening the capacity to link fraudulent VAT refund claims to money laundering networks, thereby increasing successful prosecutions and asset recovery rates. Greater use should be made of special investigative techniques and Joint Investigation Teams to dismantle the criminal organisations behind the fraud and avoid uncoordinated efforts. It is important to increase the capacity to identify false loan agreements and fictitious investments involving shell companies and to increase the ability to track rapid flows of intangible goods.

In terms of digital forensic tools, a significant challenge lies in extracting and analysing encrypted digital transactions. Authorities must develop forensic accounting capabilities and acquire advanced tools to track funds laundered through cryptocurrencies and decentralised finance. Establishing a standardised framework for cross-border digital evidence collection is also critical to facilitate international cooperation.

Finally, key challenges include adapting fraud detection models more quickly by leveraging AI and machine learning to proactively identify new MTIC fraud schemes and tackling corruption within tax and financial institutions that criminal networks exploit.

Training needs

Summary
Comprehensive training is required to address the complex and evolving challenges of VAT fraud. This spans international cooperation, intelligence analysis, financial investigation, advanced digital techniques, and adapting to new criminal trends.

A foundational training need is to enhance the capacity for international cooperation and the practical application of legal instruments. This involves in-depth training on EU tools such as the European Investigation Order, Joint Investigation Teams, and the EPPO Regulation, as well as understanding the roles of Europol and Eurojust. In particular, such training would be especially relevant for new EPPO members and for the south-east of the EU.

Another critical area is intelligence analysis and sharing. Training, both at the EU and regional levels, is essential on the legal and procedural aspects of sharing intelligence between tax authorities, Financial Intelligence Units, and law enforcement, ensuring compliance with data protection rules.

Greater capacity is required to address the financial dimension of VAT fraud by leveraging available tools for cross-border financial tracking, trade monitoring, and financial oversight.

Finally, greater capacity is required in advanced and digital investigative techniques. Training needs to address Special Investigation Techniques, such as surveillance, covert operations, OSINT, and cyber-patrolling, to detect and dismantle transnational criminal groups.

Further details
Training must address the challenges of obtaining financial intelligence and forensic evidence from non-EU countries, as well as the complexities of different national legislations and EU regulations, to foster effective transnational cooperation among prosecutors and law enforcement.

Training needs to increase the ability to leverage new technologies, such as AI, predictive analytics, and machine learning for intelligence purposes. This includes training on integrating VAT compliance data into shared fraud-tracking systems to create a more unified operational picture across Member States.

It is important to equip investigators with the skills to trace VAT fraud proceeds laundered through real estate, offshore investment schemes, and luxury assets. Understanding money laundering as an integral service in these fraud schemes and focusing on successful asset recovery are crucial dimensions to address.

Training is needed to improve capacity for digital investigations, involving digital tools, data analysis and visualisation, and the presentation of digital evidence in court. This requires specialised training on cryptocurrencies, cloud storage, and VPN services.

Training must address emerging threats in areas such as B2C e-commerce and digital goods, as well as the connection between MTIC fraud and other serious crimes (poly-criminality).

List of detailed training needs

Member States indicated that 10 444 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat VAT (incl. MTIC) fraud:

1. EU instruments and tools for cross-border cooperation and investigations, and their practical application: Art. 31 of the EPPO Regulation, European Investigation

Order, Operational Task Forces, Joint Investigation Teams, AMLA, Europol, Eurojust, EPPO.

2. Cross-border financial detection and tracking tools in VAT fraud: trade monitoring, financial oversight, and detection and tracking of illicit assets in real estate, offshore investment schemes and luxury assets.
3. Cross-border challenges in obtaining financial intelligence and forensic evidence from non-EU countries in MTIC fraud investigations.
4. Enhancing inter-agency intelligence analysis and sharing in VAT fraud cases between tax authorities, Financial Intelligence Units, and law enforcement; legal, procedural, and technological aspects, including data protection, predictive analytics, and AI compliance.
5. Digital investigations in VAT fraud: tools available, analysis and visualisation of data, presentation of digital evidence in court, cryptocurrencies, cloud storage and VPN use.
6. Enhancing cooperation between national and EU bodies to prevent and combat cross-border VAT fraud.
7. Special investigation techniques for cross-border detection and investigation of transnational criminal groups in VAT fraud: legislation, surveillance and new technologies, covert operations, Open-source intelligence, cyber-patrolling activities.
8. Money laundering as per service in VAT fraud and asset recovery.
9. Identifying and responding to emerging VAT threats and fraud patterns, sharing of bets practices.
10. Transnational prosecutorial and law enforcement cooperation in VAT fraud cases.
11. Different legislations in MS and EU regulations.
12. Poly-criminality links in VAT fraud schemes.
13. VAT fraud intelligence-sharing across Member States and integration of VAT compliance data into fraud tracking systems.

2.10 Border management and maritime security

Border and maritime security, face increasingly complex threats from criminal and hybrid actors employing strategic, networked tactics. Irregular migration is used to destabilise operational systems, while maritime container trafficking of drugs has grown in scale and sophistication. Meanwhile, cyber and hybrid attacks on maritime infrastructure are becoming more targeted and disruptive. These developments reflect a transformation in the threat landscape, requiring not only technical upgrades but also

a rethinking of cross-border security governance and strategic coordination. In this context, the use of EU Entry/Exit System followed by the European Traveler Information System operationalisation will be central to a new interoperability architecture for border management and maritime security.

Environmental challenges

Law enforcement and border management agencies face a range of significant challenges at the EU's borders and in maritime areas.

A primary concern relates to border control systems, screening, and procedures. Many border crossing points lack sufficient contingency planning for system outages, including those affecting the EES and data storage. Operational difficulties (e.g. technical complexity, legislative challenges and lack of specific equipment such as self-service kiosks for pre-registration and automated border control gates) also need to be addressed to ensure effective deployment of the EES and ETIAS.

Interagency cooperation and coordination present substantial challenges. Law enforcement requires improved integration of interoperable systems to support coordination and situational awareness across agencies and borders. The current operationalisation of interoperable information systems, such as ETIAS, and the development and progressive deployment of interoperability components, such as the European Search Portal (ESP), are expected to improve identity verification, visa control and threat information.

There are persistent barriers to real-time information exchange between Member States and EU agencies. Strengthening real-time information-sharing tools and protocols could facilitate timely responses to border and security threats. Furthermore, improved coordination with non-EU partners, such as those in the Western Balkans, could allow more rapid operational responses to smuggling and trafficking and strengthen inter-agency coordination on cross-border maritime crimes, such as drug and human trafficking. Maritime Domain Awareness (MDA) needs to be strengthened across the EU sea basins.

Exploitation of border and maritime vulnerabilities by criminal and hybrid actors poses critical challenges. Legal frameworks need to be strengthened to address state-sponsored manipulation of migration flows, and surveillance systems must be adequately equipped to detect complex hybrid tactics and migration weaponisation. Improved enforcement of return decisions could reduce repeated irregular entry attempts by individuals previously intercepted.

Finally, victim protection and human rights monitoring face significant issues. Access to legal aid and victim protection measures is limited, especially in cross-border cases, and the overwhelming number of arriving refugees, challenges resources. Victim protection programmes are uneven across Member States, meaning that more effective and systematic mechanisms are required to investigate potential human rights violations at borders, including pushbacks, ill-treatment, or deaths. Law enforcement requires greater investigative capacity to gather and process evidence for redress in cases of border-related rights violations.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Law enforcement agencies face a range of significant challenges at the EU's borders and in maritime areas, impacting their effectiveness in combating serious and organised crime.

Greater consistency in border control systems, screening, and procedures across Member States is required to improve comparability of threat assessments with a focus on the specific needs related to different types of borders at the EU or SAC level. Use of new technologies deriving from the EES and ETIAS need to be enhanced. Standardised protocols are required to improve the detection of fraudulent documents and visa fraud at border points. Port security and inspection standards across the EU need to be harmonised to improve detection and response at maritime entry points. More extensive use of the Schengen Information System (SIS) significantly improves cross-border coordination.

There are significant challenges in interagency cooperation, coordination, information exchange, and situational awareness. Intelligence-sharing on hybrid threats and instrumentalised migration is ad hoc and under-resourced, limiting early detection and coordination. Coordination between customs, border police, and port authorities needs to be strengthened to increase the effectiveness of maritime security enforcement. More robust cross-border coordination frameworks are required to improve responses to hybrid threats and migration weaponisation. Joint operational frameworks to address cross-border crime and irregular migration need further development, along with greater integration with the Common Information Sharing Environment. Addressing the fragmentation of maritime surveillance systems will improve early detection capacity, increasing situational awareness in maritime operations.

To respond to the exploitation of border and maritime vulnerabilities by criminal and hybrid actors, law enforcement needs greater capabilities to detect cannabis, cocaine, heroin, and synthetic drugs in maritime port environments, and greater capacity to understand and respond to criminal networks' use of multi-container drug shipments and evolving smuggling methods. Greater specialist skills and tools are needed to detect and respond to hybrid threats targeting maritime infrastructure. Personnel at border points require greater training and resources to address hybrid threat scenarios, including specialist abilities to detect trafficking in human beings, particularly among vulnerable groups. Forensic and chemical analysis capabilities in ports need to be improved for better detection of concealed drugs. Greater capacity is required to detect and interdict weapon smuggling at borders and to effectively identify identity fraud and document forgery. Border agencies need to increase operational readiness to counter hybrid threats and instrumentalised migration. Procedural gaps in migration and customs systems, currently exploited by criminals, need to be addressed. Operational gaps among authorities need to be reduced to improve the detection of illicit goods.

Maritime security requires a greater capacity to detect, trace, and intercept all vessels entering EU territorial waters under all weather conditions. EU-wide capabilities to detect and respond to cyber and hybrid attacks on maritime infrastructure demand improved capacity and coordination. Law enforcement requires greater detection and response capacities for unauthorised unmanned systems near offshore or underwater assets. Gaps in surveillance and protection of critical maritime infrastructure (e.g., ports, pipelines, undersea cables) need to be addressed, and agencies require greater ability to respond to large-scale, hybrid, and cyber threats targeting maritime systems.

To ensure victim protection and human rights monitoring, border authorities require specialised procedures to identify and assist victims of trafficking or abuse in migration contexts. Greater capacity to systematically monitor refugee movements and identify victims is needed, as well as standardised victim screening procedures, in order to reduce the risks of re-trafficking and child exploitation. Responding to the victim's reluctance to testify due to safety concerns, trauma, and threats from traffickers remains a significant challenge.

Training needs

Summary

Law enforcement agencies require extensive training to enhance their capabilities at borders and in maritime environments, addressing the complex challenges posed by evolving threats and technological advancements.

Training is required to secure alignment of screening and border control procedures, the practical use of new technologies, and the improved use of EU information exchange systems, including the CISE framework. This necessitates training built on sharing best practices for port security in Member States with sea borders, airport security and inspection standards.

Training should promote international and regional cooperation and information exchange, including the application of the United Nations Convention on the Law of the Sea and understanding jurisdiction in sea zones. This is especially applicable for the Eastern Mediterranean region, including Greece, Malta, and Italy. Joint simulation exercises on inter-agency cooperation mechanisms in maritime and high-risk zones are vital, especially for regions with an external sea border and particularly sensitive operational areas.

Training is essential for detecting and responding to unauthorised unmanned systems near offshore or underwater assets in Member States with sea external borders. Sharing best practices and incident response protocols for contingency planning during maritime disasters is critical.

Member States indicated that 25 786 officials need training in this area.

Further details
Greater awareness of new legal frameworks and best practices for return procedures is needed, along with training in risk analysis and vulnerability assessment. Addressing hybrid threats requires targeted training to raise awareness, share best practices for threat detection, enhance cross-border coordination, and foster cooperation with neighbouring countries.

Specialised training is needed for regions with EU external sea borders concerning the detection and response to drug shipments at border checkpoints, covering various concealment methods and modi operandi.

Training for the detection of and response to environmental offences at border checkpoints is required for Member States with EU external land borders.

Victim protection is a key area, encompassing monitoring refugee movements, identifying victims, implementing victim screening procedures, protecting unaccompanied minors, and employing effective interviewing techniques.

Personnel must be trained on the roles and tasks of national coordination centres as per Regulation 1896/2019, art. 21.

Surveillance and protection of critical maritime infrastructure in Member States with EU external sea borders, as well as the use of advanced maritime technologies in Member States neighbouring Ukraine, Moldova, and Türkiye, are key training needs.

Finally, financial investigations, trade-based money laundering, and the adoption of a "follow-the-money" approach are crucial training areas, as identified in the EU Customs Alliance for Borders action plan.

List of detailed training needs

The following list evidences the prioritisation, by the Member States, of topics in the area of training for border management and maritime security:

1. Detecting and interdicting drug shipments at land and maritime borders: concealment techniques and modi operandi.
2. Border and maritime risk analysis methodologies and vulnerability assessments with the exchange of best practices.
3. Conducting financial investigations at borders and ports: trade-based money laundering and follow-the-money techniques.
4. Exchange of best practices on security procedures and inspection standards at EU ports and airports.
5. Awareness of the EU legal framework on returns and exchanging best practices for return procedures.
6. Application of the United Nations Convention on the Law of the Sea, maritime law enforcement jurisdictions across the EU and international sea zones.
7. Enhance the detection capacities as well as a harmonised approach in verifying high-risk individuals at external borders.
8. Harmonised border screening procedures, and practical application of new technologies, ensuring high quality of biometric data.
9. Use of EU information exchange tools, including the Common Information Sharing Environment (CISE) framework, and information system, including the Entry/Exit System (EES).
10. Integrated Border Management.
11. Detecting and mitigating threats from unauthorised unmanned systems near critical maritime infrastructure.
12. Victim identification and protection at borders: screening refugees, supporting unaccompanied minors, and interviewing procedures.
13. Operational training on advanced maritime technologies, including robotics, cybersecurity, and remote sensing.

14. Identifying and addressing environmental offences detected at border checkpoints, including illegal waste or wildlife trafficking.
15. Joint simulation exercises on inter-agency coordination in maritime and high-risk border environments.
16. Exchange of best practices and incident-based learning on maritime disaster contingency planning
17. Surveillance and protection of ports, pipelines, cables, and other critical maritime infrastructure
18. Roles and operational responsibilities of National Coordination Centres under Regulation 1896/2019, Article 21.

2.11 Environmental crime

Environmental crime significantly threatens Europe's ecosystems, economies, public health, and security. Waste crime is particularly severe, with trafficking growing in scale and complexity. Criminals, often fronting legitimate businesses, exploit regulatory gaps, causing, among others, lasting pollution. Organised crime and corruption further facilitate infiltration of the legal waste sector. While wildlife crime remains stable, the illegal trade in certain wildlife species remains highly profitable. Emerging risks include environmental damage from synthetic drug production and cannabis cultivation, involving hazardous waste, deforestation as part of significant deterioration of protected habitats, and energy misuse. Weak enforcement and inconsistent legal frameworks enable exploitation, underscoring the need for stronger regulation and cross-border cooperation to address these escalating environmental security threats.

Environmental challenges

Responding to environmental crime faces several interconnected challenges spanning legal frameworks, enforcement, cooperation, and resource allocation.

Significant legal obstacles need to be addressed to allow a more effective response. Inadequate legal frameworks for prosecuting major environmental offences reduce deterrence for high-level offenders. On an international level, legal incompatibilities with non-EU countries complicate cooperation and the pursuit of transnational crime networks. Within the EU, jurisdictional conflicts and legal ambiguities complicate cross-border investigations, and greater harmonisation of national laws is required to facilitate crucial enforcement tools such as European Investigation Orders and European Arrest Warrants.

It is important to address fragmentation and inconsistency of enforcement efforts within and across Member States. Fragmentation results in uneven penalties and sentencing, creating legal loopholes that criminals exploit. The complexity of environmental crime, with the increasing level of cross-border trade, is evolving into hidden illegal conduct.

In specific sectors, such as waste management, greater oversight is required to address illegal disposal practices. It is important to strengthen cross-border cooperation structures, which are hindered by legal discrepancies, language barriers, and misaligned enforcement priorities.

Improved intelligence-sharing mechanisms between Member States are needed for real-time tracking of environmental crime networks, which are crucial to address their ability to operate across borders undetected. Greater coordination between national criminal and administrative authorities is necessary to improve intelligence flows. Structured financial investigation frameworks are required to ensure consistent approaches to asset seizure, thereby increasing the capacity to target financial enablers of these crimes.

Improving the availability of resources is a foundational challenge. This could allow greater investigative and prosecutorial capacity within judicial and law enforcement agencies, reducing delays and improving case handling. Appropriate funding, deployment of financial, technical and technological resources, as well as qualified staff, by national authorities is required to address systemic inefficiencies and allow proactive enforcement. Successfully addressing these challenges equally necessitates dedicated environmental crime units in both law enforcement and judicial systems. As part of this effort, agencies require updated tools and expertise in order to track and regulate cyber-facilitated environmental offences.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

To effectively respond to environmental crime in Europe, proactive measures are required across cooperation, intelligence, enforcement, and investigations.

To build a unified EU-wide response, Member States must improve cross-border cooperation mechanisms. This includes increasing the use of Joint Investigation Teams and Europol's Operational Taskforces for environmental crime cases and promoting better exploitation of European enforcement networks, such as EnviCrimeNet, Eurojust, the European Network of Prosecutors for the Environment (ENPE), European

Union Forum of Judges for the Environment (EUFJE), and the European Union Network for the Implementation and Enforcement of Environmental Law (IMPEL). Harmonising the investigative approaches of administrative and criminal law enforcement and strengthening coordination between financial intelligence units and environmental agencies are needed to effectively track illicit financial trails.

Action is needed to enhance intelligence-sharing frameworks between environmental regulators and law enforcement agencies. This can be achieved by increasing the utilisation of digital platforms such as SIENA and I-24/7 for operational coordination and information exchange on environmental crime cases. Structured intelligence-sharing protocols are needed, especially between customs and environmental authorities, to improve the detection of environmental offences such as illegal shipments of waste, and illegal trade of wildlife species, as well as of hazardous materials or substances. Strengthening collaboration with civil society and civil society organisations could allow leveraging their grassroots intelligence and monitoring capabilities.

Improving administrative and regulatory mechanisms, including due diligence schemes and compliance monitoring, is required to enable more effective preventive action. Greater harmonisation of Member State national strategies is needed to ensure a consistent, EU-wide response that closes legal loopholes and regulatory gaps. To disrupt criminal enterprises, authorities must ensure consistent enforcement against related financial crimes, preventing the reinvestment of illicit profits from environmental offences. Regulatory oversight of environmental crime facilitated by technology needs to be improved, with a focus on online markets for illegal trafficking.

Modernising investigative capabilities by integrating advanced technological tools, such as geospatial intelligence, remote sensing, and predictive analytics, could allow proactive detection and investigation of crimes. Law enforcement and judicial authorities both require specialised expertise in digital forensics and environmental law. Parallel financial investigations are a mandatory part of environmental crime cases to track, seize, and recover illicit profits, thereby disrupting criminal networks at their financial core.

Training needs

Summary

To effectively combat environmental crime in Europe, a comprehensive training strategy is required to strengthen cooperation, investigative techniques, and crime-specific knowledge.

Increasing awareness and practical use of existing cooperation mechanisms is foundational. Law administrative and criminal law enforcement and judicial authorities require training to better exploit European enforcement networks, such as EnviCrimeNet, Europol, Eurojust, and IMPEL. This includes practical training on tools for law enforcement and judicial cooperation, such as Joint Investigation Teams (JITs), Europol's Operational Taskforces, and the information-sharing platforms SIENA and I-24/7.

Strengthening advanced investigative capacity is a priority. Training, at both regional and EU level, must focus on the use of modern technical and technological tools, including geospatial intelligence, remote sensing, satellite monitoring, predictive modelling, and data analytics. Where appropriate, those tools shall include special investigative tools, such as those used in combatting organised crime or in other serious crime cases.

Training is needed for financial investigations that require specialised knowledge to track illicit financial flows and assess financial damages linked to environmental offences. To bolster integrity and prevent collusion, anti-corruption training within tax and financial institutions is required.

Training must support in-depth expertise on the specific modus operandi of different environmental crime categories. Key areas are wildlife crime (covering CITES, illegal logging, illegal, unreported, unregulated fishing, and illegal mining), pollution crimes affecting water, soil, and air, and complex waste crimes. In this context, strengthening regional operations could be particularly relevant for addressing challenges linked to specific modi operandi and for countering waste trafficking.

Further details

Training should strengthen understanding of the distinction between administrative and criminal investigations and overall enforcement mechanisms to improve inter-agency workflows. Increasing knowledge relating to sharing good practices is needed for the implementation of the EU Directive on environmental crime (EU 2024/1203) and on cooperating effectively with non-governmental organisations).

Specialist skills in digital investigation techniques such as Open-Source Intelligence, AI-driven intelligence gathering, and cyber-patrolling are required to address the growing threat of online criminal activity in wildlife crime.

Appropriate training in digital forensics is required to properly handle electronic evidence in environmental crime investigations.

Training is needed to address the environmental impact of interconnected offences, such as the pollution from illicit synthetic drug labs, medical waste, or similar matters. This is particularly applicable to Germany, Spain, Belgium, Netherlands, Luxembourg, and Czech Republic.

List of detailed training needs

Member States indicated that 13 709 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat environmental crime:

1. Digital investigation techniques in environmental crime, criminal data collection (Open-source intelligence AI-driven intelligence gathering, cyber-patrolling) data analysis, cyber-enabled environmental crime.
2. Exchanging good practices in investigation and operational tactics for tackling environmental crime such as the use of technological tools (e.g., geospatial intelligence, remote sensing), predictive modelling, satellite monitoring, and data analytics
3. Financial investigation techniques in environmental crime cases, financial tracking, and assessment of financial damages.
4. Modus operandi - waste-related environmental crime, including illegal shipments, disposal, and trafficking practices.
5. Modus operandi - pollution-related environmental crimes, including water, soil, and air contamination, and trafficked greenhouse gases.
6. Awareness and practical use of EU-level law enforcement cooperation mechanisms in environmental crime cases (Joint Investigation Teams, SIENA, I-24/7, Europol, Eurojust).
7. Modus operandi - wildlife crime (CITES, protected animals, plants, illegal logging and timber trade, forest fires, illegal mining, etc.).
8. Awareness of better use/exploitation of European enforcement networks, cooperation mechanisms (e.g., EnviCrimeNet, Europol, Eurojust, Implementation and Enforcement of Environmental Law, European Network of Prosecutors for the Environment, EU Forum of Judges for the Environment, Europe Trade in Wildlife Information eXchange).
9. Anti-corruption training within tax and financial institutions.
10. Digital forensics in environmental crime investigations and prosecutions.
11. Use of structured intelligence-sharing frameworks to enhance cooperation between environmental regulators and law enforcement agencies.

12. Coordination and interface between administrative and criminal investigations in environmental crime enforcement.
13. Environmental harms linked to illicit synthetic drug production and cannabis cultivation.
14. Awareness raising on the work of NGOs, sharing of good practices, and cooperation with NGOs.
15. The EU Directive on environmental crime: sharing national experiences and best practices across Member States.
16. Best practices in multi-agency coordination for environmental disaster response and management.

