CEPOL
EUROPEAN UNION AGENCY FOR
LAW ENFORCEMENT TRAINING

European Union Strategic Training Needs Assessment 2022-2025

Mid-term review

EDUCATE, INNOVATE, MOTIVATE

European Union Agency for Law Enforcement Training - CEPOL
Ó utca 27, 1066 Budapest, Hungary
Tel. +36 1803 8030/8031
Email: info@cepol.europa.eu
www.cepol.europa.eu
Budapest, November 2023

DISCLAIMER
This is a CEPOL document. Its contents do not imply the expression of any opinion whatsoever on the part of CEPOL concerning the training needs listed and elaborated in this document. It reflects the opinions of law enforcement experts from the Member States and EU entities.

ACKNOWLEDGEMENTS
The assistance of those who contributed to this document is hereby acknowledged with gratitude.

More information on the European Union is available on the internet (http://europa.eu).

Photograph: © cover: iStockPhoto.com/incoly

Contents

List of Tables

List of Figures

List of Annexes

List of abbreviations

@ON – Operational Network
ABIS – Analysis Ballistic Information System
AI – Artificial Intelligence
ALEFA – Association of Law Enforcement Forensics Accountants
API – Advanced Passenger Information
ATM – Automatic Teller Machine
CARIN – Camden Asset Recovery Inter-Agency Network
CBRN - Chemical, Biological, Radiological and Nuclear
CEPOL – European Union Agency for Law Enforcement Training
ChatGPT – Chat Generative Pre-Trained Transformer
CIC – Core International Crime
CITES – Endangered Species of Wild Fauna and Flora
CJEU – European Court of Justice
CSDP – Common Security and Defence Policy
DCP – Digital Community Policing
DeFi – Decentralised Finance
DVI – Disaster Victim Identification
ECHR – European Court of Human Rights
ECTC - European Counter Terrorism Centre
EFE – European Firearms Experts
EEAS – European External Action Service
EES – Entry/Exit System
EFCA – European Fisheries Control Agency
EJCN – European Judicial Cybercrime Network
EMCDDA - European Monitoring Centre for Drugs and Drug Addiction
EMCS – Excise Movement and Control System
EMPACT - European Multidisciplinary Platform Against Criminal Threats
EMSA – European Maritime Safety Agency
ENAA - European Network on the Administrative Approach tackling serious and organised crime
ENFPP - European Network for the Protection of Public Figures
ENLETS – European Network of Law Enforcement Technology Services
ENVICRIMNET - European Network for Environmental Crime
EPPO – European Public Prosecutor’s Office
ETIAS – European Travel Information and Authorisation System
EUCARIS - European Car and Driving Licence Information System
EU CULTNET - Informal Enforcement Authorities and Expertise Competent in the field of Cultural Goods
EUIPO - European Union Intellectual Property Office
EU IRU – EU Internet Referral Unit
EUMSS – European Maritime Security Strategy
Eurodac - European Asylum Dactyloscopy Database
Europol – European Union Agency for Law Enforcement Cooperation
Eurojust – European Union Agency for Criminal Justice Cooperation
EU-STNA - European Union Strategic Training Needs Assessment

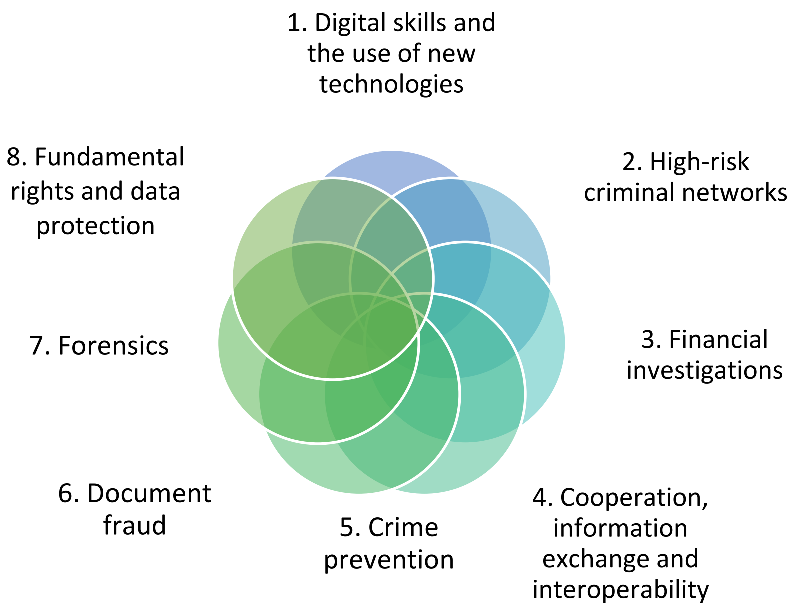
FRA – European Union Agency for Fundamental Rights
Frontex - European Border and Coast Guard Agency
FTF – Foreign Terrorist Fighter
GPS – Global Positioning System
HUMINT – Human intelligence
HRCN – High-risk criminal network
HRD – Human Rights Defender
ICS – Import Control System
INTERPOL – International Criminal Police Organization
IOM – International Organisation for Migration
IP – Intellectual Property
IPR – Intellectual Property Right/s
IT – Information Technology
JHA – Justice and Home Affairs
LE – Law Enforcement
LLM – Large Language Model
MB – Management Board
MOCG – Mobile Organised Crime Group
MS – Member State
MTIC – Missing Trader Intra-Community Fraud
MTR – Mid-Term Review
NATO – North Atlantic Treaty Organization
NGO – Non-Governmental Organisation
NTF – Non-fungible token
NPS – New psychoactive substances
OCG -Organised crime group
OLAF – European Anti-Fraud Office
OSINT – Open-Source Intelligence
PERCI - EU Platform on addressing illegal content online
PoS – Point-of-Sale
PNR – Passenger Name Record
SGBC – Sexual and gender-based crime
SIM – Subscriber Identity Module
SIS – Schengen Information System
SOCTA - Serious and Organised Crime Threat Assessment
SPD – Single Programming Document
TISPOL - European Traffic Police Network
ToT – Train the Trainers
TNA – Training Needs Analysis
UAS – Unmanned Aerial System
UAV - Unmanned Aerial Vehicle
USA – United States of America
UN – United Nations
VoIP - Voice over Internet Protocol
VPN – Virtual Private Network

Executive Summary

As defined by the Article 3 of Regulation 2015/2219[1], the European Union Law Enforcement Training Agency (CEPOL) shall support, develop, implement and coordinate training for Law Enforcement (LE) officials while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of LE, in particular in the areas of prevention of and fight against serious crime affecting two or more Members States (MS) and terrorism, maintenance of public order, international policing of major events, and planning and command of the European Union's Common Security and Defence Policy (CSDP) missions, which may also include training on LE leadership and language skills.

As part of its coordinating role, CEPOL is responsible for the European Union Strategic Training Needs Assessment (EU-STNA) process, which is a collective effort for identifying and prioritising European Union (EU) level strategic training needs in the area of LE. In 2021, CEPOL published the second EU-STNA, which defines the strategic and EU-level training priorities for the four-year cycle (2022-2025) of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). The EU-STNA 2022-2025 revealed eight core capability gaps constituting the main areas in which LE officials need capacity building and established 17 thematic clusters for EU-level priorities where training should be delivered during 2022-2025 to support the EU's response to serious and organised crime and other threats to internal security. The core capability gaps, referring to those horizontal areas that should be reflected in all LE training activities, are the following:

Figure 1. Core capability gaps


1. Digital skills and the use of new technologies
2. High-risk criminal networks
3. Financial investigations
4. Cooperation, information exchange and interoperability
5. Crime prevention
6. Document fraud
7. Forensics
8. Fundamental rights and data protection

During the first half of 2023, on the second year of the EU-STNA cycle, CEPOL conducted a Mid-Term Review (hereinafter also referred to as 'MTR' or 'the review') of the EU-STNA 2022-2025. As a due diligence check on threats and training priorities, 87 documents released after

[1] Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2219&from=EN

the finalisation of the EU-STNA 2022-2025 report were reviewed, and close to 70 stakeholders from nine EU Justice and Home Affairs (JHA) Agencies, the EU Innovation Hub for Internal Security and EU bodies, 12 other partner organisations, and 26 MS[2] were consulted to identify whether new capability challenges and related EU-level training needs have emerged. This report presents the results of the review process.

Overall, the review confirms the validity of the EU-STNA 2022-2025. While the EU-STNA 2022-2025 was prepared during the COVID-19 pandemic, its implementation cycle started with the Russian invasion of Ukraine. The review shows that the core capability gaps remain fully valid in the context of the EU's current security landscape, but reflecting changes in the different crime areas, it suggests a slight update on the EU-level training priorities in terms of the priority order and content of the thematic training areas. Also, the review findings strongly confirm the need and even indicate a potential increase in the importance of the topic of high-risk criminal networks (HRCN) reflected in most training activities.

Table 1. below presents the thematic training areas in the re-prioritised order, as communicated by the MS.

Table 1. Re-prioritisation of thematic training areas

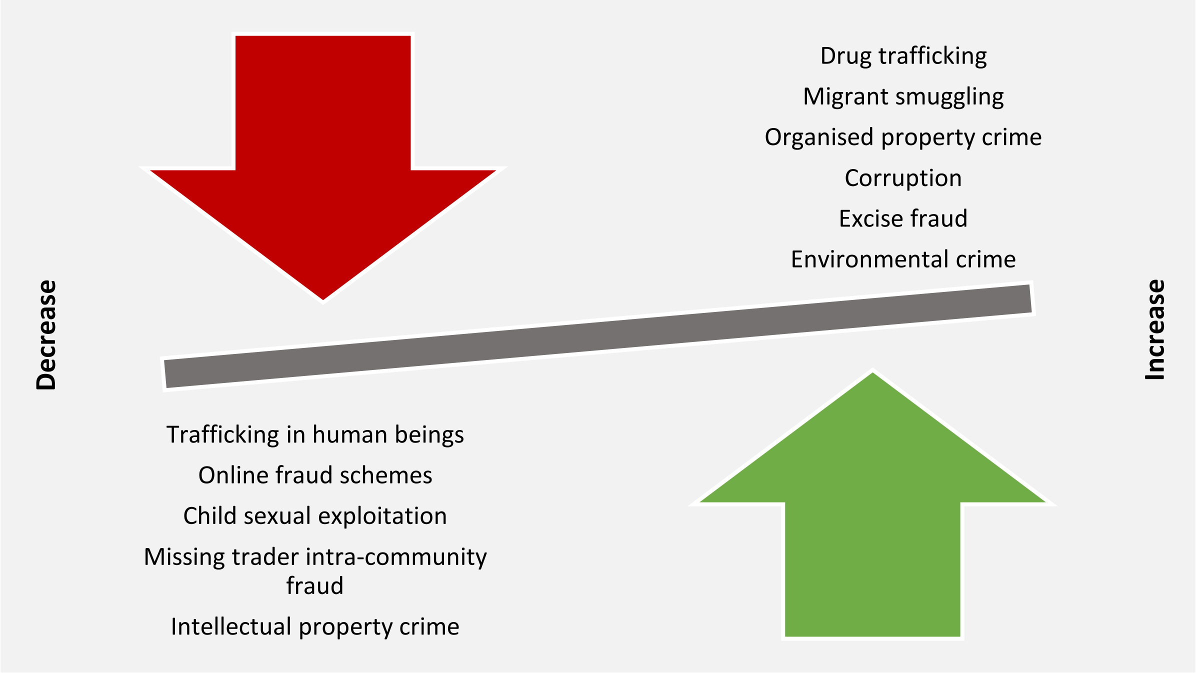
N:o	Topic
1	Cyber-attacks
2	Criminal finances, money laundering and asset recovery (Fraud, economic and financial crimes)
3	Counter-terrorism
4	Drug trafficking
5	Migrant smuggling
6	Trafficking in human beings
7	Online fraud schemes (Fraud, economic and financial crimes)
8	Organised property crime
9	Child sexual exploitation
10	Border management and maritime security
11	Firearms trafficking
12	Corruption
13	Excise fraud (Fraud, economic and financial crimes)
14	Environmental crime
15	Missing trader intra-community fraud (Fraud, economic and financial crimes)
16	Intellectual property crime, counterfeiting of goods and currencies (Fraud, economic and financial crimes)
17	External dimensions of European security

While cyber-attacks; criminal finances, money laundering and asset recovery; and counter-terrorism remain unchanged as the top three EU training priorities, 11 other topics changed their priority ranking. Like the three top priorities, also the topics of border management and maritime security, firearms trafficking, and external dimensions of European security maintained their initial priority placements. Overall, the movement of priorities was moderate, suggesting the need for relatively minor adjustments of the EU training offer.

[2] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, Sweden

Figure 2 below summarises those thematic training areas where the review process proposes a priority update.

Figure 2. Summary of thematic training areas changing priority



The review identified 16 new training needs related to ten thematic training areas and the need to adjust 38 existing training needs on 13 different topics. While the purpose of the mid-term review mechanism is not to disrupt the list of training needs included in the first EU-STNA 2022-2025 report, the review suggests new thematic additions on top of those already identified. Further training needs concern cyber-attacks, counter-terrorism, drug trafficking, migrant smuggling, trafficking in human beings, organised property crime, child sexual exploitation, border management and maritime security, and firearms trafficking.

Many of the new training needs are generated by the war in the EU's immediate neighbourhood. As commonly understood, the war in Ukraine is impacting the security landscape in the EU and at the same time, affecting the EMPACT priority areas in both the short and long term. Adding on top of the training needs identified in the EU-STNA 2022-2025 report, the mid-term review suggests the EU-level LE training to address, e.g. the potential of displaced people or migrant communities' criminal exploitation, as a part of drug trafficking and trafficking in human beings training portfolios. Furthermore, training on organised property crime and training on firearms trafficking should be extended and special attention should be paid to the conflict-borne illicit movement of firearms. A considerable expansion of training requests concerns core international crimes (CIC)[3], where the EU-level LE training should support, among other new training needs, the EU's enhanced role in fighting war crimes and crimes against humanity committed on the territory of Ukraine.

[3] In the EU-STNA 2022-2025, CIC is not considered as a standalone training area, but part of the category 'other'

Despite the war's impact on many crime areas, the highest number of new training needs concerning one training area are related to cyber-attacks, recalling for further emphasis on criminal groups engaging in organised cybercrime, with particular attention on the emerging actors. Training on cybercrime should also address the changing legal framework and its implications for cybercrime investigations. Another new addition in the area is the demand for facilitating strengthened cooperation between civilian, diplomatic and LE cyber communities, which EU-level training could support, e.g. through joint exercises. As a new need, a cybercrime training portfolio should also contribute to developing cyber-, hybrid- and space-related security skills, particularly for the maritime domain. While cyber-attacks already hold central placements as both EMPACT and EU-STNA 2022-2025 training priorities, the review findings re-confirm the need for EU-level LE training providers to continue equipping cybersecurity professionals with skills and competencies required for protecting the EU against cyber threats. The new Cybersecurity Skills Academy established in April 2023[4] shall reinforce this endeavour.

In the area of border management and maritime security, the mid-term review recommends further training emphasis on evolving maritime threats and tackling existing and emerging illicit activities at sea, supporting the operational implementation of the recently adopted, enhanced EU Maritime Security Strategy (EUMSS) and the related Action Plan. Furthermore, training on counter-terrorism recalls the addition of tools to enhance the judicial response to terrorism as a new dimension. New training needs were also identified on the topic of child sexual exploitation, where the review proposes including aspects such as working with traumatised individuals and children, particularly training specialised investigators on conducting vulnerability assessments and raising awareness on the best practices for handling victims of sexual and gender-based crimes (SGBC).

Finally, the mid-term review emphasises that EU LE training providers must continue integrating the relevant aspects of fundamental rights in all training. While other recent studies conducted by CEPOL[5] have indicated the need of an increased attention to fundamental rights, in the mid-term re-ranking of the EU-STNA 2022-2025 training priorities, the contributing MS indicated a slightly decreasing attention to fundamental rights' aspects across the different training areas. However, it must be noted that the mid-term review did not seek for re-prioritisation of the core capability gaps established for the current EU-STNA cycle. Hence, the existing training needs and priorities[6] related to fundamental rights remain valid, with an increased importance on fighting hate crime, and the review findings confirm the importance of EU-level training promoting respect for and building the capacity of rights-based LE in the EU.