2.12 Firearms and explosive crimes

Firearms and explosives crimes pose a critical and evolving threat to EU internal security. Key issues include shifting illicit market dynamics, with the Western Balkans as a crucial source and Ukraine emerging as a significant concern. Technological advances such as AI and 3D printing are accelerating illicit firearms production and online sales, diversifying the types of weapons to include privately manufactured and counterfeit firearms. Additionally, heavy pyrotechnics have gained popularity among criminal groups for use in explosive devices, ATM attacks, and even extremist plots. Such developments confront law enforcement agencies with complex challenges stemming from gaps in controls, operational capabilities, information sharing, and legislative harmonisation.

Environmental challenges

A key challenge is ensuring effective cooperation at the EU level, alongside harmonising legislation and developing common analytical, law enforcement and administrative capabilities to address the growing threat posed by the conversion of alarm and signal weapons into fully functional firearms. More effective forensic and investigative tools are needed to trace firearms assembled from legally purchased, freely available, or fraudulently sourced components. Law enforcement requires improved capacity to detect and interdict heavy pyrotechnics frequently used in violent attacks and improvised explosive devices. Regulatory and detection gaps need to be addressed to improve the ability to target the smuggling of firearm components into the EU, often through the misuse of customs procedures.

Operational tools, monitoring mechanisms, and cross-border investigation challenges include the need for improved tools to trace and control the trafficking of firearm kits

and semi-finished or unmarked components. Monitoring and control mechanisms to detect the diversion of firearms from conflict zones, such as Ukraine and the Western Balkans, as well as from legacy stockpiles, need to be improved. Cross-border investigations could be strengthened by greater harmonisation of legal definitions and criminalisation standards for firearms and explosives trafficking across EU Member States. Addressing the current fragmentation of definitions and standards, increasing the harmonisation of firearms and explosives legislation, and developing a unified EU framework for joint operational deployment could lead to significant improvements in effective law enforcement cooperation.

Access to real-time information, coordination frameworks, and harmonised databases could enable law enforcement to use an EU-wide, real-time system for reporting firearms- and explosives-related incidents and for sharing critical ballistic and traceability data. Structured frameworks for rapid operational coordination between customs, law enforcement, and judicial authorities in cross-border firearms trafficking cases require further development. It is important to develop comprehensive or harmonised systems to manage secure stockpiles and allow more effective firearms and explosives governance across the EU and its neighbouring regions. Additionally, a centralised or harmonised EU database of firearms seizures is needed to enhance situational awareness and strategic analysis at the European level.

The harmonisation of legal definitions of firearms trafficking across Member States is required to facilitate joint investigations and coordinated enforcement. Consistent transposition and implementation of EU firearms legislation by Member States are needed to strengthen the overall effectiveness of the EU's unified response. Furthermore, Member States need dedicated legal provisions and investigative powers to regulate and prosecute the trafficking of 3D-printed and AI-modified firearms and components. Consistent application of national definitions for categories, such as antique, salute, and alarm/signal weapons, is needed to reduce legal ambiguity. It is also necessary to strengthen enforcement of proper categorisation, restrict online sales and track high-risk pyrotechnics throughout their distribution chain.[6]

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

Law enforcement agencies face significant challenges in combating firearms and explosives crimes in terms of knowledge, skills, and operational capacity.

[6] https://data.consilium.europa.eu/doc/document/ST-9907-2025-INIT/en/pdf

In terms of knowledge, greater understanding, and operational use of international intelligence tools from Europol and INTERPOL (iARMS) are necessary to improve effectiveness of cross-border exchange. Agencies require more effective early warning systems to track evolving black-market dynamics, emerging trafficking methods, and new routes linked to geopolitical instability. Greater knowledge is needed to address new concealment methods used by traffickers.

Greater skill capability is required in core areas of firearms and explosives crime investigations and forensic analysis. Frontline officials need to be improved to detect converted or modified firearms during inspections. Greater technical and investigative capabilities are needed to detect and disrupt the illicit manufacturing of firearms, including converted blank-firing weapons, and to identify and counter the trafficking of 3D-printed, privately manufactured, or counterfeit components. Forensic capabilities to trace illicitly assembled weapons need to be developed. Greater technical and analytical skills are needed for more effective monitoring of online platforms, the dark web, and postal/parcel services involved in firearms and pyrotechnics trafficking.

In terms of responsibility and autonomy, more consistent intelligence and more effective use of secure data exchange platforms are required. Integrated access to ballistics and tracing data is needed, as is modern forensic infrastructure and tools for timely analysis. There is a need for EU-wide mechanisms to assess and respond to the criminal exploitation of emerging technologies, such as AI and 3D printing. Detection capacities could be increased by improved scanning and detection tools at borders and greater resources to interdict trafficking through under-monitored entry points. More consistent coordination with non-EU countries and parcel/postal operators is required. Overall, the development of harmonised databases and a unified EU framework for firearms intelligence and operational deployment could significantly increase law enforcement's collective capacity to respond to the challenge posed by trade in illicit firearms and explosives.

Training needs

To effectively counter the evolving threat of firearms and explosives trafficking, law enforcement agencies require comprehensive training that enhances knowledge, skills, and operational capabilities across several critical areas.

Efforts should focus on deepening knowledge of analysis and intelligence sharing, including legal and procedural aspects, data protection, and the use of new technologies, such as AI and predictive analytics, for tracing firearms, explosives, and ammunition. This includes understanding the functions and importance of National

Firearms Focal Points and acquiring and exchanging ballistic information using X3P standards, including via the Europol Firearms Hub. In this context, strengthening intelligence sharing is especially relevant in the Western Balkans, MENA countries, and Latin America while training needs related to ballistic information acquisition and exchange primarily apply to the Western Balkan and Ukraine. Additionally, training focused on good practices of National Firearms Focal Points in Western Balkans, MENA and EaP countries, Central Asia and Latin America could improve cooperation. Skills development should target investigations into illicit trafficking, encompassing both online and onsite methods, proactive and forensic techniques, financial investigations, and international cooperation. Specific competencies are required for cyber detection and investigation of illegal firearms and explosives trafficking.

Capacity building should enhance border and mainland detection capabilities through effective use of resources such as K9 units, specialised applications, technical equipment, X-rays, and mobile scanners. This also involves developing the ability to leverage new technologies and innovative tools, including AI and machine learning, for detecting and analysing illicit weapons.

Further details

A deep understanding of current, last, and emerging threats in illicit trafficking is crucial, particularly new trends, modi operandi, and best practices related to privately made firearms (PMF), such as counterfeit, 3D-printed, deactivated, converted, and assembled weapons, as well as pyrotechnics.

Training is required to address changes to modus operandi, emerging crime patterns, smuggling routes, and how illegal firearms trafficking serves other criminal activities, terrorism, and hybrid threats.

Knowledge of prevention strategies, administrative approaches to counter organised crime groups, and legal and policy frameworks such as the IMI module, European Firearms Pass, and electronic licensing systems is essential.

Law enforcement needs to master specialised investigative techniques for cross-border detection and investigation of transnational criminal groups, including applying relevant legislation, conducting surveillance, leveraging new technologies, and using EU instruments.

Training is needed to increase the capability for cooperation with non-EU countries, encompassing information exchange, operational response, and joint detection and investigation tools, to effectively address the transnational nature of firearms and explosives trafficking.

Enhancing skills in coordination with the private sector (e.g., X-ray services, online platforms, postal/courier services, manufacturers) is vital.

List of detailed training needs

Member States indicated that 8 478 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat firearms and explosives crimes:

1. Administrative approach to countering OCGs in the illicit trafficking of firearms and explosives, and the misuse of legal business structures.
2. New and emerging threats, modi operandi, and typologies in firearms and explosives trafficking, including Privately Made Firearms, such as 3D-printed, converted, and counterfeit weapons, and pyrotechnics.
3. Changes in modus operandi (false documents, stolen guns, etc), emerging crime patterns and smuggling routes and trends in illicit firearms and explosives trafficking.
4. Analysis and sharing of information/intelligence between national law enforcement authorities: legal and procedural aspects, compliance with data protection regulations, and the use of new technologies and innovative tools such as AI, predictive analytics, and machine learning. (Including firearms, explosives and ammunition tracing).
5. Special investigative techniques applicable at a cross-border level, the relevant legislation, surveillance tools, and EU-level instruments for dismantling transnational firearms trafficking networks.
6. Cyber-enabled detection and investigation techniques for illicit firearms, ammunition, and explosives trafficking, including activity on online platforms and the dark web.
7. Investigations into illicit trafficking in firearms and explosives (online, onsite, reactive, proactive, forensic and financial investigations, international cooperation), current, last and emerging threats.
8. Illegal firearms and explosives trafficking as per service for other criminal activities, terrorism, and hybrid threats.
9. Acquisition, identification, and exchange of ballistic information using X3P standards and relevant EU systems such as Europol Firearms Hub.
10. Application of firearms and gunshot residue forensic tools and technologies.

11. Prevention of illicit firearms and explosives trafficking (European response, mechanisms, EMPACT objectives, different models and approaches, cooperation with the private sector, etc.).
12. Cooperation frameworks, tools, and joint operations with non-EU origin, transit, and destination countries to combat illicit firearms and explosives trafficking.
13. Public–private cooperation for firearms and explosives detection and control, including coordination with postal, courier, scanning service providers, and manufacturers.
14. EU legal and policy frameworks governing firearms control and enforcement, including Internal Market Information System modules, the European Firearms Pass, and electronic licensing systems.
15. Tools and techniques for enhancing law enforcement capabilities in the detection of the illicit trade of firearms and explosives at borders and inland. This includes exploring the possibilities offered by AI, as well as the use of K9 units, scanners and mobile detection technologies.
16. Establishment, legal framework, and good practices related to National Firearms Focal Points.

2.13 Hybrid threats

Hybrid threats are rapidly expanding, leveraging geopolitical instability, and evolving criminal dynamics to undermine EU and Member State institutions, economies, and societies. State-aligned actors increasingly use criminal networks as proxies to conduct cyberattacks on critical infrastructure and exploit irregular migration flows. These operations often manifest as persistent, low-level disruptions – termed the "woodpecker modus operandi" – seeking cumulative destabilisation. This complex threat landscape increasingly blurs the lines between organised crime and state-sponsored actions, complicating detection, attribution, and coordinated countermeasures. Manifestations of these threats include sabotage of critical infrastructure through digital or physical means, instrumentalisation of irregular migration, evasion of sanctions, and facilitation of illicit drug importation. They are also present in the digital domain through cyberattacks, ransomware attacks against essential services, information theft, disinformation campaigns, and foreign information manipulation and interference (FIMI).

Environmental challenges

Hybrid threats, the criminal-state nexus, and disinformation present a multifaceted challenge, characterised by significant gaps in strategy, operational capacity, and legal frameworks. This calls for stronger strategic coherence between internal and external security policies to enable coordinated action, including establishing clear legal and operational guidance on the actions law enforcement can permissibly take in hybrid threat conditions.

In this context, border protection is increasingly part of responding to hybrid threats. Addressing these threats requires improving the quality and integrity of biometric data, as well as ensuring seamless information exchange and the interoperability of EU systems to counter the instrumentalisation of irregular migration flows by hybrid actors. A significant part of assessing hybrid threats at the border involves analysing data from various information systems. Improving interoperability between these systems is a major challenge.

To enhance the security of critical infrastructure, several challenges must be addressed. First, there is a need for stronger cross-border cooperation among law enforcement, security and cybersecurity services, military and civil protection, and private operators. The fragmentation of EU approaches among Member States regarding ICT supply chain security, which partially results from the lack of implementation of the framework provided with the 5G Cybersecurity Toolbox, must also be reduced to minimise dependencies on high-risk suppliers. Additionally, a better securitisation of transport hubs and ports could prevent infrastructure sabotage.

In parallel with these efforts, reinforcing cybersecurity and combating online threats is crucial, hybrid threats confront law enforcement with the challenge of keeping pace with the technological innovation used by adversaries. Criminals are leveraging AI for more sophisticated attacks, while states may provide them with cutting-edge tools. Moreover, dependencies on third country in terms of strategic technologies, such as AI, quantum, advanced connectivity, cloud, edge, and Internet-of-Things, also represents a major challenge in terms of security.

Overall, addressing this challenge requires greater engagement with key resources, in particular the EU Migration Preparedness and Crisis Blueprint, as well as the Hybrid Toolbox which offers robust tools to Member States and partners in preparing for and countering hybrid threats. EMPACT plays a pivotal role in addressing the threat posed by organised crime as a hybrid actor with a focus on strengthening external partnerships, border securing and cross-border crime, information sharing, resilience

against hybrid threats, and fostering public-private and civil society engagement. It is also important to note that specific tactics associated with hybrid threats frequently overlaps with other categories of crime developed in these reports. Thus, advancements in security challenges related to cyber-attacks, borders management and maritime security, migrant smuggling and external dimension of internal security could also improve the effectiveness of responses to hybrid threats.

Challenges concerning knowledge, skills, responsibility and autonomy

Challenges

This evolving threat, nurtured online and accelerated by AI, demands a proactive shift from addressing conventional crime to confronting state-aligned strategic challenges.

Law enforcement must build its capacity to detect, investigate, and counter hybrid attacks. This requires developing the expertise to identify and investigate the involvement of state-affiliated actors and the criminal networks they use as proxies. A crucial skill to strengthen is the ability to distinguish between traditional organised smuggling networks and state-driven instrumentalisation of migration, as this distinction is important for the response. Greater dedicated capabilities are required to respond to state-aligned, politically motivated cyber-attacks and to counter Foreign Information Manipulation and Interference and disinformation campaigns linked to hybrid operations.

Enhancing intelligence and threat assessment capabilities is critical. This requires developing the capacity for systematic threat assessments that integrate both internal and external security indicators. It is essential to build robust, structured information-sharing mechanisms and early-warning frameworks that can track geopolitical instability and emerging hybrid threats in a timely manner. The capability to protect critical infrastructure requires enhanced preparedness against sabotage or hybrid attacks on cross-border assets such as pipelines and undersea cables.

Responding to hybrid threats requires overcoming adversaries' technological challenges. This includes strengthening the capability to detect and respond to emerging threats such as AI-enabled cyberattacks, 3D-printed weapons, and hostile drones. Digital investigation skills need to be strengthened, including the capacity to recognise and counter social disruption. Furthermore, specialist skills in financial investigations are needed to detect and disrupt informal value transfer systems that fund hybrid activities.

Training needs

Summary

To effectively respond to hybrid threats, law enforcement in Europe must develop a range of advanced capabilities across multiple domains.

Training is required to strengthen the analytical capacity to assess hybrid threats, including the ability to distinguish between profit-driven crime, politically motivated interference, and state-sponsored activities. This entails using all available data, including border and intelligence information, to evaluate whether incidents or applicants may be linked to broader strategic campaigns aimed at eroding stability or undermining societal cohesion. It also involves understanding the strategic intent behind disinformation and influence activities, going beyond fact-checking to identify when propaganda or manipulation serve as instruments of a hybrid threat.

Preparedness for sabotage or hybrid attacks on cross-border infrastructure, such as pipelines and undersea cables must also be reinforced through trainings. These attacks, which can include ransomware or physical sabotage, are a key tactic used by hybrid actors to erode stability and trust. In this context, training to strengthen the understanding of hybrid threats in the Baltic countries and Eastern Europe could be relevant to ensure that protective frameworks are more sufficiently integrated across domains.

Another priority area is strengthening the capability to identify and counter foreign information manipulation and interference, including through training to support specialist digital analysis capability.

The key capability for disruption hybrid actors is enhanced multi-agency and cross-border operational coordination. This could be strengthened by training to increase the use of secure information-sharing tools like SIENA and developing joint investigative capacity.

Training is needed to increase the capacity to integrate cyber-investigation with geopolitical threat analysis, including the significance of Crime-as-a-Service (CaaS) models within hybrid threats and the use of AI to automate and scale up attacks.

Further details

Training for infrastructure security must address both physical sabotage and the cybersecurity vulnerabilities in critical infrastructure exploited in digitally facilitated attacks.

Training in detecting AI-generated content and understanding AI-powered social engineering techniques is required to counter the sophisticated use of AI by threat actors.

Information manipulation campaigns are a cross-border threat, often orchestrated from outside the EU and executed through transnational criminal networks. This necessitates training focused on cooperation.

Law enforcement needs to be trained to identify the methods used in propaganda and disinformation campaigns, including fake social media accounts, coordinated troll operations, and manipulated news content.

A critical element is disrupting hybrid actors is to disrupt financial enablers by tackling sanctions evasion in all EU Member States, with special emphasis on the Baltic States. Such evasion is to be considered an inherently hybrid threat.

List of detailed training needs

Member States indicated that 5 032 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat hybrid threats:

1. Awareness and response training on hybrid threats at EU borders, including detection, coordination with neighbours, and sharing operational best practices.
2. Critical infrastructure protection against hybrid, cyber, and sabotage threats, including law enforcement coordination mechanism.
3. Awareness on detection and disruption of foreign information manipulation and disinformation campaigns tied to hybrid threat strategies.
4. Awareness of identifying and investigating criminal networks acting on behalf of or in coordination with state-aligned actors in hybrid operations.
5. Detection and countering of disinformation and hybrid threats that contribute to security destabilisation.
6. Detection, investigation, and disruption of hybrid threats, including state-aligned and proxy activities.
7. Sharing good practices on detecting and investigating corruption linked to hybrid threats, and sanction evasions.
8. Law enforcement methodologies for responding to politically motivated cyber-attacks on EU infrastructure by state-aligned actors.

2.14 Intellectual property crime, counterfeiting of goods and currencies

Intellectual property (IP) crime is evolving into a sophisticated online enterprise, increasingly leveraging AI and 3D printing to produce advanced counterfeits and deepfakes. These technologies facilitate the proliferation of high-risk counterfeit goods – such as pharmaceuticals, pesticides, and automotive parts – posing serious health and safety threats. Currency counterfeiting persists through altered-design banknotes. Enforcement requires updated legal frameworks and effective use of financial investigations targeting crime-as-a-service networks. The digital shift in marketing and distribution, coupled with technological misuse, underscores the urgent need for adaptive regulatory and investigative strategies to combat the growing complexity of intellectual property violations.

Environmental challenges

Intellectual property crime, including counterfeiting of goods and currencies, remains a highly profitable and evolving criminal enterprise. Online platforms, particularly social commerce, have become prime channels for selling counterfeit goods, fraudulent pharmaceuticals, and pirated digital content, driven by strong consumer demand for low-priced items.

Criminals are increasingly exploiting technologies such as 3D printing and artificial intelligence to improve counterfeiting, automate production, and produce convincing false documentation. Digital piracy is increasingly intertwined with cybercrime, with criminals stealing login credentials for legitimate streaming services to repurpose and sell content.

Sophisticated criminal networks now mirror legitimate business operations, infiltrating supply chains through crime-as-a-service models. This illicit trade poses serious risks to consumer health and safety – particularly from counterfeit pharmaceuticals, pesticides, and automotive parts – while generating significant losses in business revenue and tax income. A primary challenge is creating more integrated and agile legal and institutional frameworks. The current tendency toward siloed legal and institutional responses impedes comprehensive enforcement, a major challenge when IP crime overlaps with other offences such as document fraud or labour exploitation. Furthermore, legal systems require greater capacity to adapt quickly, as existing frameworks lag behind the rapid evolution of AI-based IP crime techniques and tools used by criminals.

Another fundamental challenge is the difficulty in launching investigations where specific counterfeiting acts are not clearly recognised as criminal offences under national law. Developing a clear and consistent legal basis for criminalising these acts is required to provide a solid foundation for law enforcement action.

Enhancing prosecution requires greater harmonisation of legal standards and definitions across different jurisdictions. Current legal systems vary in their standards for proving wilfulness in copyright cases, a factor that complicates prosecutions. Similarly, divergent legal definitions of crucial concepts such as "commercial scale" hinder consistent criminalisation across Member States. Establishing uniformity in these areas is a critical challenge for achieving more predictable and successful prosecutions.

Finally, more consistent judicial and sentencing outcomes are required. Sentencing inconsistencies and disproportionately low penalties undermine law enforcement's prioritisation of IP crime and discourage the use of advanced investigative methods. At the same time, fragmented court practices impede the development of a consistent body of legal precedent, which is especially needed for online IP crime.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

To effectively address intellectual property crime, including the counterfeiting of goods and currencies, requires strengthening core capabilities across operational, technological, and strategic domains.

A fundamental challenge is improving general readiness and operational competence. Addressing emerging forms of IP crime calls for building cybercrime and technological expertise among investigators, prosecutors, and judges. Law enforcement must strengthen institutional capacity to collaborate with right holders, apply technical investigative methods, and anticipate criminal tactics exploiting seasonal trends and influencer marketing.

Enhanced capabilities are also needed to engage effectively with the private sector and leverage technical intelligence and reporting channels. Equally important is linking IP crime to broader offences, such as money laundering and labour exploitation, which necessitates expanded use of financial investigations and asset recovery measures.

Countering technological sophistication and adaptation requires a greater capacity to investigate the misuse of AI and 3D printing in advanced counterfeiting and piracy. This

demands advanced investigative tools and methods to identify AI-generated impersonations, algorithmic manipulation, and digital piracy systems that use stolen credentials. A proactive capability to anticipate and respond to threats from generative AI tools such as deepfakes and FraudGPT is essential.

Confronting the trade in illicit goods, counterfeit supply chains, and product safety risks requires a greater capacity to detect and disrupt the supply of high-risk counterfeit goods, such as car parts and pharmaceuticals. This involves enhancing investigative capabilities to uncover intra-EU counterfeit production hubs that mimic legitimate businesses or use crime-as-a-service models to bypass import controls. It is vital to build stronger cooperative frameworks among law enforcement, customs, and logistics firms, and to increase regulators' ability to trace diverted medicines and identify illicit goods distributed via social commerce platforms.

Finally, overcoming structural and intelligence barriers requires developing the criminal intelligence analysis capability to map IP crime networks and their connections to other criminal domains. Integrating IP crime into strategic threat assessments is a critical capability to ensure the issue receives appropriate prioritisation and resources.

Training needs

Summary

To effectively respond to the challenges of intellectual property crime, including the counterfeiting of goods and currencies, a comprehensive training is required to build a range of specialised capabilities among law enforcement and judicial authorities.

A primary focus is the development of advanced digital and technological competencies to address crimes in the online space. Training should equip participants with practical skills to identify and analyse AI-generated, falsified promotional content used for marketing and deception across websites and social media. Improving expertise in Open-Source Intelligence and digital investigation techniques for e-commerce platforms is required. This should nevertheless be applied differently across convenience regions such as Southeast Europe, Scandinavia and the Baltics, and Central Europe.

Secondly, there is a critical need to enhance investigative and supply chain disruption capabilities. This involves training focused on identifying and disrupting illicit supply chains, with approaches tailored to convenience-based regional grouping. Particular attention should be given to detection techniques for small parcel shipments and railway freight. Training should cover the use of risk assessment tools, non-intrusive

scanning technologies, and integrated investigative platforms like IP Enforcement Portal (IPEP).

Finally, training should foster the cross-disciplinary and collaborative capabilities required to address the polycriminal nature of IP offences. This involves strengthening the capacity to connect IP crime investigations with related offences, such as environmental crime, document fraud, labour exploitation, tax evasion, and money laundering. Training to strengthen partnerships between law enforcement agencies and the private sector, especially logistics and shipping companies, is crucial. A key focus of training should be to enhance the capacity for effective sharing of criminal intelligence across sectors and jurisdictions through multidisciplinary cooperation.

Further details

Training is required to better address legal considerations with social media providers, as well as methods for the collection, securing, and sharing of digital evidence to ensure its admissibility in court.

Specific training is needed to prevent and detect illegal Internet Protocol TV services, including how to conduct investigations into the use of stolen credentials.

Training is needed to improve the capacity to identify high-risk counterfeit goods, to distinguish legitimate from illegitimate pharmaceuticals, and to understand agri-food products with geographical indications. This requires greater training, both at the regional and EU level, addressing the modus operandi of organised crime groups, key hotspots for counterfeit activity, and the importance of packaging and labels in investigations.

Training to improve the capacity to understand the way organised crime groups use legal business structures to conceal illicit activities is also required.

List of detailed training needs

Member States indicated that 10 395 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training to combat intellectual property crime:

1. Across-agency coordination: enhancing partnerships between the different law enforcement services and the private sector, especially logistics and shipping companies, when tackling IP crimes.
2. Open-source intelligence and digital investigations: E-commerce; social media platforms; digital evidence; legal considerations with social media providers.

3. Illicit disruption of supply chains: identifying, detecting, and addressing illicit disruptions of supply chains, with particular attention to distribution (e.g., detection and disruption techniques for small parcel shipments and railway freight). Trends, risk assessment tools and methods, non-intrusive scanning, and use of IP Enforcement Portal.
4. Illegal importation methods: detection methods for goods imported from outside the EU and within the EU.
5. Emerging use of artificial intelligence for online marketing and deception: practical skills in identifying and analysing falsified promotional content across websites, social media, and messaging platforms.
6. Document fraud analysis: understanding overlaps with IP crime, labour exploitation, and document forgery.
7. Pharmaceuticals: distinguishing legitimate vs illegitimate pharmaceuticals, hotspots, and knowledge-sharing on available surveillance tools.
8. Integrated investigative tools for IP crime: IP Enforcement Portal; multi-disciplinary collaboration.
9. Poly-criminality and business misuse: connections to organised crime groups, use of legal business structures, best practice exchange.
10. Geographical indications (agri-food products): identification, protection strategies, modus operandi of organised crime groups.
11. IP crime tactics in digital spaces: seasonal trends and targeted advertising.
12. Secure collection, handling, and cross-border sharing of admissible evidence in IP crime prosecution.
13. Illegal Internet Protocol Television: prevention and detection, stolen-credentials investigations, collaboration between crime areas groups/units/specialists.
14. Linking IP crime, environmental crime, and related financial investigations (tax evasion, money laundering, etc.).
15. Sharing of criminal intelligence: emphasising multidisciplinary cooperation across sectors and jurisdictions.
16. The importance of packaging and labels in IP investigations, protection of designs at the EU/regional level, and collaboration with rights-holders.

2.15 External dimensions of European security

The external dimension of European security is characterised by the growing threat of hybrid actors exploiting geopolitical instability, often using criminal networks as proxies to destabilise the EU and its Member States. This threat is manifest in politically motivated cyber-attacks on critical infrastructure and the instrumentalisation of

irregular migration flows. A critical development is the potential for arms diversion from conflict zones, with Ukraine as a potentially significant source. Sanctions evasion fuels external threats by strengthening sanctioned economies. Enforcement requires coherent legal and operational responses to smuggling and trafficking via unstable neighbouring regions, disruption of external logistical and digital facilitation networks, and a more unified EU framework to counter these threats.

Environmental challenges

To effectively address the external dimensions of European security, the EU must strengthen its strategic, operational, and cooperative capabilities. This is consistent with the Security Union Strategy (2020), the Strategic Compass (2022), and the recent ProtectEU Strategy (2025), which all stress moving beyond reactive measures towards anticipation, resilience, and integrated security. Developing such a security architecture requires not only stronger internal coordination but also the ability to link EU internal policies with its external action and partnerships.

A primary area for development is achieving greater strategic and institutional coherence. To enhance coherence in the EU's law enforcement framework, stronger strategic alignment is required between internal and external security policies, including the Common Security and Defence Policy (CSDP), the external dimension of Justice and Home Affairs, and other foreign policy instruments. Developing a structured, joint mechanism to address hybrid threats posed by external actors is essential for a coordinated response. This includes clarifying law enforcement's operational role during external crises and establishing harmonised frameworks for judicial and law enforcement cooperation with key regions.

Operationally, it is crucial to build the capacity to detect, investigate, and counter hybrid and cyber threats, including state-aligned cyber threats, FIMI campaigns, criminal networks acting as proxies for state actors, and sabotage of critical infrastructure. This must be supported by developing systematic threat assessments that integrate internal and external security indicators and by establishing robust intelligence-sharing structures and early-warning frameworks.

Geopolitical instability and conflict zones near the EU present a major external challenge. Criminal threats from conflicts, such as the potential for arms diversion from Ukraine or the Middle East and North Africa (MENA) region, as well as firearms trafficking from the Western Balkans, directly challenge the EU's internal security. Effectively countering these threats requires a more coherent legal framework to allow

more effective operational responses to smuggling and trafficking of weapons originating in unstable neighbouring regions.

A fundamental challenge is to build harmonised frameworks for law enforcement and judicial cooperation with key regions, such as the MENA and Eastern Partnership countries. This also involves strengthening operational cooperation mechanisms with third countries and strategic partners like North Atlantic Treaty Organisation (NATO) and the UN to combat transnational organised crime, firearms trafficking, and terrorism. Developing structured cooperation frameworks with Ukraine and Moldova is needed for joint responses to shared threats. The EU must increase its capacity to address vulnerabilities stemming from external dependencies on critical goods and develop stronger operational partnerships with regions like Latin America to tackle organised crime and cyber threats.

Challenges concerning knowledge, skills, responsibility and autonomy and related training needs

Challenges

To effectively address the external dimensions of European security, law enforcement confronts challenges across intelligence, operations, cooperation, and information exchange mechanisms.

A primary challenge for law enforcement is to strengthen intelligence, threat assessment and situational analysis capacity. A key area to strengthen is the capacity for systematic threat assessments integrating internal and external security indicators. This requires more robust intelligence-sharing structures to enable more timely and effective responses to cross-border or state-linked threats and to improve law enforcement access to the relevant intelligence frameworks. Greater use needs to be made of key tools and frameworks to support this intelligence sharing effort. These include Europol, and the EU Intelligence and Situation Centre (INTCEN).

There is a critical need to build a unified EU law-enforcement framework for responding to hybrid threats, especially at external borders. Joint training centres of excellence, mobility programme, and CEPOL-led training could effectively contribute to this aim.

Increasing capacity to respond to hybrid threats and state-orchestrated destabilisation at the EU's external borders is a key challenge and is essential for improving the effectiveness of Europe's responses to external security threats[7].

[7] Further information on this specific category of threat is provided in the section on hybrid threats.

Enhancing understanding of law enforcement's operational role in crisis management contexts while on external deployment and in CSDP teams is crucial, including readiness and interoperability of CSDP forces together with their alignment with NATO standards.

Law enforcement must address the challenge of building the operational and intelligence capacity to counter organised crime groups that exploit external vulnerabilities. A critical capability to develop is the ability to disrupt transnational criminal infrastructure and facilitation networks that operating outside the EU.

Law enforcement faces the challenge of strengthening strategic coherence between internal and external security policies, to increase capacity for coordinated responses. Addressing this requires strengthening the capacity to participate in structured, joint mechanisms that respond to hybrid threats from external actors, moving beyond fragmented, reactive approaches. Clarifying law enforcement's operational role during crises abroad is a key part of this effort.

Training needs

Summary

To effectively respond to the external dimensions of European security, law enforcement must develop and strengthen capacity to counter hybrid threats, protect critical systems, and enhance the effectiveness of EU external actions.

Strengthening the capacity to detect and investigate hybrid threats requires training and awareness-raising on the tools and methods to identify, investigate, and disrupt criminal networks that act as proxies for state-aligned actors, with special attention to African countries. It is critical to develop the capacity to counter Foreign Information Manipulation and Interference (FIMI) and disinformation campaigns linked to hybrid operations.

Protecting critical systems requires building the capacity for robust threat assessment and infrastructure protection. Law enforcement must improve its knowledge and application of threat assessment methodologies and tools, especially for overseas border such as those along the Caribbean Sea, while also enhancing interoperability tools and frameworks with regard to African countries to ensure a coordinated response. This is directly linked to strengthening the practical capability to protect critical infrastructure and systems from attack.

It is essential to strengthen capabilities related to the EU's external missions and policies. This includes training on Common Security and Defence Policy planning and

capability development to better address new operational realities and threats. Awareness-raising about law enforcement's role in external deployments and EU crisis management is crucial to improving response effectiveness.

Further details
Training must establish a clear methodology for law enforcement to respond to state-aligned, politically motivated cyberattacks targeting EU infrastructure and institutions.

Training and exercises are required to improve the readiness and interoperability of CSDP forces, including alignment with NATO standards.

Training should build the capacity for mentoring and advising partner countries on structural reforms and for upholding human rights and gender mainstreaming in CSDP missions.

Specialised training is needed to build awareness of the existing EU framework for tackling the evasion of EU sanctions.

List of detailed training needs

Member States indicated that 2 606 officials need training in this area.

The following list evidences the prioritisation, by the Member States, of topics in the area of training on the external dimensions of European security:

1. An SDP planning and capability development to better address operational realities and new threats. (Strategic and operational preparedness)
2. Awareness on EU crisis management expectations, role of law enforcement services, related to external deployments. (Strategic and operational preparedness)
3. Design, preparation, and deployment of law enforcement-led specialised teams for civilian CSDP missions. (Strategic and operational preparedness)
4. Integrated threat assessment methodologies and early warning tools for external threats. (Intelligence and threat assessment)
5. Awareness and operational training on integrating climate security and environmental risk adaptation into law enforcement external actions. (Emerging and cross-cutting security areas)
6. Operational use and application of interoperability frameworks and information exchange systems across EU and partner country contexts. (Intelligence and threat assessment)

7. Improve law enforcement readiness and interoperability in Common Security and Defence Policy missions, aligned with NATO and EU frameworks. (Emerging and cross-cutting security areas)
8. Mentoring and advising techniques for law enforcement engagement in partner country reform processes under EU external action. (Partnership and ethical capacities)
9. Improving operational response and investigative techniques in missing persons cases. (Specific operational priorities)
10. Human rights, gender, and civilian protection in the context of Common Security and Defence Policy and law enforcement external deployments. (Partnership and ethical capacities)

2.16 Other training needs

The training needs listed in this chapter do not align with any of the thematic or horizontal categories identified elsewhere in the assessment. As they constitute standalone topics, they are presented here without prioritisation.

Training on *core international crimes* (such as genocide, war crimes and crimes against humanity) was identified as an emerging need. This reflects law enforcement's increasing engagement in investigations with international dimensions, as well as the EU's commitment to global justice, accountability and support for partner countries affected by conflict. Officials require enhanced knowledge of relevant legal frameworks, evidence collection methodologies, and cooperation mechanisms with international judicial bodies.

Effective cross-border cooperation is further dependent on proficiency in *English law enforcement terminology*. Given English's role as a de facto working language among EU agencies and practitioners, targeted training in specialised terminology can enhance operational communication, reduce misunderstandings, and improve the quality of joint investigations and mutual assistance.

The need for *joint training of dog handlers* underscores the importance of operational consistency and efficiency in using canine units for detection, tracking, crowd control and other law enforcement applications. Differences in training methodologies across Member States currently hinder interoperability. Joint training would promote harmonised standards and improve deployment during cross-border operations.

A further operational need relates to *law enforcement response to kidnapping and extortion*, reflecting the sophisticated and often transnational nature of these crimes.

Training should focus on both prevention and response, integrating crisis negotiation, intelligence analysis, victim safeguarding and collaboration with private sector and communication service providers. The rise in digital facilitation of extortion schemes reinforces the urgency of developing this competence area.

In the area of professional development, *leadership, and management training*, including modules on EU funding mechanisms and EU project management, was identified as a key enabler of institutional development and innovation. Future leaders must possess not only strategic and operational leadership skills but also the ability to navigate EU financing frameworks, design and execute international cooperation initiatives, and ensure sustainable capacity-building within their organisations.

Training on *Disaster Victim Identification* was identified as a specialised operational need, particularly for responding to mass casualty incidents. Officials require awareness of recognised procedures and coordination mechanisms to ensure accurate and dignified identification processes, support investigations, and mitigate the impact on affected families.

Training needs listed in this chapter contribute to strengthening law enforcement's operational readiness, cross-border cooperation, and strategic capabilities. Addressing these gaps will not only improve specialised competencies but also reinforce broader EU policy objectives related to justice, security, and fundamental rights.

3. CONSULTATIONS WITH THE TRAINING PROVIDERS

Following contributions from several law enforcement expert groups and networks to the EU-STNA 2026–2029 process to identify training needs, CEPOL invited EU agencies, networks, and other bodies active in internal security training to participate in the consultation phase. The consultation was carried out through an online survey, in which training providers were asked to review the identified training needs, indicate which were addressed by their organisation, and provide any additional observations. In total, 15 training providers were contacted in this respect, and survey-based feedback was received from the following organisations:

- European Union Intellectual Property Office (EUIPO)
- European Network on the Administrative Approach to Prevent and Fight Organised Crime (ENAA)
- European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
- European Crime Prevention Network (EUCPN)
- European Union Agency for Asylum (EUAA)
- European Public Prosecutor's Office (EPPO)
- European Institute for Gender Equality (EIGE)
- European Union Drugs Agency (EUDA)
- European Union Agency for Fundamental Rights (FRA)
- European Union Agency for Law Enforcement Training (CEPOL)
- European Union Agency for Criminal Justice Cooperation (Eurojust)
- European Union Agency for Law Enforcement Cooperation (Europol)
- European Border and Coast Guard Agency (Frontex)
- European Network of Forensic Science Institutes (ENFSI)

Across all responses, providers largely confirmed that many of the priority training needs identified by Member States correspond to ongoing EU-level activities, mandates, or technical expertise. Several agencies emphasised that although a wide range of crime areas is already covered in principle, the volume of available EU-level training remains far below operational demand. Multiple organisations used the consultation to clarify the limits of their mandate, stressing that their input relates only to their legally defined remit, such as Eu-LISA to large-scale IT systems, EIGE to analytical tools, EUAA to the asylum domain and ENFSI to forensic science. A recurring theme was the need for greater coherence, better coordination, and more frequent training delivery at the EU level. Providers also pointed out where their activities intersect with horizontal priorities, such as fundamental rights, digitalisation, victims' rights, data protection, or administrative prevention tools.

CEPOL reported that its training portfolio already covers a very broad range of the identified priority needs, including drugs, cybercrime, counterterrorism, migrant smuggling, trafficking in human beings, environmental crime, firearms, excise fraud, IP crime and hybrid threats. It emphasised that although these needs are addressed through existing courses, webinars and operational training, the number of EU-level training opportunities remains too limited compared with Member States' demand and the scale of the criminal phenomena. CEPOL repeatedly stressed the need for a more comprehensive and frequent EU-level training offer in several thematic areas that already supports, noting that coverage exists "in principle", but the volume and frequency remain inadequate.

Europol confirmed that it maintains operational expertise across virtually all major crime areas featured in the EU-STNA, including drugs, cybercrime, firearms trafficking, counterterrorism, migrant smuggling, trafficking in human beings, environmental crime, excise fraud and IP crime. Europol clarified that while it does not necessarily deliver these topics as stand-alone training courses, it possesses operational knowledge, analytical tools, and training materials relevant to all of them. It also highlighted ongoing work on mass data, digital investigations, cyber-enabled crime, AI-driven threats, and the fundamental rights' considerations linked to these technologies. Europol concurred with CEPOL that EU-level training availability remains insufficient to meet demand.

Eurojust emphasised its continued contribution to training in judicial cooperation, including the European Investigation Order, Joint Investigation Teams, operational task forces, and other tools used in cross-border criminal justice. The agency confirmed its readiness to support training in areas linked to money laundering and financial crime, excise fraud, trafficking in human beings, and environmental crime, particularly by raising awareness of judicial instruments and operational coordination mechanisms. Eurojust also noted that Joint Investigation Teams remain central to its training activities and that it supports awareness-raising on judicial tools for prosecutors and investigative authorities.

Frontex provided feedback closely aligned with its mandate on external border management. It highlighted its extensive data collection on modus operandi and emerging trends at the EU's external borders, particularly in relation to drugs, synthetic drugs, document fraud, migrant smuggling, firearms, and hybrid threats. The agency clarified that its contribution to crime-area training applies only where a clear border-related link exists. Frontex reported that its training portfolio covers integrated border management, border and maritime risk analysis, return procedures, screening of vulnerable persons, cooperation with maritime and border authorities, detection of criminal activities at border checkpoints and joint simulation exercises in high-risk environments. It also noted its work on specialised maritime technologies, including robotics, cybersecurity, and remote sensing.

eu-LISA stated that it provides only technical training to Member States on the large-scale IT systems it manages and on interoperability. Its input therefore relates strictly to training on system usage, data management, data quality, technical operations and support to networks using EU information systems. The agency emphasised that its training activities for the 2026–2027 period are already planned and that it does not engage in broader operational, investigative, or crime-specific training.

EUIPO reported that it has educational materials available for most IP crime-related topics covered in the survey. Some areas are currently only partially covered but are expected to be complemented through future training courses or webinars. The agency noted that its materials relate to a wide range of issues in IP enforcement and that updates will continue as new trends emerge. It indicated readiness to further expand its training offer in areas such as digital investigations linked to online IP infringement, cooperation with rights-holders, and investigative approaches to illicit distribution channels.

EUCPN highlighted ongoing work in evidence-based crime prevention, particularly a toolkit currently being developed on youth recruitment into organised crime. It noted that it has materials and experience relevant to several prevention-related topics, including labour exploitation prevention, focused deterrence, online recruitment, community-oriented policing, family- and school-based interventions, and the evaluation of crime-prevention initiatives. EUCPN clarified that its work is strongly oriented toward evidence-based prevention methodologies and that many of its analytical products already cover specific topics reflected in the priority list.

EUAA clarified that although it delivers extensive training on vulnerability, trauma-informed approaches, victim protection, interviewing, leadership, and related subjects, all such training is situated within the asylum and international-protection context. It stressed that its training does not address organised crime, migrant smuggling investigations, cyber-enabled criminality, or operational law-enforcement approaches. EUAA noted that while many topics listed in the survey, fall outside its mandate, its training on vulnerability assessment, interviewing techniques, trauma-informed support, and victims' rights may be relevant to horizontal aspects, such as screening vulnerable persons at borders.

EPPO reaffirmed its primary training contributions in relation to EU judicial instruments and cross-border investigations, including the European Investigation Order, Joint Investigation Teams, operational task forces and cooperation with Europol, Eurojust and AMLA. It expressed readiness to support EU-level training on financial crime, excise fraud and the use of judicial cooperation tools. EPPO also confirmed its involvement in areas linked to money laundering, prosecutorial coordination and the legal frameworks governing cross-border investigations.

FRA highlighted its work in several relevant areas, including cyber violence against women and girls, counterterrorism legislation, online content moderation, the instrumentalisation of migration, child protection online and the rights implications of return procedures. FRA referred to its monitoring activities on fundamental rights at borders, procedural safeguards, vulnerabilities, non-discrimination, interoperability, data protection, and the rights of the child. While FRA does not itself provide operational training in many of the listed crime areas, it considers its analytical work and thematic expertise highly relevant to the development of training content, particularly in connection with data protection, procedural rights, victims' rights, and fundamental rights safeguards in technology-driven investigations.

EIGE emphasised that it does not provide training but highlighted ongoing analytical projects and tools that could support future training development. These include a gender-sensitive victim-identification project, an early-identification tool for victims, work on gender and security, and joint publications with Eurojust. EIGE indicated that although it does not train practitioners, its materials may be valuable as reference tools for designing gender-sensitive components of EU-level training.

EUDA provided observations related to drug trafficking, synthetic drugs, precursors, poly-drug networks, environmental harms from drug production and cooperation between drug and environmental crime investigators. It described its role in gathering and sharing intelligence on heroin, cannabis, and synthetic drugs, tracking market shifts, monitoring smuggling routes, sharing modi operandi and supporting investigations involving precursor misuse, postal parcels, and alternative trafficking corridors. EUDA also underlined the environmental dimension of drug-production activities and the need for coordination between drug and environmental regulators.

ENAA provided insights relevant to prevention, administrative controls, and multi-agency coordination. It highlighted areas such as early-stage detection, regulatory measures, administrative enforcement, and the use of administrative tools to close loopholes exploited by organised crime. ENAA pointed to its experience in administrative-prevention approaches and risk-based methods to prevent or disrupt emerging criminal trends.

ENFSI clarified that its ability to contribute is limited, strictly to forensic science. It can support training in forensic analysis of drugs, toxicology, digital forensics, cybercrime forensics, forensic readiness for terrorism, firearms examination, gunshot residue analysis and forensic approaches to child-sexual-abuse material and trafficking in human beings. ENFSI noted that it can only cover the forensic dimensions of these topics, including digital evidence collection, and cannot contribute operational or investigative components.

The consultation confirmed broad agreement with the prioritised training needs and highlighted several cross-cutting themes. Digitalisation and cyber-enabled crime

emerged as areas requiring sustained investment across agencies. Fundamental rights safeguards, particularly in relation to data-driven investigations, were emphasised by several providers. Border-related training intersects with multiple crime areas and remains a foundational component for Frontex. Drug-related training spans the investigative, regulatory, and forensic dimensions, as reflected by EUDA, Europol, CEPOL, and ENFSI. Judicial cooperation and financial crime remain central to Eurojust and EPPO contributions. Prevention-oriented insights from ENAA and EUCPN show a growing recognition of administrative and evidence-based approaches. Forensic science, as detailed by ENFSI, underpins a wide array of crime areas, and complements operational training needs. Overall, the consultation provides an overview of the current EU-level training ecosystem: substantial expertise exists across agencies, but the volume and reach of training remain below the demand. The inputs also demonstrate where mandates limit the scope of contributions and where coordination among EU-level providers will be essential to implementing the EU-STNA 2026–2029 findings.

CONCLUSION

Summary of main findings

The 2026–2029 EU-STNA reconfirms a stable set of horizontal capability gaps that cut across all thematic areas and therefore anchor EU-level training priorities for the coming cycle. In essence, they span cooperation, interoperability between EU systems, information exchange, end-to-end financial investigation focused on tracing, restraining and recovering criminal proceeds, digital competence including the operational use of AI and emerging technologies, forensic readiness, rights-based practice, prevention and administrative approaches, integrity safeguards and protection against infiltration and corruption, document security, and the disruption of the most threatening criminal networks and individuals.