[4] Available on: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

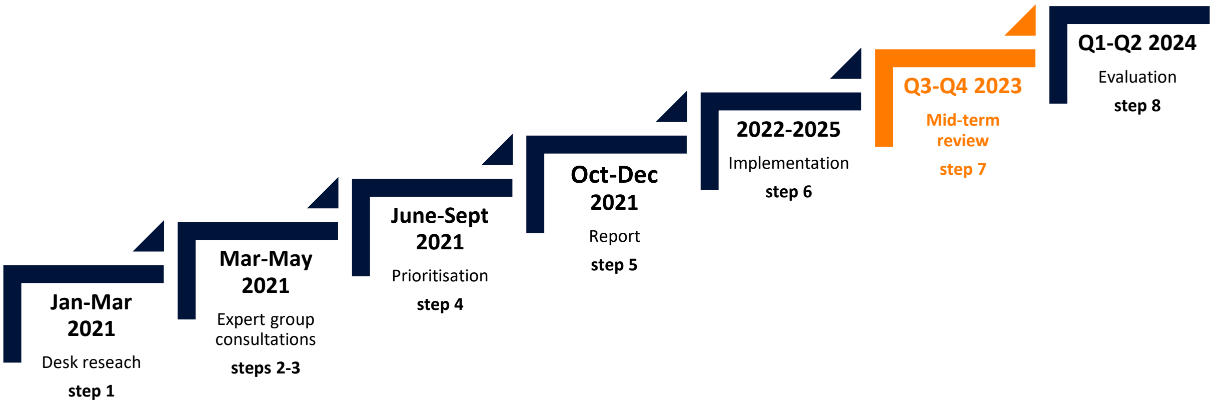
[5] Particularly, the Training Needs Analysis (TNA) report on the impact of the war in Ukraine on the training needs of law enforcement published in 2022, available on: https://www.cepol.europa.eu/training-education/training-needs-analysis/training-needs-analyses

[6] For full details, please see p. 23-25 of the EU-STNA 2022-2025 report, available on: https://www.cepol.europa.eu/documents/eu-stna-report

Introduction

CEPOL is responsible for coordinating the EU-STNA process, which is a multi-stakeholder and multistep exercise conducted for the identification and prioritisation of the EU-level strategic training needs in the area of LE. The overall process starts with desk research involving the analysis of relevant regulations and policy documents and continues by establishing the grounds for profound expert discussions, with the aim of identifying capability gaps and training needs at the EU level. Subsequently, the identified training needs are prioritised by the MS, which also indicate the volume of training needed. Finally, the process findings are published in the EU-STNA Report and presented to the Standing Committee on Internal Security for endorsement and to the European Parliament for information.

Figure 3. Overview of the EU-STNA 2022-2025 methodology and timeline



In 2021, CEPOL published the second EU-STNA, defining the strategic and EU-level training priorities for the four-year (2022-2025) EMPACT cycle. The EU-STNA 2022-2025 process revealed eight core capability gaps constituting the main areas in which LE officials need capacity building through training. These are horizontal areas that should be reflected in all training activities targeting LE, independent of the thematic area, and should therefore be included in the training curricula of EU training providers. Furthermore, 17 thematic clusters (training needs on specific topics) were identified, establishing priorities in which EU-level training should be delivered to LE officials during the four-years' implementation cycle (2022-2025) in order to support the EU's response to serious and organised crime and other threats to internal security.

As per the EU-STNA methodology, due diligence checks on the identified threats and training priorities must be conducted once in each EU-STNA cycle, more specifically, during months 27-30 of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) cycle. The main aim of this mechanism is to ensure that new documents released after the finalisation of the EU-STNA report are considered in the EU-level LE training provision. The review mechanism can also identify possible new initiatives for which no actual capability challenge can be identified (yet), but that will surely necessitate training to allow for their implementation.

For the current EU-STNA 2022-2025, CEPOL conducted the mid-term review during the first half of 2023, and the report presents the outcomes of the process. This introductory section briefly describes the methodology used and the steps taken to complete the process. The second section forms the main body of the report and contains the review results. The third section is devoted to conclusions and recommendations. Finally, annexes include the reviewed documents and stakeholders consulted as a part of the review process and an updated list of EU-level training needs.

Review process and timeline

In practical terms, the due diligence checks on threats and training priorities aim at identifying whether any new capability challenges and related EU-level training needs have emerged. Extending this primary scope of the EU-STNA mid-term review, the process was also used to gain information on training needs that should be addressed at the regional level, support the information needs for the implementation of CEPOL's new strategy[7], and establish that the Agency will also respond to regional training needs and priorities of the MS. The data on regional training needs has been processed as a separate analysis stream, of which results were presented to the CEPOL Management Board (MB) in May 2023; hence, they do not form part of this report.

The findings presented in this report are based on the examination of strategic and policy documents, as well as on consultations with practitioners, experts and stakeholders. Documentation and data used in the review were gathered in a highly consultative manner, including three different online questionnaires programmed by using the Qualtrics® survey tool and addressed to various stakeholder groups.

As the first step of the process, an online survey for the mapping of new documents, emerging capability challenges and related EU-level training needs was prepared and launched. In total, 87 documents containing policy documents, reports and other relevant material issued after the EU-STNA 2022-2025 process were analysed, as part of the desk research feeding into the review of changes in the EU's LE environment and identifying emerging training needs. The complete list of documents reviewed is available in Annex 1. Based on the input from the first two surveys and the desk research, a list of identified training needs was circulated amongst the MS through their designated EU-STNA contact persons, with a clear description of the process, asking the ministerial/political level to prioritise the EU training needs for their country. The list of prioritised training needs was then shared with the agencies for their opinion. Finally, the list, including the opinion of both the agencies and MS, is to be presented to the Commission, as a state of play and potential responsibility sharing among training providers.

The first survey gained **17 individual responses from the Agencies and EU bodies[8].** The second survey with similar content was shared with other relevant partners and resulted in

[7] Available on https://www.cepol.europa.eu/documents/annex-management-board-decision-15-2022-mb

[8] European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA); European Commission (EC); European Union Agency for Law Enforcement

27 contributions from 12 partners, such as specialised networks[9]. In total, 44 responses from those respondents were included in the analysis, feeding into the identification of training needs. **Finally, 26 MS[10]** contributed to the prioritisation of identified and emerging training needs. Table 2. below summarises the number and type of stakeholders consulted during the process[11]. For a complete list of details on the consulted parties, please see Annex 2.

Table 2. Number and type of stakeholder organisations consulted[12]

Type	Number	% of total
European Commission	1	2.1
JHA Agencies	7	14.6
Professional networks	12	25
Other organisations	2	4.2
Member States	26	54.2
Total	**48**	**100,0**

The prioritised list of topics received from the contributing MS was analysed and the overall results checked against the EU-STNA 2022-2025 training priorities, as originally established, which then led to a re-prioritised list of EU-training priorities and training needs on each topic, as described in the next chapter.

Cooperation (Europol); European Union Agency for Asylum (EUAA); European Monitoring Centre for Drugs and Drug Addiction (EMCDDA); European Union Agency for Criminal Justice Cooperation (Eurojust); European Border and Coast Guard Agency (Frontex); European Union Intellectual Property Office (EUIPO); European Union External Action Service (EEAS), EU Agency for Fundamental Rights (FRA)

[9] Operational Network (@ON); Experts in the area of Disaster Victim identification (DVI); European Firearms Experts (EFE); European Judicial Cybercrime Network (EJCN); European Network on the Administrative Approach tackling serious and organised crime (ENAA); European Network of Law Enforcement Technology Services (ENLETS); European Network for the Protection of Public Figures (ENPPF); European Network for Environmental Crime (ENVICRIMENET); Informal enforcement authorities and expertise competent in the field of cultural goods (EU CULTNET); Pan-European Think Thank of football safety and security experts; SIS/SIRENE Committee - Schengen Information System; European Traffic Police Network (TISPOL)

[10] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, Sweden. For those areas not prioritised in this consultation, the priority scores given in the actual EU-STNA 2022-2025 process were applied in the analysis.

[11] Please note that these statistics refer to those parties consulted during the delivery of the analysis. After issuing a draft final report, CEPOL organised a round of consultation during which additional feedback was received from EU Agencies, namely Europol, the EU Innovation Hub, EMCDDA, eu-LISA, EUIPO, FRA, and Frontex.

[12] Data presented at organisation level and not reflecting the distribution of individual responses

Results of the review

This chapter presents the training needs identified and prioritised by the MS in the area of LE that the EU is recommended to address during the second half of the EU-STNA cycle (2024-2025). The first part of the chapter provides an overview of the re-prioritisation of the EU-training priorities. The following thematic subchapters review the changes within each training area in more detail, including a discussion of findings and a detailed summary of re-prioritised training needs. A renewed list of training needs without the change indicators and the related narrative can be found in Annex 3 of this report.

Reviewed EU-training priorities

Overall, the review confirms the validity of the EU-STNA 2022-2025, while the need to adjust the EU training priorities is moderate. Table 3 below suggests an updated ranking of EU training priorities. A column entitled 'change' refers to the difference from the original priority placement initially given in the EU-STNA 2022-2025.[13]

Table 3. Reviewed EU-training priorities

N:o	Topic	Change
1	Cyber-attacks	➡ 0
2	Criminal finances, money laundering and asset recovery (Fraud, economic and financial crimes)	➡ 0
3	Counter-terrorism	➡ 0
4	Drug trafficking	⬆ 1
5	Migrant smuggling	⬆ 1
6	Trafficking in human beings	⬇ -2
7	Online fraud schemes (Fraud, economic and financial crimes)	⬇ -1
8	Organised property crime	⬆ 1
9	Child sexual exploitation	⬇ -2
10	Border management and maritime security	➡ 0
11	Firearms trafficking	➡ 0
12	Corruption	⬆ 1
13	Excise fraud (Fraud, economic and financial crimes)	⬆ 1
14	Environmental crime	⬆ 2
15	Missing trader intra-community fraud (Fraud, economic and financial	⬇ -3
16	Intellectual property crime, counterfeiting of goods and currencies	⬇ -1
17	External dimensions of European security	➡ 0

The top three priorities (cyber-attacks, criminal finances and counter-terrorism) remain unchanged, and the topics of border management and maritime security, firearms trafficking, and external dimensions of European security, maintain their initial ranking.

[13] The yellow arrow means no change and the priority continues unchanged, the green arrow pointing up indicates an increased priority, and the red arrow pointing down shows decreased ranking.

Compared to the original EU-STNA 2022-2025 ranking of priorities, drug trafficking, migrant smuggling, organised property crime, corruption and excise fraud all increased their priority with one rank, and environmental crime with two rank steps. Topics of which the priority was reduced slightly include trafficking in human beings, online fraud schemes, child sexual exploitation, missing trader intra-community fraud and intellectual property crime.

Overall, the movement of priorities was moderate, the most considerable change ranging between +2 and -3 rank positions and in most cases, even less, suggesting a relatively little need for adjusting the EU training offer overall.

Re-prioritised training needs

The following part of this paper describes in greater detail the changes within the different training priorities. Each thematic subchapter summarises the main findings concerning the potential change of priorities, identification of new training needs and/or additions or adjustments introduced to the existing training needs. After a summary of the review findings on each topic, a detailed list of reviewed training needs is presented in re-prioritised order. In the list, a column entitled 'change' refers to the difference compared to the original priority placement identified in the EU-STNA 2022-2025 process in 2021[14].

Cyber-attacks

1

Cyber-attacks remain the highest priority for EU-level training. Changes in the ranking of training priorities within the cyber-attacks domain were moderate; however, the review suggests the addition of **four new training needs**, namely Organised crime groups (OCG) committing cybercrime, e.g the Balkan criminal groups recognised as agile and emerging actors (training priority 11), changing legal framework and its implications to cybercrime investigations (training priority 13); cooperation between civilian, diplomatic and law enforcement cyber communities, joint exercises supporting the building of trust and common understanding (training priority 14) and cyber, hybrid and space-related security skills for the maritime domain (training priority 15). Furthermore, the review identified the need to **expand three of the existing training needs**. These include the latest challenges for dealing with encryption, anonymisation and bulletproof hosting services (priority 2) to also cover ransomware, cryptocurrencies, and the use of the dark web. Similarly, the digital data dimension has been incorporated into priority 3 on identifying, handling, securing, preserving, analysing and exchanging e-evidence. Effective international cooperation, which also slightly increased its priority placement and now establishes priority 4, has been extended to cover mutual operational assistance between the MS, commonly shared and/or interoperable communication tools for secure communication in the cyber field. In the field of cyber defence training, education, situational awareness and exercises, the mid-term review also suggests a strengthened cooperation between the EU and the North Atlantic Treaty Organization (NATO).

[14] The yellow arrow means no change and the priority continues unchanged, the green arrow pointing up indicates an increased priority, and the red arrow pointing down shows decreased ranking.

The following table presents the reviewed list of training needs in the area of cyber-attacks, including the new training needs as re-prioritised by the MS.

Table 4. Prioritised list of training needs – Cyber-attacks

N:o	Training need	Change
1	Investigating cyber-attacks on information systems and modus operandi: analysing latest cyber-attacks and EU emergency response; developing alternative investigation techniques and EU tools, including their use	➡ 0
2	Latest challenges for dealing with encryption, ransomware, cryptocurrencies, anonymisation and bulletproof hosting services and the use of dark web	➡ 0
3	Identifying, handling, securing, preserving, analysing and exchanging digital data and e-evidence	➡ 0
4	Effective international cooperation, including mutual operational assistance between Member States; commonly shared and/or interoperable communication tools for secure communication in the cyber field. Strengthened EU-NATO cooperation in the field of cyber defense training, education, situational awareness and exercises	⬆ 1
5	Protocols to tackle large-scale cyber-attacks	⬆ 1
6	Combatting crime-as-a-service used by criminals and criminal groups in illegal activities	⬇ -2
7	Big data analysis	⬆ 1
8	Raising awareness of cyber-attacks for EU agencies, law enforcement agencies and the public, including a coordinated approach for prevention; cyber-enabled and cyber-dependent crime awareness, cyber threats and cybercrime investigation	⬇ -1
9	Using artificial intelligence, machine learning and deep learning in cybercrime investigation	⬆ 1
10	Blockchain analysis	⬇ -2
11	Organised crime groups (OCG) committing cybercrime, e.g the Balkan criminal groups recognised as agile and emerging actors	☆ 100
12	Cybercriminal profiling and motivation analysis	⬇ -1
13	Changing legal framework and its implications to cybercrime investigations	☆ 100
14	Cooperation between civilian, diplomatic and law enforcement cyber communities, joint exercises supporting building of trust and common understanding	☆ 100
15	Cyber-, hybrid- and space-related security skills for the maritime domain	☆ 100
16	Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection	⬇ -4

Criminal finances, money laundering and asset recovery

2

Criminal finances, money laundering and asset recovery remain the second highest priority for EU-level training. Training needs related to this training area remained largely unchanged as well. The review process **did not uncover completely new training needs,** but it indicates **adjustments concerning four of the existing training needs**. Focus on the modus operandi remains the highest priority and with a slight expansion of topics to be covered such as Chinese underground banking, as a part of training on informal value transfer systems. Training on financial investigations and asset recovery for investigators of other crime areas (priority 3) should cover integrating financial investigations into serious crimes.

The following table presents the reviewed list of training needs in the area of criminal finances, money laundering and asset recovery as re-prioritised by the MS.

Table 5. Prioritised list of training needs – Criminal finances, money laundering and asset recovery

N:o	Criminal finance, money laundering and asset recovery - training needs	Change
1	Modus operandi: existing and emerging crime patterns (non-tangible tokens, new modes of terrorist financing), criminal financing methods: cash-based (cash carriers, money mules) money laundering, money laundering via normal financial system (electronic), offshore challenge to conceal beneficial ownership, informal value transfer systems (e.g. Hawala, Chinese underground banking), underground banking, international money laundering bolstered by fictitious contracts and invoices, trade-based money laundering, money laundering via virtual currencies, and complex financial schemes. Training should also cover money laundering as crime-as-a-service, illegal sale of unlicensed financial services, money laundering via high value goods and services, corporate economic crime and fraud schemes (subsidy fraud, bank fraud, investment fraud, CEO fraud and social benefit fraud)	➡ 0
2	Tracking, tracing, freezing and confiscating assets, opportunities to hide assets quickly, intelligence on criminal turnovers and profits, including training for judicial investigators; application of parallel financial investigations in serious crimes; pre-seizure planning; importance of interlocutory sales	➡ 0
3	Financial investigation and asset recovery for investigators of other crime areas: general basic knowledge on financial investigation and asset recovery, EU/international framework, new EU/international initiatives, directives, rules, tools, multidisciplinary approach, administrative cooperation, role of customs and tax authorities, cooperation with tax authorities and the judiciary; application of integrated financial investigations in serious crimes ; pre-seizure planning; importance of interlocutory sales; management of confiscated assets and social reuse of criminal assets	➡ 0
4	Technicalities and information priorities, technical aspects of investigation, modern technologies, use of AI, big data analysis and Open-Source Intelligence (OSINT), technicality of virtual coins (seizures)	➡ 0
5	Training on cryptocurrencies for general investigators	➡ 0
6	Financial analysis methods and financial forensics	⬆ 1
7	Institutional training addressing a new landscape: implementation of European Public Prosecutor's Office (EPPO) Regulation, roles of EPPO, European Anti-Fraud Office (OLAF), European Union Agency for Law Enforcement Cooperation (Europol), European Union Agency for Criminal Justice Cooperation (Eurojust), European Judicial Cybercrime Network (EJCN) and national authorities. EU directives, tools available at MS and EU level	⬇ -1
8	Cooperation with customs authorities, EU agencies, existing and new instruments, Naples II Convention, administrative customs cooperation mechanisms, Camden Asset Recovery Inter-agency Network (CARIN), Anti-Money Laundering Operational Network (AMON), EGMONT Group of Financial Intelligence Units, Association of Law Enforcement Forensic Accountants (ALEFA), sharing good cooperation practices, information collected by customs (e.g. cash declarations, trade data); cooperation with tax authorities (exchange of	⬆ 1
9	Investigation of crime enablers such as lawyers, financial service providers and real estate agents who knowingly and wittingly provide services to facilitate criminal financial flows	⬇ -1
10	Roles of financial institutions in anti-money laundering, public–private partnership; roles of EU bodies such as the European Court of Justice (CJEU) and European Court of Human Rights (ECHR) in anti-money laundering; case studies on fundamental rights and data protection issues in criminal investigations	➡ 0
11	Roles of the police, tax and customs agencies and the financial sector in prevention/control mechanisms	➡ 0
12	Fundamental rights and data protection	➡ 0

Counter-terrorism

3

Counter-terrorism maintains its place as the third EU training priority. While training needs overall remain largely unchanged and with very little changes in terms of prioritisation, the mid-term review proposes the addition of **one new training need** concerning the tools to enhance the judicial response to terrorism (priority 10). Also, **eight of the existing training needs were slightly adjusted** based on the review findings. Due to the addition of the new training need, the topic of the use of AI by LE shifted down by one rank place, at the same time suggesting that the training take into consideration new dimensions, such as the metaverse threat and the Large Language Models (LLM) currently undergoing rapid advancements and holding potential implications for all industries – including criminal ones.[15] Training on the protection of public spaces and resilience of critical entities, suggests including the cyber domain. In many areas, slight additions were made regarding details to be covered by the training. Training on radicalisation (priority 1) should add a further focus on the victims' and perpetrators' profiles. Priority 3, the use of Open-Source Intelligence (OSINT) in counter-terrorism, has been extended to cover OSINT, the dark web and online undercover operations. Training on the prevention of dissemination, detection and investigation of terrorist content online (priority 4) should cover the Cross-Border Access to Electronic Evidence (SIRIUS) project, co-implemented by Europol and Eurojust, in partnership with the European Judicial Network, and establishes a central reference point in the EU for knowledge sharing on cross-border access to electronic evidence. Similarly, the role of the EU Internet Referral Unit (EU IRU), based at Europol’s European Counter Terrorism Centre (ECTC) that detects and investigates malicious content on the internet and in social media, should be mainstreamed through training. The SIRIUS dimension has also been included in training needs on regional and cross-border cooperation on specific terrorism cases (priority 8). Training related to the foreign terrorist fighter phenomenon (priority 5) should be extended to cover disengagement and exit programmes focusing on reintegration with society, battlefield information exchange, and cumulative prosecutions of foreign terrorist fighters for Core International Crimes (CIC). Based on the review findings, the training need on the use of information systems and cooperation mechanisms in the fight against terrorism (priority 6) has been slightly adjusted, suggesting that capacity development should be provided to multiple LE profiles, including the judiciary, police and intelligence services. Finally, the protection of public spaces and resilience of critical entities (priority 7) now covers new elements, including the overall cyber domain, protection of places of worship, and the use of unmanned aerial vehicles (UAV) used for terrorism purposes.