On the thematic side, demand concentrates around large-scale drug trafficking, cyber-attacks and cyber-enabled criminality (including online fraud and online child sexual exploitation), counterterrorism, migrant smuggling and trafficking in human beings, economic and customs fraud, border management and maritime security, environmental crime, firearms and explosives, hybrid threats, intellectual property crime and counterfeiting, and the external dimension of internal security. Compared with 2022–2025, the new cycle shows continuity with a sharper focus on AI within digital skills, a more end-to-end approach to asset recovery, a stronger emphasis on prevention, integrity, and anti-corruption, and heightened attention to resilience against infiltration into the legal and public sectors. The process also, for the first time, reflected the direct involvement of customs authorities, expanding the range of perspectives and leading to stronger attention to excise and MTIC-related training needs.

The consolidated lists and order of priorities are presented in the Executive Summary and detailed in the thematic chapters.

Key conclusions

The EU-STNA 2026–2029 reaffirms that European LE operates in an environment of accelerating change, deep interdependence, and increasingly hybrid security challenges that transcend traditional boundaries. Crime, technology, and geopolitics are now intertwined in ways that require law enforcement to think and act systemically. While the core capability gaps identified in this cycle remain broadly consistent with

those of the previous EU-STNA, their operational complexity and interconnection have intensified. Training must therefore evolve in accordance with this changing reality: it is no longer a discrete response to individual threats but a strategic investment in preparedness, resilience, and joint operational capacity across borders. The horizontal foundations outlined in the findings, provide the basis for addressing the full spectrum of thematic crime areas and ensuring a coherent European approach to capacity building.

Two environmental factors continue to shape this operational context: the fragmentation of legal and regulatory frameworks across Member States, which hampers cooperation and prosecution, and resource limitations that constrain both the implementation of training and the operational deployment of trained officials. While these challenges fall outside the direct remit of the EU-STNA, they form the backdrop against which training needs and priorities must be addressed.

Within this context, the analysis confirms the continuity of trends observed in earlier EU-STNA cycles: crime phenomena are increasingly overlapping and interlocking, requiring law enforcement to operate with multidisciplinary toolkits and to cooperate across agencies and borders by default. Training should therefore integrate specialised expertise with cross-cutting competencies, notably intelligence-led information exchange, end-to-end financial investigation and asset recovery, and digital evidence competencies, to ensure that knowledge and skills are transferable across crime areas.

Law enforcement agencies also face a dual transformation: adapting to the constant evolution of criminal methods while embedding new operational and analytical capabilities driven by data, digital systems, and artificial intelligence. This technological acceleration is reshaping how law enforcement gathers intelligence, investigates crime, and cooperates across borders, requiring a sustained effort to build digital literacy and analytical capacity at all levels. At the same time, the effectiveness of this transformation depends on fostering a culture of continuous learning and exchange across agencies and Member States.

The findings also show that cooperation remains the single most enabling factor for effective law enforcement. Operational outcomes increasingly depend on the ability to exchange information, collectively interpret intelligence, and act through interoperable systems. Beyond police-to-police cooperation, this includes collaboration with prosecutors, customs, financial investigators, and border authorities, as well as extending to academia and the private sector, whose technical expertise is essential in areas such as AI, cybercrime, and environmental forensics. Existing EU cooperation mechanisms function well overall; however, continuous awareness-raising and

promotion of their use remain necessary to ensure that all Member States benefit equally from the available frameworks.

The EU-STNA 2026–2029 further highlights the growing interconnection between internal and external security. Hybrid threats, weaponised migration, environmental crime, and the exploitation of global digital infrastructures demonstrate that criminal and geopolitical domains are now closely linked. Law enforcement training must therefore integrate a broader, outward-looking perspective, reinforcing cooperation with non-EU partners and enhancing understanding of the external dimensions of EU internal security.

Another cross-cutting observation concerns the uneven distribution of training capacities and institutional readiness across Member States. The analysis and expert consultations indicate significant regional variation in available resources and expertise, leading to differing levels of demand. A more differentiated or "two-speed" approach to EU-level training provision, where basic and advanced training can be tailored to the maturity of national systems, would help ensure that all Member States can progress effectively. This differentiated approach can be supported through greater standardisation of competencies and the gradual development of a Sectoral Qualifications Framework on Policing, which remains a strategic priority for CEPOL.

Strategic considerations for EU-level training

Building on these conclusions, the EU-STNA 2026–2029 points to several directions for the further development of EU-level law enforcement training.

The analysis confirms that demand for training significantly exceeds current EU-level provision. Although the training needs identified in the EU-STNA are addressed by existing EU training providers, the overall volume of available training remains considerably lower than required. There is particular demand for awareness-raising on key capability gaps and across several crime areas. This highlights the necessity of investing in online training activities and platforms – such as CEPOL's LEEd – which are critical to extending outreach and accessibility.

Effective coordination of EU-level training provision is essential, not only to optimise resources but also to equip law enforcement with the knowledge, skills, and competencies necessary to operate in an increasingly complex and rapidly evolving environment. Establishing a central hub for EU-level training, supported by the development of a Sectoral Qualifications Framework for policing and a robust quality assurance framework for EU law enforcement training, would substantially enhance coherence, standardisation, and impact.

Training provision should continue its evolution towards joint, multidisciplinary, and practice-oriented formats that mirror the operational realities of cross-border cooperation. Training design and delivery should systematically incorporate advanced technologies, data-driven approaches, and simulation-based learning to ensure both relevance and adaptability. Given the volume and breadth of training needs identified by the EU-STNA 2026-2029, it is essential to promote consistent, large-scale training delivery across Member States to ensure comparable competencies and operational coherence within the EU law enforcement community. This also calls for the gradual strengthening of common quality standards, accreditation mechanisms and mutual recognition of training outcomes to ensure coherence and trust across the EU training landscape.

The findings underline that EU-level training must address both the horizontal competencies and the thematic operational areas where Member States report the most acute capability gaps. In practice, this means strengthening training in intelligence-led and interoperable information exchange, end-to-end financial investigation and asset recovery, the operational use of digital tools, AI, and forensic technologies, rights-based and preventive policing approaches, and resilience against corruption, infiltration, and hybrid threats. Digital and AI competencies should be treated as foundational enablers across all thematic areas, rather than specialised domains. The integration of forensic, preventive, and rights-based dimensions into mainstream training could help ensure a balanced and professional approach to security operations.

In addition, several expert discussions highlighted recurring needs for EU-level guidance and standardisation to support more coherent implementation of EU legislation and policies. Targeted EU workshops or guidance documents could help Member States align their interpretation and operational application of new directives and frameworks. Such efforts should be seen within a broader, career-long learning perspective, where EU-level guidance and training opportunities continuously reinforce professional competence and alignment throughout the different stages of law enforcement careers.

Thematic areas such as large-scale drug trafficking, cyber-enabled crime (including online fraud and child sexual exploitation), counterterrorism, trafficking in human beings, and environmental and financial crime remain the principal operational domains where EU-level training should be concentrated. These priorities collectively reflect where EU-level coordination and specialised expertise add most value to Member States' national training systems. Thematic priorities remain closely aligned with the

main EMPACT crime areas, encompassing high-risk criminal networks, financial investigations, cyber-enabled crime, trafficking-related offences, terrorism, and environmental threats. These are complemented by emerging domains such as hybrid and technology-driven threats, as well as the cross-cutting need to reinforce institutional integrity and public trust in law enforcement. Alongside the clear thematic clusters of training priorities, several training needs, such as leadership, crisis management, and public order, labelled as "other", remain relevant to maintaining operational readiness and crisis response capacities. While not among the highest-ranked thematic priorities, they continue to underpin the overall resilience and professionalism of the European law enforcement community.

Furthermore, some training needs are also subject to regional variations, especially within thematic clusters related to the EU's external borders, such as border management and maritime security, hybrid threats, the external dimension of internal security, and migrant smuggling. Geographically, countries along the Eastern external borders are particularly affected by external threat to internal security. Subsequently, training needs related to crimes with a stronger cross-border dimension, such as drug trafficking, counterfeiting of goods, excise fraud, or firearms trafficking, also tend to reflect more regional specificities.

To translate these findings into practical directions for future planning, the following considerations are proposed for EU-level policy makers, training providers, and partners:

- Further strengthen coordination and complementarity among EU-level training providers to maximise synergies, promote coherence, and avoid unnecessary overlaps.
- Use the EU-STNA as a shared strategic reference point for training planning at EU and national levels, embedding its findings in agency work programmes and funding frameworks.
- Scale up and further harmonise EU-level training provision to meet the growing demand for cross-border and specialised learning opportunities, ensuring the EU-STNA remains a regular, transparent, and evidence-based mechanism for aligning training provision with operational needs and for promoting the development of common curricula and standards.
- Integrate digital and AI competence development as a horizontal objective across all EU-level training initiatives.

- Promote joint and multidisciplinary training formats that involve the full justice chain, encompassing law enforcement, judicial, customs, financial, and border authorities, to enhance cooperation and mutual understanding.
- Deepen cooperation with research, academia, and the private sector, particularly in technology-driven domains, to foster innovation and evidence-based practice.
- Enhance cooperation with non-EU partners in areas of shared concern, reflecting the growing external dimension of EU internal security.
- Encourage the development of common standards and qualifications frameworks to ensure consistency of competence development and facilitate mobility and mutual recognition of training outcomes across Member States.

Closing outlook

Continuous professional development is an operational imperative for 21st-century law enforcement. As crime evolves faster than institutional adaptation cycles, investment in learning and competence should be increasingly recognised as a strategic enabler of European internal security and preparedness. By translating empirically assessed capability gaps into concrete training priorities, the EU-STNA 2026–2029 ensures that EU-level capacity building directly supports operational cooperation under EMPACT and aligns with the objectives of the new ProtectEU, and the EU Preparedness Union. More than a planning instrument, the EU-STNA 2026–2029 can serve as a shared framework for professional excellence, trust, and resilience within the European law enforcement community, embodying the Union's commitment to a coherent, competent, and future-ready law enforcement system capable of safeguarding Europe's security in a rapidly changing and interconnected world.

ANNEXES

Annex 1. Glossary of terms

EU Strategic Training Needs Assessment (EU-STNA): Detailed examination and identification, among EU priorities in the area of internal security, of those priorities with a training dimension that should be tackled through training activities at the EU level. It results from the practical implementation of the EU-STNA Methodology and its different steps. The EU-STNA should answer the following question: What training should be delivered at the EU level to address LE capability challenges?

EU-STNA Methodology: The step-by-step process to be followed to assess training-related EU priorities in the area of internal security and its external aspects, in line with the relevant policy cycles.

Security threats and sub threats: Security threats refer to areas of serious and organised crime and other threat areas (e.g., terrorism) that pose security risks within the EU. Sub-threats are the more detailed subcategories of threats.

Core capability gaps: 1. Tools or activities that, although not necessarily crimes as such, facilitate the commission of various crimes (for example, the use of the darknet, the financing of organised crime or terrorist financing); 2. Aspects relating to the combating and prevention of crime that are common to various crime areas (for example, law enforcement information exchange); 3. Societal challenges, for example, migration flows or the use of the internet.

Capability challenge: Deficiencies in the performance of law enforcement officials, i.e., their environment, awareness, knowledge, skills, or responsibility and autonomy. Responsibility and autonomy refer to the learner's ability to apply knowledge and skills independently and responsibly. The main difference from skills is that responsibility and autonomy are the capacity to perform, whereas a skill is the actual manipulation of things or data. Acting with responsibility and autonomy implies an ability to demonstrate substantial authority, innovation, scholarly and professional integrity, and sustained commitment to the development of new ideas or processes in work or study contexts, including research. Examples include problem-solving, strategic thinking, coaching, and mentoring.

Environment: The aggregate of surroundings, conditions, or influences. When environmental deficiencies create an obstacle to performance, it is clear that the desired result cannot be achieved by influencing the official's (personal) characteristics. Rather, the conditions in which the official operates are the cause of the issue. An example of this could be when the technical tools for examining travel documents to identify document fraud are missing.

Awareness: The knowledge that something exists, or the understanding of a situation or subject at the present time, based on information or experience. Awareness is an important element in change management, seen as a prerequisite for change. Recognising a problem, deficiency, or expectation can be sufficient to establish the desired change, without the need for increased knowledge, skills, or competencies.

Knowledge: The result of an interaction between intelligence (capacity to learn) and situation (opportunity to learn) and is therefore more socially constructed than intelligence alone. Knowledge includes theory and concepts, as well as tacit knowledge gained from experience performing certain tasks. Understanding refers to more holistic knowledge of processes and contexts and may be distinguished from know-that.

Skill: Skills reflect the practical application of knowledge and are measurable through testing and observation. They refer to the proficient manipulation of data or things, whether manual, verbal, or mental. Skills can be readily measured through a performance test that assesses both quantity and quality of performance, usually within an established time limit. An example of proficient manipulation is vehicle operation skills. An example of proficient data or evidence manipulation is investigative skills.

Training: Activities aimed at increasing law enforcement officials' awareness, knowledge, skills, responsibility and autonomy, etc., in order to ensure the correct performance of their tasks.

Annex 2. List of Documents Consulted

Number	Author	Title	Date
1	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 8 March 2022 on the shrinking space for civil society in Europe (2021/2103(INI))	2022
2	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 19 May 2022 on the Commission's 2021 Rule of Law Report (2021/2180(INI))	2022
3	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 15 September 2022 on the situation of fundamental rights in the European Union in 2020 and 2021 (2021/2186(INI))	2022
4	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 10 November 2022 on racial justice, non-discrimination and anti-racism in the EU (2022/2005(INI))	2022
5	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 13 December 2022 towards equal rights for persons with disabilities (2022/2026(INI))	2022
6	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 18 January 2024 on extending the list of EU crimes to hate speech and hate crime (2023/2068(INI))	2024
7	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 18 January 2024 on the situation of fundamental rights in the European Union – annual report 2022 and 2023 (2023/2028(INI))	2024
8	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 8 February 2024 on the implementation of the EU LGBTIQ Equality Strategy 2020-2025 (2023/2082(INI))	2024
9	Committee on Civil Liberties, Justice and Home Affairs	Resolution of 28 February 2024 report on the Commission's 2023 Rule of Law report (2023/2113(INI))	2024
F 10	Council of the European Union	Consultation for the preparation of the 13th Law Enforcement Working Party (LEWP-C) Action Plan for the years 2026-2027	2025
11	EIGE	Tackling cyber violence against women and girls: The role of digital platforms	2024
12	EIGE	Combating Cyber Violence against Women and Girls	2022
13	EIGE	Improving legal responses to counter femicide in the European Union: Perspectives from victims and professionals	2023
14	EIGE	Combating coercive control and psychological violence against women in the EU Member States	2022
15	EPPO	EPPO ANNUAL REPORT 2021	2022
16	EPPO	EPPO ANNUAL REPORT 2022	2023

17	EPPO	EPPO ANNUAL REPORT 2023	2024
18	EPPO	EPPO ANNUAL REPORT 2024	Mar-25
19	EUAA	EUAA Annual Training Report	2023
20	EUAA	Annual Report on Migration and Asylum for 2023	2024
21	EUAA	Latest Asylum Trends Mid-Year Review 2024	2024
22	EUAA	Asylum Report 2023: The Situation of Asylum in the European Union	2023
23	EUAA	National Asylum Developments 2023	2023
24	EUAA	Annual Trend Analysis Report 2021	2021
25	EUAA	Asylum Report 2021: The situation of asylum in the European Union	2021
26	EUAA	National Asylum Developments in 2020	2020
27	EUAA	Annual Trend Analysis Report 2020	2020
28	EUAA	Asylum Report 2022 (added as requested)	2022
29	EUAA	Asylum Report 2024 (added as requested)	2024
30	EUCPN	Artificial intelligence and predictive policing: risks and challenges	2022
31	EUCPN	Law enforcement has to be part of the prevention workforce. The question is: how and where?	2023
32	EUCPN	Recommendation paper: A victim-centred approach to preventing repeat hate crime victimisation of LGBTI people	2022
33	EUCPN	Mythbuster - The fight against serious and organised crime: international LE cooperation or local approaches?	2021
34	EUCPN	Public-private partnerships in crime prevention: CHALLENGES AND RECOMMENDATIONS	2023
35	EUCPN	How to prevent maritime theft?	2023
36	EUCPN	High-risk victim groups: Preventing repeat and secondary victimisation	2022
37	EUCPN	EUCPN Evidence-based prevention strategy: Towards evidence-based crime prevention in the EU	2021
38	EUCPN	Straw men in organised property crime: using the administrative approach	2023
39	EUCPN	Labour exploitation and work-related crime: a problem analysis and prevention framework	2023
40	EUCPN/ENAA	ENAA roadmap 'How to get started with the administrative approach'	2023
41	European Commission	EU Drugs Strategy 2021 - 2025	2021
42	European Commission	EU Drugs Action Plan 2021-2025	2021
43	EUDA	European Drug Report 2022: Trends and Developments	2022
44	EUDA	European Drug Report 2023: Trends and	2023

		Developments	
45	EUDA	European Drug Report 2024: Trends and Developments	2024
46	EUDA	EU Drug Markets Analysis: Key insights for policy and practice	2024
47	EUDA	EU Drug Market: New psychoactive substances – In-depth analysis	2023
48	EUDA	EU Drug Market: Heroin and other opioids – In-depth analysis	2024
49	EUDA	EU Drug Market: Amphetamine – In-depth analysis	2024
50	EUDA	EU Drug Market: Cannabis – In-depth analysis	2024
51	EUDA	EU Drug Market: Cocaine	2024
52	EUDA	EU Drug Market: Methamphetamine	2024
53	EUIPO	EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2023 (November 2024)	2024
54	EUIPO	Problems related to counterfeiting and piracy	2024
55	EUIPO	Study on Business Models Infringing IP	2022
56	EUIPO	OPERATION JAD PIRATES I Tackling the smuggling of counterfeit goods at the external borders of the EU	2024
57	EUIPO	Uncovering the ecosystem of intellectual property crime	2024
58	EUIPO	Operation Fake Star Report	2023
59	EUIPO	IP crime investigation handbook	2023
60	eu-LISA	Industry roundtable 2024 Nov. report	2024
61	eu-LISA	Seamless Travel Report 2022	2022
62	eu-LISA	Paper 2023 Fingerprint Quality	2023
63	eu-LISA	Eurodac Annual report 2022	2023
64	eu-LISA	Eurodac Annual report 2023	2024
65	eu-LISA	Report on SIS technical functioning 2021 2022	2023
66	eu-LISA	Vis 2021 2023 report	2024
67	EUROJUST	Eurojust Casework on Corruption: 2016-2021 Insights	2022
68	EUROJUST	Eurojust Report on Money Laundering	2022
69	EUROJUST	Eurojust Meeting on Counterterrorism, 22 - 23 November 2023	2023
70	EUROJUST	Eurojust Report on Drug trafficking	2021
71	EUROJUST	Report on Eurojust's Casework on Environmental Crime	2021
72	EUROJUST	SIRIUS EU Digital Evidence Situation Report 2022	2022
73	EUROJUST	SIRIUS EU Digital Evidence Situation Report 2023	2023

74	EUROJUST	DIGITAL SERVICES ACT ensuring a safe and accountable online environment	2022
75	EUROJUST	Report on Eurojust's casework on victims' rights	2022
76	EUROJUST	Eurojust Report on the Transfer of Proceedings in the European Union	2023
77	EUROJUST	Assessment of national legislative approaches and court practice regarding online copyright piracy	2023
78	EUROJUST	GENERATIVE ARTIFICIAL INTELLIGENCE The impact on intellectual property crimes	2023
79	EUROJUST	Report on Eurojust's Casework in the Field of the European Arrest Warrant	2021
80	EUROJUST	FOURTH JITS EVALUATION REPORT	2023
81	EUROJUST	TOOLS AND RESOURCES FOR JIT PRACTITIONERS	2024
82	EUROJUST	Eurojust Meeting on Migrant Smuggling The Hague, 8-9 November 2023	2023
83	EUROJUST	Application of the principle of legality, right to a fair trial and other protected rights in core international crimes cases	2023
84	EUROJUST	Eurojust Report on Trafficking in Human Beings	2021
85	European Commission	Communication from the Commission establishing the multiannual strategic policy for European integrated border management	2023
86	European Commission	Report from the Commission – Interim Evaluation under Regulation (EU) 2021/785 establishing the Union Anti-Fraud Programme and repealing Regulation (EU) No 250/2014	2024
87	European Commission	Report from the Commission – High-risk areas of corruption in the EU: A mapping and in-depth analysis	2024
88	European Commission	Report from the Commission to the Council and the European Parliament "35th Annual Report on the protection of the European Union's financial interests and the Fight against fraud - 2023"	2023
89	European Commission	Statistical evaluation of irregularities reported for 2023: own resources, agriculture, cohesion and fisheries policies, pre-accession and direct expenditure	2023
90	European Commission	Communication from the Commission on countering potential threats posed by drones	2023
91	European Commission	Report from the Commission to the European Parliament and the Council evaluating Directive (EU) 2017/541 on combatting terrorism	2021

92	European Commission	Joint Action Plan on Counterterrorism in the Western Balkans	2022
93	European Commission	Strategic orientations on a coordinated EU approach to prevention of radicalisation for 2022-2023	2022
94	European Commission	Commission Staff Working Document: "Security by Design: Protection of Public Spaces from Terrorist Attacks".	2022
95	European Commission	Report from the Commission on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online	2024
96	European Commission	Strategic Orientations on a Coordinated EU Approach to Prevention of Radicalisation for 2024-2025	2024
97	European Commission	Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)	Q 1 2025
98	European Commission	Communication on the EU roadmap to fight drug trafficking and organised crime	2023
99	European Commission	EU Action Plan on the Western Balkans	2022
100	European Commission	EU Action Plan for the Central Mediterranean	2022
101	European Commission	EU Action Plan for the Western Mediterranean and Atlantic Routes	2023
102	European Commission	EU Action Plan for the Eastern Mediterranean Route	2023
103	European Commission	EU Action Plan on firearms trafficking 2020-25	2020
104	European Commission	Report from the Commission to the European Parliament and the Council on the application of Directive (EU) 2021/555	2021
105	European Commission	Scoreboard of the Commission on the implementation of National Firearms Focal Points in the EU Member States	2024
106	European Commission	Regulation (EU) 41/2025 on import, export and transit measures for firearms, their essential components and ammunition.	2025
107	European Commission	High-Level Group on Access to Data for Effective Law Enforcement – Concluding report	2024
108	European Commission	EU Roadmap on lawful access to data	Mid-2025
109	European Commission	LGBTIQ Equality Strategy 2020-2025	2021
110	European Commission	Report on the Implementation of the LGBTIQ Equality Strategy 2020-2025	2024
111	European Commission	EU Roma strategic framework on equality, inclusion, and participation	2020

112	European Commission	Report on the implementation of the national Roma strategic frameworks in light of the EU Roma strategic framework	2024
113	European Commission	EU Strategy on combating antisemitism and fostering Jewish life (2021 – 2030)	2021
114	European Commission	First progress report of the EU Strategy on combating antisemitism and fostering Jewish life	2024
115	European Commission	EU anti-racism action plan 2020-2025	2020
116	European Commission	Joint communication to the European Parliament and the Council No place for hate: a Europe united against hatred	2023
117	European Commission	EU Strategy on Victims' Rights	2020
118	European Commission	Communication from the Commission to the European Parliament and the Council: A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime	2021
119	European Commission	Commission Delegated Regulation 2023/2450 of 17 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services	2023
120	European Commission	Strategic guidelines for legislative and operational planning within the area of freedom, security, and justice	2024
121	European Commission	EU Strategy to tackle Organised Crime 2021-2025	2021
122	European Commission	EMPACT 2022 Results	2022
123	European Commission	EMPACT 2023 Results	2023
124	European Commission	Communication from the Commission on countering hybrid threats from the weaponisation of migration and strengthening security at the EU's external borders	2024
125	European Commission	Proposal for a Regulation on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls	2022
126	European Commission	State of Schengen Report 2022	2022
127	European Commission	State of Schengen report 2023	2023
128	European Commission	State of Schengen Report 2024	2024
129	European Commission	EES handbook	2024
130	European Commission	ETIAS handbook	To be adopted in 2025

131	European Commission	Commission Recommendation of 31.3.2023 establishing a Practical Handbook to be used by Member States' competent authorities and SIRENE Bureaux when carrying out tasks related to the Schengen Information System ('SIS Handbook') C(2023) 2152 final	2023
132	European Commission	Commission implementing decision of 29.1.2024 amending Implementing Decision C(2021) 7900 final as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union C(2024) 451 final (SIRENE Manual - Borders)	2024
133	European Commission	Commission implementing decision of 29.1.2024 laying down detailed rules for the tasks of the SIRENE Bureaux and the exchange of supplementary information regarding alerts in the Schengen Information System in the field of police LE cooperation and judicial LE cooperation in criminal matters ('SIRENE Manual - Police') and repealing Implementing Decision C(2021) 7901 final C(2024) 290 final	2024
134	European Commission	Interoperability handbook	To be adopted in 2025
135	European Commission	Proposal for a Regulation on enhancing police LE cooperation in relation to the prevention, detection, and investigation of Migrant smuggling and trafficking in human beings, and on enhancing Europol's role to preventing and combating such crimes and amending Regulation (EU) 2016/794	2023
136	European Commission	Commission Recommendation of 23.11.2023 on LE cooperation between the Member States with regards to serious threats to internal security and public policy in the area without internal border controls	2023
137	European Commission	A renewed action plan against Migrant smuggling 2021-2025	2021
138	European Commission	Joint Roadmap on the organisation, coordination, and implementation of the timeline for the negotiations between the co-legislators on the CEAS and the New European Pact on migration and asylum	2022
139	European Commission	Towards an operational strategy for more effective returns	2023

140	European Commission	Proposal for a Directive laying down minimum rules to prevent and counter the facilitation of unauthorised entry, transit and stay in the Union, and replacing Council Directive 2002/90/EC and Council Framework Decision 2002/946 JHA	2023
141	European Commission	Commission Recommendation of 16.3.2023 on mutual recognition of return decisions and expediting returns when implementing Directive 2008/115/EC	2023
142	European Commission	The launch of the Global Alliance to counter Migrant smuggling	2023
143	European Commission	Communication from the Commission on the Common Implementation Plan for the Pact on Migration and Asylum	2024
144	European Commission	Commission Staff Working Document on the return of illegally staying third-country nationals posing a security threat	2024
145	European Commission	2023-2024 Horizon Europe Work Programme	2022
146	European Commission	Common Anti-Trafficking Plan to prevent and fight trafficking in human beings and protect the victims fleeing Ukraine	2022
147	European Commission	Report on the progress made in the fight against trafficking in human beings (Fifth Report)	2022
148	European Commission	COMMISSION STAFF WORKING DOCUMENT Assessment of the effect given by the Member States to COUNCIL RECOMMENDATION (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation	2025
149	European Commission	Concluding report of the High-Level Group on access to data for effect	2024
150	European Commission	Proposal for a COUNCIL RECOMMENDATION on Roma equality, inclusion and participation	2020
151	European Commission	Commission Implementing Decision setting the date on which operations of the Schengen Information System start pursuant Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862 of the European Parliament and of the Council	2023
152	European Council	Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan	2023
153	European Council	Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.	2022

154	European Council	Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance	2024
155	European Council	Council Conclusions on reinforcing external-internal connections in the fight against terrorism and violent extremism	2024
156	European Council	Council Decision (EU) 2022/895 authorising the opening of negotiations on behalf of the European Union for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes	2022
157	European Council	Council conclusions on combating cross-border Environmental crime (14182/24)	2024
158	European Council	Council Conclusions (10726/21) on the implementation of the National Firearms Focal Points (NFFPs) in the EU Member States	2021
159	European Council	Council Decision (EU) 2022/722 authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence	2022
160	European Council	Council Decision (EU) 2023/436 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced LE cooperation and disclosure of electronic evidence	2023
161	European Council	Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law	2008
162	European Council	Council Conclusions setting the 2022-2025 EMPACT priorities	2022
163	European Council	Council Conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022+	2023
164	European Council	Council Recommendation on operational law enforcement LE cooperation (CROLEC)	2022
165	European Council	Council Resolution on customs cooperation in the area of law enforcement and its contribution to the internal security of the EU	2023

166	European Council	Strategy for customs cooperation in the area of law enforcement and its contribution to the internal security of the EU	2023
167	European Council	Council recommendation on law enforcement operational cooperation implementation roadmap	2023
168	European Council	Council Implementing Decision extending temporary protection as introduced by Implementing Decision (EU) 2022/382	2024
169	European Council	Council Conclusions on the fight against trafficking in cultural goods	2023
1710	European Council	Council conclusions on a way forward for crime prevention in Europe	2023
171	European Parliament and European Council	Regulation (EU) 2023/2685 of the European Parliament and of the Council of 22 November 2023 amending Council Regulation (EC) No 1683/95 as regards the digitalisation of the visa procedure	2023
172	European Parliament and European Council	Directive (EU) 2024/1233 of the European Parliament and of the Council of 24 April 2024 on a single application procedure for a single permit for third-country nationals to reside and work in the territory of a Member State and on a common set of rights for third-country workers legally residing in a Member State (recast)	2024
173	European Parliament and European Council	Proposal for a Directive on combating corruption	2023
174	European Parliament and European Council	Directive (EU) 2024/1260 on asset recovery and confiscation	2024
175	European Parliament and European Council	Proposal for a Regulation laying down rules to prevent and combat child sexual abuse	2022
176	European Parliament and European Council	Regulation (EU) 2024/1307 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse	2024
177	European Parliament and European Council	Proposal for a directive on combating the sexual exploitation of children and child sexual abuse material (recast)	2024
178	European Parliament and European Council	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities	2022

179	European Parliament and European Council	Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)	2024
180	European Parliament and European Council	Regulation (EU) 2023/1322 on the European Union Drugs Agency (EUDA)	2023
181	European Parliament and European Council	Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC	2024
182	European Parliament and European Council	Joint communication to the European Parliament and the Council - A new outlook on the climate and security nexus: Addressing the impact of climate change and environmental degradation on peace, security and defence	2023
183	European Parliament and European Council	Joint communication to the European Parliament and the Council A New Agenda for Relations between the EU and Latin America and the Caribbean	2023
184	European Parliament and European Council	Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings	2023
185	European Parliament and European Council	Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings	2023
186	European Parliament and European Council	Directive (EU) 2024/1226 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673	2024
187	European Parliament and European Council	Regulation (EU) 2025/13 on the collection and transfer of advance passenger information for the prevention, detection, and investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818	2025

188	European Parliament and European Council	Regulation (EU) 2022/1190 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union	2022
189	European Parliament and European Council	Regulation (EU) 2024/982 on the automated search and exchange of data for police LE cooperation, and amending Council Decisions 2008/615/JHA, and 2018/616/JHA	2024
190	European Parliament and European Council	EES Regulation 2017/2226	2017
191	European Parliament and European Council	ETIAS Regulation 2018/1240	2018
192	European Parliament and European Council	Revised VIS amending Regulation 2021/1134	2021
193	European Parliament and European Council	Interoperability Regulation 2019/817	2019
194	European Parliament and European Council	Interoperability Regulation 2019/818	2019
195	European Parliament and European Council	Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794	2022
196	European Parliament and European Council	Directive (EU) 2023/977 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA	2023
197	European Parliament and European Council	Regulation (EU) 2023/2844 on the digitalisation of judicial LE cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial LE cooperation	2023
198	European Parliament and European Council	Directive (EU) 2023/2843 amending Directives 2011/99/EU and 2014/41/EU of the European Parliament and of the Council, Council Directive 2003/8/EC and Council Framework Decisions 2002/584/JHA, 2 0 0 3 /577/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA, 2008/947/JHA, 2009/829/JHA and 2009/948/JHA, as regards digitalisation of judicial LE cooperation	2023
199	European Parliament and European Council	Regulation (EU) 2024/1351 on asylum and migration management, amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and repealing Regulation (EU) No 604/2013	2024
200	European Parliament and European Council	Regulation (EU) 2024/1348 establishing a common procedure for international	2024

		protection in the Union and repealing Directive 2013/32/EU	
201	European Parliament and European Council	Regulation (EU) 2024/1349 establishing a return border procedure, and amending Regulation (EU) 2021/1148	2024
202	European Parliament and European Council	Regulation (EU) 2024/1359 addressing situations of crisis and force majeure in the field of migration and asylum and amending Regulation (EU) 2021/1147	2024
203	European Parliament and European Council	Regulation (EU) 2024/1358 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes.	2024
204	European Parliament and European Council	Regulation (EU) 2024/1356 introducing the screening of third- country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817	2024
205	European Parliament and European Council	Regulation (EU) 2024/1347 on standards for the qualification of third country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection and for the content of the protection granted, amending Council Directive 2003/109/EC and repealing Directive 2011/95/EU of the European Parliament and of the Council	2024
206	European Parliament and European Council	Directive (EU) 2024/1346 laying down standards for the reception of applicants for international protection.	2024
207	European Parliament and European Council	Regulation (EU) 2024/1350 establishing a Union Resettlement and Humanitarian Admission Framework, and amending Regulation 2021/1147	2024
208	European Parliament and European Council	Directive 2019/713 on combating fraud and counterfeiting of non-cash means of payment	2019

209	European Parliament and European Council	Proposal for a Directive of the European Parliament and the Council on combating violence against women and domestic violence	2023
210	European Parliament and European Council	Directive 2011/36/EU on preventing and combatting trafficking in human beings and protecting victims as amended by Directive (EU) 2024/1712.	2024
211	European Parliament and European Council	Directive (EU) 2024/1712 amending Directive 2011/36/EC on preventing and combating trafficking in human beings and protecting its victims	2024
212	Europol	The other side of the coin Analysis of Financial and economic Crime	2023
213	Europol	European Union Terrorism situation and trend report 2021	2021
214	Europol	European Union Terrorism situation and trend report 2022	2022
215	Europol	European Union Terrorism situation and trend report 2023	2023
216	Europol	European Union Terrorism situation and trend report 2024	2024
217	Europol	Cyber-attacks the apex of crime as a service	2023
218	Europol	Internet Organised Crime Threat Assessment (IOCTA) 2021	2021
219	Europol	Internet Organised Crime Threat Assessment (IOCTA) 2023	2023
220	Europol	Internet Organised Crime Threat Assessment (IOCTA) 2024	2024
221	Europol	AI and policing	2024
222	Europol	Frist report on Encryption	2024
223	Europol	The Second Quantum Revolution: The impact of quantum computing and quantum technologies on law enforcement	2023
224	Europol	Biometric vulnerabilities - Ensuring future law enforcement preparedness	March 2025
225	Europol	ChatGPT The impact of Large Language Models on Law Enforcement	2023
226	Europol	Europol's SIRIUS EU Electronic Evidence Situation Report	2023
227	Europol	Europol's SIRIUS EU Electronic Evidence Situation Report	2024
228	Europol	Country contributions to SOCTA	Mid-2025

229	Europol	SOCTA	March
230	Europol	Europol in brief	2024
231	Europol	Criminal networks in migrant smuggling	2023
232	Europol	Criminal networks in EU ports	2023
233	Europol	Decoding the EU-s most threatening criminal networks	2024
234	Europol	Leveraging legitimacy - How the EU most threatening criminal networks abuse legal business structures	2024
235	Europol	Intelligence notification: The recruitment of young perpetrators for criminal networks	2024
236	Europol	Undercovering the ecosystem of IP Crime	2024
237	Europol	Europol's Internet Organised Threat Assessment	2024
238	Europol	Online fraud schemes web of deceit 2023	2023
239	Europol	Early warning notification: War in Ukraine – refugees arriving to the EU from Ukraine at risk of exploitation as part of THB	2022
240	EUSPR/EUCPN/EUDA	Law enforcement has to be part of the prevention workforce. The question is: how and where?	2023
241	FRA	DIRECTIVE (EU) 2017/541 ON COMBATING TERRORISM IMPACT ON FUNDAMENTAL RIGHTS AND FREEDOMS	2022
242	FRA	Children as suspects or accused persons in criminal proceedings – procedural safeguards	2022
243	FRA	Handbook on European law relating to the rights of the child - 2022 edition	2022
244	FRA	Underpinning victims' rights: support services, reporting and protection	2023
245	FRA	Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update	2023
246	FRA	Being Black in the EU – Experiences of people of African descent	2023
247	FRA	European Arrest Warrant proceedings - Room for improvement to guarantee rights in practice	2024
248	FRA	European Arrest Warrant and Fundamental Rights ECtHR and CJEU Case-Law - Joint Factsheet	2024
249	FRA	Stepping up the response to victims of crime: FRA's findings on challenges and solutions |	2024
250	FRA	Addressing Racism in Policing	2024
251	FRA	LGBTIQ at a crossroads: progress and challenges	2024
252	FRA	Jewish People's Experiences and Perceptions of Antisemitism	2024

253	FRA	Being Muslim in the EU - Experiences of Muslims	2024
254	FRA	EU gender-based violence survey - Key results	2024
255	FRA	Guidance on investigating alleged ill-treatment at borders	2024
256	FRONTEX	STRATEGIC RISK ANALYSIS REPORT	2024
257	FRONTEX	Annual Risk Analysis 2024/2025	2024
258	FRONTEX	Risk Analysis for 2023/2024	2024
259	FRONTEX	Risk Analysis for 2022/2023	2022
260	FRONTEX	Strategic Risk Analysis 2022	2022
261	OLAF	Casebook of OLAF investigations in the field of external aid - Red flags and lessons learnt, identified through OLAF investigations of EU funded projects in development and humanitarian aid.	2024
262	OLAF	Anti-Fraud Advice for EU funded Environmental crime investment projects	2022
263	OLAF	ANTI-FRAUD ADVICE for the purchase of IT hardware and software under EU funded projects	2022
264	OLAF	Developing anti-Fraud IT tools for the Recovery and Resilience Facility: The experiences of Member States	2024

Annex 3. Law enforcement groups contributing to EU-STNA

EMPACT groups 2022-2025

Number	Name
1	Cannabis, Cocaine and Heroin
2	Criminal Finances, Money Laundering and Facilitated Asset Recovery
3	Corruption
4	Cybercrime – Child Sexual Abuse and Child Sexual Exploitation
5	Cyberattacks
6	Digital skills
7	Document fraud
8	Environmental Crime
9	Excise Fraud
10	Firearms trafficking
11	Migrant smuggling
12	High-risk criminal networks
13	Intellectual property crime
14	Missing Trader Intra-Community Fraud
15	Online fraud schemes
16	Synthetic Drugs, New Psychoactive Substances
17	Trafficking in Human Beings

Other thematic Expert Groups convened

Number	Name
1	EU-STNA Expert Group on Border Management and Maritime Security
2	CEPOL Knowledge Centre on Counter Terrorism
3	EU-STNA Expert Group on External Dimensions of European Security
4	EU-STNA Expert Group on Fundamental Rights
5	CEPOL Knowledge Centre on Law Enforcement Cooperation, Information Exchange and Interoperability

Annex 4. Other professional groups/networks consulted

Number	Name
1	@ON – Operational Network to Counter Mafia-style Serious and Organised Crime Groups
2	AIRPOL – Law enforcement network of police and border guard units at European airports
3	ATLAS Network – European Special Intervention Units combating terrorism and violent crime
4	CARPOL – Network of EU law enforcement contact points for tackling cross-border vehicle crime
5	DVI – Experts in the area of disaster victim identification
6	EFE – European Firearms Experts
7	EJCN – European Judicial Cybercrime Network
8	EMPEN – European Medical and Psychological Experts Network for Law Enforcement
9	ENAA – European Network on the Administrative Approach tackling serious and organised crime
10	ENFAST – European Network of Fugitive Active Search Teams
11	ENISA – European Union Agency for Cybersecurity
12	ENLETS – European Network of Law Enforcement Technology Services
13	RCEG – Radio Communication Expert Group
14	ENPPF – European Network for the Protection of Public Figures
15	EnviCrimeNet – Network of European law enforcement agencies against environmental crime
16	EU CULTNET – Informal network of law enforcement authorities and experts competent in the field of cultural goods
17	EUIPO – European Union Intellectual Property Office
18	High-level Expert Group on Information Systems and Interoperability
19	KYNOPOL – Police Network for Law Enforcement Dog Professionals
20	LOs – Liaison officers' services
21	MSE – Experts for major sports events
22	Pan-European Think Tank of Football Safety and Security Experts
23	SIS-SIRENE Committee – Schengen Information System – Supplementary Information Request at the National Entries Committee
24	TISPOL – European Traffic Police Network

Annex 5. Summary table of expert consultations

Topic	Groups consulted	Type of consultation	Date
Fundamental rights	EU-STNA Expert Group	Focus group meeting	17 February 2025
Trafficking in human beings	EMPACT Group	Focus group meeting	18 February 2025
MTIC Fraud	EMPACT Group	Focus group meeting	27 February 2025
Environmental crime	EMPACT Group	Focus group meeting	6 March 2025
Law enforcement cooperation, information exchange and Interoperability	CEPOL Knowledge Centre	Focus group meeting	11 March 2025
Cannabis, cocaine, heroin	EMPACT Group	Focus group meeting	17 March 2025
Synthetic drugs and new psychoactive substances	EMPACT Group	Focus group meeting	20 March 2025
Border management and maritime security	EU-STNA Expert Group	Focus group meeting	2 March 2025
External dimensions of EU security	EU-STNA Expert Group	Focus group meeting	8 March 2025
Excise fraud	EMPACT Group	Focus group meeting	9 March 2025
Firearms	EMPACT Group	Focus group meeting	11 March 2025
Counterterrorism	CEPOL Knowledge Centre	Focus group meeting	3 April 2025
Forensics	ENFSI	Online meetings	16 April 2025 12 June 2025
Digital skills, use of new technologies, AI	EU-STNA Expert Group EU Innovation Hub	Focus group meeting	24 April 2025
Migrant smuggling	EMPACT Group	Focus group meeting	29 April 2025
Child sexual exploitation	EMPACT Group	Focus group meeting	30 April 2025

Corruption	EU-STNA Expert Group	Focus group meeting	6 May 2025
Document fraud	EMPACT Group	Focus group meeting	6 May 2025
Cyberattacks	EMPACT Group	Focus group meeting	8 May 2025
Online fraud schemes	EMPACT Group	Focus group meeting	14 May 2025
Intellectual property crimes and counterfeiting of currencies	EMPACT Group	Focus group meeting	21 May 2025
High-risk criminal networks	EMPACT Group	Focus group meeting	3 June 2025
Criminal finance, money laundering and asset recovery	EMPACT Group	Focus group meeting	5 June 2025
Other needs	Other LE training providers	Online survey	May 2025

Annex 6 List of identified EU-level training needs and potential training providers

Thematic training needs

The production, trafficking and distribution of cannabis, cocaine and heroin (Drug trafficking)	Training providers
Following the crime script, cocaine address detection of cocaine and its intermediate products (chemically concealed cocaine, as well as cocaine base) and the processing and production laboratories.	CEPOL Europol
Financial investigations linked to drug production and trafficking, including tracking proceeds through cryptocurrencies and decentralised platforms.	CEPOL Europol
Gathering and sharing of intelligence on heroin trafficking; tracking and detecting heroin, heroin precursor chemicals; monitoring heroin market shifts and trafficking through alternative smuggling corridors.	CEPOL EUDA Europol
Gather and share structured intelligence related to smuggling cannabis through different routes (North America, North Africa, Western Balkans, Italy, Türkiye, Northern and Eastern Europe).	CEPOL Frontex EUDA Europol
Criminal infiltration into and misuse of legal business structures, the potential role of legal business structures in every stage of the crime script.	CEPOL ENAA Europol
Investigation of poly-drug trafficking routes, including the use of drugs as currency in exchanges between organised crime groups.	CEPOL EUDA Europol
Application of administrative measures and licensing controls to prevent diversion of precursors and legal substances to illicit drug production, in conjunction with a criminal justice approach.	ENAA CEPOL Europol
Share modi operandi as well as responses to smuggling cannabinoids via postal services/parcels.	CEPOL EUDA Europol
Gather and share structured intelligence related to production and emerging product trends of cannabinoids.	CEPOL Frontex Europol
Undercover cyber investigations, including social media platforms, darknet and encrypted communication, operation of cyber patrolling teams, and collection of digital evidence.	CEPOL Europol
Countering drug-related violence and youth recruitment by organised crime groups	
Recognition of waste coming from illegal drug laboratories and plantations, energy theft, deforestation, as part of significant deterioration of protected habitats, and exploitation of water infrastructure has a negative impact on the environment; they should be prosecuted. Coordination between drug and environmental crime investigators is necessary.	CEPOL EUDA Europol

The production, trafficking and distribution of synthetic drugs and new psychoactive substances (Drug trafficking)	Training providers
Diversion and trafficking of drugs and precursors, both wholesale and retail, via postal parcels and courier services, courier walls, cooperation between police and customs and the private sector.	CEPOL EUDA Europol
Financial investigations linked to drug production and trafficking, including tracking proceeds through cryptocurrencies and decentralised platforms.	CEPOL Europol
Detecting and interdicting illicit synthetic drugs and NPS shipments, including concealment in postal parcels, cargo, and commercial supply chains.	CEPOL EUDA Europol
Investigating and dismantling the synthetic drug and NPS production and distribution infrastructure, including labs, transport routes, and waste dump sites	CEPOL ENFSI Europol
Awareness and use of EU information-sharing platforms and cooperation tools in synthetic drug investigations.	CEPOL EUDA Europol
Investigating poly-drug trafficking networks and overlapping smuggling routes involving synthetic drugs.	CEPOL EUDA Europol
Import, production, diversion, export of licit medicine, to the illicit drug market, e.g., ketamine, tramadol, fentanyl and etomidate, use of legal business structures.	CEPOL Europol
Identifying and reporting on precursor chemical misuse, including regulatory updates and techniques to detect mislabelled substances.	CEPOL EUDA Europol
Forensic analysis and interpretation of drug samples; application of innovative tools and technologies for drugs and toxicological analysis and profiling.	CEPOL ENFSI Europol
Application of administrative measures and licensing controls to prevent diversion of precursors and legal substances to illicit synthetic drug production, in conjunction with a criminal justice approach.	CEPOL Europol
Undercover cyber investigations, including social media platforms, darknet and encrypted communication, operation of cyber patrolling teams, and collection of digital evidence.	CEPOL Europol
Risks and law enforcement response strategies for synthetic opioids and high-potency stimulants.	CEPOL EUDA Europol Frontex
Identifying and addressing environmental harms from synthetic drug production: coordination between drug and environmental crime investigators.	CEPOL EUDA Europol
Understanding different judicial systems and legal frameworks regarding drug trafficking.	CEPOL Europol