Finally, while playing an important role in the development and maintenance of the EU’s capacity to prevent and respond to harmful acts of terrorism, training must promote awareness and educate on the protection of fundamental rights and freedoms in counter-terrorism operations.

[15] ChatGPT – the impact of large language models on law enforcement”: https://www.europol.europa.eu/publications-events/publications/chatgpt-report#downloads and “Policing in the metaverse: what law enforcement needs to know” https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

The following table presents the reviewed list of training needs in the area of counter-terrorism, including the new training needs as re-prioritised by the MS.

Table 6. Prioritised list of training needs – Counter-terrorism

N:o	Counterterrorism - training needs	Change
1	Radicalisation: preventing and countering radicalisation that leads to violent extremism and terrorism (with the focus on the victims and perpetrators profiles); new forms of radicalisation; fundamental rights and data protection, including non-discrimination	➡ 0
2	Countering the financing of terrorism: emerging threats, financial links to other types of crime and criminal organisations (e.g. tax fraud, money laundering, illicit trafficking in cultural goods, drugs, small arms and abuse of non-profit organisations); setting up and managing private–public partnerships, modus operandi and new modes of terrorist financing (e.g. crowdfunding platforms, use of crypto assets and bitcoin trading (including use non-fungible tokens (NFT)); collection and use of financial intelligence.	⬆ 1
3	Use of OSINT in counter-terrorism; value of digital evidence; methods of lawful interception; OSINT in the Darkweb. Online undercover Operations (Virtual Agents)	⬇ -1
4	Prevention of dissemination; detection and investigation of terrorist content online; digital trends; use of EU platform to combat illegal content online (PERCI) and implementation of regulation on addressing dissemination of terrorist content online; SIRIUS Project - Cross-Border Access To Electronic Evidence. Role of The EU Internet Referral Unit (EU IRU)	➡ 0
5	Foreign terrorist fighters (FTF), travelling terrorists and returnees; law enforcement approach to family members of foreign terrorist fighters; disengagement and exit programmes(focus on reintegration with society); Battlefield Information Exchange; cumulative prosecutions of FTF's for Core International Crimes	➡ 0
6	Use of information systems and cooperation mechanisms in the fight against terrorism by competent actors from the judiciary, the police and intelligence services	➡ 0
7	Protection of public spaces and resilience of critical entities; sharing best practices on handling attacks including cyber domain; protection of places of worship; use of Drones for terrorism	➡ 0
8	Regional and cross-border cooperation on specific terrorism cases; SIRIUS Project - Cross-Border Access To Electronic Evidence	➡ 0
9	Unmanned aerial vehicles: threats and opportunities for LE	➡ 0
10	Tools to enhance the judicial response to terrorism	☆ 100
11	Use of AI by LE; Metaverse Threat; use of Chat Generative Pre-Trained Transformer (ChatGPT)	⬇ -1
12	Tackling document fraud	➡ 0

Drug trafficking

4

Drug trafficking increased its priority ranking by one step. The mid-term review process indicates that training related to drug trafficking should address the consequences of the war in Ukraine, mitigating the challenge of displaced people or migrant communities at increased risk, both of experiencing drug-related problems and of being vulnerable to exploitation by criminal groups involved in drug production, trafficking, or sales, which now establishes **a new training need** (priority 11). Otherwise, changes concerning the training needs or their priority ranking is moderate. **One training need has been slightly adjusted,** namely, the latest trends and developments in drug production and trafficking (priority 5), now covering the monitoring of fentanyl and other synthetic opioids, due to the vast outbreak in the United States of America (USA).

The following table presents the reviewed list of training needs in the area of drug trafficking, including the new training needs as re-prioritised by the MS.

Table 7. Prioritised list of training needs – Drug trafficking

N:o	Drug trafficking - training needs	Change
1	Drug smuggling: drug trafficking in bulk through EU container ports; online trade in drugs at retail level; increased use of the darknet and social networks including in response to COVID-19; innovations and use of digital technologies in drug trafficking; drug trafficking using postal and parcel delivery services; drug smuggling using alternative maritime distribution modes via pleasure and fishing vessels; tackling digitally-enabled drug trafficking	⇨ 0
2	Criminal networks: business models and modi operandi of organised criminal networks engaged in drug production and trafficking; structure, organisation and specialisation of criminal networks involved in drug trafficking (cannabis, cocaine, heroin, synthetic drugs/NPS and poly-drugs)	⬆ 1
3	Investigation: use of digital investigation tools, OSINT, darknet, decryption, AI, social networks, operational intelligence analysis; training of first responders on synthetic opioid poisoning	⬇ -1
4	Financial investigation related to drug production and trafficking; money laundering and asset recovery in drug cases, including use of sophisticated parallel and multi-layered financial systems; training for judicial investigators and law enforcement	⬆ 1
5	Latest trends and developments in drug production and trafficking: new trends in NPS availability and types; emerging evidence of South Asia's role as producer/supplier of ephedrine and methamphetamine; monitoring situation regarding fentanyls and other synthetic opioids due to the huge break-out in USA changing behavioural trends regarding drug supply and consumption	⬇ -1
6	Drug production: innovative methods using digital technologies; new/innovative technology, sophisticated cannabis cultivation methods (growth, lighting, monitoring); heroin/cocaine conversion and extraction; production of synthetic drugs on an industrial scale; new ways of hiding drug production/production stages	⇨ 0
7	Law enforcement cooperation: global tools for drug monitoring linked to international cooperation, cooperation with non-EU countries	⇨ 0
8	Tackling document fraud, including mislabelling of (pre-)precursors and NPS	⇨ 0
9	Legal challenges and solutions in prosecuting cases related to drugs, precursors and NPS	⬇ -1
10	Forensics	⇨ 0
11	Consequences of the war in Ukraine: mitigating the challenge of displaced people or migrant communities at increased risk both of experiencing drug-related problems and of being vulnerable to exploitation by criminal groups involved in drug production, trafficking or sales.	☆ 100
12	General aviation: definition and legal framework, types of aircraft and characteristics, flight basics, API and PNR, and available monitoring tools	⬇ -1
13	Drugs in prison: increasing capacity of prison staff to better detect drugs entering prisons and to implement evidence-based health-related drug responses within the prison environment	⬇ -1
14	Fundamental rights and data protection	⬇ -1

Migrant smuggling

5

In the reprioritisation process, migrant smuggling gained an increase of one step as an EU-training priority. The results of the mid-term review propose **two new training needs**, suggesting that training on migrant smuggling should pay further attention to the trends and recent developments in the operating tactics of Organised Crime Groups (OGC) involved in migrant smuggling (priority 11) and to the impact of shifts in migrant smuggling routes and the currently active sea entry corridors, such as the Central Mediterranean route, the Western Mediterranean routes and the smuggling corridor from Turkiÿe into Greece changes in Western Balkans route due to Ukrainian war (priority 14). Otherwise, **two of the current training needs have been complemented** by adding new elements identified by the mid-term review, suggesting including lessons learnt from landmark migrant smuggling investigations (priority 1) in training on investigations. Another addition concerns fundamental rights aspects and trust-based approaches to the questioning of migrants (priority 15). Consultations of other EU JHA Agencies[16] also emphasised the continued importance of training migrant smuggling investigators on information exchange (priority 4) and the related large-scale IT systems, particularly the new alerts on e.g. return decisions and/or refusal of entry or stay available in the Schengen Information System (SIS).

The following table presents the reviewed list of training needs in the area of migrant smuggling, including the new training needs as re-prioritised by the MS.

[16] Namely eu-LISA

Table 8. Prioritised list of training needs – Migrant smuggling

N:o	Migrant smuggling - training needs	Change
1	Investigation: sharing best practices, OSINT, ability to respond to the use of digital platforms, social media and mobile applications by criminals, intelligence gathering, decryption, lessons learnt from landmark migrant smuggling investigations	⇨ 0
2	Modus operandi: sham marriages, bogus paternity, false employment contracts, fake invitation letters, false medical visas, and false claims of being victims of trafficking or refugees; use of digital platforms for all phases of migrant smuggling, mass mobilisation for migration, arranging secondary movements, and monitoring law enforcement movements; profiling and behaviour analysis; surveillance including use of drones; use of cryptocurrencies; use of encrypted communication; smuggling techniques	⇨ 0
3	Understanding the operation of organised crime groups	⇨ 0
4	Information exchange: European Asylum Dactyloscopy Database (Eurodac), SIS, role of large-scale IT systems in combatting migrant smuggling under the EMPACT framework	⇨ 0
5	Partnerships and cooperation with non-EU countries: supporting host countries in participating in regional and international cooperation mechanisms that are meant to address migrant smuggling and trafficking in human beings; comprehensive approach (involving consulates, civil registries, etc.)	⬆ 2
6	Improving knowledge on financial models including hawala and money service bureaux, cryptocurrencies, financial investigations and asset recovery	⬇ -1
7	Nexus between migrant smuggling and trafficking in human beings: exploitation of migrants after arrival in the EU	⬇ -1
8	Document and identity fraud with a focus on visa fraud and forged supporting documents; biometrics; networking and support	⇨ 0
9	EU cooperation tools and mechanisms, JITs; cooperation between administrative and law enforcement units and the judicial sector (prosecutors, lawyers and judges)	⇨ 0
10	Dealing with requests concerning unaccompanied minors	⇨ 0
11	Trends and new developments in the operating tactics of OCGs involved in migrant smuggling: particularly operations of e.g. OCGs connected with the Gambia, Mauritania, Morocco and Senegal facilitating illegal travels through the Western Mediterranean routes	☆ 100
12	Procedures and tools used in migration crisis situations	⇨ 0
13	Detecting secondary movements	⬇ -2
14	Impact of shifts in migrant smuggling routes and the currently active sea entry corridors, such as the Central Mediterranean route, the Western Mediterranean routes and the smuggling corridor from Turkÿe into Greece, especially Cyprus, changes in Western Balkans route due to Ukrainian war	☆ 100
15	Fundamental rights, including access to international protection, non-discrimination and data protection; trust-based approaches to the questioning of migrants	⬇ -2

Trafficking in human beings

6

Trafficking in human beings reduced its priority by two rank steps. The review process suggests that the war dimension to human trafficking should be considered as a part of training on the topic, resulting in **one new training need** on the list (priority 10). As a result of the re-prioritisation, some training needs changed their priority ranking, but in terms of content, **other training needs remain** as initially established in the EU-STNA 2022-2025. Similar to migrant smuggling, further introducing the use of SIS in relevant training activities targeted to LE practitioners investigating human trafficking could be beneficial in tackling this type of criminal activity.

The following table presents the reviewed list of training needs in the area of trafficking in human beings, including the new training needs as re-prioritised by the MS.

Table 9. Prioritised list of training needs – Trafficking in human beings

N:o	Trafficking in human beings - training needs	Change
1	Modus operandi of trafficking in human beings, with increased reliance on digital technology, including the online recruitment of minors; different forms of human trafficking and their indicators, including the purpose of exploitation: human trafficking for purposes of sexual exploitation, labour exploitation and forced criminality; psychological and physical violence and drugs used to control and coerce victims	⇨ 0
2	Trafficking for sexual exploitation: modus operandi including online; detection, victim identification, safeguards, support and referral, with a focus on women and	⇧ 1
3	Child trafficking	⇧ 2
4	Business model of human trafficking, including the use of crime-as-a-service as well as the infiltration and use of legal business structures by criminals; links with migrant smuggling networks, with a special focus on non-EU country nationals arriving illegally to the EU and being exploited, in particular vulnerable groups such as unaccompanied minors and women; links to organised property crime, drug trafficking and document fraud	⇩ -2
5	Investigations on the increasing use of digital technology at different stages of trafficking, particularly on encrypted communication and moving assets	⇩ -1
6	Victim identification at borders, by first responders and online (use of OSINT and darknet), with a special focus on vulnerable groups such as women and children	⇨ 0
7	Links to criminal finances and money laundering; financial investigations: tracing, seizing and confiscating criminal proceeds, asset recovery.	⇨ 0
8	Use of existing information and cooperation channels (e.g. Europol, International Criminal Police Organization (Interpol); how to start a JIT; use of large-scale IT	⇨ 0
9	Multidisciplinary and victim-centred approach; working with victims of trafficking for forced criminality such as organised property crime, drug-related crime, etc.;support for reporting; cultural differences; psychological harm to victims influencing their behaviour during investigation; fundamental rights of victims	⇧ 1
10	Human trafficking due to the crisis in Ukraine and the war refugees at high risk of all types of exploitation	☆ 100
11	International cooperation with the United Nations (UN) and International Organisation for Migration (IOM), cooperation with non-EU countries, cooperation with Non-Govermental Organisations (NGO)/institutions providing victim support;	⇩ -2
12	Prevention of human trafficking	⇩ -1
13	Detection of criminal forms of labour exploitation in workplaces	⇩ -1
14	Forensics	⇩ -1

Online fraud schemes

7

The topic of online fraud schemes reduced its priority by two rank positions. Changes in terms of ranking of training needs were relatively moderate, apart from cyber scams, international LE cooperation and high-risk criminal networks gaining one rank position of higher priority, and alternatively, card-not-present fraud, intrusions into system networks of financial institutions, and legal challenges in non-cash payment methods moving one down. Entirely **new training needs were not detected**, but the mid-term review suggests **extending two of the current training needs**. In terms of further training needs, training on cybercrime facilitators recalls for inclusion of Decentralised finance (DeFi) as an emerging model for organising and enabling cryptocurrency-based transactions. On international LE cooperation, training should cover an overview of parallel or linked investigations at the national and international levels.

The following table presents the reviewed list of training needs in the area of online fraud schemes, as re-prioritised by the MS.

Table 10. Prioritised list of training needs – Online fraud schemes

N:o	Online fraud schemes - training needs	Change
1	Cyber scams: online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud, mimic and voice fraud, helpdesk fraud, social engineering	↑ 1
2	Card-not-present fraud: compromise online payments, e-skimming, mobile banking fraud, online payment requests, Subscriber Identity Module (SIM) swapping, smishing, phishing and vishing, e-commerce fraud, carding platforms and darknet marketplaces	↓ -1
3	Cybercrime facilitators: cryptocurrencies including Decentralized finance (DeFi) as an emerging model for organising and enabling cryptocurrency-based transactions, exchanges and financial services, encryption, anonymisation, online forgery, new online tools and digital techniques, use of deepfakes created with AI, money muling	→ 0
4	Card-present fraud: skimming, contactless card fraud, mobile payment fraud	→ 0
5	Cyber threat intelligence, dark web and OSINT	→ 0
6	International LE cooperation, public–private partnership, inter-agency cooperation (cooperation with financial institutions, internet service providers and online platforms); Overview of parallel or linked investigations at national and international levels	↑ 1
7	Intrusions into system networks of financial institutions: banking malware/Point-of-Sale (PoS) malware, logical attacks against Automatic Teller Machines (ATM), use of malware to intercept login details for online banking services	↓ -1
8	Information exchange and cross-border exchange of evidence	→ 0
9	High-risk criminal networks	↑ 1
10	Legal challenges in non-cash payment methods	↓ -1
11	Crime prevention	→ 0
12	Fundamental rights and data protection	→ 0

Organised property crime

8

In the mid-term re-prioritisation, organised property crime moved one rank up. A large majority of training needs within this training area remained unchanged in terms of their priority and contents. However, the war in Ukraine has impacted the related crime area. Hence, the review process suggests adding **a new training need** (priority 14) related to effectively safeguarding cultural property and preserving the movable heritage from looting, illegal excavations and illicit trafficking; illicit trafficking and trade of cultural goods. Without considerably changing the original prioritisation of training needs, the impact of the war also requires some **expansion of two of the existing training** needs to comprehensively cover the fight against the illicit import, export and transfer of ownership of cultural property (priority 5), and expertise building on OSINT within the framework of the illegal trafficking of cultural goods (priority 7).