Cyber-attacks (Fastest growing crimes in the online sphere)	Training providers
Advanced cybercrime forensics, including ransomware forensics, malware analysis, dark web investigations, phishing attack analysis, forensic imaging and device acquisition	CEPOL Europol ENFSI
Advanced cybercrime forensics, including ransomware forensics, malware analysis, dark web investigations, phishing attack analysis, forensic imaging and device acquisition	CEPOL Europol
Emerging cyber threats, including AI-driven attacks, Internet of Things vulnerabilities, decentralised platforms, and quantum-related risks.	CEPOL Europol
Joint training for law enforcement and Computer Security Incident Response Teams on malware investigations, supply-chain attacks, and incident response coordination, involving public–private partnerships.	CEPOL Europol
Hybrid threat-linked cyber-attacks.	CEPOL Europol
Tracing cryptocurrency transactions and financial flows linked to ransomware, extortion, and hybrid threat-driven cyber-attacks.	CEPOL Europol
Monitoring and investigating cybercriminal recruitment and operational communications on encrypted, anonymised, deep and dark web platforms	CEPOL Europol
Training to enhance awareness of emerging technologies exploited in cybercrime, including blockchain, Artificial Intelligence, quantum computing, malware trends, Internet of Things, deep and dark web, and the metaverse.	CEPOL Europol
Forensic investigation of online legal business structure (LBS) abuse, including identification of digital criminal activity via LBS, evidence collection from online commercial platforms, integration of forensic practices in LBS-related investigations	CEPOL Europol ENFSI
Training on cyber offender prevention strategies, including behavioural pathways to cybercrime and early intervention models such as InterCOP's 4D, approach advanced decryption.	Europol CEPOL
Enhance awareness of relevant legislative frameworks such as the NIS2 Directive.	CEPOL

Counterterrorism	Training providers
Online radicalisation: digital tools to monitor and assess trends, use of AI by law enforcement, how to structure a monitoring tool in MS, sharing of evidence-based practices, countering the online gamification of violent extremism, identification of gaming platforms and psychological manipulation tactics for radicalisation.	CEPOL Europol Frontex
Counterterrorism risk assessment and response to emerging technologies, including Artificial Intelligence, drones, and 3D-printed weapons.	CEPOL Europol

Detection and early risk assessment of lone actors and small autonomous cells, including behavioural indicators.	CEPOL Europol Frontex
Financial investigation techniques in terrorism cases, including crypto-based and informal value transfer systems, the abuse of non-profit organisations, exchange of best practices between Financial Intelligence Units, and building Public Private Partnerships	CEPOL Europol
Forensic readiness for terrorism, including digital evidence collection in terrorism cases, cross-border online intelligence gathering, and coordination with cyber threat intelligence efforts.	CEPOL Europol ENFSI
Cross-border critical infrastructure protection, public-private partnerships, threat assessment, risk assessment, vulnerability assessment, and emerging threats to critical infrastructure	CEPOL Europol
Cross-border monitoring and coordination mechanisms to detect returning foreign fighters and persons involved in terrorist activities, and to build appropriate operational partnerships.	CEPOL Europol Frontex
Detection, containment, and incident management of Chemical, Biological, Radiological and Nuclear e-threats in counterterrorism contexts	CEPOL Europol
Coordination mechanisms for managing the transition of terrorism offenders and radicalised individuals, best practices on the coordination of reintegration.	CEPOL Europol
Assessment tools for detecting radicalisation in detention centres and prisons, including staff awareness and the use of evidence-based models.	CEPOL Europol
EU-level coordination mechanisms and protocols for response to terrorism-related crises	CEPOL Europol
Strategic communication on the prevention of radicalisation, law enforcement, and multi-stakeholder cooperation	CEPOL Europol
Operational use of EU counterterrorism cooperation and information exchange tools, including EU information systems (e.g., SIS) and interoperable components, Europol's information exchange and analytical systems (e.g., SIENA, EIS and PERCI), protocols, reporting standards, and platform engagement (e.g., Internal Referral Units) and Eurojust frameworks (e.g., Counter-Terrorism Register).	CEPOL Europol
Protection and support of victims of terrorism, international victim support mechanisms, cooperation with the European Network of Associations of Victims of Terrorism (NAVT)	Europol
Law enforcement coordination with health services to identify and manage radicalisation linked to mental health vulnerabilities.	Europol

Online fraud schemes (Fastest growing crimes in the online sphere)	Training providers
AI-Enhanced Fraud and Crime-as-a-Service Schemes - Examine how artificial intelligence, deepfake technology, and CaaS tools are revolutionising online fraud, including identity spoofing and scalable scams.	CEPOL Europol

Cryptocurrency tracing and countering money laundering techniques - methods for tracing crypto transactions, identifying laundering patterns, and seizing illicit digital assets used in fraud and underground economies.	CEPOL Europol
Deanonymisation and lawful decryption in online investigations - advanced techniques for unmasking digital identities and conducting lawful decryption to access critical evidence in encrypted environments.	CEPOL Europol
Electronic Evidence and Jurisdiction in Cross-Border Investigations - tools and procedures for accessing electronic evidence across borders, including legal frameworks, such as European Investigation Order, Mutual Legal Assistance, and voluntary disclosures.	CEPOL Europol
Cross-border fraud campaigns and international cooperation: investigation of transnational fraud operations exploiting call centres, virtual infrastructure, and global messaging, with an emphasis on inter-agency and cross-border collaboration.	CEPOL Europol
Artificial Intelligence and Fundamental Rights: the ethical and legal implications of AI in fraud detection, balancing innovation with privacy and fundamental rights.	Europol
Detecting payment fraud in digital and tokenised environments – investigation of fraud schemes targeting digital payment systems, including card-not-present fraud, skimming, mobile wallets, and token-based platforms.	CEPOL Europol
Investigating investment fraud, including fake trading platforms, Ponzi schemes, and social media-based scams - human-targeted fraud schemes involving impersonation, spoofing, and manipulation, with emphasis on psychological tactics and digital traces.	CEPOL Europol
Emerging Fraud Vectors in Fintech and Automated Platforms - new attack surfaces related to fintech innovations, platform automation, mobile payments, and how criminals exploit these ecosystems.	Europol
Investigating Gambling and Investment Platforms Used for Laundering – understanding of how criminals exploit gambling and investment platforms to launder money, and how to disrupt these mechanisms through financial and operational analysis.	CEPOL Europol
Social Engineering Tactics and Fraud Crime Scripts - behavioural patterns, manipulation techniques, and crime scripts commonly used in online fraud, enabling better detection and prevention strategies.	Europol
Monitoring Online Threat Actors and Disrupting Illicit Platforms - techniques and legal instruments for identifying, tracking, and dismantling platforms used by cybercriminals and fraud networks.	CEPOL Europol
Socio-Economic Trends and Fraud Narrative Analysis - Identify emerging fraud themes by analysing societal trends, disinformation, and economic shifts that influence scam evolution and victim behaviour.	Europol

Migrant smuggling	Training providers
Digital investigations, including Open-source intelligence, AI, and social media monitoring, to detect smuggling-related content and dismantle online migrant smuggling networks.	CEPOL Europol Frontex
Financial investigation techniques in migrant smuggling cases, including tracking informal transfer systems such as hawala and cryptocurrency flows.	CEPOL Europol
Detecting and investigating document and identity fraud linked to migrant smuggling, including but not limited to breeder documents, forensics, securing admissible evidence and creating forensic reports.	CEPOL Europol Frontex
Digital forensic tools and procedures, including data security, forensic reporting, and judicial cooperation to ensure the admissibility of evidence.	CEPOL Europol ENFSI
Operational use of EU cooperation tools and databases (e.g., Joint Investigation Teams, Operational Task Forces, SIENA) to support joint investigations and intelligence exchange in migrant smuggling cases.	CEPOL Europol
Investigative methods to detect and dismantle institutionalised or socially embedded support networks (brotherhoods) enabling migrant smuggling and serving as legal organisations to cover organised crime groups.	CEPOL Europol
Migrant smuggling risk assessment, behavioural analysis, document screening with focus on vulnerable persons, including but not limited to minors, interviewing techniques.	CEPOL Europol Frontex
Indicators and investigative linkages between migrant smuggling and trafficking in human beings.	CEPOL Europol Frontex
Techniques, tools, and investigative approaches to detect and counter migrant smuggling conducted through digital platforms and encrypted communication channels.	CEPOL Europol
Instrumentalisation of migration: sources of information and intelligence exchange on smuggling flows; judicial cooperation against state actors involved in the instrumentalisation of migrant smuggling; cooperation with other intelligence services (defence, intelligence, security).	CEPOL Europol
Public-private cooperation in migrant smuggling prevention and detection, including engagement with banks, accommodation providers, and other relevant sectors.	CEPOL Europol
English law enforcement terminology related to migrant smuggling domain.	CEPOL Europol Frontex
Vulnerability risk assessment, identification and management of vulnerable persons, use of trauma-informed approach.	Europol Frontex
Various types of crime as a service: maritime logistics, including but not limited to small boats, chain of supply, rental companies;	Europol

supplying vehicles to smuggling networks, chain of supply, rental companies.	

Online child sexual exploitation (Fastest growing crimes in the online sphere)	Training providers
AI-assisted and digital forensic tools for detecting, analysing, and disrupting online child sexual exploitation, including synthetic child-sexual abuse material and livestreamed abuse.	CEPOL Europol
Emerging child sexual exploitation trends and new investigative technologies, including AI-generated child-sexual abuse material, deepfakes, and grooming in virtual environments.	CEPOL Europol
Forensic approaches to child sexual exploitation (child sexual exploitation), including detection of AI-generated child-sexual abuse material, forensic investigation of live-streamed abuse, online behavioural analysis, trauma-informed handling of digital evidence, and undercover operations in online environments.	CEPOL Europol ENFSI
Cooperation mechanisms with private sector providers and the use of platforms, such as SIRIUS, for intelligence sharing and joint operations.	CEPOL Europol
Financial investigations in child sexual exploitation cases, including tracing payments through cryptocurrencies, symbolic transfers, and informal value transfer systems.	CEPOL Europol
Blockchain analytics for tracing digital financial transactions linked to the production, purchase, or distribution of child-sexual abuse material.	CEPOL Europol
Legal and technical investigative tools to detect grooming and exploitation in gaming platforms, social apps, and immersive digital spaces.	CEPOL Europol
Undercover and proactive investigative methods, including operations in encrypted and dark web environments used for child sexual exploitation.	CEPOL Europol
International cooperation tools and procedures, including Mutual Legal Assistance, for cross-border investigations and real-time data exchange in child sexual exploitation cases.	CEPOL Europol
Victim identification techniques, including tools for analysing anonymised or self-generated child-sexual abuse material and identifying minors.	CEPOL Europol
Offender profiling, risk assessment, and behavioural analysis to support early intervention and targeted child sexual exploitation offender management.	Europol
Trauma-informed, victim-centred law enforcement practices to reduce re-victimisation and support child protection.	Europol
Legal frameworks and ethical standards for AI use in child sexual exploitation investigations, including data protection and evidentiary admissibility.	CEPOL Europol

Excise and customs fraud (Economic and financial crimes)	Training providers
Analysis and sharing of intelligence between tax authorities, Financial Intelligence Units and law enforcement: legal and procedural aspects, compliance with data protection regulations and use of new technologies and tools such as Artificial Intelligence, predictive analytics and machine learning.	Europol Frontex
Cooperation tools and instruments with non-EU countries, international organisations, Interpol, World Customs Organisation; cooperation with the UK, the exchange of information that can be used as evidence in the UK; challenges in obtaining financial intelligence and forensic evidence.	CEPOL Europol Frontex
Available tools for cross-border financial tracking and detection and sharing best practices of using them: trade monitoring, financial oversight, tracking of Excise and customs fraud proceeds laundered through real estate, offshore investment schemes and luxury assets.	CEPOL Europol
Emerging crime patterns and the misuse of legal business structures in excise and customs fraud, including crisis-driven adaptations and sanctions circumvention.	CEPOL Europol
Cross-border special investigation techniques for excise and customs fraud, including surveillance, covert operations, Open-source intelligence, cyber patrolling and digital monitoring tools.	CEPOL Europol
Emerging excise and customs fraud modi operandi, including trends in vapes, novel nicotine products, and designer fuels.	CEPOL Europol Frontex
Money laundering typologies and asset recovery strategies linked to excise and customs fraud, with a focus on cross-border financial flows.	Europol Frontex
Digital investigations: digital tools available, Open-source intelligence, analysis and visualisation of data, presentation of digital evidence in court, cryptocurrencies, cloud storage, Virtual Private Network services, use of Artificial Intelligence.	CEPOL Europol
EU instruments and tools for cross-border cooperation, intelligence sharing and investigations, and their practical application: Art. 31 of the EPPO Regulation, European Investigation Order, Operational Task Forces, Joint Investigation Teams, Anti-Money Laundering Authority, Europol, Eurojust, European Public Prosecutor`s Office, Naples II Convention.	CEPOL EPPO Europol
Awareness raising on the exiting EU framework to tackle evasion of EU sanctions.	Europol
Poly-criminal networks engaged in excise and customs fraud, with a focus on cross-border structures, operations, and disruption strategies.	CEPOL Europol

Tools and methods for tracking and tracing smuggled excisable goods across the EU, the Excise Movement and Control System (EMCS)	CEPOL Europol
Training on harmonised customs laboratory methodologies for detecting excise and customs fraud, with EU-level experience sharing and analytical techniques.	Europol

Trafficking in human beings	Training providers
Detecting and investigating traffickers' use of encrypted communication platforms, the dark web, and hidden online marketplaces	CEPOL Europol
Investigations and prosecutions of all forms of THB (sexual exploitation, child trafficking, labour exploitation, exploitation of forced marriages, of surrogacy and of illegal adoption, and trafficking for organ trafficking., etc.), with emphasis on Open-source intelligence use and crime-type specific approaches.	CEPOL Eurojust Europol
The use of AI tools in THB detection, monitoring, and investigative strategies while addressing risks and safeguards.	Europol
Coordination between national authorities on all forms of exploitation through the exchange of operational best practices.	CEPOL Eurojust Europol
Emerging forms of THB forced criminality: legal, investigative, and victim protection perspectives.	CEPOL Europol
EU cooperation tools and instruments, intelligence-sharing and investigative coordination across jurisdictions.	CEPOL Europol
Cooperation with technology and private sector actors in THB investigations: tools, data sharing, and privacy safeguards.	CEPOL Europol
Digital forensic techniques, including behavioural analysis and footprint tracking, to detect and identify THB victims.	CEPOL ENFSI Europol
Identifying and disrupting operational links between migrant smuggling and human trafficking in investigative and preventive efforts.	CEPOL Europol
Financial investigations within THB: emerging areas, such as cryptocurrencies, work with Asset Recovery Offices; forensic financial investigations targeting informal THB-related economic flows.	CEPOL Europol
Victim identification.	CEPOL EUAA Europol FRA Frontex
Protection of victims: trauma-informed support, victim-centred intervention, child victims, support vulnerable groups, interviewing victims, exchange of best practices, collaborative workshops.	CEPOL EUAA Eurojust Europol FRA

	Frontex

VAT (incl. MTIC) fraud (Economic and financial crimes)	Training providers
EU instruments and tools for cross-border cooperation and investigations, and their practical application: Art. 31 of the EPPO Regulation, European Investigation Order, Operational Task Forces, Joint Investigation Teams, AMLA, Europol, Eurojust, EPPO	CEPOL EPPO Europol
Cross-border financial detection and tracking tools in VAT fraud: trade monitoring, financial oversight, and detection and tracking of illicit assets in real estate, offshore investment schemes and luxury assets.	CEPOL Europol
Cross-border challenges in obtaining financial intelligence and forensic evidence from non-EU countries in MTIC fraud investigations.	CEPOL Europol
Enhancing inter-agency intelligence analysis and sharing in VAT fraud cases between tax authorities, Financial Intelligence Units and law enforcement; legal, procedural, and technological aspects, including data protection, predictive analytics and AI compliance	CEPOL Europol
Digital investigations in VAT fraud: tools available, analysis and visualisation of data, presentation of digital evidence in court, cryptocurrencies, cloud storage and VPN use	CEPOL Europol
Enhancing cooperation between national and EU bodies to prevent and combat cross-border VAT fraud.	
Special investigation techniques for cross-border detection and investigation of transnational criminal groups in VAT fraud: legislation, surveillance and new technologies, covert operations, Open-source intelligence, cyber-patrolling activities	CEPOL Europol
Money laundering as per service in VAT fraud and asset recovery	CEPOL Europol
Identifying and responding to emerging VAT threats and fraud patterns, sharing of bets practices	CEPOL Europol
Transnational prosecutorial and law enforcement cooperation in VAT fraud cases	CEPOL Europol
Different legislations in MS and EU regulations	CEPOL Europol
Poly-criminality links in VAT fraud schemes	Europol
VAT fraud intelligence-sharing across Member States and integration of VAT compliance data into fraud tracking systems	CEPOL Europol

Border management and maritime security	Training providers
Detecting and interdicting drug shipments at land and maritime borders: concealment techniques and modi operandi.	CEPOL Europol Frontex

Border and maritime risk analysis methodologies and vulnerability assessments with the exchange of best practices.	Europol Frontex
Conducting financial investigations at borders and ports: trade-based money laundering and follow-the-money techniques.	Europol
Exchange of best practices on security procedures and inspection standards at EU ports and airports.	Europol
Awareness of the EU legal framework on returns and exchanging best practices for return procedures.	EUAA Europol FRA Frontex
Application of the United Nations Convention on the Law of the Sea, maritime law enforcement jurisdictions across the EU and international sea zones.	
Enhance the detection capacities as well as a harmonised approach in verifying high-risk individuals at external borders.	Europol
Harmonised border screening procedures, practical application of new technologies, ensuring high quality of biometric data.	Eu-LISA Europol Frontex
Use of EU information exchange tools, including the Common Information Sharing Environment (CISE) framework, and information system, including the Entry/Exit System (EES).	Eu-LISA Europol Frontex
Integrated Border Management.	Eu-LISA Europol Frontex
Detecting and mitigating threats from unauthorised unmanned systems near critical maritime infrastructure.	EUAA Europol Frontex
Victim identification and protection at borders: screening refugees, supporting unaccompanied minors, and interviewing procedures.	
Operational training on advanced maritime technologies, including robotics, cybersecurity, and remote sensing.	Frontex
Identifying and addressing environmental offences detected at border checkpoints, including illegal waste or wildlife trafficking.	CEPOL Europol Frontex
Joint simulation exercises on inter-agency coordination in maritime and high-risk border environments.	Frontex
Exchange of best practices and incident-based learning on maritime disaster contingency planning	
Surveillance and protection of ports, pipelines, cables, and other critical maritime infrastructure	
Roles and operational responsibilities of National Coordination Centres under Regulation 1896/2019, Article 21	

Environmental crime	Training providers

Digital investigation techniques in environmental crime, criminal data collection (Open-source intelligence AI-driven intelligence gathering, cyber-patrolling), data analysis, cyber-enabled environmental crime.	CEPOL Europol
Exchanging good practices in investigation and operational tactics for tackling environmental crime such as the use of technical and technological tools (e.g., geospatial intelligence, remote sensing), predictive modelling, satellite monitoring, and data analytics.	CEPOL Europol
Financial investigation techniques in environmental crime cases, financial tracking, and assessment of financial damages.	CEPOL Europol
Modus operandi - waste-related environmental crime, including illegal shipments, disposal, and trafficking practices.	CEPOL Europol Frontex
Modus operandi - pollution-related environmental crime, including water, soil, and air contamination, and trafficked greenhouse gases.	CEPOL Europol Frontex
Awareness and practical use of EU-level law enforcement cooperation mechanisms in environmental crime cases (Joint Investigation Teams, SIENA, I-24/7, Europol, Eurojust).	CEPOL Eurojust Europol
Modus operandi - wildlife crime (CITES, protected animals, plants, illegal logging and timber trade, forest fires, illegal mining, etc.).	CEPOL Europol Frontex
Awareness of better use/exploitation of European enforcement networks, cooperation mechanisms (e.g., EnviCrimeNet, Europol, Eurojust, EU Network for the Implementation and Enforcement of Environmental Law, European Network of Prosecutors for the Environment, EU Forum of Judges for the Environment, Europe Trade in Wildlife Information eXchange).	CEPOL Europol
Anti-corruption training within tax and financial institutions.	Eurojust
Digital forensics in environmental crime investigations and prosecutions.	CEPOL
Use of structured intelligence-sharing frameworks to enhance cooperation between environmental regulators and law enforcement agencies.	CEPOL Europol
Coordination and interface between administrative and criminal investigations in environmental crime enforcement.	CEPOL Europol
Environmental harms linked to illicit synthetic drug production and cannabis cultivation.	CEPOL EUDA Europol
Awareness raising on the work of NGOs, sharing of good practices, and cooperation with NGOs and civil society.	CEPOL Europol
The EU Directive on environmental crime: sharing national experiences and best practices across Member States.	CEPOL Europol
Best practices in multi-agency coordination for environmental disaster response and management.	CEPOL Europol

Firearms and explosive crimes	Training providers

Administrative approach to countering OCGs in the illicit trafficking of firearms and explosives, and the misuse of legal business structures.	CEPOL Europol
New and emerging threats, modi operandi, and typologies in firearms and explosives trafficking, including Privately Made Firearms, such as 3D-printed, converted, and counterfeit weapons, and pyrotechnics.	CEPOL ENFSI Europol Frontex
Changes in modus operandi (false documents, stolen guns, etc), emerging crime patterns and smuggling routes and trends in illicit firearms and explosives trafficking.	CEPOL Europol Frontex
Analysis and sharing of information/intelligence between national law enforcement authorities: legal and procedural aspects, compliance with data protection regulations, and the use of new technologies and innovative tools such as AI, predictive analytics, and machine learning. (Including firearms, explosives and ammunition tracing).	CEPOL Europol
Special investigative techniques applicable at a cross-border level, the relevant legislation, surveillance tools, and EU-level instruments for dismantling transnational firearms trafficking networks.	CEPOL Europol
Cyber-enabled detection and investigation techniques for illicit firearms, ammunition, and explosives trafficking, including activity on online platforms and the dark web.	CEPOL Europol
Investigations into illicit trafficking in firearms and explosives (online, onsite, reactive, proactive, forensic and financial investigations, international cooperation), current, last and emerging threats.	CEPOL ENFSI Europol
Illegal firearms and explosives trafficking as per service for other criminal activities, terrorism, and hybrid threats.	CEPOL Europol Frontex
Acquisition, identification, and exchange of ballistic information using X3P standards and relevant EU systems such as Europol Firearms Hub.	CEPOL Europol
Application of firearms and gunshot residue forensic tools and technologies.	CEPOL ENFSI Europol
Prevention of illicit firearms and explosives trafficking (European response, mechanisms, EMPACT objectives, different models and approaches, cooperation with the private sector, etc.).	CEPOL Europol
Cooperation frameworks, tools, and joint operations with non-EU origin, transit, and destination countries to combat illicit firearms and explosives trafficking.	CEPOL Europol
Public–private cooperation for firearms and explosives detection and control, including coordination with postal, courier, scanning service providers, and manufacturers.	CEPOL Europol
EU legal and policy frameworks governing firearms control and enforcement, including Internal Market Information System modules, the European Firearms Pass, and electronic licensing systems.	CEPOL Europol
Tools and techniques for enhancing law enforcement capabilities in the detection of the illicit trade of firearms and explosives at borders	CEPOL Europol

and inland. This includes exploring the possibilities offered by AI, as well as the use of K9 units, scanners and mobile detection technologies.	
Establishment, legal framework, and good practices related to National Firearms Focal Points.	CEPOL Europol

Hybrid threats	Training providers
Awareness and response training on hybrid threats at EU borders, including detection, coordination with neighbours, and sharing operational best practices.	CEPOL Europol Frontex
Critical infrastructure protection against hybrid, cyber, and sabotage threats, including law enforcement coordination mechanism.	CEPOL Europol
Awareness on detection and disruption of foreign information manipulation and disinformation campaigns tied to hybrid threat strategies.	CEPOL Europol
Awareness of identifying and investigating criminal networks acting on behalf of or in coordination with state-aligned actors in hybrid operations.	CEPOL Europol
Detection and countering of disinformation and hybrid threats that contribute to security destabilisation.	CEPOL Europol
Detection, investigation, and disruption of hybrid threats, including state-aligned and proxy activities.	CEPOL Europol
Sharing good practices on detecting and investigating corruption linked to hybrid threats, and sanction evasions.	Europol
Law enforcement methodologies for responding to politically motivated cyber-attacks on EU infrastructure by state-aligned actors.	CEPOL Europol

Intellectual property crime, counterfeiting of goods and currencies (Economic and financial crimes)	Training providers
Cross-agency coordination: enhancing partnerships between the different law enforcement services and the private sector, especially logistics and shipping companies, when tackling IP crimes.	CEPOL EUIPO Europol
Open-source intelligence and digital investigations: E-commerce; social media platforms; digital evidence; legal considerations with social media providers.	CEPOL EUIPO Europol
Illicit disruption of supply chains: identifying, detecting, and addressing illicit disruptions of supply chains, with particular attention to distribution (e.g., detection and disruption techniques for small parcel shipments and railway freight). Trends, risk assessment tools and methods, non-intrusive scanning, and use of IP Enforcement Portal.	CEPOL EUIPO Europol
Illegal importation methods: detection methods for goods imported from outside the EU and within the EU.	CEPOL EUIPO Europol

Emerging use of artificial intelligence for online marketing and deception: practical skills in identifying and analysing falsified promotional content across websites, social media, and messaging platforms.	EUIPO
Document fraud analysis: understanding overlaps with IP crime, labour exploitation, and document forgery.	EUIPO
Pharmaceuticals: distinguishing legitimate vs illegitimate pharmaceuticals, hotspots, and knowledge-sharing on available surveillance tools.	CEPOL EUIPO Europol
Integrated investigative tools for IP crime: IP Enforcement Portal; multi-disciplinary collaboration.	CEPOL EUIPO Europol
Poly-criminality and business misuse: connections to organised crime groups, use of legal business structures, best practice exchange.	CEPOL EUIPO Europol
Geographical indications (agri-food products): identification, protection strategies, modus operandi of organised crime groups.	CEPOL EUIPO Europol
IP crime tactics in digital spaces: seasonal trends and targeted advertising.	CEPOL EUIPO Europol
Secure collection, handling, and cross-border sharing of admissible evidence in IP crime prosecution.	CEPOL EUIPO Europol
Illegal Internet Protocol Television: prevention and detection, stolen-credentials investigations, collaboration between crime areas groups/units/specialists.	CEPOL EUIPO Europol
Linking IP crime, environmental crime, and related financial investigations (tax evasion, money laundering, etc.).	CEPOL EUIPO Europol
Sharing of criminal intelligence: emphasising multidisciplinary cooperation across sectors and jurisdictions.	CEPOL EUIPO Europol
The importance of packaging and labels in IP investigations, protection of designs at the EU/regional level, and collaboration with rights-holders.	CEPOL EUIPO Europol

External dimensions of internal security	Training providers
CSDP planning and capability development to better address operational realities and new threats. (Strategic and operational preparedness)	CEPOL EEAS
Awareness on EU crisis management expectations, role of law enforcement services, related to external deployments. (Strategic and operational preparedness)	CEPOL EEAS

Design, preparation, and deployment of law enforcement-led specialised teams for civilian CSDP missions. (Strategic and operational preparedness)	EEAS
Integrated threat assessment methodologies and early warning tools for external threats. (Intelligence and threat assessment)	EEAS
Awareness and operational training on integrating climate security and environmental risk adaptation into law enforcement external actions. (Emerging and cross-cutting security areas)	EEAS
Operational use and application of interoperability frameworks and information exchange systems across EU and partner country contexts. (Intelligence and threat assessment)	Eu-LISA
Improve law enforcement readiness and interoperability in Common Security and Defence Policy missions, aligned with NATO and EU frameworks. (Emerging and cross-cutting security areas)	EEAS
Mentoring and advising techniques for law enforcement engagement in partner country reform processes under EU external action. (Partnership and ethical capacities)	CEPOL
Improving operational response and investigative techniques in missing persons cases. (Specific operational priorities)	EEAS
Human rights, gender, and civilian protection in the context of Common Security and Defence Policy and law enforcement external deployments. (Partnership and ethical capacities)	EEAS

Other training needs	Training providers
Core International Crimes	Europol
English law enforcement terminology	CEPOL
Joint training of dog handlers	Frontex
Law enforcement response to kidnapping and extortion	
Leadership and management	CEPOL EUAA Eurojust Europol Frontex
Disaster Victim Identification	

Core capability gaps

Law enforcement cooperation, information exchange and Interoperability
Awareness of EU interoperability components and tools, and their added value in facilitating secure and streamlined access to information necessary for the performance of law enforcement and border management tasks, including the detection of identity misuse.
Ensuring quality and integrity of biometric data in EU information exchange systems: standards, vulnerabilities, and best practices.

Large-scale EU IT information systems, and main interoperability components and tools (e.g. Multiple-Identity Detector (MID), European Search Portal (ESP), Common Identity Repository (CIR), the Central Repository for Reporting and Statistics (CRRS)).
Lawful data collection, handling, and processing in EU information exchange systems, including data protection principles and access rights.
Operational use of Advanced Passenger Information and Passenger Name Record data in border security and law enforcement, including integration, accuracy, and legal frameworks
Preparing end users to effectively access and use existing EU security and migration databases.
Risk assessment procedures using ETIAS, VIS, and other interoperable EU systems to identify potential security threats in visa and ETIAS application processes.
Technical training on operational use and functionalities of large-scale EU information systems (e.g., SIS, VIS, Eurodac, ETIAS).
Follow, catch and seize the proceeds of crime
Asset recovery techniques, tools, legal channels, and cross-border cooperation, multi-agency approach.
Cross-border cooperation tools and techniques, as outlined in Article 31 of the EPPO Regulation.
Cross-border exchange of electronic evidence along with preservation of e-evidence and related legislation.
Deep and dark web investigative techniques, advanced OSINT.
Detecting and disrupting cross-border cash courier networks used to move illicit funds physically requires cross-border cooperation.
Early detection techniques, including identifying red flags and indicators of relevant transfers, revenue or EU expenditure fraud, as well as disruption techniques.
Emerging technologies, including non-financial tokens, peer-to-peer platforms, and pseudonymous tokens.
Enablers and crime-as-a-service; typologies, investigative techniques related to parallel financial systems; operation of shell companies.
Financial and cryptocurrency forensics, including: blockchain analysis, cryptocurrency tracing, cross-chain laundering detection, and forensic investigation of DeFi systems.
Overview of DeFi and money laundering implications.
Regulatory issues: mutual recognition of freezing and confiscation orders; interpretation of "beneficial ownership" and "commercial scale".
Techniques for money mule recruitment include monitoring social media and other online platforms.
Tracing cryptocurrencies (including crypto basics such as typology, crypto forensics for specialists in the financial crime area.

The use of digital tools, AI and new technologies
AI-related risks that impact fundamental rights, discriminatory profiling, surveillance, and data handling.
Application and operational use of AI-assisted capabilities developed for or used by law enforcement agencies.
Awareness for first responders on emerging technologies (e.g., connected vehicles, smart systems) and their forensic relevance in digital crime scenes.
Cross-border intelligence exchange platforms, coordination mechanisms, and secure communication tools.
Digital forensic investigative methodologies; technical knowledge on search, collection and seizure of admissible evidence from next-gen digital infrastructures, forensics in investigating piracy networks; AI-assisted digital forensics (real-time filtering, triage, prioritisation) tools.
Digital investigative techniques and forensic tools related to vehicle theft, including the latest offender methods.
Drone-based threats, operational response frameworks, and counter-drone detection and mitigation systems.
Identification and investigative response to AI-based techniques used in sanction evasion, document fraud, and synthetic identity creation.
Implications and risks of AI use in organisational decision-making and personnel management in law enforcement.
Investigating cyber-enabled fraud and theft involving digital assets, including cryptocurrencies, non-financial tokens, vIBANs, and decentralised financial systems.
Investigative frameworks and available tools to address online-facilitated crimes, including cybercrime-as-a-service and criminal use of encryption.
Lawful decryption techniques and advanced threat intelligence analysis, including handling encrypted communications and devices, digital decryption tools and procedures, legal aspects of decryption in investigations and threats enhanced by AI.
Legal and ethical frameworks (Artificial Intelligence Act, Digital Services Act, GDPR) and the use of AI, restrictions on high-risk or prohibited uses of AI in law enforcement and justice contexts, big data, and quantum technologies by law enforcement and criminals.
OSINT techniques for digital investigations and situational awareness.
Techniques for identifying, accessing, and analysing content on anonymised websites and darknet platforms.
Use of satellite surveillance, predictive modelling, and real-time analytics to identify and respond to evolving security risks.

Forensics
Applications of chemometrics on forensic data.
Audit and risk management for forensic laboratories.

Basic digital forensics, including mobile device forensics, chain of custody and lawful evidence handling, acquisition, analysis, and reporting of digital evidence, and courtroom presentation of forensic findings.
Expression of results, understanding, and application of Likelihood Ratio to forensic evidence.
Innovative tools and technologies for forensic practices across multiple disciplines.
Introduction to Data Science.
ISO 21043 parts 1, 2, 3, 4 and 5.
Synthetic media and AI-generated content forensics, including: deepfake detection, AI-generated evidence analysis, adversarial AI techniques used in fraud and impersonation, and real-time monitoring of AI-driven cyberattacks.
Updated crime scene forensics, including digital trace detection, scene reconstruction using tech-enabled tools.
Use of AI in forensics and investigations (e.g., analysis, legal compliance, generation of evidence and documentation).
Fundamental rights
Cooperation with online platforms to address hate speech while balancing freedom of expression and legal obligations.
Disinformation and fake news: developing counter-narratives to combat online disinformation.
EU-level practices on investigations and prosecutions of hate crime: identifying motivations, sharing good practices at the EU level, case studies, victim support, marginalised groups, special needs of victims, misogynism, discriminatory content targeting children and marginalised groups, basic awareness to sensitise the public, and recognition of biased motivation.
Fundamental Rights and Data Protection: transparency and accountability in data retention, processing, and use but also compliance during surveillance practices.
Identifying and investigating hate crimes and hate speech online, including detection, removal, and the right to be forgotten.
Safeguards in intelligence surveillance and cross-border information exchange: legal and operational perspectives.
Training on EU-level guidance for identifying and addressing discriminatory motives in law enforcement operations.
Victim protection through EU instruments and cross-sectoral cooperation, with emphasis on migration-related vulnerabilities and the new Victims' Rights Directive.
Victims of domestic violence, GBV, trafficking, and terrorism through the lens of Fundamental Rights
Prevention and administrative approach

Application of administrative and regulatory measures to prevent and disrupt organised crime, including licensing, compliance, permit systems, and the use of sanctions, procurement and business-authorisation regimes.
Asset tracing and recovery competencies, including financial oversight, use of legal channels for confiscation, and coordination with administrative controls.
Comprehensive administrative and judicial investigations through coordinated EPPO – OLAF investigations
Community-based and strategic communication approaches to prevention, including cooperation with local authorities and civil society, and targeted awareness-raising and counter-radicalisation initiatives.
Cross-border and judicial cooperation skills, including the use of EU platforms (SIENA, P2P, CISE), mutual legal assistance procedures, and an understanding of different judicial systems for the admissibility of evidence.
Integration of administrative and criminal investigations, ensuring coherent workflows and effective intelligence-sharing between regulatory and law enforcement authorities.
Integrity and anti-corruption safeguards in regulatory, licensing, and inspection functions to prevent misuse or infiltration of public authority.
Multi-agency coordination and information exchange, covering cooperation models between administrative, regulatory, and criminal enforcement bodies, including joint investigations, task forces, and environmental enforcement cooperation.
Risk and vulnerability assessment methods for early detection of emerging threats, protection of critical and public infrastructure, and integration of foresight and hybrid-threat preparedness.
Risk-based inspection, due diligence, and trade-monitoring techniques to detect criminal infiltration of legal business structures, supply chains, and high-risk sectors such as excise goods, chemicals, firearms, and waste.
Barriers to crime, infiltration and corruption
Analysing corruption trends, enablers, and risk patterns in organised crime, using structured analytical and risk assessment tools.
Awareness of using SIENA and P2P platforms for intelligence exchange in corruption and financial crime investigations.
Best practices in detecting and investigating corruption across crime types, including drug trafficking, firearms trafficking, and waste crime, revenue and EU expenditure fraud.
Corruption risk assessments in EU-funded projects involve detecting red flags and identifying sector-specific vulnerabilities.
Detecting, analysing, and investigating corruption in sport, including match-fixing, illegal betting, and governance-related risks.
Financial investigation techniques linked to corruption cases; detection and investigation of the use of emerging financial technologies, such as cryptocurrencies and alternative value transfer methods.

Systems in corruption cases, information exchange with non-EU countries, and cooperation with AMLA.
Internal corruption risks and investigative practices within law enforcement institutions.
Legal and investigative methods for detecting and investigating political corruption, including campaign financing, undue influence, and conflicts of interest.
Legal framework and the new anti-corruption Directive.
Specialised investigative techniques for corruption in high-risk sectors and administrative procedures.
Sharing of corruption detection and investigation best practices in agriculture, infrastructure, healthcare, public procurement, education, construction, and energy sectors.
The use of cultural goods in corruption-linked money laundering schemes.
Use of Joint Investigation Teams and other EU cooperation instruments, use of art. 31 of EPPO Reg. when the EPPO is competent and participating MSs involved, understanding EPPO mandate.

Document fraud
Awareness of the use of fraudulent documents to travel and stay in the EU. Detecting counterfeit and forged documents across countries, sharing information, and developing suitable investigative techniques to tackle forgery. CaaS operations.
Common forgery techniques, document specifications, and verification methods.
Document verification, integrating techniques and the use of different databases.
Effective use of data sharing systems, investigative tools, and awareness of developments in the criminal landscape.
Investigating document fraud networks.
OSINT and financial fraud techniques.
Risk analysis.
Stakeholder engagement, including communication with third parties.
Train the Trainers or multiplier course on identity verification procedures and facial comparison.
Understanding AI technologies and their use in counterfeiting documents.
Visa verification techniques, including security features, and visa counterfeiting modus operandi.

The most threatening criminal networks and individuals
Criminal misuse of AI, including detection of synthetic identities, deepfakes, and automation in criminal operations.
Digital forensics and investigative approaches to encrypted platforms, including decryption strategies and lawful evidence gathering with special regards to the recruitment of your perpetrators.

Emerging platforms and tools employed for recruitment, with a focus on monitoring and the early identification of criminal grooming tactics aimed at young people.
Enablers and crime-as-a-service ecosystems, including document fraud, logistics, and laundering services.
Exploitation of legal businesses and political structures, including the role of EPPO and the application of Article 31 of the EPPO Regulation.
Financial crime investigations linked to the most threatening criminal networks and individuals, including shell companies, cryptocurrency tracing, money laundering techniques, insider facilitation, and typologies of illicit financial flows.
Impact of geopolitical instability and post-conflict dynamics on the evolution, expansion, and recruitment strategies of the most threatening criminal networks.
Investigative best practices and modus operandi of resilient criminal groups, including remote and prison-based leadership models.
OSINT, investigation techniques for encrypted channels and the dark web.
Structural intelligence analysis and cross-border intelligence sharing for mapping and dismantling the most threatening criminal networks.
Structures of criminal groups and reasons for using violence (analysis of different structures, operations of organised crime groups).

Annex 7 Estimated volume of training

The production, trafficking and distribution of cannabis, cocaine and heroin (Drug trafficking)	Number of trainees
Following the crime script, cocaine address detection of cocaine and its intermediate products (chemically concealed cocaine, as well as cocaine base) and the processing and production laboratories.	1317
Financial investigations linked to drug production and trafficking, including tracking proceeds through cryptocurrencies and decentralised platforms.	1005
Gathering and sharing of intelligence on heroin trafficking; tracking and detecting heroin, heroin precursor chemicals; monitoring heroin market shifts and trafficking through alternative smuggling corridors.	1218
Gather and share structured intelligence related to smuggling cannabis through different routes (North America, North Africa, Western Balkans, Italy, Türkiye, Northern and Eastern Europe).	1038
Criminal infiltration into and misuse of legal business structures, the potential role of legal business structures in every stage of the crime script.	867
Investigation of poly-drug trafficking routes, including the use of drugs as currency in exchanges between organised crime groups.	1295
Application of administrative measures and licensing controls to prevent diversion of precursors and legal substances to illicit drug production, in conjunction with a criminal justice approach.	946
Share modi operandi as well as responses to smuggling cannabinoids via postal services/parcels.	1312
Gather and share structured intelligence related to production and emerging product trends of cannabinoids.	1012
Undercover cyber investigations, including social media platforms, darknet and encrypted communication, operation of cyber patrolling teams, and collection of digital evidence.	1198
Countering drug-related violence and youth recruitment by organised crime groups	939

The production, trafficking and distribution of synthetic drugs and new psychoactive substances (Drug trafficking)	Number of trainees
Diversion and trafficking of drugs and precursors, both wholesale and retail, via postal parcels and courier services, courier walls, cooperation between police and customs and the private sector.	1344
Financial investigations linked to drug production and trafficking, including tracking proceeds through cryptocurrencies and decentralised platforms.	1003
Detecting and interdicting illicit synthetic drugs and NPS shipments, including concealment in postal parcels, cargo, and commercial supply chains.	1276
Investigating and dismantling the synthetic drug and NPS production and distribution infrastructure, including labs, transport routes, and waste dump sites	992
Awareness and use of EU information-sharing platforms and cooperation tools in synthetic drug investigations.	1076

Investigating poly-drug trafficking networks and overlapping smuggling routes involving synthetic drugs.	1060
Import, production, diversion, export of licit medicine, to the illicit drug market, e.g., ketamine, tramadol, fentanyl and etomidate, use of legal business structures.	1066
Identifying and reporting on precursor chemical misuse, including regulatory updates and techniques to detect mislabelled substances.	1002
Forensic analysis and interpretation of drug samples; application of innovative tools and technologies for drugs and toxicological analysis and profiling.	860
Application of administrative measures and licensing controls to prevent diversion of precursors and legal substances to illicit synthetic drug production, in conjunction with a criminal justice approach.	946
Undercover cyber investigations, including social media platforms, darknet and encrypted communication, operation of cyber patrolling teams, and collection of digital evidence.	1064
Risks and law enforcement response strategies for synthetic opioids and high-potency stimulants.	1190
Identifying and addressing environmental harms from synthetic drug production: coordination between drug and environmental crime investigators.	911
Understanding different judicial systems and legal frameworks regarding drug trafficking.	1331

Cyber-attacks (Fastest growing crimes in the online sphere)	Number of trainees
Advanced cybercrime forensics, including ransomware forensics, malware analysis, dark web investigations, phishing attack analysis, forensic imaging and device acquisition	918
Emerging cyber threats, including AI-driven attacks, Internet of Things vulnerabilities, decentralised platforms, and quantum-related risks.	1264
Joint training for law enforcement and Computer Security Incident Response Teams on malware investigations, supply-chain attacks, and incident response coordination, involving public–private partnerships.	665
Hybrid threat-linked cyber-attacks.	908
Tracing cryptocurrency transactions and financial flows linked to ransomware, extortion, and hybrid threat-driven cyber-attacks.	662
Monitoring and investigating cybercriminal recruitment and operational communications on encrypted, anonymised, deep and dark web platforms	669
Training to enhance awareness of emerging technologies exploited in cybercrime, including blockchain, Artificial Intelligence, quantum computing, malware trends, Internet of Things, deep and dark web, and the metaverse.	739
Forensic investigation of online legal business structure (LBS) abuse, including identification of digital criminal activity via LBS, evidence collection from online commercial platforms, integration of forensic practices in LBS-related investigations	619

Training on cyber offender prevention strategies, including behavioural pathways to cybercrime and early intervention models such as InterCOP's 4D approach, advanced decryption.	474
Enhance awareness of relevant legislative frameworks such as the NIS2 Directive.	/