The following table presents the reviewed list of training needs in the area of organised property crime, including the new training needs, as re-prioritised by the MS.

Table 11. Prioritised list of training needs – Organised property crime

N:o	Organised property crime - training needs	Change
1	Organised burglaries, robberies and thefts and new trends in modus operandi	⇨ 0
2	International investigation, operational cooperation, cross-border observation, best practices, joint investigation teams; communication channels used by criminals (e.g. SKY ECC)	⇨ 0
3	Criminal networks, OCGs, Mobile Organised Crime Groups (MOCG), clans and different roles of members	⇨ 0
4	Fighting vehicle crime: transit, export and trade of stolen vehicles and parts; lease and rental fraud; wrongly registered vehicles; use of EUCARIS; geolocation of vehicles; cooperation with manufacturers to localise vehicles	⇨ 0
5	Fight against the illicit import, export and transfer of ownership of cultural property, resulting from theft from cultural heritage institutions or private collections, looting of archaeological sites and displacement of artefacts: interconnected databases of stolen artefacts, cooperation; identification of cultural goods; legislation from the European countries on the transit of the cultural goods	⇨ 0
6	Financial investigation and asset recovery related to organised property crime	⇨ 0
7	OSINT focused on organised property crime with special focus on OSINT within the framework of the illicit trafficking of cultural goods	↑ 1
8	Tackling theft and attacks on ATMs	↓ -1
9	Fencing, online activities, processes, networks and routes used for stolen goods	⇨ 0
10	Capacity building among cultural heritage experts, including a network of experts that Member States could use within the EMPACT framework	⇨ 0
11	Forensics	⇨ 0
12	Prevention: using the European barrier model for organised property crime; administrative approach	⇨ 0
13	Document fraud; forgery (e.g. knowledge on usual methods) related to cultural goods crime	⇨ 0
14	Due to the war in Ukraine, further needs to effectively safeguard cultural property and preserve the movable heritage from looting, illegal excavations and illicit trafficking, illicit trafficking and trade of cultural goods	☆ 100
15	Fundamental rights and data protection	↓ -1

Child sexual exploitation

9

The topic of child sexual exploitation was de-prioritised by two steps. Two new training needs were identified in the mid-term review process (related to working with traumatised individuals and children, and the victims of sexual and gender-based crimes), now establishing new priorities 10 and 12. Otherwise, **training needs mainly remained unchanged** in terms of both content and priority placements.

The following table presents the reviewed list of training needs in the area of child sexual exploitation, including the new training needs, as re-prioritised by the MS.

Table 12. Prioritised list of training needs – Child sexual exploitation

N:o	Child sexual exploitation - training needs	Change
1	Identifying victims of sexual abuse and exploitation, analysis of big data, images and videos for victim identification purposes; detecting child abuse material	➡ 0
2	Investigation: detecting child abuse material; use of new forensic tools; online undercover operations	➡ 0
3	Use of OSINT and the dark web	➡ 0
4	Developing and applying innovative investigation methods	➡ 0
5	Law enforcement cooperation to tackle child sexual exploitation and abuse cases; joint investigation teams; cooperation between law enforcement and judicial authorities to tackle child sexual abuse and exploitation	⬆ 1
6	Handling encryption and anonymisation services in online child sexual abuse (VPNs, proxy servers, Tor)	⬇ -1
7	Identification of high-risk criminal networks involved in child sexual abuse and exploitation	⬆ 1
8	Financial investigations related to child sexual exploitation cases (online payment methods including virtual currencies)	⬇ -1
9	Tackling gender-related cyber violence against women and girls	➡ 0
10	Working with traumatised individuals and children: specialised training for investigators on conducting vulnerability assessment	☆ 100
11	Victims' rights, offenders' rights, suspects' rights	➡ 0
12	Victims of sexual and gender-based crimes (SGBC): awareness and best practices for questioning potentially traumatised SGBC victims	☆ 100
13	Tools and techniques for mental health/psychological support for law enforcement officers dealing with child abuse	⬇ -2
14	International offender management	⬇ -2

Border management and maritime security

10

Border management and maritime security remain the tenth EU training priority, while two new training needs were identified. Reflecting the update of the EUMSS and its Action Plan[17], adopted in March 2023, the mid-term review process suggests an added training emphasis on evolving maritime threats and creates a new training dimension (priority 12). Another new training need concerns the digitalisation of visa procedures and the related electronic travel systems (priority 6). While the **contents of other training needs remained the same**, training on the EU-level intelligence analysis and information exchange systems (priority 2) should be extended to support the strengthening of cooperation between relevant actors such as customs, financial crime/money laundering experts, police, port security officers and the port authority; and should pay attention on improving the capacity of customs officials to carry out local and contextual risk assessments. Other training needs remained unchanged regarding their contents, but many changed rankings slightly, reflecting the addition of new training needs. During the consultations, Frontex as a centre of excellence for border control activities at the EU's external borders expressed their interest for further interagency training cooperation on border management and maritime security and related topics, which would greatly benefit EU LE training in these areas.

The following table presents the reviewed list of training needs in the area of border management, including the new training needs, as re-prioritised by the MS.

[17] Available on: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1483

Table 13. Prioritised list of training needs – Border management and maritime security

N:o	Border management and maritime security - training needs	Change
1	Identifying cross-border crime and security threats at the border with a focus on foreign terrorist fighters, drugs, smuggling of excise goods, firearms and explosives, signs of environmental crime (at maritime border/in international waters and on land) and trafficking in human beings, with particular attention being paid to victims of trafficking	➡ 0
2	EU-level intelligence analysis and information exchange systems; enhanced cooperation by forming specialist units comprising all relevant actors such as customs, financial crime/money laundering experts, police, port security officers and the port authority, with special emphasis on improving the capacity of customs officials to carry out local and contextual risk assessment	➡ 0
3	Document fraud detection at border crossing points	⬆ 1
4	Common as well as new digitalisation practices (three dimensions: border security, information exchange and humanitarianism)	⬇ -1
5	Cross-border criminal networks	➡ 0
6	Digitalisation of the Schengen visa procedure, Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS) entry into operation, including biometric data	☆ 100
7	Border management in non-EU countries with shared external borders; experience sharing with CSDP missions mandated with border management aspects	⬇ -1
8	Dignified treatment of persons at the border in compliance with principles of non-discrimination, right to liberty, respect for privacy and use of force	⬇ -1
9	Cooperation with Member States and training academies	➡ 0
10	Communication and language skills needed for interactions with those crossing the border	⬇ -2
11	Screening and debriefing	⬇ -1
12	Maritime security: Exchange of information, expertise, technical assistance and best practices on tackling illicit activities at sea; Specialised cross-sectoral maritime security training on law enforcement, military, border control, coast guards, cyber security, protection of critical maritime infrastructure etc.; training programmes open to non-EU partners to tackle existing and emerging threats to maritime security; cross-border investigative capacities between law enforcement and port authorities in SEE and parts of the world where goods are loaded for the region, including Asian and Latin American countries and key trans-shipment nodes such as Italy, Malta and Egypt	☆ 100
13	Access to international protection, prohibition of refoulement, prohibition of collective expulsion and push-backs	⬇ -2
14	Procedural safeguards related to decisions taken at the border	⬇ -2
15	Improving capacity to implement coast guard functions	⬇ -2

Firearms trafficking

11

Firearms trafficking maintains its position as the 11th EU training priority. Like other trafficking-related crime areas, firearms trafficking has been impacted by the conflict in Ukraine, while the mid-term review process confirmed **two new training needs** on the topic. Trafficking of firearms into the EU from conflict countries now establishes a new training need (priority 7) and interlinkages with the other related crime areas (priority 11) appeared as another new addition. While the original EU-STNA 2022-2025 training needs have given a high priority to linkages between firearms trafficking and organised crime and terrorism activities (priority 2), the review process now suggests adding more emphasis also on its multi-dimensional nature and linkages to other crime areas (such as environmental crime, human trafficking, maritime piracy) fuelling firearms trafficking.

Also, **eight training needs were slightly adjusted** based on the review findings. Training on the modus operandi of firearms trafficking (priority 1) should cover kits to assemble firearms traded on online platforms. Priority 2, related to illicit trafficking in weapons linked to organised crime and terrorism and supplying the OCGs with firearms and ammunition from an illegal market, now also concerns the criminal networks specialised in the procurement and (pre-) handling of alarm and signal weapons and other kinds of convertible weapons, as well as Private Made Firearms (PMF) also referred to as "ghost guns". The mid-term review adds further emphasis on the nexus between firearms trafficking and other crime areas such as (but not limited to) drugs trafficking and migrant smuggling in sharing routes and criminal infrastructure, noting its potential linkages to hybrid threats[18] (e.g. threats against critical infrastructure) as well. Since a significant increase has been witnessed in the use of the parcel and postal services to traffic firearms and firearm components, training on online aspects of firearms trafficking (priority 3) should also concern the dimension of postal services. Training on firearms forensics (priority 5), which in the review increased its priority by one step, should also cover aspects such as ballistics, identification of explosives and pyrotechnic devices, and provide training for analysts. Raising awareness of the firearms threat and initiatives to counter illicit firearms production and trafficking (priority 8) should pay attention to countering firearms diversion from the legal supply and cover the firearms technical terms. Related to the best practices for prevention campaigns (priority 9), a new element identified in the review process concerns the role of administrative authorities in firearms crime prevention to target cargo, express and postal consignments before they arrive at the external borders.

The following table presents the reviewed list of training needs in the area of firearms trafficking, including the new training needs, as re-prioritised by the MS.

[18] As highlighted in the Interim report 2023 (not public) of the EU's Serious and Organised Crime Threat Assessment (SOCTA)

Table 14. Prioritised list of training needs – Firearms trafficking

N:o	Firearms trafficking - training needs	Change	
1	Modus operandi: conversion of flobert/gas/alarm/signal weapons into firearms, legislative discrepancies, Western Balkans, conflict areas, trafficking routes, vessels/containers, fast parcel delivery/courier services, 3D printing/self-made, fake/lost/stolen identity documents;kits for assembly of firearms traded on online platforms, fake/lost/stolen identity documents	➡	0
2	Illicit trafficking in firearms linked to organised crime and terrorism; supplying OCGs with firearms and ammunition from an illegal market; criminal networks specialised in the procurement and (pre-) handling of alarm and signal weapons, other kinds of convertible weapons and PMFs; nexus between drugs trafficking, migrant smuggling, and firearms trafficking, in the context of sharing routes and criminal infrastructure	➡	0
3	Online aspects of firearms trafficking: OSINT, dark web, open web, other communication platforms, (e.g. encrypted), and postal services, etc.	➡	0
4	Financial investigations related to firearms trafficking	➡	0
5	Firearms forensics: use of Analysis Ballistic Information System (ABIS) and different systems, forensic evidence, ballistics, identification of explosives and pyrotechnic devices, training for analysts	⬆	1
6	Cooperation with Member States, non-EU countries, international organisations and the private sector	⬇	-1
7	Trafficking of firearms into the EU from post (or active) conflict countries, particularly the current armed conflict in Ukraine facilitating illicit movement of firearms; Advanced knowledge on less known routes and hubs for smuggling of firearms, among other illegal goods, from Ukraine to the EU	☆	100
8	Raising awareness of the firearms threat and initiatives to counter illicit firearms production and trafficking as well as to counter firearms diversion from legal supply; national and international firearms legislation, firearms technical terms	⬇	-1
9	Best practices for prevention campaigns; role of administrative authorities in firearms crime prevention (Use of the customs import control system (ICS/ICS2) to target cargo, express and postal consignments before their arrivals at the external borders).	➡	0
10	Human Intelligence (HUMINT) management in illicit firearms related crime	⬇	-2
11	Related crime areas such as document fraud and corruption; environmental crime	☆	100
12	Fundamental rights and data protection	⬇	-2

Corruption

12

In the review process, the topic of corruption increased in importance. Despite the priority increase, training needs and priorities within this area remained unchanged, suggesting only the swap of priorities 2 and 3. **New training needs were not identified**, and only **one minor addition** has been made **to the existing training** need on promoting anti-corruption strategies, the culture of integrity and integrity testing (priority 9).

The following table presents the reviewed list of training needs in the area of corruption, as re-prioritised by the MS.

Table 15. Prioritised list of training needs - Corruption

N:o	Corruption - training needs	Change
1	“Follow the money” approach/financial investigations following up corruption cases, recovery of assets, corrupt payments in the financial system, cash-based corruption, offshore structures, cryptocurrencies used for making payments to corrupt officials and for money laundering purposes	⇨ 0
2	Recognition/awareness of different forms of corruption (health industry, sports, match-fixing, public procurement, law enforcement, grand corruption, manipulation of digital processes in public administration)	⇧ 1
3	Cooperation between national, EU and international agencies and with judicial professionals, roles of EPPO and OLAF	⇩ -1
4	Investigation and intelligence practices	⇨ 0
5	Corruption as a crime enabler	⇨ 0
6	Sharing expertise, best practices, data and information between the MS and with civil society	⇨ 0
7	Understanding the risks and threats caused by corruption before they materialise into corruption-related crime	⇨ 0
8	Digital skills of law enforcement	⇨ 0
9	Promoting anti-corruption strategies, culture of integrity and integrity testing in law enforcement and other state offices	⇨ 0
10	Internal investigations	⇨ 0
11	Protecting and handling whistleblowers and witnesses	⇨ 0
12	Police ethics	⇨ 0
13	Tackling document fraud	⇨ 0

Excise fraud

13

Excise fraud increased its priority ranking by one step. The mid-term review process did not identify **any substantial changes to the training needs** but suggested some changes regarding the priority order of the training subjects. Training needs that gained importance concern the topics of crime patterns, intelligence and investigation methods, techniques, and tools in the area of alcohol fraud; integration of financial investigation methods into excise fraud investigations accompanied by enhanced asset recovery and big data analysis, and covert surveillance, Global Positioning System (GPS), covert investigation, informant handling practices, interviewing techniques.

The following table presents the reviewed list of training needs in the area of excise fraud, as re-prioritised by the MS.

Table 16. Prioritised list of training needs – Excise fraud

N:o	Excise fraud - training needs	Change
1	Crime patterns, intelligence and investigation methods, techniques and tools in the area of illegal tobacco fraud including illegal cigarette production within the EU, new products, smuggling of cheap whites (Eastern border), maritime contraband (counterfeit cigarettes), waterpipe tobacco, manufacturing equipment and raw tobacco	⇨ 0
2	Crime patterns, intelligence and investigation methods, techniques and tools in the area of mineral oil fraud including designer fuel fraud, fuel laundering, and paying attention to missing traders, with a focus on products and modus operandi through case studies and through deepening knowledge on the entire phenomenon	⇨ 0
3	Crime patterns, intelligence and investigation methods, techniques and tools in the area of alcohol fraud	⇧ 3
4	Integration of financial investigation methods into excise fraud investigation accompanied by enhanced asset recovery and big data analysis	⇧ 1
5	International cooperation (bilateral, multilateral), building trust among law enforcement officials, EU cooperation (OLAF, EPPO, Europol, Eurojust, Frontex); law enforcement (police, customs, tax authorities, border guards, etc.); cooperation at national level, sharing best practices; cooperation with excise industry (tobacco companies, trading companies), in particular tracking and tracing illicit production and tobacco analysis	⇩ -1
6	Use of crime analysis methods	⇩ -3
7	Border control, mobile unit control, customs risk analysis	⇨ 0
8	Means of transport/smuggling: road/land border crossing points, sea, railway, green border	⇨ 0
9	OSINT, online undercover operations on darknet markets, decryption	⇨ 0
10	Covert surveillance, GPS, covert investigation, informant handling practice, interviewing techniques	⇧ 2
11	Common approach to legislation, types of data needed from different MS, ways of sharing and comparing, enforcement of investigation activities in other countries, sharing experience of tackling criminal organisations active in other countries via transnational law enforcement cooperation, case studies on successful investigations	⇩ -1
12	EU legislation and international agreements, Framework Convention on Tobacco Control	⇩ -1
13	External Union transit procedure (T1), transit fraud, abuse of the Excise Movement and Control System (EMCS) (doubling/mirroring legal consignments)	⇨ 0
14	High-risk criminal networks	⇨ 0
15	Tackling document fraud	⇨ 0
16	Good practices on prevention, closely related to control mechanisms	⇨ 0
17	Forensics	⇨ 0

Environmental crime

14

Environmental crime increased its priority placement by two rank positions. However, changes in terms of training needs and priorities are moderate. The mid-term review suggests a slight re-prioritisation of the current training needs and **extending the contents of three of them**. Training on the investigation (priority 2) should cover the monitoring of virtual markets, machine-learning capabilities and dynamic database management. Maritime exploitation and pollution (priority 7) related training, which also suggests increased importance, should also pay attention to preparing for and responding to the effects of climate change and environmental degradation on maritime security. Cooperation (priority 6) should also be extended including environmental inspectorates.

The following table presents the reviewed list of training needs in the area of environmental crime, as re-prioritised by the MS.

Table 17. Prioritised list of training needs – Environmental crime

N:o	Environmental crime - training needs	Change
1	Waste crime (modus operandi, investigation techniques): waste trafficking (hazardous and non-hazardous waste), export and import of waste, dumping at sea, landfills, mixture of waste, disposal, dismantling, waste fires	⇨ 0
2	Investigation: digitalisation, OSINT, monitoring of virtual markets, darknet; collection of intelligence, dealing with whistleblowers; undercover actions, surveillance, wiretapping as part of environmental crime investigation; machine-learning capabilities and dynamic database management	⇨ 0
3	Economic crime investigation techniques, national and international asset recovery to seize gains derived from environmental crime; enhancing the use of financial investigations in environmental crime cases	⇧ 1
4	Criminal infiltration of legal business, system exploitation (e.g. systems relating to renewable energy, recycling, and quotas); crime enablers (e.g. legal experts and technical experts) supporting organised crime	⇩ -1
5	Wildlife crime: emerging patterns, trends, crime groups. Wildlife crime shall cover crime against flora and fauna in line with Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), including illegal logging and timber trade (modus operandi, investigation techniques), trafficking protected species (glass eels, reptiles, mammals, birds), illicit pet trade, etc.	⇧ 1
6	Cooperation: interagency cooperation between different agencies dealing with environmental issues, especially with environmental inspectorates; EU cooperation instruments and networks; cooperation with non-EU countries, global cooperation tools	⇩ -1
7	Maritime exploitation and pollution; illegal, unreported and unauthorised fishing (modus operandi, investigation techniques); preparing for and responding to the effects of climate change and environmental degradation on maritime security	⇧ 2
8	New legislative trends related to the circular economy to help in identifying crime enablers	⇩ -1
9	Related crime areas such as document fraud and corruption	⇩ -1
10	Pollution or illegal exploitation of air, ozone depletion; F-gas Regulation	⇨ 0
11	Administrative tools to combat environmental crime	⇨ 0
12	Raising general public awareness of the costs of environmental crime to society	⇨ 0
13	Role of CSDP missions in spreading good practices and standards in host countries (training for mission personnel as part of pre-deployment training)	⇨ 0
14	Fundamental rights and data protection	⇨ 0

Missing trader intra-community fraud

15

In contrast to the original EU-STNA 2022-2025 prioritisation, missing trader intra-community fraud was re-prioritised three steps below the initial ranking. No new training needs were identified in the review process, and within the training area, the order of training needs remained nearly unchanged compared to the original. As a part of the review process, **one training need has been slightly amended**, namely financial investigations to detect money laundering (priority 3), now also covering financial analysis methods. Also, while the priority ranking concerning missing trader intra-community (MTIC) fraud linkages to other crime areas remains unchanged (priority 5), the review process proposes that on top of addressing the traditional MTIC fraud schemes, training should pay attention to the MTIC fraud linkages to the so-called "white collar" environmental crime, such as illicit waste trafficking and unlawful importing or exporting of used vehicles to/from the European Union's territories.

The following table presents the reviewed list of training needs in the area of missing trader intra-community fraud, as re-prioritised by the MS.

Table 18. Prioritised list of training needs – Missing trader intra-community fraud

N:o	Missing trader intra-community fraud - training needs	Change
1	Modus operandi: organised crime groups specialised in offering fake invoices; financial flows and schemes used for Missing trader intra-community fraud (MTIC) fraud; exploitation of legal structures, versatility, adaptability to new trends and specialised advising	⇨ 0
2	Investigation: intelligence-led investigation focusing on transnational organised crime; operational cooperation; sharing best practices	⇨ 0
3	Financial investigations to detect money laundering; financial analysis methods	⇨ 0
4	Technology and digital infrastructure as essential components in concealing and facilitating criminal activities (data storage, alternative payment methods, Virtual Private Network (VPN) services, encryption, Voice over Internet Protocol (VoIP) fraud)	⇨ 0
5	Links to other crime areas, such as environmental crime	⇨ 0
6	Tax confidentiality issues at EU level in the context of information exchange	⇨ 0
7	Raising awareness of MTIC fraud among the judiciary and the public	⇨ 0
8	Data analysis and data protection	⇨ 0
9	Tackling document fraud	⇧ 1
10	Forensics	⇩ -1
11	Crime prevention	⇨ 0

Intellectual property crime, counterfeiting of goods and currencies

16

Intellectual property crime, counterfeiting goods and currencies moved one place down in the re-prioritisation of training areas. Desk review for the mid-term review **did not expose considerable new training needs** but suggested adjusting **two** existing ones. The original training need of digital investigation techniques and cyber patrolling has been extended to cover investigations of intellectual property crime cases more comprehensively (priority 3).

Financial investigations (priority 9), which also increased their ranking by one step, now contain the ENLETS cryptocurrency network. The review process reminds that intellectual property (IP) crime is being increasingly linked to organised crime and other serious criminal offences, including in the online dimension, and training in this thematic area should consider the interlinked nature of such criminality. The process of consultations with other EU agencies resulted in a proposal that training on cyber patrolling (patrols conducted on the internet) should consider covering intellectual property right (IPR) cases, counterfeit detecting canines and their handlers, and when relevant, educate on using new technological tools and/or techniques.

The following table presents the reviewed list of training needs in the area of intellectual property crime and counterfeiting of goods and currencies, as re-prioritised by the MS.

Table 19. Prioritised list of training needs – Intellectual property crime, counterfeiting of goods and currencies

N:o	Criminal finance, money laundering and asset recovery - training needs	Change
1	Modus operandi: existing and emerging crime patterns (non-tangible tokens, new modes of terrorist financing), criminal financing methods: cash-based (cash carriers, money mules) money laundering, money laundering via normal financial system (electronic), offshore challenge to conceal beneficial ownership, informal value transfer systems (e.g. Hawala, Chinese underground banking), underground banking, international money laundering bolstered by fictitious contracts and invoices, trade-based money laundering, money laundering via virtual currencies, and complex financial schemes. Training should also cover money laundering as crime-as-a-service, illegal sale of unlicensed financial services, money laundering via high value goods and services, corporate economic crime and fraud schemes (subsidy fraud, bank fraud, investment fraud, CEO fraud and social benefit fraud)	⇨ 0
2	Tracking, tracing, freezing and confiscating assets, opportunities to hide assets quickly, intelligence on criminal turnovers and profits, including training for judicial investigators; application of parallel financial investigations in serious crimes; pre-seizure planning; importance of interlocutory sales	⇨ 0
3	Financial investigation and asset recovery for investigators of other crime areas: general basic knowledge on financial investigation and asset recovery, EU/international framework, new EU/international initiatives, directives, rules, tools, multidisciplinary approach, administrative cooperation, role of customs and tax authorities, cooperation with tax authorities and the judiciary; application of integrated financial investigations in serious crimes ; pre-seizure planning; importance of interlocutory sales; management of confiscated assets and social reuse of criminal assets	⇨ 0
4	Technicalities and information priorities, technical aspects of investigation, modern technologies, use of AI, big data analysis and Open-Source Intelligence (OSINT), technicality of virtual coins (seizures)	⇨ 0
5	Training on cryptocurrencies for general investigators	⇨ 0
6	Financial analysis methods and financial forensics	⇧ 1
7	Institutional training addressing a new landscape: implementation of European Public Prosecutor's Office (EPPO) Regulation, roles of EPPO, European Anti-Fraud Office (OLAF), European Union Agency for Law Enforcement Cooperation (Europol), European Union Agency for Criminal Justice Cooperation (Eurojust), European Judicial Cybercrime Network (EJCN) and national authorities. EU directives, tools available at MS and EU level	⇩ -1
8	Cooperation with customs authorities, EU agencies, existing and new instruments, Naples II Convention, administrative customs cooperation mechanisms, Camden Asset Recovery Inter-agency Network (CARIN), Anti-Money Laundering Operational Network (AMON), EGMONT Group of Financial Intelligence Units, Association of Law Enforcement Forensic Accountants (ALEFA), sharing good cooperation practices, information collected by customs (e.g. cash declarations, trade data); cooperation with tax authorities (exchange of information and intelligence on missing traders)	⇧ 1
9	Investigation of crime enablers such as lawyers, financial service providers and real estate agents who knowingly and wittingly provide services to facilitate criminal financial flows	⇩ -1
10	Roles of financial institutions in anti-money laundering, public–private partnership; roles of European Union Agency for Fundamental Rights Agency (FRA), European Court of Justice (CJEU) and European Court of Human Rights (ECHR) in anti-money laundering; case studies on fundamental rights and data protection issues in criminal investigations	⇨ 0
11	Roles of the police, tax and customs agencies and the financial sector in prevention/control mechanisms	⇨ 0
12	Fundamental rights and data protection	⇨ 0

External dimensions of European security

17

The external dimensions of European security remain in their original position as the 17th EU training priority. The review conducted did **not identify new training needs** but suggested some re-prioritisations of the existing training topics within this area. As the highest priority, training should contribute to the development and implementation of existing concepts regarding, e.g. evaluation, analysis, benchmarking and operational impact assessments, identification of best practices and the use of lessons learned in missions' planning, management, and review. The same applies to the mainstreaming of the integrated approach, strategic cooperation and local ownership in the planning and conduct of the Union's missions. Other topics that increased their priority ranking concern the continued development of civil-military cooperation, the EU's global actorness, and the role as a security provider through the Common Civilian and Defence Policy (CSDP) Missions, and the strengthening of the advisory capacity of those.

The following table presents the reviewed list of training needs in the area of external dimensions of European security, as re-prioritised by the MS.

Table 20. Prioritised list of training needs – External dimensions of European security

N:o	External dimensions of European security - training needs	Change
1	Enhancing the support, development and policy implementation of existing concepts regarding evaluation, analysis, benchmarking and operational impact assessments, identification of best practices and use of lessons learned in missions' planning, management and review; more integrated approach, EU and beyond, to programming strategic cooperation (consultations, concept development, planning, assessments and evaluation) and local ownership	↑ 2
2	Leadership in CSDP missions, planning and command, change management in host country	↓ -1
3	The EU's role as a security provider through CSDP, including CSDP policy on strategic ambitions and capability limitations	↑ 1
4	Pre-deployment training	↓ -2
5	Analytical, planning and decision-making structures and procedures	→ 0
6	Building advisory capacity of CSDP missions	↑ 2
7	Knowledge and expertise in CSDP relevant structures and missions regarding the rule of law, criminal justice, anti-corruption, and policing in line with international human rights standards	↓ -1
8	Role of CSDP missions in supporting EU internal security (external dimension of internal security)	↓ -1
9	Civil-military cooperation and its conceptual development	↑ 2
10	Language training: English communication skills; French as a foreign language	↓ -1
11	Association of non-EU countries to EMPACT and counter-terrorism activities, providing capacity building to partner states, in particular neighbouring and enlargement countries, so as to support operational cooperation with EU Member States and agencies as well as to provide partners with adequate tools (e.g. digital ecosystems and information on how to adopt national legislative reforms and adhere to international standards)	↓ -1
12	Political, economic and budgetary aspects of cooperative projects in defence and security within the framework of CSDP	→ 0
13	Digital skills of law enforcement	→ 0
14	Duty of care in CSDP missions	→ 0
15	High-risk criminal networks	↑ 1
16	JHA actors; identifying and disseminating best practices; cooperation and exchange of information in Western Balkans to ensure uniform and efficient application of EU law for EU membership	↓ -1
17	Tackling document fraud	→ 0
18	Crime prevention	→ 0

Other training needs

18

Other training needs covers those specific training needs that fall outside the scope of the actual 17 thematic areas presented above. The mid-term review process did not uncover considerable new training needs to be added under this category, and the ranking of training needs remains mostly unchanged, except for the increased and expanded need for training on topics related to public order (priority 2) and the slightly lower attention towards language training (priority 4). Despite the reduced priority of providing education in the English language, the review suggests a potential need to add other languages, particularly Arabic, into the EU-level LE training offer. Regarding training content, the most notable changes concern the topics of public order (priority 2) and even more, CIC (priority 6). Related to public order, the review identified the need to add the online dimension of community policing, suggesting the need for training on digital community policing (DCP). Also, as a new aspect of counter-drone measures, training should cover the concept of U-space, the European system developed for managing unmanned aerial systems (UAS) traffic, and the new EU rules on dedicated airspace for drones.

While the ranking remained unchanged, the review process suggests a considerable expansion of training supporting the action towards accountability for core international crimes (CICs) and human rights violations. With full details given in the list below (Table 21), new training needs identified include, for example, investigations (also digital) and prosecution of CICs. Training should support the experts in navigating multiple evidence sources, such as OSINT, satellite imagery, and battlefield information, and continuously exploit new technologies and digital tools to benefit the investigations. Related to the victims of CIC, is the collection of testimonies and the provision of support and protection meeting their individual needs and in line with the Victim's Right Directive, which establishes minimum standards on the rights, support, and protection of victims of crime and ensures that persons who have fallen victim to crime are recognised and treated with respect. As a new need, it was identified that human rights defenders (HRD), judges and prosecutors would benefit from training on digital evidence and digital registration of human rights violations. Another addition arising from the review process is the monitoring or sanctions, adequate penalisation of the violations of restrictions imposed, and effective cooperation and information exchange between the authorities involved in their implementation and monitoring.

The following table presents the reviewed list of other training needs, as re-prioritised by the MS.

Table 21. Prioritised list of training needs – Other

N:o	Other - training needs	Change
1	Leadership and management	⇨ 0
2	Public order: community policing also considering its digital dimension; innovative information exchange with civilians (front line policing, community policing) making use of digital tools; policing football events, including international football dynamics, international police information exchange and cooperation, key components of EU legal framework, dedicated football policing functions, risks, crowd management dynamics, proportionate and targeted approach, effective communication at planning and operational stages, early intervention, sharing experiences, challenges and remedial actions; international police cooperation mechanisms; protection of public figures, including preventive protection, threat and risk assessment, strategic and operational planning of protective measures, counter-drone measures (U-space, new EU rules on dedicated airspace for drones), managing crowd events with very important persons' (VIP) participation, chemical, biological, radiological and nuclear (CBRN)	⬆ 1
3	Emergencies requiring law enforcement response: early detection, prevention and rapid response to crises (migration, COVID-19, upcoming economic recession); integrated and coordinated approach; joint crisis management at EU and national level; inter-agency cooperation and coordination; first responders	⇨ 0
4	English language and potentially Arabic	⬇ -2
5	EU funding and EU project management	⇨ 0
6	Core international crimes: genocide, crimes against humanity, war crimes, sexual and gender-based violence committed by the Islamic State of Iraq and the Levant; Renewed and global support of action toward accountability for core international crimes and human rights violations; Investigation and prosecution of core international crimes (investigations and prosecutions of alleged core international crimes, including war crimes and crimes against humanity, committed on the territory of Ukraine), including digital means; Navigating multiple evidence sources – open-source information, satellite imagery, battlefield information – and exploit new technologies and investigative tools, such as the possibilities offered by AI; Collection of victims' testimonies; Provision of support and protection to victims of core international crimes, in accordance with their specific needs and in line with the Victims' Rights Directive; Activities facilitating training and awareness for human rights defenders as well as for judges and prosecutors, on digital evidence and digital registration of human rights violations in order to increase clarity on criteria of admissibility in domestic and international courts; Sanctions monitoring and the adequate penalisation of sanctions violations; Coordinated approach to facilitate information exchange between national actors dealing with the implementation and monitoring of restrictive measures; Multidisciplinary approach and involve – alongside investigators and prosecutors – analysts, digital experts, historians, anthropologists, asset recovery and financial investigation experts, as well as media and military specialists; Nexus between internal and external security/external dimension of internal security; information exchange, coordination and enhancement of national investigations and prosecutions to	⇨ 0
7	Stress management, conflict management and communication	⇨ 0
8	Disaster victim identification: international collaboration; harmonisation of identification procedures for individual cases; identification of deceased persons in non-disaster contexts	⇨ 0
9	Training of service dog handlers: training handlers and dogs for new scents and new disciplines, including searching for different objects such as computer parts, memory sticks, mobile phones, and improvised explosive devices	⇨ 0

Consultation with Justice and Home Affairs agencies, the EU Innovation Hub and the European Union Intellectual Property Office

After finalising the draft report, CEPOL shared the mid-term review outcomes with other EU Agencies. Such a consultation mechanism aimed to communicate the review findings, collect feedback on the updated list of EU-STNA 2022-2025 priorities and coordinate training falling under the competencies of the different EU actors. This chapter summarises the feedback received from Europol, the EU Innovation Hub, EMCDDA, EUIPO, eu-LISA, FRA, Frontex and CEPOL (internally).

On 20 June 2023, CEPOL presented a draft mid-term review report at the meeting of the EU Innovation Hub for Internal Security, a collaborative network that provides the latest innovation updates and effective solutions to support the work of internal security actors in the EU MS, including justice, border security, immigration, asylum and LE practitioners. Without any request for changes, the Hub team acknowledged the review findings as presented. As suggested by Europol (Innovation Lab), the EU Innovation Hub should be considered as a consulting party for the future EU-STNA processes as well.

In the area of drug trafficking, which increased its position as a training priority by one rank step, the EMCDDA acknowledged that the findings of the EU-STNA 2022-2025 mid-term review generally reflect well the evolving LE training needs across the EU. As a limitation of this study, they pointed out that some ongoing and yet unpublished analyses related to cannabis, amphetamine and heroin may further impact the training needs on drug trafficking. Once available, these analyses are to be reviewed and the relevant aspects incorporated into a joint flagship course of EMCDDA-CEPOL on drugs crime and markets for the year 2024.

EUIPO provided comments concerning IP crime, counterfeiting goods and currencies that moved one place down as an EU-level training priority. Both EUIPO and CEPOL agree on the importance to continue raising awareness on this relatively new, but due to its poly-criminal nature and linkages to other serious organised crimes, critical EMPACT priority. In the Intellectual Property Crime Threat Assessment 2022[19], produced jointly by EUIPO and Europol, criminals and criminal networks, as well as money laundering and money flows, are viewed as horizontal issues that impact several different crime areas. EU-level LE training should further emphasise this interlinked nature of IP crime, expand training on cyber patrolling to cover IPR cases, counterfeit detecting canines and their handlers, and when relevant, educate on using new technological tools and/or techniques. To ensure continuity of capacity building in this area, EUIPO and CEPOL will continue cooperation in the area of EMPACT Operational Action on IP crime training, including a joint plan to define a comprehensive learning path on IP crime, identify and support the strengthening of expert networks, as well as establish a Train the Trainer (TTT) pool of experts with the capacity to

[19] Available on: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_IP_Crime_Threat_Assessment/IP_Crime_Threat_Assessment_2022_FullR_en.pdf

train further enforcers on basic IPR knowledge at national level in their customs and police schools. Furthermore, seamless training cooperation should continue with Europol and OLAF.

Related to fundamental rights, FRA expressed concerns about the decrease in ranking of fundamental rights-related topics across the different training areas. Despite this finding, the EU-STNA 2022-2025 considers fundamental rights and data protection as one of the eight core capability gaps and reiterates that fundamental rights are a cross-cutting element that should be mainstreamed across all areas and integrated into each training session in an applicable manner. FRA's opinion, supported by the findings of CEPOL's recent studies[20], emphasised the importance of continuing training efforts on fighting hate crime. Largely seconding the existing training needs and priorities[21] established in the EU-STNA 2022-2025, LE training should also continue, in a comprehensive manner, addressing the different aspects of fundamental rights and data protection when using different modern technologies and countering the steadily increasing phenomena of hate speech and hate crime in the EU, as well as respectfully deal with different -isms (such as anti-semitism) in society. Raising awareness among police officers of standards applicable to police stops should continue, ensuring that in the performance of their duty, LE officials respect and protect human dignity and maintain and uphold the human rights of all persons without any discriminatory profiling. Training in the area of counter-terrorism should continue maintaining the right balance between the need for effective measures to combat international terrorism and respecting fundamental rights and freedoms in the context of strengthening the fight against terrorism.

Frontex acknowledged the findings of the mid-term review and provided comments on the topics of migrant smuggling, trafficking in human beings, border management and maritime security, and child sexual exploitation (including working with traumatised individuals and vulnerable groups). These constitute the areas where Frontex holds the leading role in the development and delivery of training for border and coast guard officers across the EU, as well as the European Standing Corps officers. While Frontex already cooperates with the central EU actors that have connected responsibilities in the areas of maritime security, namely the European Maritime Safety Agency (EMSA) and the European Fisheries Control Agency (EFCA), the agency expressed their interest in further strengthening interagency training cooperation on the above topics.

eu-LISA emphasised the continued importance of training migrant smuggling investigators on information exchange and related large-scale IT systems. Relevant to trafficking in human beings as well, it was suggested that training should cover the new categories of SIS alerts (irregular migration, vulnerable persons) now available and provide the user authorities with information on the refusal of entry or stay and missing persons, and enable entering preventive alerts to protect vulnerable persons on e.g. children at risk, trafficking in human beings, gender-based violence, etc.

[20] Particulary the TNA on the impact of the war in Ukraine on the training needs of law enforcement published in 2022, available on: https://www.cepol.europa.eu/training-education/training-needs-analysis/training-needs-analyses

[21] For full details, please see p. 23-25 of the EU-STNA 2022-2025 report, available on: https://www.cepol.europa.eu/documents/eu-stna-report

Conclusions

EU-STNA 2022-2025 is the core document guiding the EU-level LE training delivery during the four-year EMPACT cycle. It builds around eight core capability gaps and 17 thematic training areas as priorities for developing LE officials' skills and knowledge.

Following the methodology established[22] for assessing the EU-level training needs, the EU-STNA was mid-term reviewed during the first half of 2023. The main goal of the process was to ensure that the needs emerging after publishing the report are considered in the design and delivery of EU-level LE training.

The results of this review show that the training priorities set in the EU-STNA 2022-2025 remain valid. However, it goes without saying that since the EU-STNA 2022-2025 was published, the European security landscape continued to evolve. While the exercise for assessing the EU-level training needs was conducted during the global health pandemic that has impacted the security environment and LE operations, the beginning of the EU-STNA 2022-2025 implementation cycle was then marked by the Russian invasion of Ukraine. The return of large-scale conflict to Europe has fundamentally changed the environment over the past years, as it continued adding new security threats while transforming the existing ones.

Without introducing drastic changes, these developments have created the need to slightly adjust the EU-training priorities and extend the training offer to cover new aspects. For the remaining part of the EU-STNA 2022-2025 cycle, the priority order of the EU-level LE training priorities should be considered as follows:

Table 22. Core capability gaps and re-prioritised main thematic training areas

Core capability gaps		Thematic training areas	
	1. Digital skills and the use of new technologies 2. High-risk criminal networks 3. Financial investigations 4. Cooperation, information exchange and interoperability 5. Crime prevention 6. Document fraud 7. Forensics 8. Fundamental rights and data protection		1. Cyber-attacks 2. Criminal finances, money laundering and asset recovery 3. Counter-terrorism 4. Drug trafficking 5. Migrant smuggling 6. Trafficking in human beings 7. Online fraud schemes 8. Organised property crime 9. Child sexual exploitation 10. Border management and maritime security 11. Firearms trafficking 12. Corruption 13. Excise fraud 14. Environmental crime 15. Missing trader intra-community fraud 16. Intellectual property crime, counterfeiting of goods and currencies 17. External dimensions of European security 18. Other thematic training areas

[22] Explained in brief at https://www.cepol.europa.eu/training-and-education/training-needs-analysis/strategic-training-needs-assessments

In terms of thematic training areas, (i) cyber-attacks, (ii) criminal finances, money laundering and asset recovery, and (iii) counter-terrorism remain unchanged, and EU-level training delivery on these topics should continue as a priority, including in the training portfolios the new needs identified in the mid-term review process.

While the overall change of training priorities was not considerable, thematic training areas that increased their ranking include drug trafficking, migrant smuggling, organised property crime, corruption, excise fraud and environmental crime. In most cases, the new elements associated with these topics relate to the ongoing conflict in Ukraine. The increased priority also reflects quite well the forecasted war impact on EMPACT priorities, as well as EU-level training needs, which as a part of the EU's joint effort to assess, anticipate, prevent and counter existing or emerging serious and organised crime threats linked to or entailed by the war in Ukraine, were examined by an extraordinary Training Needs Analysis (TNA) in 2022. In most cases, the additional elements in this review, considered as new training needs (since they were not part of the initial EU-STNA 2022-2025 findings), might already be recognised and/or responded to by EU training providers. Regardless, the review confirms that during the remaining implementation cycle, attention should be paid to addressing the war dimension of topics such as drug trafficking, trafficking in human beings, organised property crime and firearms trafficking.

One interesting finding is that while a large majority of the new training needs suggesting adjustments in different thematic areas are related to the war, cyber-attacks as a continuing top training priority mark an area associated with most of the new training needs. Continuous cyber threats, added to the recognised shortage of cybersecurity professionals in the EU, recalls CEPOL's Cybercrime Academy - together with other EU-training providers - to continue efforts in capacitating the cyber workforce in the LE sector in a coordinated manner and become part of the joint policy initiative, the Cyber Skills Academy[23] established for bringing together the different cyber skills initiatives in Europe. Furthermore, the increased priority of environmental crime is a reminder of the importance of not only focusing on the thematic training delivery on those illegal acts which directly harm the environment, but of also considering its strongly converged nature and linkages to other crime areas.

Overall, the review proposes that the EU-level training for LE should be expanded on 13 thematic training areas established as priorities for the EU-STNA 2022-2025 cycle, although the majority of them concern rather an expansion of already identified training topics than entirely new needs. Relevant learning resources might already be available on most of the EU-STNA 2022-2025 priorities, but it should be ensured that the new dimensions are included in the training offer and considered as part of the priorities for the remaining EU-STNA implementation cycle. The findings also indicate a strongly continued, even further increased, need for integrating HRCN as a cross-cutting aspect across the different thematic training areas.

Considering the adjustments proposed in this review and being further guided by the continuous assessment of the latest security trends and the related training needs, the

[23] Available on: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

effective provision of training to European LE officials should continue in line with the overall framework established in EU-STNA 2022-2025.

Annex 1. List of documents reviewed

N:o	Author	Title	Date
1	EUROPEAN COMISSION	A new EU policy to support Disarmament, Demobilisation and Reintegration of former combatants	21.12.2021
2	EUROPEAN COMISSION	JOINT DECLARATIONS EUROPEAN PARLIAMENT COUNCIL EUROPEAN COMMISSION European Declaration on Digital Rights and Principles for the Digital Decade	23.01.2023
3	EUROPEAN COUNCIL	COUNCIL RECOMMENDATION of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (Text with EEA relevance)	20.01.2023
4	EUROPEAN COUNCIL	Council conclusions on the cross-border regarding crimes committed in connection with Russia's war of aggression against Ukraine	29.11.2022
5	EUROPEAN COUNCIL	DRAFT COUNCIL CONCLUSIONS ON ENHANCING THE CAPACITIES OF THE EUROPEAN JUDICIAL CYBERCRIME NETWORK	25.11.2022
6	EUIPO	THE INTELLECTUAL PROPERTY CRIME INVESTIGATION HANDBOOK	31.01.2023
7	EUIPO	The Intellectual Property Crime Investigation Handbook Flyer	31.12.2020
8	EMCDDA	EUROPEAN DRUG REPORT TRENDS AND DEVELOPMENTS	2021
9	EUROPEAN COMISSION	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on import, export and transit measures for firearms, their essential components and ammunition, implementing Article 10 of the United Nations' Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against Transnational Organised Crime (UN Firearms Protocol) (recast)	27.10.2022
10	RUGGERO SCATURRO WALTER KEMP	PORTHOLES Exploring the maritime Balkan routes	07.2022
11	Simone Haysom and Mark Shaw	An analytic review of past responses to ENVIRONMENTAL CRIME and programming recommendations	09.2022
12	EUROPEAN COUNCIL	Working document of the European External Action Service Implementing Guidelines for the EU Policy on Training for CSDP	15.07.2022
13	EUROPEAN COUNCIL	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on EU Policy on Cyber Defence	06.12.2022
14	EUROPEAN COUNCIL	Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text	20.01.2023
15	EMCDDA	EU Drug Market: Cocaine	06.05.2022
16	EMCDDA	EU Drug Market: Methamphetamine	06.05.2022
17	eu-LISA	Enabling Seamless Travel to the European Union	12.2022

N:o	Author	Title	Date
		Research Monitoring Report	
18	EUROPEAN COMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Ensuring justice in the EU — a European judicial training strategy for 2021-2024	02.12.2020
19	Council of the EU Press release	Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence	25.01.2023
20	EUROPEAN COUNCIL	Horizontal Working Party on Cyber issues	08.12.2022
21	EUROPEAN COUNCIL	Report on the Follow-up Baseline Study on Integrating Human Rights and Gender Equality into the European Union’s Common Security and Defence Policy	17.05.2022
22	EUROPEAN COUNCIL	Concept on Cultural heritage in conflicts and crises. A component for peace and security in European Union’s external action	18.06.2021
23	EUROPEAN COUNCIL	Concept for an Integrated Approach on Climate Change and Security	05.10.2021
24	EUROPEAN COUNCIL	Council Conclusions on the Civilian CSDP Compact	12.12.2022
25	EUROPEAN COMISSION	A STRATEGIC COMPASS FOR SECURITY AND DEFENCE For a European Union that protects its citizens, values and interests and contributes to international peace and security	2023
26	EUROPEAN COMISSION	Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union’s Foreign and Security Policy	06.2016
27	EMCDDA	Drug-related health and security threats in the Western Balkans	2022
28	EMCDDA	Overview of drug markets in the European Neighbourhood Policy-East countries	2022
29	EMCDDA	Overview of drug markets in the European Neighbourhood Policy-South countries	2022
30	EUROPEAN COMISSION	Study strengthening the fight against organised crime: Assessing the legislative framework - final report	12.2022
31	EUROJUST	First Eurojust report on transfer of proceedings	01.2023.
32	EUROJUST	Eurojust Written Recommendations on Jurisdiction: Follow-up at the National Level	09.2023
33	EUROJUST	Case-law by the Court of on import, export and transit measures for firearms of the European Union on the Principle of ne bis in idem in Criminal Matters	12.2021
34	EUROJUST	Report on Eurojust’s casework in the field of the EAW	07.2021
35	EUROJUST	Update on Eurojust Overview of CJEU Case Law on EAW	12.2022
36	EUROJUST	Joint report by Eurojust and EJN on the extradition of EU citizens to third countries	12.2020
37	EUROJUST	Guidelines on Joint Investigation Teams involving third countries	06.2022
38	EUROJUST	Migrant Smuggling In Focus - Issue 1	10.2021
39	EUROJUST	Eurojust meeting on migrant smuggling 4-5 November 2021 - Outcome Report	12.2021
40	EUROJUST	Eurojust’s Work in the Fight Against Migrant Smuggling - leaflet	12.2022

N:o	Author	Title	Date
41	EUROJUST	Eurojust meeting on migrant smuggling 2022, The Hague, 19-20 October 2022 Outcome Report	12.2022
42	EUROJUST	Eurojust Guidelines on How to Prosecute Investment Fraud	07.2021
43	EUROJUST	Eurojust Casework on Counter-Terrorism: Insights 2020 – 2021	12.2021
44	EUROJUST	Eurojust Meeting on Counter-Terrorism 17-18 November 2021 - Outcome Report	04.2022
45	EUROJUST	Conclusions of the 30th meeting of the Genocide Network, 8-9 November 2021	26.11.2021
46	EUROJUST	Expert Report – Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis	30.11.2021
47	EUROJUST	Addendum – Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis	21.01.2022
48	EUROJUST	Conclusions of the 31st Genocide Network meeting, 6-7 April 2022	03.05.2022
49	EUROJUST	20 Years On: Main Developments in the Fight Against Impunity for Core International Crimes in the EU	22.05.2022
50	EUROJUST	Key factors for successful investigations and prosecutions of core international crimes	23.05.2022
51	EUROJUST	NGO Atlas	18.07.2022
52	EUROJUST	Guidance for National Authorities on the identification of victims and witnesses of core international crimes	29.07.2022
53	EUROJUST	Documenting international crimes and human rights violations for criminal accountability purposes: Guidelines for civil society organisations	21.09.2022
54	EUROJUST	Conclusions of the 32nd Genocide Network meeting, 23-24 November 2022	14.12.2022
55	EUROJUST	Conclusions of the 17th Annual Meeting of National Experts on Joint Investigation Teams, 13-14 October 2021	06.12.2021
56	EUROJUST	Highlights of the 18th Annual Meeting of the National Experts on JITs – Supporting JITs in times of conflict, 5-6 October 2022	20.12.2022
57	EUROJUST	Update to the JIT Evaluation form	14.12. 2022
58	EUROJUST	Joint Investigation Teams: Practical Guide	16.12. 2021
59	EUROJUST	Update to the Model Agreement for setting up a Joint Investigation Team, including revised Appendix I	22. 12. 2021
60	EUROJUST	Update to the Guidelines on Joint Investigation Teams Involving Third Countries	17.06. 2022
61	EUROJUST	Checklist for Practitioners on Joint Investigation Teams Involving Third Countries	17.06. 2022
62	EMCDDA	European Drug Report 2022: Trends and Developments	2022
63	EUROPEAN PARLIAMENT	Situation of fundamental rights in the EU in 2020 and 2021	15.09.2022
64	EUROPEAN PARLIAMENT	Negotiations for a cooperation agreement between the EU and Interpol	05.07.2022
65	EUROPEAN PARLIAMENT	Cooperation on the fight against organised crime in the Western Balkans	15.12.2022
66	EUROPEAN PARLIAMENT	Growing hate crimes against LGBTIQ people across Europe in light of the recent homophobic murder in Slovakia	20.10.2022

N:o	Author	Title	Date
67	EUROPEAN PARLIAMENT	The fight against impunity for war crimes in Ukraine	19.05.2022
68	EUROPEAN PARLIAMENT	A STRATEGIC COMPASS FOR SECURITY AND DEFENCE For a European Union that protects its citizens, values and interests and contributes to international peace and security	2023
69	European Council	ANNEX to the Joint Communication to the European Parliament and the Council on the update of the EU Maritime Security Strategy and its Action Plan "An enhanced EU Maritime Security Strategy for evolving maritime threads"	10.03.2022
70	European Council	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the update of the EU Maritime Security Strategy and its Action Plan "An enhanced EU Maritime Security Strategy for evolving maritime threads"	10.03.2022
71	European Council	Council Conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022 +	09.03.2023
72	European Council	COUNCIL CONCLUSIONS ON SETTING THE EU'S PRIORITIES FOR THE FIGHT AGAINST SERIOUS AND ORGANISED CRIME FOR EMPACT 2022-2025	09.03.2023
73	European Council	REGULATION (EU) 2019/818 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816	20.05.2019
74	European Council	Council Recommendation (EU) 2022/915 on operational law enforcement cooperation	09.06.2022
75	FRA	Getting the future right – artificial intelligence and fundamental rights (and related annexes)	2020
76	FRA	DIRECTIVE (EU) 2017/541 ON COMBATING TERRORISM —IMPACT ON FUNDAMENTAL RIGHTS and freedoms, with annexes	2021
77	FRA	Your rights matter – Police stops, Fundamental Rights Survey	2022
78	FRA	Antisemitism - Overview of antisemitic incidents recorded in the European Union 2011-2021	2022
79	FRA	Bias in Algorithms – Artificial Intelligence and Discrimination	2022
80	FRA	Fundamental Rights Report 2022	2022
81	FRA	Social rights and equality in the light of the recovery from the Covid-19 pandemic	2022
82	EUROPOL	ChatGPT – the Impact of Large Language Models in Law Enforcement	2023

N:o	Author	Title	Date
83	EUROPOL	Policing in the metaverse – what law enforcement needs to know	2023
84	EUROPOL	European Union Terrorism Situation and Trend report 2022 (TE-SAT)	2022
85	EUROPOL	European Union Terrorism Situation and Trend report 2023 (TE-SAT)	2023
86	EUROPOL	European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021	2021
87	EUROPOL	Internet Organised Crime Threat Assessment (IOCTA) 2021	2021

Annex 2. Stakeholders consulted

European Union agencies, institutions and bodies
European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
European Commission - DG HOME
European Union Agency for Law Enforcement Cooperation (Europol)
European Union Agency for Asylum (EUAA)
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)
European Union Agency for Criminal Justice Cooperation (Eurojust)
European Union Agency for Fundamental Rights (FRA)
European Border and Coast Guard Agency (Frontex)
European Union Intellectual Property Office (EUIPO)
European External Action Service (EEAS)
Professional groups and networks
Operational Network (@ON)
Experts in the area of Disaster Victim identification (DVI)
European Firearms Experts (EFE)
European Judicial Cybercrime Network (EJCN)
European Network on the Administrative Approach tackling serious and organised crime (ENAA)
European Network of Law Enforcement Technology Services (ENLETS)
European Network for the Protection of Public Figures (ENPPF)
European Network for Environmental Crime (ENVICRIMENET)
Informal enforcement authorities and expertise competent in the field of cultural goods (EU CULTNET)
Pan-European Think Thank of football safety and security experts
SIS/SIRENE Committee - Schengen Information System
European Traffic Police Network (TISPOL)
Member States
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
The Netherlands
Poland
Portugal
Romania
Spain
Slovakia
Slovenia

Sweden

Annex 3. List of re-prioritised EU-level training needs

Cyber-attacks

N:o	Training need
1	Investigating cyber-attacks on information systems and modus operandi: analysing latest cyber-attacks and European Union (EU) emergency response; developing alternative investigation techniques and EU tools, including their use
2	Latest challenges for dealing with encryption, ransomware, cryptocurrencies, anonymisation and bulletproof hosting services and the use of dark web
3	Identifying, handling, securing, preserving, analysing and exchanging digital data and e-evidence
4	Effective international cooperation, including mutual operational assistance between Member States (MS); commonly shared and/or interoperable communication tools for secure communication in the cyber field. Strengthened EU-North Atlantic Treaty Organization (NATO) cooperation in the field of cyber defense training, education, situational awareness and exercises
5	Protocols to tackle large-scale cyber-attacks
6	Combatting crime-as-a-service used by criminals and criminal groups in illegal activities
7	Big data analysis
8	Raising awareness of cyber-attacks for EU agencies, law enforcement agencies and the public, including a coordinated approach for prevention; cyber-enabled and cyber-dependent crime awareness, cyber threats and cybercrime investigation
9	Using Artificial Intelligence (AI), machine learning and deep learning in cybercrime investigation
10	Blockchain analysis
11	Organised crime groups (OCG) committing cybercrime, e.g the Balkan criminal groups recognised as agile and emerging actors
12	Cybercriminal profiling and motivation analysis
13	Changing legal framework and its implications to cybercrime investigations
14	Cooperation between civilian, diplomatic and law enforcement cyber communities, joint exercises supporting building of trust and common understanding
15	Cyber-, hybrid- and space-related security skills for the maritime domain
16	Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection

Criminal finance, money laundering and asset recovery

N:o	Training need
1	Modus operandi: existing and emerging crime patterns (non-tangible tokens, new modes of terrorist financing), criminal financing methods: cash-based (cash carriers, money mules) money laundering, money laundering via normal financial system (electronic), offshore challenge to conceal beneficial ownership, informal value transfer systems (e.g. Hawala, Chinese underground banking), underground banking, international money laundering bolstered by fictitious contracts and invoices, trade-based money laundering, money laundering via virtual currencies, and complex financial schemes. Training should also cover money laundering as crime-as-a-service, illegal sale of unlicensed financial services, money laundering via high value goods and services, corporate economic crime and fraud schemes (subsidy fraud, bank fraud, investment fraud, CEO fraud and social benefit fraud)
2	Tracking, tracing, freezing and confiscating assets, opportunities to hide assets quickly, intelligence on criminal turnovers and profits, including training for judicial investigators; application of parallel financial investigations in serious crimes; pre-seizure planning; importance of interlocutory sales
3	Financial investigation and asset recovery for investigators of other crime areas: general basic knowledge on financial investigation and asset recovery, EU/international framework, new EU/international initiatives, directives, rules, tools, multidisciplinary approach, administrative cooperation, role of customs and tax authorities, cooperation with tax authorities and the judiciary; application of integrated financial investigations in serious crimes ; pre-seizure planning; importance of interlocutory sales; management of confiscated assets and social reuse of criminal assets

4	Technicalities and information priorities, technical aspects of investigation, modern technologies, use of AI, big data analysis and Open-Source Intelligence (OSINT), technicality of virtual coins (seizures)
5	Training on cryptocurrencies for general investigators
6	Financial analysis methods and financial forensics
7	Institutional training addressing a new landscape: implementation of European Public Prosecutor’s Office (EPPO) Regulation, roles of Eppo, European Anti-Fraud Office (OLAF), European Union Agency for Law Enforcement Cooperation (Europol), European Union Agency for Criminal Justice Cooperation (Eurojust), European Judicial Cybercrime Network (EJCN) and national authorities. EU directives, tools available at MS and EU level
8	Cooperation with customs authorities, EU agencies, existing and new instruments, Naples II Convention, administrative customs cooperation mechanisms, Camden Asset Recovery Inter-agency Network (CARIN), Anti-Money Laundering Operational Network (AMON), EGMONT Group of Financial Intelligence Units, Association of Law Enforcement Forensic Accountants (ALEFA), sharing good cooperation practices, information collected by customs (e.g. cash declarations, trade data); cooperation with tax authorities (exchange of information and intelligence on missing traders)
9	Investigation of crime enablers such as lawyers, financial service providers and real estate agents who knowingly and wittingly provide services to facilitate criminal financial flows
10	Roles of financial institutions in anti-money laundering, public–private partnership; roles of European Court of Justice and European Court of Human Rights (ECHR) in anti-money laundering; case studies on fundamental rights and data protection issues in criminal investigations
11	Roles of the police, tax and customs agencies and the financial sector in prevention/control mechanisms
12	Fundamental rights and data protection

Counter-terrorism

N:o	Training need
1	Radicalisation: preventing and countering radicalisation that leads to violent extremism and terrorism (with the focus on the victims and perpetrators profiles); new forms of radicalisation; fundamental rights and data protection, including non-discrimination
2	Countering the financing of terrorism: emerging threats, financial links to other types of crime and criminal organisations (e.g. tax fraud, money laundering, illicit trafficking in cultural goods, drugs, small arms and abuse of non-profit organisations); setting up and managing private–public partnerships, modus operandi and new modes of terrorist financing (e.g. crowdfunding platforms, use of crypto assets and bitcoin trading (including use non-fungible tokens); collection and use of financial intelligence.
3	Use of OSINT in counter-terrorism; value of digital evidence; methods of lawful interception; OSINT in the Darkweb. Online undercover Operations (Virtual Agents)
4	Prevention of dissemination; detection and investigation of terrorist content online; digital trends; use of EU platform to combat illegal content online (PERCI) and implementation of the regulation on addressing dissemination of terrorist content online; SIRIUS Project - Cross-Border Access To Electronic Evidence. Role of The EU Internet Referral Unit (EU IRU)
5	Foreign terrorist fighters, travelling terrorists and returnees; law enforcement approach to family members of foreign terrorist fighters (FTF); disengagement and exit programmes (focus on reintegration with society); Battlefield Information Exchange; cumulative prosecutions of FTF’s for Core International Crimes
6	Use of information systems and cooperation mechanisms in the fight against terrorism by competent actors from the judiciary, the police and intelligence services
7	Protection of public spaces and resilience of critical entities; sharing best practices on handling attacks including cyber domain; protection of places of worship; use of Drones for terrorism
8	Regional and cross-border cooperation on specific terrorism cases; SIRIUS Project - Cross-Border Access To Electronic Evidence
9	Unmanned aerial vehicles: threats and opportunities for law enforcement
10	Tools to enhance the judicial response to terrorism

11	Use of AI by law enforcement; Metaverse Threat; use of Chat Generative Pre-Trained Transformer (ChatGPT)
12	Tackling document fraud

Drug trafficking

N:o	Training need
1	Drug smuggling: drug trafficking in bulk through EU container ports; online trade in drugs at retail level; increased use of the darknet and social networks including in response to COVID-19; innovations and use of digital technologies in drug trafficking; drug trafficking using postal and parcel delivery services; drug smuggling using alternative maritime distribution modes via pleasure and fishing vessels; tackling digitally-enabled drug trafficking
2	Criminal networks: business models and modi operandi of organised criminal networks engaged in drug production and trafficking; structure, organisation and specialisation of criminal networks involved in drug trafficking (cannabis, cocaine, heroin, synthetic drugs/new psychoactive substances (NPS) and poly-drugs)
3	Investigation: use of digital investigation tools, OSINT, darknet, decryption, AI, social networks, operational intelligence analysis; training of first responders on synthetic opioid poisoning
4	Financial investigation related to drug production and trafficking; money laundering and asset recovery in drug cases, including use of sophisticated parallel and multi-layered financial systems; training for judicial investigators and law enforcement
5	Latest trends and developments in drug production and trafficking: new trends in NPS availability and types; emerging evidence of South Asia’s role as producer/supplier of ephedrine and methamphetamine; monitoring situation regarding fentanyl and other synthetic opioids due to the huge break-out in the United States of America (USA); changing behavioural trends regarding drug supply and consumption
6	Drug production: innovative methods using digital technologies; new/innovative technology, sophisticated cannabis cultivation methods (growth, lighting, monitoring); heroin/cocaine conversion and extraction; production of synthetic drugs on an industrial scale; new ways of hiding drug production/production stages
7	Law enforcement cooperation: global tools for drug monitoring linked to international cooperation, cooperation with non-EU countries
8	Tackling document fraud, including mislabelling of (pre-)precursors and NPS
9	Legal challenges and solutions in prosecuting cases related to drugs, precursors and NPS
10	Forensics
11	Consequences of the war in Ukraine: mitigating the challenge of displaced people or migrant communities at increased risk both of experiencing drug-related problems and of being vulnerable to exploitation by criminal groups involved in drug production, trafficking or sales.
12	General aviation: definition and legal framework, types of aircraft and characteristics, flight basics, Advanced Passenger Information (API) and Passenger Name Record (PNR), and available monitoring tools
13	Drugs in prison: increasing capacity of prison staff to better detect drugs entering prisons and to implement evidence-based health-related drug responses within the prison environment
14	Fundamental rights and data protection

Migrant smuggling

N:o	Training need
1	Investigation: sharing best practices, OSINT, ability to respond to the use of digital platforms, social media and mobile applications by criminals, intelligence gathering, decryption, lessons learnt from landmark migrant smuggling investigations
2	Modus operandi: sham marriages, bogus paternity, false employment contracts, fake invitation letters, false medical visas, and false claims of being victims of trafficking or refugees; use of digital platforms for all phases of migrant smuggling, mass mobilisation for migration, arranging secondary

	movements, and monitoring law enforcement movements; profiling and behaviour analysis; surveillance including use of drones; use of cryptocurrencies; use of encrypted communication; smuggling techniques
3	Understanding the operation of organised crime groups
4	Information exchange: European Asylum Dactyloscopy Database (Eurodac), Schengen Information System (SIS), role of large-scale IT systems in combatting migrant smuggling under the European Multidisciplinary Platform Against Criminal Threats (EMPACT) framework
5	Partnerships and cooperation with non-EU countries: supporting host countries in participating in regional and international cooperation mechanisms that are meant to address migrant smuggling and trafficking in human beings; comprehensive approach (involving consulates, civil registries, etc.)
6	Improving knowledge on financial models including hawala and money service bureaux, cryptocurrencies, financial investigations and asset recovery
7	Nexus between migrant smuggling and trafficking in human beings: exploitation of migrants after arrival in the EU
8	Document and identity fraud with a focus on visa fraud and forged supporting documents; biometrics; networking and support
9	EU cooperation tools and mechanisms, Joint Investigation Teams (JIT); cooperation between administrative and law enforcement units and the judicial sector (prosecutors, lawyers and judges)
10	Dealing with requests concerning unaccompanied minors
11	Trends and new developments in the operating tactics of OCGs involved in migrant smuggling: particularly operations of e.g. OCGs connected with the Gambia, Mauritania, Morocco and Senegal facilitating illegal travels through the Western Mediterranean routes
12	Procedures and tools used in migration crisis situations
13	Detecting secondary movements
14	Impact of shifts in migrant smuggling routes and the currently active sea entry corridors, such as the Central Mediterranean route, the Western Mediterranean routes and the smuggling corridor from Turkÿe into Greece, especially Cyprus, changes in Western Balkans route due to Ukrainian war
15	Fundamental rights, including access to international protection, non-discrimination and data protection; trust-based approaches to the questioning of migrants

Trafficking in human beings

N:o	Training need
1	Modus operandi of trafficking in human beings, with increased reliance on digital technology, including the online recruitment of minors; different forms of human trafficking and their indicators, including the purpose of exploitation: human trafficking for purposes of sexual exploitation, labour exploitation and forced criminality; psychological and physical violence and drugs used to control and coerce victims
2	Trafficking for sexual exploitation: modus operandi including online; detection, victim identification, safeguards, support and referral, with a focus on women and children
3	Child trafficking
4	Business model of human trafficking, including the use of crime-as-a-service as well as the infiltration and use of legal business structures by criminals; links with migrant smuggling networks, with a special focus on non-EU country nationals arriving illegally to the EU and being exploited, in particular vulnerable groups such as unaccompanied minors and women; links to organised property crime, drug trafficking and document fraud
5	Investigations on the increasing use of digital technology at different stages of trafficking, particularly on encrypted communication and moving assets
6	Victim identification at borders, by first responders and online (use of OSINT and darknet), with a special focus on vulnerable groups such as women and children
7	Links to criminal finances and money laundering; financial investigations: tracing, seizing and confiscating criminal proceeds, asset recovery.
8	Use of existing information and cooperation channels, e.g. Europol, International Criminal Police (Interpol); how to start a JIT; use of large-scale IT systems

9	Multidisciplinary and victim-centred approach; working with victims of trafficking for forced criminality such as organised property crime, drug-related crime, etc.; support for reporting; cultural differences; psychological harm to victims influencing their behaviour during investigation; fundamental rights of victims
10	Human trafficking due to the crisis in Ukraine and the war refugees at high risk of all types of exploitation
11	International cooperation with the United Nations (UN) and International Organisation for Migration (IOM), cooperation with non-EU countries, cooperation with Non-Governmental Organisations (NGO)/institutions providing victim support; referral of victims
12	Prevention of human trafficking
13	Detection of criminal forms of labour exploitation in workplaces
14	Forensics

Online fraud schemes

N:o	Training need
1	Cyber scams: online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud, mimic and voice fraud, helpdesk fraud, social engineering
2	Card-not-present fraud: compromise online payments, e-skimming, mobile banking fraud, online payment requests, Subscriber Identity Module (SIM) swapping, smishing, phishing and vishing, e-commerce fraud, carding platforms and darknet marketplaces
3	Cybercrime facilitators: cryptocurrencies including Decentralised Finance (DeFi) as an emerging model for organising and enabling cryptocurrency-based transactions, exchanges and financial services, encryption, anonymisation, online forgery, new online tools and digital techniques, use of deepfakes created with AI, money muling
4	Card-present fraud: skimming, contactless card fraud, mobile payment fraud
5	Cyber threat intelligence, dark web and OSINT
6	International law enforcement cooperation, public–private partnership, inter-agency cooperation (cooperation with financial institutions, internet service providers and online platforms); Overview of parallel or linked investigations at national and international levels
7	Intrusions into system networks of financial institutions: banking malware/POS malware, logical attacks against Automatic Teller Machines (ATM), use of malware to intercept login details for online banking services
8	Information exchange and cross-border exchange of evidence
9	High-risk criminal networks
10	Legal challenges in non-cash payment methods
11	Crime prevention
12	Fundamental rights and data protection

Organised property crime

N:o	Training need
1	Organised burglaries, robberies and thefts and new trends in modus operandi
2	International investigation, operational cooperation, cross-border observation, best practices, joint investigation teams; communication channels used by criminals (e.g. SKY ECC)
3	Criminal networks, OCGs, Mobile Organised Crime Groups (MOCG), clans and different roles of members
4	Fighting vehicle crime: transit, export and trade of stolen vehicles and parts; lease and rental fraud; wrongly registered vehicles; use of European car and driving licence information system (EUCARIS); geolocation of vehicles; cooperation with manufacturers to localise vehicles
5	Fight against the illicit import, export and transfer of ownership of cultural property, resulting from theft from cultural heritage institutions or private collections, looting of archaeological sites and displacement of artefacts: interconnected databases of stolen artefacts, cooperation; identification of cultural goods; legislation from the European countries on the transit of the cultural goods

6	Financial investigation and asset recovery related to organised property crime cases
7	OSINT focused on organised property crime with special focus on OSINT within the framework of the illicit trafficking of cultural goods
8	Tackling theft and attacks on ATMs
9	Fencing, online activities, processes, networks and routes used for stolen goods
10	Capacity building among cultural heritage experts, including a network of experts that MS could use within the EMPACT framework
11	Forensics
12	Prevention: using the European barrier model for organised property crime; administrative approach
13	Document fraud; forgery (e.g. knowledge on usual methods) related to cultural goods crime
14	Due to the war in Ukraine, further needs to effectively safeguard cultural property and preserve the movable heritage from looting, illegal excavations and illicit trafficking, illicit trafficking and trade of cultural goods
15	Fundamental rights and data protection

Child sexual exploitation

N:o	Training need
1	Identifying victims of sexual abuse and exploitation, analysis of big data, images and videos for victim identification purposes; detecting child abuse material
2	Investigation: detecting child abuse material; use of new forensic tools; online undercover operations
3	Use of OSINT and the dark web
4	Developing and applying innovative investigation methods
5	Law enforcement cooperation to tackle child sexual exploitation and abuse cases; joint investigation teams; cooperation between law enforcement and judicial authorities to tackle child sexual abuse and exploitation
6	Handling encryption and anonymisation services in online child sexual abuse (Virtual Private Network (VPN), proxy servers, Tor)
7	Identification of high-risk criminal networks involved in child sexual abuse and exploitation
8	Financial investigations related to child sexual exploitation cases (online payment methods including virtual currencies)
9	Tackling gender-related cyber violence against women and girls
10	Working with traumatised individuals and children: specialised training for investigators on conducting vulnerability assessment
11	Victims' rights, offenders' rights, suspects' rights
12	Victims of sexual and gender-based crimes (SGBC): awareness and best practices for questioning potentially traumatised SGBC victims
13	Tools and techniques for mental health/psychological support for law enforcement officers dealing with child abuse
14	International offender management

Border management and maritime security

N:o	Training need
1	Identifying cross-border crime and security threats at the border with a focus on foreign terrorist fighters, drugs, smuggling of excise goods, firearms and explosives, signs of environmental crime (at maritime border/in international waters and on land) and trafficking in human beings, with particular attention being paid to victims of trafficking
2	EU-level intelligence analysis and information exchange systems; enhanced cooperation by forming specialist units comprising all relevant actors such as customs, financial crime/money laundering experts, police, port security officers and the port authority, with special emphasis on improving the capacity of customs officials to carry out local and contextual risk assessment
3	Document fraud detection at border crossing points

4	Common as well as new digitalisation practices (three dimensions: border security, information exchange and humanitarianism)
5	Cross-border criminal networks
6	Digitalisation of the Schengen visa procedure, Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS) entry into operation, including biometric data
7	Border management in non-EU countries with shared external borders; experience sharing with Common Security and Defence Policy (CSDP) missions mandated with border management aspects
8	Dignified treatment of persons at the border in compliance with principles of non-discrimination, right to liberty, respect for privacy and use of force
9	Cooperation with MS and training academies
10	Communication and language skills needed for interactions with those crossing the border
11	Screening and debriefing
12	Maritime security: Exchange of information, expertise, technical assistance and best practices on tackling illicit activities at sea; Specialised cross-sectoral maritime security training on law enforcement, military, border control, coast guards, cyber security, protection of critical maritime infrastructure etc.; training programmes open to non-EU partners to tackle existing and emerging threats to maritime security; cross-border investigative capacities between law enforcement and port authorities in SEE and parts of the world where goods are loaded for the region, including Asian and Latin American countries and key trans-shipment nodes such as Italy, Malta and Egypt
13	Access to international protection, prohibition of refoulement, prohibition of collective expulsion and pushbacks
14	Procedural safeguards related to decisions taken at the border
15	Improving capacity to implement coast guard functions

Firearms trafficking

N:o	Training need
1	Modus operandi: conversion of flobert/gas/alarm/signal weapons into firearms, legislative discrepancies, Western Balkans, conflict areas, trafficking routes, vessels/containers, fast parcel delivery/courier services, 3D printing/self-made, fake/lost/stolen identity documents; kits for assembly of firearms traded on online platforms, fake/lost/stolen identity documents
2	Illicit trafficking in firearms linked to organised crime and terrorism; supplying OCGs with firearms and ammunition from an illegal market; criminal networks specialised in the procurement and (pre-) handling of alarm and signal weapons and other kinds of convertible weapons; nexus between drugs trafficking, migrant smuggling, and firearms trafficking, in the context of sharing routes and criminal infrastructure
3	Online aspects of firearms trafficking: OSINT, dark web, open web, other communication platforms, , and postal services, etc.
4	Financial investigations related to firearms trafficking
5	Firearms forensics: use of Analysis Ballistic Information System (ABIS) and different systems, forensic evidence, ballistics, identification of explosives and pyrotechnic devices, training for analysts
6	Cooperation with MS, non-EU countries, international organisations and the private sector
7	Trafficking of firearms into the EU from post (or active) conflict countries, particularly the current armed conflict in Ukraine facilitating illicit movement of firearms; Advanced knowledge on less known routes and hubs for smuggling of firearms, among other illegal goods, from Ukraine to the EU
8	Raising awareness of the firearms threat and initiatives to counter illicit firearms production and trafficking as well as to counter firearms diversion from legal supply; national and international firearms legislation, firearms technical terms
9	Best practices for prevention campaigns; the role of administrative authorities in firearms crime prevention (Use of the customs import control system (ICS) or ICS II to target cargo, express and postal consignments before their arrivals at the external borders).
10	Human Intelligence (HUMINT) management in illicit firearms related crime
11	Related crime areas such as document fraud and corruption
12	Fundamental rights and data protection

Corruption

N:o	Training need
1	“Follow the money” approach/financial investigations following up corruption cases, recovery of assets, corrupt payments in the financial system, cash-based corruption, offshore structures, cryptocurrencies used for making payments to corrupt officials and for money laundering purposes
2	Recognition/awareness of different forms of corruption (health industry, sports, match-fixing, public procurement, law enforcement, grand corruption, manipulation of digital processes in public administration)
3	Cooperation between national, EU and international agencies and with judicial professionals, roles of EPPO and OLAF
4	Investigation and intelligence practices
5	Corruption as a crime enabler
6	Sharing expertise, best practices, data and information between MS and with civil society
7	Understanding the risks and threats caused by corruption before they materialise into corruption-related crime
8	Digital skills of law enforcement
9	Promoting anti-corruption strategies, culture of integrity and integrity testing in law enforcement and other state offices
10	Internal investigations
11	Protecting and handling whistleblowers and witnesses
12	Police ethics
13	Tackling document fraud

Excise fraud

N:o	Training need
1	Crime patterns, intelligence and investigation methods, techniques and tools in the area of illegal tobacco fraud including illegal cigarette production within the EU, new products, smuggling of cheap whites (Eastern border), maritime contraband (counterfeit cigarettes), waterpipe tobacco, manufacturing equipment and raw tobacco
2	Crime patterns, intelligence and investigation methods, techniques and tools in the area of mineral oil fraud including designer fuel fraud, fuel laundering, and paying attention to missing traders, with a focus on products and modus operandi through case studies and through deepening knowledge on the entire phenomenon
3	Crime patterns, intelligence and investigation methods, techniques and tools in the area of alcohol fraud
4	Integration of financial investigation methods into excise fraud investigation accompanied by enhanced asset recovery and big data analysis
5	International cooperation (bilateral, multilateral), building trust among law enforcement officials, EU cooperation (OLAF, EPPO, Europol, Eurojust, Frontex); law enforcement (police, customs, tax authorities, border guards, etc.); cooperation at national level, sharing best practices; cooperation with excise industry (tobacco companies, trading companies), in particular tracking and tracing illicit production and tobacco analysis
6	Use of crime analysis methods
7	Border control, mobile unit control, customs risk analysis
8	Means of transport/smuggling: road/land border crossing points, sea, railway, green border
9	OSINT, online undercover operations on darknet markets, decryption
10	Covert surveillance, Global Positioning System (GPS), covert investigation, informant handling practice, interviewing techniques
11	Common approach to legislation, types of data needed from different Member States, ways of sharing and comparing, enforcement of investigation activities in other countries, sharing experience of tackling criminal organisations active in other countries via transnational law enforcement cooperation, case studies on successful investigations

12	EU legislation and international agreements, Framework Convention on Tobacco Control
13	External Union transit procedure (T1), transit fraud, abuse of Excise Movement and Control System (EMCS) (doubling/mirroring legal consignments)
14	High-risk criminal networks
15	Tackling document fraud
16	Good practices on prevention, closely related to control mechanisms
17	Forensics

Environmental crime

N:o	Training need
1	Waste crime (modus operandi, investigation techniques): waste trafficking (hazardous and non-hazardous waste), export and import of waste, dumping at sea, landfills, mixture of waste, disposal, dismantling, waste fires
2	Investigation: digitalisation, OSINT, monitoring of virtual markets, darknet; collection of intelligence, dealing with whistleblowers; undercover actions, surveillance, wiretapping as part of environmental crime investigation; machine-learning capabilities and dynamic database management
3	Economic crime investigation techniques, national and international asset recovery to seize gains derived from environmental crime; enhancing the use of financial investigations in environmental crime cases
4	Criminal infiltration of legal business, system exploitation (e.g. systems relating to renewable energy, recycling, and quotas); crime enablers (e.g. legal experts and technical experts) supporting organised crime
5	Wildlife crime: emerging patterns, trends, crime groups. Wildlife crime shall cover crime against flora and fauna in line with the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), including illegal logging and timber trade (modus operandi, investigation techniques), trafficking protected species (glass eels, reptiles, mammals, birds), illicit pet trade, etc.
6	Cooperation: interagency cooperation between different agencies dealing with environmental issues, especially with environmental inspectorates; EU cooperation instruments and networks; cooperation with non-EU countries, global cooperation tools
7	Maritime exploitation and pollution; illegal, unreported and unauthorised fishing (modus operandi, investigation techniques); preparing for and responding to the effects of climate change and environmental degradation on maritime security
8	New legislative trends related to the circular economy to help in identifying crime enablers
9	Related crime areas such as document fraud and corruption
10	Pollution or illegal exploitation of air, ozone depletion; F-gas Regulation
11	Administrative tools to combat environmental crime
12	Raising general public awareness of the costs of environmental crime to society
13	Role of CSDP missions in spreading good practices and standards in host countries (training for mission personnel as part of pre-deployment training)
14	Fundamental rights and data protection

Missing trader intra-community fraud

N:o	Training need
1	Modus operandi: organised crime groups specialised in offering fake invoices; financial flows and schemes used for missing trader intra-community fraud (MTIC); exploitation of legal structures, versatility, adaptability to new trends and specialised advising
2	Investigation: intelligence-led investigation focusing on transnational organised crime; operational cooperation; sharing best practices
3	Financial investigations to detect money laundering; financial analysis methods
4	Technology and digital infrastructure as essential components in concealing and facilitating criminal activities (data storage, alternative payment methods, VPN services, encryption, Voice over Internet Protocol (VoIP) fraud)

5	Links to other crime areas
6	Tax confidentiality issues at EU level in the context of information exchange
7	Raising awareness of MTIC fraud among the judiciary and the public
8	Data analysis and data protection
9	Tackling document fraud
10	Forensics
11	Crime prevention

Intellectual property crime

N:o	Training need
1	Protection of industrial property rights, in particular trademarks, designs, patents, geographical indications, plant variety rights, as well as trade secrets (e.g. risk of cyber theft)
2	Modus operandi: use of legal business structures; use of online services (e.g. e-commerce marketplaces, social media platforms, (encrypted communication) mobile app stores, domain names, payment services) for advertising and sale; manufacturing finished or semi-finished products outside or within the EU, distribution within the EU; use of fraudulent documents; use of virtual currencies as payment for digital piracy
3	Investigating intellectual property crime cases: Steps in an intellectual property crime case; Transversal collection of investigative practices; Digital investigation techniques, cyber patrolling
4	Pharmaceutical crime: falsified medicines, counterfeit medical products, including COVID-19 related vaccines and products
5	Copyright protection: piracy of digital content, literary works, artistic works
6	Issues related to fraud in commercial items, e.g. food, drinks, textiles, etc.
7	Tackling currency counterfeiting
8	Cooperation between customs, the police (including border police), and market surveillance authorities and the judiciary
9	Financial investigations, European Network of Law Enforcement Technology Services (ENLETS) cryptocurrency framework
10	Customs risk analysis related to (trade in) counterfeit goods
11	Cooperation with Intellectual Property Rights (IPR) holders as well as with online/offline intermediaries
12	Forensics
13	Fundamental rights and data protection

External dimension of European security

N:o	Training need
1	Enhancing the support, development and policy implementation of existing concepts regarding evaluation, analysis, benchmarking and operational impact assessments, identification of best practices and use of lessons learned in missions' planning, management and review; more integrated approach, EU and beyond, to programming strategic cooperation (consultations, concept development, planning, assessments and evaluation) and local ownership
2	Leadership in CSDP missions, planning and command, change management in host country
3	The EU's role as a security provider through CSDP, including CSDP policy on strategic ambitions and capability limitations
4	Pre-deployment training
5	Analytical, planning and decision-making structures and procedures
6	Building advisory capacity of CSDP missions
7	Knowledge and expertise in CSDP relevant structures and missions regarding the rule of law, criminal justice, anti-corruption, and policing in line with international human rights standards
8	Role of CSDP missions in supporting EU internal security (external dimension of internal security)
9	Civil-military cooperation and its conceptual development
10	Language training: English communication skills; French as a foreign language

11	Association of non-EU countries to EMPACT and counter-terrorism activities, providing capacity building to partner states, in particular neighbouring and enlargement countries, so as to support operational cooperation with EU Member States and agencies as well as to provide partners with adequate tools (e.g. digital ecosystems and information on how to adopt national legislative reforms and adhere to international standards)
12	Political, economic and budgetary aspects of cooperative projects in defence and security within the framework of CSDP
13	Digital skills of law enforcement
14	Duty of care in CSDP missions
15	High-risk criminal networks
16	Cooperation: synergies between CSDP structures, Commission services and Justice and Home Affairs (JHA) actors; identifying and disseminating best practices; cooperation and exchange of information in Western Balkans to ensure uniform and efficient application of EU law for EU membership
17	Tackling document fraud
18	Crime prevention

Other training needs

N:o	Training need
1	Leadership and management
2	Public order: community policing also considering its digital dimension; innovative information exchange with civilians (front line policing, community policing) making use of digital tools; policing football events, including international football dynamics, international police information exchange and cooperation, key components of EU legal framework, dedicated football policing functions, risks, crowd management dynamics, proportionate and targeted approach, effective communication at planning and operational stages, early intervention, sharing experiences, challenges and remedial actions; international police cooperation mechanisms; protection of public figures, including preventive protection, threat and risk assessment, strategic and operational planning of protective measures, counter-drone measures (U-space, new EU rules on dedicated airspace for drones), managing crowd events with VIP participation, chemical, biological, radiological and nuclear (CBRN) supervision and defence, sharing best practices, case studies, quality assurance for an EU model for training protection officers; protection of public spaces;
3	Emergencies requiring law enforcement response: early detection, prevention and rapid response to crises (migration, COVID-19, upcoming economic recession); integrated and coordinated approach; joint crisis management at EU and national level; inter-agency cooperation and coordination; first responders
4	English language and potentially Arabic
5	EU funding and EU project management

6	Core international crimes: genocide, crimes against humanity, war crimes, sexual and gender-based violence committed by the Islamic State of Iraq and the Levant; Renewed and global support of action toward accountability for core international crimes and human rights violations; Investigation and prosecution of core international crimes (investigations and prosecutions of alleged core international crimes, including war crimes and crimes against humanity, committed on the territory of Ukraine), including digital means; Navigating multiple evidence sources – open-source information, satellite imagery, battlefield information – and exploit new technologies and investigative tools, such as the possibilities offered by AI; Collection of victims’ testimonies; Provision of support and protection to victims of core international crimes, in accordance with their specific needs and in line with the Victims’ Rights Directive; Activities facilitating training and awareness for human rights defenders as well as for judges and prosecutors, on digital evidence and digital registration of human rights violations in order to increase clarity on criteria of admissibility in domestic and international courts; Sanctions monitoring and the adequate penalisation of sanctions violations; Coordinated approach to facilitate information exchange between national actors dealing with the implementation and monitoring of restrictive measures; Multidisciplinary approach and involve – alongside investigators and prosecutors – analysts, digital experts, historians, anthropologists, asset recovery and financial investigation experts, as well as media and military specialists; Nexus between internal and external security/external dimension of internal security; information exchange, coordination and enhancement of national investigations and prosecutions to bring perpetrators to justice and close the impunity gap for genocide, crimes against humanity and war crimes; investigating and prosecuting core international crimes; OSINT; evidence collection and transmission by military; tools to be used in an operational situation by authorities on the ground
7	Stress management, conflict management and communication
8	Disaster victim identification: international collaboration; harmonisation of identification procedures for individual cases; identification of deceased persons in non-disaster contexts
9	Training of service dog handlers: training handlers and dogs for new scents and new disciplines, including searching for different objects such as computer parts, memory sticks, mobile phones, and improvised explosive devices