Counterterrorism	Number of trainees
Online radicalisation: digital tools to monitor and assess trends, use of AI by law enforcement, how to structure a monitoring tool in MS, sharing of evidence-based practices, countering the online gamification of violent extremism, identification of gaming platforms and psychological manipulation tactics for radicalisation.	539
Counterterrorism risk assessment and response to emerging technologies, including Artificial Intelligence, drones, and 3D-printed weapons.	544
Detection and early risk assessment of lone actors and small autonomous cells, including behavioural indicators.	543
Financial investigation techniques in terrorism cases, including crypto-based and informal value transfer systems, the abuse of non-profit organisations, exchange of best practices between Financial Intelligence Units, and building Public Private Partnerships	672
Forensic readiness for terrorism, including digital evidence collection in terrorism cases, cross-border online intelligence gathering, and coordination with cyber threat intelligence efforts.	460
Cross-border critical infrastructure protection, public-private partnerships, threat assessment, risk assessment, vulnerability assessment, and emerging threats to critical infrastructure	747
Cross-border monitoring and coordination mechanisms to detect returning foreign fighters and persons involved in terrorist activities, and to build appropriate operational partnerships.	1546
Detection, containment, and incident management of Chemical, Biological, Radiological and Nuclear e-threats in counterterrorism contexts	478
Coordination mechanisms for managing the transition of terrorism offenders and radicalised individuals, best practices on the coordination of reintegration.	313
Assessment tools for detecting radicalisation in detention centres and prisons, including staff awareness and the use of evidence-based models.	416
EU-level coordination mechanisms and protocols for response to terrorism-related crises	642
Strategic communication on the prevention of radicalisation, law enforcement, and multi-stakeholder cooperation	290
Operational use of EU counterterrorism cooperation and information exchange tools, including EU information systems (e.g., SIS) and interoperable components, Europol's information exchange and analytical systems (e.g., SIENA, EIS and PERCI), protocols, reporting standards, and platform engagement (e.g., Internal Referral Units) and Eurojust frameworks (e.g., Counter-Terrorism Register).	909

Protection and support of victims of terrorism, international victim support mechanisms, cooperation with the European Network of Associations of Victims of Terrorism (NAVT)	274
Law enforcement coordination with health services to identify and manage radicalisation linked to mental health vulnerabilities.	353

Online fraud schemes (Fastest growing crimes in the online sphere)	Number of trainees
AI-Enhanced Fraud and Crime-as-a-Service Schemes - Examine how artificial intelligence, deepfake technology, and CaaS tools are revolutionising online fraud, including identity spoofing and scalable scams.	1030
Cryptocurrency tracing and countering money laundering techniques - methods for tracing crypto transactions, identifying laundering patterns, and seizing illicit digital assets used in fraud and underground economies.	1340
Deanonymisation and lawful decryption in online investigations - advanced techniques for unmasking digital identities and conducting lawful decryption to access critical evidence in encrypted environments.	979
Electronic Evidence and Jurisdiction in Cross-Border Investigations - tools and procedures for accessing electronic evidence across borders, including legal frameworks, such as European Investigation Order, Mutual Legal Assistance, and voluntary disclosures.	973
Cross-border fraud campaigns and international cooperation: investigation of transnational fraud operations exploiting call centres, virtual infrastructure, and global messaging, with an emphasis on inter-agency and cross-border collaboration.	1031
Artificial Intelligence and Fundamental Rights: the ethical and legal implications of AI in fraud detection, balancing innovation with privacy and fundamental rights.	1281
Detecting payment fraud in digital and tokenised environments – investigation of fraud schemes targeting digital payment systems, including card-not-present fraud, skimming, mobile wallets, and token-based platforms.	1181
Investigating investment fraud, including fake trading platforms, Ponzi schemes, and social media-based scams - human-targeted fraud schemes involving impersonation, spoofing, and manipulation, with emphasis on psychological tactics and digital traces.	1117
Emerging Fraud Vectors in Fintech and Automated Platforms - new attack surfaces related to fintech innovations, platform automation, mobile payments, and how criminals exploit these ecosystems.	875
Investigating Gambling and Investment Platforms Used for Laundering – understanding of how criminals exploit gambling and investment platforms to launder money, and how to disrupt these mechanisms through financial and operational analysis.	1064
Social Engineering Tactics and Fraud Crime Scripts - behavioural patterns, manipulation techniques, and crime scripts commonly used in online fraud, enabling better detection and prevention strategies.	1156

Monitoring Online Threat Actors and Disrupting Illicit Platforms - techniques and legal instruments for identifying, tracking, and dismantling platforms used by cybercriminals and fraud networks.	927
Socio-Economic Trends and Fraud Narrative Analysis - Identify emerging fraud themes by analysing societal trends, disinformation, and economic shifts that influence scam evolution and victim behaviour.	851

Migrant smuggling	Number of trainees
Digital investigations, including Open-source intelligence, AI, and social media monitoring, to detect smuggling-related content and dismantle online migrant smuggling networks.	670
Financial investigation techniques in migrant smuggling cases, including tracking informal transfer systems such as hawala and cryptocurrency flows.	398
Detecting and investigating document and identity fraud linked to migrant smuggling, including but not limited to breeder documents, forensics, securing admissible evidence and creating forensic reports.	1592
Digital forensic tools and procedures, including data security, forensic reporting, and judicial cooperation to ensure the admissibility of evidence.	456
Operational use of EU cooperation tools and databases (e.g., Joint Investigation Teams, Operational Task Forces, SIENA) to support joint investigations and intelligence exchange in migrant smuggling cases.	1528
Investigative methods to detect and dismantle institutionalised or socially embedded support networks (brotherhoods) enabling migrant smuggling and serving as legal organisations to cover organised crime groups.	404
Migrant smuggling risk assessment, behavioural analysis, document screening with focus on vulnerable persons, including but not limited to minors, interviewing techniques.	668
Indicators and investigative linkages between migrant smuggling and trafficking in human beings.	448
Techniques, tools, and investigative approaches to detect and counter migrant smuggling conducted through digital platforms and encrypted communication channels.	541
Instrumentalisation of migration: sources of information and intelligence exchange on smuggling flows; judicial cooperation against state actors involved in the instrumentalisation of migrant smuggling; cooperation with other intelligence services (defence, intelligence, security).	432
Public-private cooperation in migrant smuggling prevention and detection, including engagement with banks, accommodation providers, and other relevant sectors.	384
English law enforcement terminology related to migrant smuggling domain.	1581
Vulnerability risk assessment, identification and management of vulnerable persons, use of trauma-informed approach.	405
Various types of crime as a service: maritime logistics, including but not limited to small boats, chain of supply, rental companies; supplying vehicles to smuggling networks, chain of supply, rental companies.	402

Online child sexual exploitation (Fastest growing crimes in the online sphere)	Number of trainees
AI-assisted and digital forensic tools for detecting, analysing, and disrupting online child sexual exploitation, including synthetic child-sexual abuse material and livestreamed abuse.	590
Emerging child sexual exploitation trends and new investigative technologies, including AI-generated child-sexual abuse material, deepfakes, and grooming in virtual environments.	531
Forensic approaches to child sexual exploitation (child sexual exploitation), including detection of AI-generated child-sexual abuse material, forensic investigation of live-streamed abuse, online behavioural analysis, trauma-informed handling of digital evidence, and undercover operations in online environments.	533
Cooperation mechanisms with private sector providers and the use of platforms, such as SIRIUS, for intelligence sharing and joint operations.	413
Financial investigations in child sexual exploitation cases, including tracing payments through cryptocurrencies, symbolic transfers, and informal value transfer systems.	527
Blockchain analytics for tracing digital financial transactions linked to the production, purchase, or distribution of child-sexual abuse material.	492
Legal and technical investigative tools to detect grooming and exploitation in gaming platforms, social apps, and immersive digital spaces.	661
Undercover and proactive investigative methods, including operations in encrypted and dark web environments used for child sexual exploitation.	464
International cooperation tools and procedures, including Mutual Legal Assistance, for cross-border investigations and real-time data exchange in child sexual exploitation cases.	518
Victim identification techniques, including tools for analysing anonymised or self-generated child-sexual abuse material and identifying minors.	500
Offender profiling, risk assessment, and behavioural analysis to support early intervention and targeted child sexual exploitation offender management.	681
Trauma-informed, victim-centred law enforcement practices to reduce re-victimisation and support child protection.	640
Legal frameworks and ethical standards for AI use in child sexual exploitation investigations, including data protection and evidentiary admissibility.	398

Excise and customs fraud (Economic and financial crimes)	Number of trainees
Analysis and sharing of intelligence between tax authorities, Financial Intelligence Units and law enforcement: legal and procedural aspects, compliance with data protection regulations and use of new technologies and tools such as Artificial Intelligence, predictive analytics and machine learning.	1319
Cooperation tools and instruments with non-EU countries, international organisations, Interpol, World Customs Organisation; cooperation with the	959

UK, the exchange of information that can be used as evidence in the UK; challenges in obtaining financial intelligence and forensic evidence.	
Available tools for cross-border financial tracking and detection and sharing best practices of using them: trade monitoring, financial oversight, tracking of Excise and customs fraud proceeds laundered through real estate, offshore investment schemes and luxury assets.	1099
Emerging crime patterns and the misuse of legal business structures in excise and customs fraud, including crisis-driven adaptations and sanctions circumvention.	943
Cross-border special investigation techniques for excise and customs fraud, including surveillance, covert operations, Open-source intelligence, cyber patrolling and digital monitoring tools.	1027
Emerging excise and customs fraud modi operandi, including trends in vapes, novel nicotine products, and designer fuels.	1241
Money laundering typologies and asset recovery strategies linked to excise and customs fraud, with a focus on cross-border financial flows.	1211
Digital investigations: digital tools available, Open-source intelligence, analysis and visualisation of data, presentation of digital evidence in court, cryptocurrencies, cloud storage, Virtual Private Network services, use of Artificial Intelligence.	1135
EU instruments and tools for cross-border cooperation, intelligence sharing and investigations, and their practical application: Art. 31 of the EPPO Regulation, European Investigation Order, Operational Task Forces, Joint Investigation Teams, Anti-Money Laundering Authority, Europol, Eurojust, European Public Prosecutor`s Office, Naples II Convention.	997
Awareness raising on the exiting EU framework to tackle evasion of EU sanctions.	621
Poly-criminal networks engaged in excise and customs fraud, with a focus on cross-border structures, operations, and disruption strategies.	1046
Tools and methods for tracking and tracing smuggled excisable goods across the EU, the Excise Movement and Control System (EMCS)	959
Training on harmonised customs laboratory methodologies for detecting excise and customs fraud, with EU-level experience sharing and analytical techniques.	594

Trafficking in human beings	Number of trainees
Detecting and investigating traffickers' use of encrypted communication platforms, the dark web, and hidden online marketplaces	602
Investigations and prosecutions of all forms of THB (sexual exploitation, child trafficking, labour exploitation, forced marriages, organ trafficking, exploitation of forced marriages, of surrogacy and of illegal adoption, and trafficking for organ trafficking., etc.), with emphasis on Open-source intelligence use and crime-type specific approaches,	620
The use of AI tools in THB detection, monitoring, and investigative strategies while addressing risks and safeguards.	576

Coordination between national authorities on all forms of exploitation through the exchange of operational best practices.	503
Emerging forms of THB forced criminality: legal, investigative, and victim protection perspectives.	527
EU cooperation tools and instruments, intelligence-sharing and investigative coordination across jurisdictions.	647
Cooperation with technology and private sector actors in THB investigations: tools, data sharing, and privacy safeguards.	429
Digital forensic techniques, including behavioural analysis and footprint tracking, to detect and identify THB victims.	543
Identifying and disrupting operational links between migrant smuggling and human trafficking in investigative and preventive efforts.	658
Financial investigations within THB: emerging areas, such as cryptocurrencies, work with Asset Recovery Offices; forensic financial investigations targeting informal THB-related economic flows.	565
Victim identification.	802
Protection of victims: trauma-informed support, victim-centred intervention, child victims, support vulnerable groups, interviewing victims, exchange of best practices, collaborative workshops.	605

VAT (incl. MTIC) fraud (Economic and financial crimes)	Number of trainees
EU instruments and tools for cross-border cooperation and investigations, and their practical application: Art. 31 of the EPPO Regulation, European Investigation Order, Operational Task Forces, Joint Investigation Teams, AMLA, Europol, Eurojust, EPPO	823
Cross-border financial detection and tracking tools in VAT fraud: trade monitoring, financial oversight, and detection and tracking of illicit assets in real estate, offshore investment schemes and luxury assets.	916
Cross-border challenges in obtaining financial intelligence and forensic evidence from non-EU countries in MTIC fraud investigations.	884
Enhancing inter-agency intelligence analysis and sharing in VAT fraud cases between tax authorities, Financial Intelligence Units and law enforcement; legal, procedural, and technological aspects, including data protection, predictive analytics and AI compliance	926
Digital investigations in VAT fraud: tools available, analysis and visualisation of data, presentation of digital evidence in court, cryptocurrencies, cloud storage and VPN use	929
Enhancing cooperation between national and EU bodies to prevent and combat cross-border VAT fraud.	609
Special investigation techniques for cross-border detection and investigation of transnational criminal groups in VAT fraud: legislation, surveillance and new technologies, covert operations, Open-source intelligence, cyber-patrolling activities	828
Money laundering as per service in VAT fraud and asset recovery	936
Identifying and responding to emerging VAT threats and fraud patterns, sharing of bets practices	886

Transnational prosecutorial and law enforcement cooperation in VAT fraud cases	723
Different legislations in MS and EU regulations	600
Poly-criminality links in VAT fraud schemes	626
VAT fraud intelligence-sharing across Member States and integration of VAT compliance data into fraud tracking systems	758

Border management and maritime security	Number of trainees
Detecting and interdicting drug shipments at land and maritime borders: concealment techniques and modi operandi.	395
Border and maritime risk analysis methodologies and vulnerability assessments with the exchange of best practices.	2407
Conducting financial investigations at borders and ports: trade-based money laundering and follow-the-money techniques.	546
Exchange of best practices on security procedures and inspection standards at EU ports and airports.	3509
Awareness of the EU legal framework on returns and exchanging best practices for return procedures.	3522
Application of the United Nations Convention on the Law of the Sea, maritime law enforcement jurisdictions across the EU and international sea zones.	418
Enhance the detection capacities as well as a harmonised approach in verifying high-risk individuals at external borders.	3383
Harmonised border screening procedures, practical application of new technologies, ensuring high quality of biometric data.	439
Use of EU information exchange tools, including the Common Information Sharing Environment (CISE) framework, and information system, including the Entry/Exit System (EES).	439
Integrated Border Management.	3559
Detecting and mitigating threats from unauthorised unmanned systems near critical maritime infrastructure.	230
Victim identification and protection at borders: screening refugees, supporting unaccompanied minors, and interviewing procedures.	4677
Operational training on advanced maritime technologies, including robotics, cybersecurity, and remote sensing.	283
Identifying and addressing environmental offences detected at border checkpoints, including illegal waste or wildlife trafficking.	322
Joint simulation exercises on inter-agency coordination in maritime and high-risk border environments.	312
Exchange of best practices and incident-based learning on maritime disaster contingency planning	267
Surveillance and protection of ports, pipelines, cables, and other critical maritime infrastructure	253
Roles and operational responsibilities of National Coordination Centres under Regulation 1896/2019, Article 21	1264

Environmental crime	Number of trainees
Digital investigation techniques in environmental crime, criminal data collection (Open-source intelligence AI-driven intelligence gathering, cyber-patrolling) data analysis, cyber-enabled environmental crime.	815
Exchanging good practices in investigation and operational tactics for tackling environmental crime such as the use of technological tools (e.g., geospatial intelligence, remote sensing), predictive modelling, satellite monitoring, and data analytics	784
Financial investigation techniques in environmental crime cases, financial tracking, and assessment of financial damages.	718
Modus operandi - waste-related environmental crime, including illegal shipments, disposal, and trafficking practices.	1385
Modus operandi - pollution-related environmental crimes, including water, soil, and air contamination, and trafficked greenhouse gases.	1130
Awareness and practical use of EU-level law enforcement cooperation mechanisms in environmental crime cases (Joint Investigation Teams, SIENA, I-24/7, Europol, Eurojust).	946
Modus operandi - wildlife crime (CITES, protected animals, plants, illegal logging and timber trade, forest fires, illegal mining, etc.).	1198
Awareness of better use/exploitation of European enforcement networks, cooperation mechanisms (e.g., EnviCrimeNet, Europol, Eurojust, EU Network for the Implementation and Enforcement of Environmental Law, European Network of Prosecutors for the Environment, EU Forum of Judges for the Environment, Europe Trade in Wildlife Information eXchange).	890
Anti-corruption training within tax and financial institutions.	658
Digital forensics in environmental crime investigations and prosecutions.	639
Use of structured intelligence-sharing frameworks to enhance cooperation between environmental regulators and law enforcement agencies.	729
Coordination and interface between administrative and criminal investigations in environmental crime enforcement.	580
Environmental harms linked to illicit synthetic drug production and cannabis cultivation.	770
Awareness raising on the work of NGOs, sharing of good practices, and cooperation with NGOs and civil society.	825
The EU Directive on environmental crime: sharing national experiences and best practices across Member States.	759
Best practices in multi-agency coordination for environmental disaster response and management.	883

Firearms and explosive crimes	Number of trainees
Administrative approach to countering OCGs in the illicit trafficking of firearms and explosives, and the misuse of legal business structures.	333

New and emerging threats, modi operandi, and typologies in firearms and explosives trafficking, including Privately Made Firearms, such as 3D-printed, converted, and counterfeit weapons, and pyrotechnics.	668
Changes in modus operandi (false documents, stolen guns, etc), emerging crime patterns and smuggling routes and trends in illicit firearms and explosives trafficking.	993
Analysis and sharing of information/intelligence between national law enforcement authorities: legal and procedural aspects, compliance with data protection regulations, and the use of new technologies and innovative tools such as AI, predictive analytics, and machine learning. (Including firearms, explosives and ammunition tracing).	486
Special investigative techniques applicable at a cross-border level, the relevant legislation, surveillance tools, and EU-level instruments for dismantling transnational firearms trafficking networks.	379
Cyber-enabled detection and investigation techniques for illicit firearms, ammunition, and explosives trafficking, including activity on online platforms and the dark web.	541
Investigations into illicit trafficking in firearms and explosives (online, onsite, reactive, proactive, forensic and financial investigations, international cooperation), current, last and emerging threats.	637
Illegal firearms and explosives trafficking as per service for other criminal activities, terrorism, and hybrid threats.	742
Acquisition, identification, and exchange of ballistic information using X3P standards and relevant EU systems such as Europol Firearms Hub.	332
Application of firearms and gunshot residue forensic tools and technologies.	381
Prevention of illicit firearms and explosives trafficking (European response, mechanisms, EMPACT objectives, different models and approaches, cooperation with the private sector, etc.).	544
Cooperation frameworks, tools, and joint operations with non-EU origin, transit, and destination countries to combat illicit firearms and explosives trafficking.	448
Public–private cooperation for firearms and explosives detection and control, including coordination with postal, courier, scanning service providers, and manufacturers.	317
EU legal and policy frameworks governing firearms control and enforcement, including Internal Market Information System modules, the European Firearms Pass, and electronic licensing systems.	323
Tools and techniques for enhancing law enforcement capabilities in the detection of the illicit trade of firearms and explosives at borders and inland. This includes exploring the possibilities offered by AI, as well as the use of K9 units, scanners and mobile detection technologies.	894
Establishment, legal framework, and good practices related to National Firearms Focal Points.	460

Hybrid threats	Number of trainees
Awareness and response training on hybrid threats at EU borders, including detection, coordination with neighbours, and sharing operational best practices.	1621
Critical infrastructure protection against hybrid, cyber, and sabotage threats, including law enforcement coordination mechanism.	560
Awareness on detection and disruption of foreign information manipulation and disinformation campaigns tied to hybrid threat strategies.	515
Awareness of identifying and investigating criminal networks acting on behalf of or in coordination with state-aligned actors in hybrid operations.	346
Detection and countering of disinformation and hybrid threats that contribute to security destabilisation.	596
Detection, investigation, and disruption of hybrid threats, including state-aligned and proxy activities.	503
Sharing good practices on detecting and investigating corruption linked to hybrid threats, and sanction evasions.	472
Law enforcement methodologies for responding to politically motivated cyber-attacks on EU infrastructure by state-aligned actors.	419

Intellectual property crime, counterfeiting of goods and currencies (Economic and financial crimes)	Number of trainees
Cross-agency coordination: enhancing partnerships between the different law enforcement services and the private sector, especially logistics and shipping companies, when tackling IP crimes.	695
Open-source intelligence and digital investigations: E-commerce; social media platforms; digital evidence; legal considerations with social media providers.	767
Illicit disruption of supply chains: identifying, detecting, and addressing illicit disruptions of supply chains, with particular attention to distribution (e.g., detection and disruption techniques for small parcel shipments and railway freight). Trends, risk assessment tools and methods, non-intrusive scanning, and use of IP Enforcement Portal.	465
Illegal importation methods: detection methods for goods imported from outside the EU and within the EU.	726
Emerging use of artificial intelligence for online marketing and deception: practical skills in identifying and analysing falsified promotional content across websites, social media, and messaging platforms.	620
Document fraud analysis: understanding overlaps with IP crime, labour exploitation, and document forgery.	795
Pharmaceuticals: distinguishing legitimate vs illegitimate pharmaceuticals, hotspots, and knowledge-sharing on available surveillance tools.	660
Integrated investigative tools for IP crime: IP Enforcement Portal; multi-disciplinary collaboration.	567
Poly-criminality and business misuse: connections to organised crime groups, use of legal business structures, best practice exchange.	472

Geographical indications (agri-food products): identification, protection strategies, modus operandi of organised crime groups.	477
IP crime tactics in digital spaces: seasonal trends and targeted advertising.	669
Secure collection, handling, and cross-border sharing of admissible evidence in IP crime prosecution.	544
Illegal Internet Protocol Television: prevention and detection, stolen-credentials investigations, collaboration between crime areas groups/units/specialists.	666
Linking IP crime, environmental crime, and related financial investigations (tax evasion, money laundering, etc.).	623
Sharing of criminal intelligence: emphasising multidisciplinary cooperation across sectors and jurisdictions.	380
The importance of packaging and labels in IP investigations, protection of designs at the EU/regional level, and collaboration with rights-holders.	1269

External dimensions of internal security	Number of trainees
CSDP planning and capability development to better address operational realities and new threats. (Strategic and operational preparedness)	231
Awareness on EU crisis management expectations, role of law enforcement services, related to external deployments. (Strategic and operational preparedness)	327
Design, preparation, and deployment of law enforcement-led specialised teams for civilian CSDP missions. (Strategic and operational preparedness)	258
Integrated threat assessment methodologies and early warning tools for external threats. (Intelligence and threat assessment)	
Awareness and operational training on integrating climate security and environmental risk adaptation into law enforcement external actions. (Emerging and cross-cutting security areas)	244
Operational use and application of interoperability frameworks and information exchange systems across EU and partner country contexts. (Intelligence and threat assessment)	209
Improve law enforcement readiness and interoperability in Common Security and Defence Policy missions, aligned with NATO and EU frameworks. (Emerging and cross-cutting security areas)	380
Mentoring and advising techniques for law enforcement engagement in partner country reform processes under EU external action. (Partnership and ethical capacities)	157
Improving operational response and investigative techniques in missing persons cases. (Specific operational priorities)	246
Human rights, gender, and civilian protection in the context of Common Security and Defence Policy and law enforcement external deployments. (Partnership and ethical capacities)	361

CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

Read our digital publication
on our website
https://www.cepol.europa.eu/eustna-report

European Union Agency for Law Enforcement Training (CEPOL)
Offices: 1101 Budapest, Üllői út 114-116, Hungary
Email: info@cepol.europa.eu
www.cepol.europa.eu

Find CEPOL on: