European Union Strategic Training Needs Assessment 2022-2025

EDUCATE, INNOVATE, MOTIVATE

CEPOL European Union Agency for Law Enforcement Training
Ó utca 27, 1066 Budapest, Hungary
Tel. +36 18038030
www.cepol.europa.eu
Budapest, December 2021
CEPOL

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
This document has been prepared by CEPOL in close cooperation with the European Commission, Member States and EU Agencies. Other European organisations, professional groups and networks also contributed to it, and their assistance is hereby acknowledged with gratitude.

Luxembourg: Publications Office of the European Union, 2022

Print	ISBN 978-92-9211-394-0	doi:10.2825/37545	QR-09-22-117-EN-C
PDF	ISBN 978-92-9211-395-7	doi:10.2825/690443	QR-09-22-117-EN-N

CONTENTS

Preface

CEPOL is the agency of the European Union dedicated to develop, implement and coordinate training for law enforcement officials. With more than two decades of experience in delivering training, we know that correctly identifying from the ground up what and who needs to be trained is at the core of any effective and successful programme.

To this end, and in line with our current mandate, CEPOL has conducted the second EU Strategic Training Needs Assessment (EU-STNA), which aims at identifying the EU-level training priorities in the area of internal security and its external aspects from a strategic perspective for the years 2022-2025. This report aims to contribute to a deeper understanding of the capacity-building needs of law enforcement officials in the next four years, while seeking to avoid duplication of efforts and achieve better training coordination among different EU agencies and other law enforcement training providers.

This report is published at a moment in time where sufficient evidence shows that COVID-19 has given rise to an exponential increase of malicious and criminal activities, which are posing a serious threat to society. Proficiency is essential for law enforcement staff who must be prepared to face these new, emerging threats on a daily basis. This publication identifies what skills gaps need to be addressed to ensure law enforcement officials stay on the cutting edge of technology, knowledge and information.

The need for digital skills and the use of new technologies emerges from this report as a main core capability gap. This finding was somehow to be expected, taking into account that the pandemic has accelerated a second digital revolution sparking new forms of crime. Moreover, the report confirms the need for intensified training efforts in tackling high-risk criminal networks and in building financial investigation capacities among law enforcement officials.

The analysis and recommendations outlined in this report are the result of a participative process, including extensive consultations with policy makers and experts across the EU. To undertake this major multiannual diagnostic exercise, CEPOL has polled, after extensive desk research of strategic documents, more than 80 organisations and expert groups, which gives an indication of the scope of this EU-wide multi-stakeholder consultation.

Also noteworthy, for the first time, the volume of law enforcement officials requiring EU-level training in the European Union has been assessed in absolute terms. Based on the data collected from Member States, more than 110,000 officials would need EU-level training in any of the thematic areas identified during the EU-STNA.

This report would not have been possible without the hard work done by colleagues here at CEPOL, who have provided first-hand contributions to the drafting of this document: organising and moderating workshops, reading and processing a large amount of documents, summarising outcomes of consultations, and so forth.

Lastly, I am also grateful for the involvement of experts and contact points in the EU Member States, EU agencies and other partners who worked with CEPOL to enable the production of this report, and for the excellent cooperation with our colleagues at the European Commission (Directorate-General for Migration and Home Affairs).

I trust that EU and Member States providers of law enforcement training will read and use this report and I very much hope they will deem its findings useful for the purpose of providing strategic guidance on law enforcement training priorities during the period 2022-2025.

Dr.h.c. Detlef Schröder

CEPOL Executive Director

(16 February 2018 – 15 February 2022)

EXECUTIVE SUMMARY

The European Union Strategic Training Needs Assessment (EU-STNA) is a collective and EU-wide effort involving the Member States, European Commission, key experts and stakeholders such as the European Union Agency for Law Enforcement Cooperation (Europol), the European Border and Coast Guard Agency (Frontex) and other EU Justice and Home Affairs (JHA) agencies, established for the identification and prioritisation of EU-level training needs in the area of law enforcement. The coordination of the EU-STNA exercise, serving as a multiannual strategic training needs analysis, forms part of CEPOL's core mandate to support, develop, implement and coordinate training for law enforcement officials. The EU-STNA was piloted in 2017 and the first EU-STNA Report was published in 2018, listing training needs and recommended EU-level training guidelines for the period 2018-2021. It has been found useful as a strategic guideline and lookup tool that helps to align the planning of internal training delivered to the Member States, whereby the findings of the EU-STNA are translated into the work programmes of JHA agencies and guide more detailed training needs analyses that feed into their training portfolios.

Aim of the Report

In order to define the strategic and EU-level training priorities of law enforcement officials for the next 4-year cycle, 2022-2025, of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), CEPOL launched the new EU-STNA in 2020 to identify gaps in knowledge, skills and competences as well as the related training needs. The EU-STNA as a process, and hence this Report, focuses solely on the training dimension in the context of internal security and its external aspects, without mapping or prioritising crime areas. The Report presents the findings of the second EU-STNA exercise conducted during the year 2021, providing an overview of horizontal and thematic areas and listing the capability challenges and the related training needs of law enforcement for the period 2022-2025 in order of priority. The findings are based on the examination of strategic and policy documents as well as on consultations with practitioners, experts and stakeholders. Ultimately, the list of identified EU-level training needs was prioritised by the Member States which also indicated the volume of the necessary training and then shared this with potential EU training providers so as to guide them in building up their training portfolio, thus supporting effective, coordinated and coherent law enforcement training delivery at EU level.

Legal and policy background

Law enforcement training was already intensified through the introduction of the Stockholm Programme for the period 2010-2014, which aimed to foster a genuine European judicial and law enforcement culture. It was noted that more effort would be needed to raise the profile of EU instruments for police cooperation and the role of EU agencies created to support law enforcement services in fighting crime. Although it had been long acknowledged at EU level that training should adequately respond to real needs and more firmly support jointly agreed priorities, for years the EU was lacking a systematic process for identifying and addressing strategic training needs in the constantly evolving area of law enforcement. The year 2013 marked the establishment of the Law Enforcement Training Scheme (LETS), aiming to equip law enforcement officials with the knowledge and skills needed to effectively prevent and combat cross-border crime through efficient cooperation with EU colleagues. The European Agenda on Security, adopted in 2015, identified training as one of the supporting cross-cutting actions to combat serious and organised cross-border crime and terrorism. Furthermore, the Security Union Strategy adopted in 2020 confirms that the current and emerging technological threats call for more investment in upskilling law enforcement personnel at the earliest stage and throughout their career in order to ensure a strong European security ecosystem. The Council Conclusions on setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022-2025 highlight the importance of training, awareness raising and communication on EMPACT and the EU crime priorities in Member States, EU institutions, agencies and bodies. The importance of law enforcement training is confirmed in the Communication from the Commission on the EU Strategy to tackle Organised Crime 2021-2025. One of the key actions set for the Commission is to support the development of training modules and materials and support training delivery by CEPOL. The Council Conclusions on the impact of the COVID-19 pandemic on internal security: threats, trends, resilience and lessons learned for EU law enforcement note that sharing knowledge and information that leads to the detection of crime threats and trends in organised crime groups is crucial for informed and strategic decision-making on how to approach and anticipate future developments in criminal networks. The Council Conclusions on Internal Security and European Police Partnership emphasises that it is especially necessary for law enforcement to receive comprehensive training on how to reap the benefits of using digital technologies, including artificial intelligence. As defined by the Preamble of the CEPOL Regulation, CEPOL should assess strategic training needs and address the EU's priorities in the area of internal security and its external aspects. Pursuant to Article 4.1 of the Regulation, CEPOL is tasked with preparing multiannual strategic training needs analyses and multiannual learning programmes. Against this background and in collaboration with the Commission and the Member States, CEPOL developed the methodology and launched the first EU-STNA on 25 September 2017. The first, pilot EU-STNA was concluded in 2018 and evaluated in 2020. The EU-STNA methodology has been updated based on the outcomes of the evaluation process. Subsequently, the next (present) EU-STNA cycle was launched in 2020 to deliver a comprehensive EU-level training needs assessment for the period 2022-2025.

Findings of the EU-STNA 2022-2025

The second EU-STNA process has revealed eight core capability gaps constituting the main areas in which law enforcement officials need capacity building through training. Furthermore, it has identified 230 training needs clustered in 17 thematic areas as well as 9 other specific training needs included under a separate category. It

has to be noted that the core capability gaps are relevant for all thematic areas of training. Member States have indicated that at present 110 368 law enforcement officials would need EU-level training in the areas presented in this Report.

The core capability gaps of law enforcement officials that can and should be addressed through training are the following (in a weighted order):

- Digital skills and use of new technologies
- High-risk criminal networks
- Financial investigations
- Cooperation, information exchange and interoperability
- Crime prevention
- Document fraud
- Forensics
- Fundamental rights and data protection

Core capability gaps are those areas for training that were identified in all expert group discussions and which therefore apply to all thematic areas. All training activities for law enforcement across the EU should include elements concerning these horizontal aspects.

Given the cross-cutting nature of criminality, the training needs arising from the core capability gaps are often interlinked; hence, the use of a holistic and multidisciplinary approach should be continued and strengthened in addressing them.

Following the presentation of the core capability gaps, the Report provides details on each thematic area in a separate subchapter outlining the main challenges hindering the performance of law enforcement officials in the given area and describing the related training needs.

The training needs on specific topics in the area of law enforcement have been recorded as an outcome of the consultations with experts and are the result of prioritisation by the Member States. In general, the training needs on horizontal aspects that apply to all thematic areas have become even more accentuated than they were 4 years ago when the first EU-STNA exercise was conducted. Largely, training needs in the main thematic areas have remained stable compared to the findings of the previous round of analysis; however, the needs related to the digitalisation of society, economy and criminal operations have become even more evident. In addition to the horizontal aspects covered in the previous EU-STNA, the operation of high-risk criminal networks is now a separate theme as it is also addressed as a distinct category by the EMPACT. Cross-cutting elements such as fundamental rights should continue to be integrated into all training activities and become the norm.

The list below presents the thematic clusters (in order of priority, as communicated by the Member States) in which EU-level training should be delivered to law enforcement officials in the next 4 years (2022-2025) in order to support the EU's response to serious and organised crime and other threats to internal security:

1. Cyber-attacks
2. Criminal finances, money laundering and asset recovery (Fraud, economic and financial crimes)
3. Counter-terrorism
4. Trafficking in human beings
5. Drug trafficking
6. Migrant smuggling
7. Child sexual exploitation

8. Online fraud schemes (Fraud, economic and financial crimes)
9. Organised property crime
10. Border management and maritime security
11. Firearms trafficking
12. Missing trader intra-community fraud (Fraud, economic and financial crimes)
13. Corruption
14. Excise fraud (Fraud, economic and financial crimes)
15. Intellectual property crime, counterfeiting of goods and currencies (Fraud, economic and financial crimes)
16. Environmental crime
17. External dimensions of European security
18. Other thematic areas

The EU-STNA distinguishes between environmental challenges and those concerning the knowledge, skills, responsibility and autonomy of law enforcement officials. While the former are determined by the conditions in which law enforcement officials operate and cannot be solved by training (e.g. lack of technical equipment, differences in legislation across Member States, etc.), the latter refer to the capabilities, attitude and behaviour of officials and can be addressed through training.

While a number of law enforcement groups contributed to the overall process of the EU-STNA (see Annex 4 for the complete list of contributors), CEPOL also invited relevant European agencies and other entities actively involved in internal security and the related training delivery to share their opinions on the prioritisation of training needs and to indicate their availability to support the training efforts in different thematic areas. In total, twelve EU-level training providers[1] submitted their contributions in writing. The majority of the consulted parties endorsed the prioritisation carried out by the Member States; however, the consultation phase also brought to light sensible insights and complementary training aspects, indicated areas where training providers could establish further cooperation and uncovered specific plans for training and programmes as well as suggestions to improve the strategic training needs analysis in future. Annex 6 provides an overview of all training needs and potential training providers. The list resulting from the participatory process is indicative, paving the way for an EU-level law enforcement training offering; however, it does not define specific training activities or their form, level, content and target group. Therefore, a more detailed analysis will be necessary at operational level before specific training activities can be developed. The findings of the consultations are presented in a dedicated chapter, but the overall Report includes the advice and expert opinions of the practitioners consulted.

EU-level training provision

In the context of the EU-STNA, EU-level training activities refer to Strands 3 and 4 of the LETS as identified in Commission Communication COM (2013)172, namely EU thematic policing specialism and civilian missions and capacity building in third countries. Thus, the EU-STNA focuses solely on EU-level priorities, as national training and bilateral/regional training cooperation remain outside the scope of the process. Since the importance of training has only grown in recent years, as a result of evolving criminal matters, there is a continuous demand for a high-quality training offering. In brief, EU-level training should:

(1) European Asylum Support Office, European Border and Coast Guard Agency, European Commission, European Crime Prevention Network, European Institute for Gender Equality, European Judicial Training Network, European Monitoring Centre for Drugs and Drug Addiction, European Public Prosecutor's Office, European Union Agency for Criminal Justice Cooperation, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, and European Union Agency for Fundamental Rights

- cover recent policies as well as operational (modus operandi), tactical, technological, scientific, research and other developments, with a strong focus on emerging digital technologies and the next-generation platforms for key law enforcement processes;
- continue applying the effective method of practice-oriented training based on real-life scenarios, investing in new means to engage participants and achieve performance objectives (such as scenario-based virtual reality training, which has a high potential in the area of law enforcement), and increase the use of the train-the-trainers approach;
- promote the concept of administrative crime prevention measures and, where possible, the organisation of joint training to bring together law enforcement, prosecution, the judiciary, tax authorities, and other competent officials with the aim of improving multidisciplinary and inter-agency cooperation;
- integrate research findings into curricula design, notably findings and training materials developed by the projects funded through the EU Security Research Programme, i.e. under the Horizon 2020 (H2020) and Horizon Europe (HE) Fighting Crime and Terrorism (FCT) and Border Management (BM) strands;
- enhance partnerships with non-law enforcement actors, the judiciary, the private sector as well as academia and other relevant research entities through, among others, a closer cooperation with the Community of European Research and Innovation for Security (CERIS), which brings together all these actors;
- support the exchange of experience and the sharing of best practices among Member States and practitioners on top of building their subject-matter expertise, such as through the EU Innovation Hub for Internal Security, since common and coordinated action, close cooperation and information sharing are needed at tactical and operational levels in the area of law enforcement;
- consider the external dimensions of internal security and further develop cooperation with third countries, e.g. by training officials in non-EU countries or inviting international participants for training in Europe, when applicable;
- as a lesson learned from the COVID-19 pandemic, support European law enforcement in being prepared for effective response to crisis situations.

Furthermore, while the Member States are responsible for providing basic-level training at national level, ensuring that law enforcement officials are prepared for duty in general, the EU-STNA has pointed out that, due to the volume of emerging challenges, EU training providers such as JHA agencies should have more resources to develop training packages and explore other awareness-raising measures on emerging trends. In addition, the EU-STNA has once again revealed the importance of deepening cooperation and coordination among different EU agencies and with other European law enforcement training providers.

Considerations related to EMPACT priorities

While the aim of the EU-STNA is to identify training priorities instead of ranking crime threats, the findings are in line with the European Multi-disciplinary Platform Against Criminal Threats (EMPACT) priorities for the next 4-year cycle, 2022-2025. Being the EU's flagship initiative for the fight against organised crime, EMPACT is now recognised as a permanent instrument against criminal threats through which the Member States, agencies and other partners work closely together. In this respect, it was noted during the consultations that EU-level training should also focus on raising awareness among EU law enforcement officials and beyond on how EMPACT works as an instrument. Furthermore, now that the new EMPACT cycle, 2022-2025, started, it is important to analyse the need for more in-depth and thematic trainings for specific target groups (e.g. EMPACT Drivers and Co-drivers). This approach is supported by the fact that CEPOL is the coordinator of the EMPACT common horizontal strategic goal "Capacity building through training, networking and innovation" during the cycle 2022-2025.

Final considerations

Regardless of the field, continuous learning and the constant expansion of skills and knowledge through training are essential in today's world. Considering the rapidly shifting security landscape, with challenges on every front, and the speed of developments impacting the field, training has a central role to play in ensuring enhanced skills in the field of law enforcement. The importance of investing in upskilling law enforcement personnel and equipping them to adapt and respond to unprecedented challenges has been acknowledged at EU level in the new European Security Union Strategy for the period 2020-2025, which focuses on priority areas where the EU can bring value to support Member States in fostering security for all those living in Europe. Needs-based and timely

training must be an essential component of an EU culture of security, to which all European training providers in the field of law enforcement should contribute.

The volume of training needed across Member States is considerably higher than the training capacities of training providers for law enforcement, which calls for the allocation of additional human and financial resources to these institutions. While Member States can benefit from the Internal Security Fund to ensure national-level training activities, the resources of EU-level training providers should be increased so that they can address the growing requirements.

This EU-STNA Report will be shared with the European Commission and will be presented to the Standing Committee on Internal Security for endorsement and to the European Parliament for information with a view to establishing a structured policy for law enforcement training at EU level. While awaiting an opinion from these EU institutions, EU training providers are encouraged to coordinate their training provision with others and align it with the identified training priorities, thus ensuring that the capability gaps of law enforcement officials are addressed.

1. INTRODUCTION

With the aim of identifying the strategic and EU-level training needs of law enforcement officials for the next 4-year cycle, 2022-2025, of the European Multidisciplinary Platform Against Criminal Threats, CEPOL launched the second EU Strategic Training Needs Assessment in December 2020.

The EU-STNA is primarily used as a strategic guideline and lookup tool. Furthermore, it is used at EU level to align the planning of internal training delivered to the Member States, whereby the findings of the EU-STNA are integrated into the work programmes of Justice and Home Affairs agencies. CEPOL relies on the EU-STNA training priorities when conducting operational-level training needs analyses that feed into its training portfolio. Europol and Frontex implement the EU-STNA in their yearly training needs assessment. Additionally, the EU-STNA has been used as a source of information and as a tool to avoid training offer overlaps.

The EU-STNA is a multi-stakeholder and multistep exercise coordinated by CEPOL every 4 years. 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 EU level. Subsequently, the identified training needs are prioritised by the Member States which also indicate the volume of training needed. Finally, the findings of the process 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.

1.1. Background

Back in 2012/2013, it was noted that the European Union lacked a systematic process for identifying and addressing strategic training needs, which are constantly evolving. This was then included in the draft CEPOL Regulation, which was finally adopted by the European Parliament and the Council of the EU in late 2015 (Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA). In the new CEPOL Regulation, the co-legislators mandate CEPOL to assess the strategic training needs of the Union.

As set out in the Preamble of the Regulation, to avoid duplication or overlap and to ensure better coordination of training activities for competent law enforcement officials carried out by Union agencies and other relevant bodies, CEPOL should assess strategic training needs and address Union priorities in the area of internal security and its external aspects. Pursuant to Article 4.1 of the Regulation, CEPOL is tasked with preparing multi-annual strategic training needs analyses and multi-annual learning programmes.

At the same time, the European Agenda on Security identified training as one of the supporting cross-cutting actions to combat serious and organised cross-border crime and terrorism. Training is essential in order to allow authorities on the ground to 'exploit the tools' in an operational situation. This is also confirmed by the current EU Security Union Strategy.

Taking into consideration the complex and rapidly evolving environment in which law enforcement officials operate as well as the presence of several training providers, the EU-STNA aims to assess strategic training needs and address EU priorities in the area of internal security and its external aspects, with a view to better coordinating training activities for law enforcement officials and avoiding the duplication of efforts.

The findings of the first, pilot EU-STNA were published in 2018 and helped to define the strategic training priorities of European law enforcement up to 2021. The present EU-STNA covers the period from 2022 to 2025.

1.2. Methodology

The EU-STNA entails a detailed analysis and the identification of those priorities in the area of internal security that have a training dimension and should be addressed at EU level.

Based on the outcomes of an external evaluation of the first, pilot EU-STNA for the period 2018-2021, CEPOL has updated the methodology, adding two additional steps on top of the established process architecture. Thus, the updated EU-STNA methodology also covers the implementation of the outcomes with increased political support and a mid-term review of threats and training priorities.

The overall process consists of a systematic analysis of strategic EU documents detailing crime threats, the findings of which are then discussed in expert and focus groups by Member State and EU specialists with a view to identifying capability gaps and training needs that should be addressed by training activities implemented at EU level.

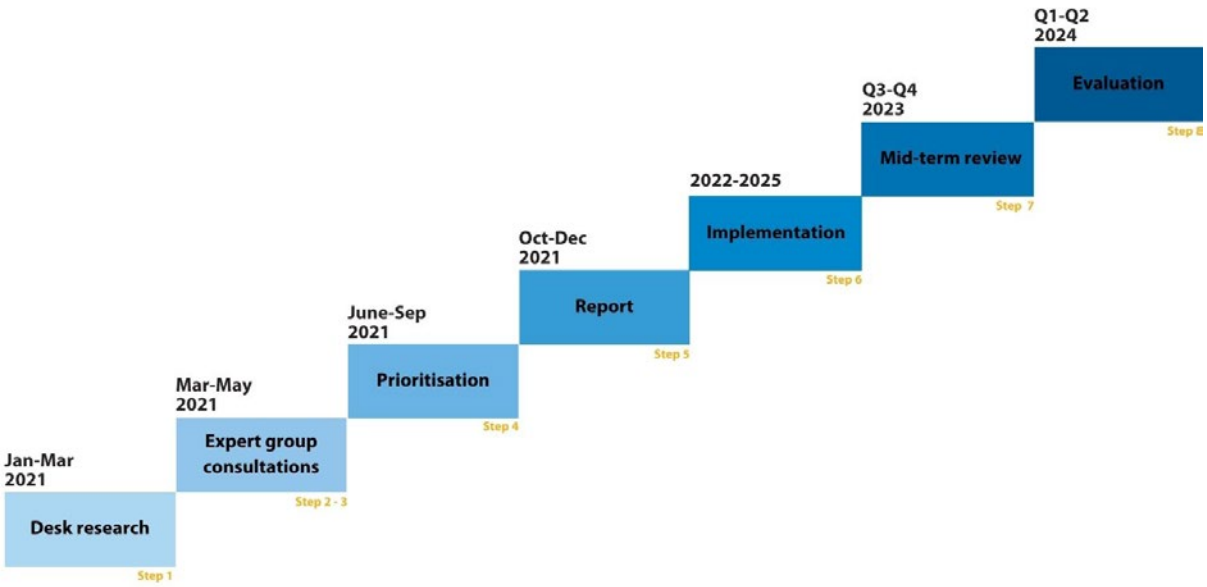


Figure 1. Overview of EU-STNA methodology and timeline

In order to establish the basis for further discussion and prioritisation, the EU-STNA starts with a comprehensive desk research exercise, a form of qualitative research using already existing secondary data, collected without fieldwork, such as the key policy documents on EU internal security issues and on serious and organised cross-border crime provided by the Directorate-General for Migration and Home Affairs (DG Home) and JHA agencies. The EU-STNA desk research focuses on gathering information on security threats, horizontal aspects and law enforcement capability challenges, which is then clustered into thematic categories.

After the completion of the thorough desk research, CEPOL consults the existing expert groups and networks, applying the research method of focus groups in order to collect data through group interaction. The expertise of these groups is absolutely essential for understanding the capability challenges that the law enforcement community is facing in a specific field. Subsequently, the identified training needs are prioritised by the Member States at the strategic level, which also indicate the volume of training needed, and the outcomes are shared with EU training providers for their comments and for training coordination purposes.

At the end of the analysis phase, the EU-STNA Report (the present document) is drafted and presented to the Standing Committee on Internal Security for endorsement and to the European Parliament for information. Thus, the EU-STNA will suggest a distribution of tasks among EU-level training providers and will inform and facilitate the planning of training activities.

In order to ensure that new documents released after the finalisation of the EU-STNA Report are also taken into account, a mid-term review will look at whether any new capability challenges and related EU-level training needs have emerged. Finally, the EU-STNA process will be completed with an evaluation phase, during which the lessons learned will be identified with the aim of improving the next EU-STNA cycle and its methodology, always covering a 4-year period aligned with the EMPACT cycle.

1.3. Timeline and process

In order to define strategic and EU-level training priorities in the area of law enforcement for the EMPACT cycle 2022-2025, CEPOL launched the second EU-STNA in December 2020.

Step 1 of the EU-STNA process was conducted between January and March 2021. The list of documents to be analysed through desk research was approved in two rounds by DG Home on 26 January and 11 February 2021. The processing of the research data, containing policy documents, reports and other relevant material, was carried out by CEPOL, supported by a group of three external researchers. In total, 316 documents (see Annex 3 for the complete list of documents) were analysed as part of the desk research. Later on, CEPOL completed and updated the desk research, taking into consideration the findings of the Serious and Organised Crime Threat Assessment (SOCTA), published by Europol, as well as the draft regulations on the establishment of funds to support activities related to European security. The desk research was further revised and supplemented in May 2021 to incorporate crime threats as prioritised by the European Council in the Council conclusions setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022–2025.

During the first half of 2021, CEPOL implemented Steps 2-3 by initially launching 20 online focus groups with experts and networks, including all 14 EMPACT groups of the 2018-2021 Policy Cycle (see Annex 4 for the complete list of expert groups consulted). In order to gather further information on the strategic-level training needs of law enforcement, CEPOL invited 24 professional networks to a written consultation, 13 of which provided input (see Annex 5 for the complete list of professional networks consulted). As stipulated in the Roadmap for implementing the recommendations of the independent evaluation of the EU policy cycle 2018-2021, CEPOL briefed the community of National EMPACT Coordinators (NECs) and asked for feedback on the outcomes of the expert group meetings. This written consultation resulted in six Member States providing comments and feedback on the draft list of training priorities defined by the focus groups in the EMPACT thematic areas. The European Union Agency for Fundamental Rights (FRA) gave feedback on the draft list of training priorities and core capability gaps via a Skype interview. Table 1 below summarises the number and type of parties consulted during the process (see Annexes 4 and 5 for full details on the consulted parties):

Type	Number	% of total
European Commission	1	1.3
JHA agencies	9	11.1
Professional networks	24	29.6
National EMPACT Coordinators	27	33.3
EMPACT groups	14	17.3
CEPOL Knowledge Centres	2	2.5
CEPOL Expert Group	1	1.2
Other organisations (EJTN, EUCPN, EEAS, ESDC, EPPO)	5	3.7
Total	**83**	**100**

Table 1. Number and type of organisations consulted

In the framework of the consultations, the participating experts highlighted and discussed the challenges faced by law enforcement officials in specific fields and identified areas that should be addressed by training at EU level. The outcomes of the discussions, complemented with the findings of the initial desk research and the information gathered via the written consultation, resulted in a list of 8 core capability gaps with 93 related horizontal training needs to be addressed in all crime areas, 17 main thematic categories comprising 230 training needs, and 1 category covering 9 other thematic areas.

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

Table 2. Core capability gaps and thematic training areas identified

In June-August 2021, as part of Step 4, the findings were distributed among the Member States with a request to prioritise the training needs and estimate the volume of training needed. The Member States were approached via the contact points communicated to CEPOL by the Law Enforcement Working Party, which nominated national representatives in January 2021 to express the Member States' official positions. All EU Member States responded. The communicated ranking was then weighted accordingly by the coefficient equal to the proportion of the country's representation in the European Parliament. The final list of priorities was shared with the European Commission, JHA agencies, the European Judicial Training Network (EJTN), the European Security and Defence College (ESDC), the European Crime Prevention Network (EUCPN), the European Union Intellectual Property Office (EUIPO), the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO) for their opinion on the prioritisation and for potential training coordination. Lastly, both the results of the prioritisation and the draft report were shared with the European Commission.

The priority list of topics in each main area was cross-checked for core capability gaps. The training priorities related to core capability gaps were selected, while maintaining the ranking assigned by the Member States in each main area, which resulted in a prioritised list of core capability gaps as described in the next chapter.

In parallel with the prioritisation process, Member States were asked to specify the volume of training needed. This is the first exercise of this kind to estimate the number of law enforcement officials who would need EU-level training. Some respondents indicated a range of potential trainees, while others estimated over a certain number. In order to ensure consistency, the minimum number indicated was taken into account in all cases. As this was the first time this indicator was measured, special attention will be given to this aspect in the next methodology review.

Altogether, 110 368 law enforcement officials need EU-level training in the main thematic areas identified dur-

ing the EU-STNA. This volume was specified by the Member States during the prioritisation process, where they disclosed the estimated volume of training needed on each subtopic. It has to be noted that this figure does not include officials to be trained in non-EU countries. The volume of training needed to address core capability gaps is included in the volume indicated under the main topics. The largest number of officials need training in relation to drug trafficking, criminal finances, money laundering and asset recovery, and cyber-attacks. The lowest volume of training is requested on topics related to the external dimensions of EU security, which can be explained by the fact that it is a narrower category than the others and the estimate does not refer to the training needs of non-EU officials. The estimated volume of training is listed in Annex 7.

In October 2021, CEPOL initiated Step 5, the drafting of the EU-STNA Report, which lists the key EU training needs and indicates potential training providers. The Report was finalised in November 2021, then shared with DG HOME. The final Report will be presented to the Standing Committee on Internal Security for endorsement and to the European Parliament for information, providing these bodies with a basis for the development of a law enforcement training policy for the upcoming years.

The mid-term review (Step 7) of possible new threats and training priorities will be conducted in 2023, more precisely during months 27–30 of the EU policy cycle. Step 8, focusing on assessing the impact of the second EU-STNA and identifying possible improvements for the next cycle, will be carried out by an external evaluator, contracted by CEPOL in 2023. Thus, the evaluation will be conducted during the first half of 2024 in order to allow sufficient time for possible methodology adjustments and for the alignment of the next EU-STNA with the future EMPACT cycle 2026–2029.

2. CORE CAPABILITY GAPS

Core capability gaps are those horizontal areas that came up frequently as training needs during the EU-STNA process, in the course of both document analysis and expert consultations. These topics should be reflected in all training activities targeting law enforcement, independent of the thematic area, and should therefore be included in the training curricula of EU training providers.

List of core capability gaps:

1. Digital skills and 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

Based on the information gathered from the regulations, policy documents and reports analysed, which was further processed with the expert groups and networks possessing specific knowledge on the challenges faced by the law enforcement community in a given field, and then acknowledged by the Member States, the EU-STNA process has identified eight core capability gaps constituting the main areas where the capacity building of law enforcement officials should be addressed through training. Most of the capability challenges registered during the second EU-STNA process were the same as those identified in the previous cycle, indicating that further investment in training is necessary to ensure that law enforcement capacity is in line with the requirements of the complex and continuously evolving security environment. Nevertheless, the renewed EU-STNA exercise has also brought up some new aspects resulting, on the one hand, from the continuously changing practices of both authorities and criminal groups and, on the other hand, from the recent COVID-19 pandemic. As these aspects are and will continue to be tackled by H2020 and HE FCT projects that also develop related training materials for law enforcement, cooperation with these projects would optimize the efforts and the EU investment, creating synergies and avoiding duplications.

This chapter presents the core capability gaps and their key features and provides a detailed list of the training needs related to each gap.

Figure 2. Core capability gaps

The highest priority has been given to the need for ***digital skills and the use of new technologies***. Technological innovations continue to change the law enforcement landscape, and the related training needs have been revealed by the process of identifying the core capability challenges across the European law enforcement community. Despite the investments already made in improving digital skills and the use of new technologies among

law enforcement officials, the EU-STNA process has identified a number of specific areas where further efforts are required, both in terms of building professionals' capacity to use advanced technology and deepening their understanding of how technology is utilised for criminal purposes. Based on the need for enhanced skills in today's law enforcement professions, the main categories identified during the EU-STNA analysis and consultations include law enforcement's advanced cybersecurity knowledge regarding how to use online surfaces, such as open source intelligence (OSINT), the dark web, and social media, as well as other methods (e.g. artificial intelligence, big data analysis, methodologies applied to quantitative and qualitative analysis of information, etc.) for investigation. The European Counter-Terrorism Centre (ECTC) observed that the use of artificial intelligence (AI) should be given high priority. FRA noted that all training activities addressing AI and big data should make reference not only to data protection but also to other fundamental rights, in particular non-discrimination and access to an effective remedy. As indicated by Europol, there is a gap in generic training on topics related to mass data, data protection, machine learning, and law enforcement cooperation and EU cooperation tools.

Detailed list of training needs:

Digital skills and use of new technologies
Cybersecurity fundamentals for EU officials' everyday use (cyber hygiene, cybersecurity guidelines, secure exchange of information, physical security).
Raising awareness of the most important cyber-threats (e-mail based attacks, web-based attacks, DDoS attacks, social media scams). Understanding the cybersecurity challenges from the modern technologies, like AI or 5G.
Better, modern and validated tools and training materials for tackling activities related to disinformation and fake news that are considered as crime or could lead to crime and are supported by advanced digital technologies.
Digital investigation: OSINT, dark net, cyber threat intelligence (CTI) knowledge management, decryption, use of AI, big data analysis, quantitative and qualitative analysis methods, internet of things, advanced use of camera systems, drones, exoskeletons and speech processors, big data analysis for prediction of criminal behaviour, cryptocurrencies
Digital forensics
Victims' protection
Fundamental rights and data protection

As indicated by the National EMPACT Coordinator of the Czech Republic, training should also address some technological challenges related to streamlining police work, such as the advanced use of camera systems, drones and exoskeletons, the use of speech processors in communication between police officers and clients speaking foreign languages, and big data analysis for the prediction of criminal behaviour.

Organised crime being a major threat to European security overall, the EU-STNA findings confirm the need for intensified training efforts in tackling ***high-risk criminal networks***, with special emphasis being placed on those using corruption, acts of violence, firearms and money laundering through parallel underground financial systems. Further efforts are required at various levels, ranging from advanced training on the functioning and operations of criminal networks to the identification of high-value targets during investigations. Law enforcement training should support the EU goals to disrupt organised crime structures and equip authorities with an advanced skillset for tackling particularly serious forms of organised crime, such as those crimes committed by mafia-style groups. The Operational Network to Counter Mafia-style Serious and Organised Crime Groups (@ON) expressed that training would be necessary mostly for senior law enforcement officials engaged in investigations countering international organised crime groups and mafia-style groups. Training should focus on the differences in legislation across Member States, elements of transnational cooperation and specific aspects (organisational structure, modus operandi, communication, etc.) of different top-level criminal organisations and mafia-style

groups. As these aspects are and will continue to be tackled by H2020 and HE FCT projects that also develop related training materials for law enforcement, cooperation with these projects would optimize the efforts and the EU investment, creating synergies and avoiding duplications.

Detailed list of training needs:

High-risk criminal networks
Structure and operation of criminal networks; identification of criminal networks, new technologies facilitating crime, emerging threats, corruption
Identification of high-value targets during investigations, and addressing these
Sharing of strategic and operational data
Common and coordinated action, close cooperation and information sharing among Member States (e.g. common legal, judicial and investigative frameworks; prevention-oriented information) and with other actors, including Common Security and Defence Policy (CSDP) missions and operations
Cooperation with other initiatives, projects and relevant actors
Operational Network to Counter Mafia-style Serious and Organised Crime (@ON)

Given the increasing volume of criminals orchestrating fraud and economic and financial crimes, ***financial investigation*** capacities stand out as one of the core capability gaps to be addressed through training. Financial investigation is an essential tool of a modern and effective response to criminal threats including terrorist financing. The EU-STNA has identified a number of requirements for skills and knowledge enhancement in this area, ranging from general basic knowledge on financial investigation and asset recovery to new crime patterns, including the evolution of fraud and financial crime in the age of cybersecurity. An emerging theme within this area concerns the measures for further strengthening the fight against dirty money, e.g. anti-money laundering in the era of crypto assets and countering the financing of terrorism. Another need is related to the technical aspects of investigation and the use of modern technologies (such as AI, big data analysis, and OSINT technicity for cryptocurrency seizures) in today's financial investigations.

Detailed list of training needs:

Financial investigations
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, financial intelligence units (FIUs), judicial cooperation
Modus operandi: existing and new crime patterns (non-tangible tokens, new modes of terrorist financing), criminal financing methods, cash-based (cash carriers, money mules), money laundering via normal financial system (electronic), offshore challenge to conceal beneficial ownership, informal value transfer system (e.g. hawala), underground banking, international transfers bolstered by fictitious contracts and invoices, bitcoin trading, trade-based money laundering, money laundering via virtual currencies, virtual currency conversions/cryptocurrency tumblers, complex financial schemes, money laundering as crime-as-a-service, corporate economic crime, fraud schemes (subsidy fraud, bank fraud, investment fraud, CEO fraud, non-delivery fraud, romance fraud, social benefit fraud);
Technicalities and information priorities, technical aspects of investigation, modern technologies, use of AI, big data analysis, OSINT technicity of virtual coins (seizures)

In line with the EU's integrated approach to internal security, the EU-STNA process has revealed the need for greater cooperation and information exchange among police, border and coast guard, customs, judicial, administrative and tax authorities, as well as with EU institutions, bodies, agencies and relevant networks. In the area of ***law enforcement cooperation, information exchange and interoperability***, the capability challenges that should be addressed through training concern operational cooperation among Member States' law enforcement authorities, including information exchange as an essential aspect of ensuring internal security. The Schengen Information System – Supplementary Information Request at the National Entries (SIS–SIRENE) Committee mentioned the importance of delivering basic and advanced SIRENE seminars on how SIS could enhance the work of law enforcement and the continuous updating of officials' knowledge on new regulations concerning EU information systems. Coordination in terms of control and operations related to trade in illicit goods and services was highlighted as one of the capability challenges, which brings to light the need to extend cooperation even outside the European law enforcement community and further strengthen partnerships with the judiciary and the private sector. Furthermore, to overcome the cooperation challenges in an area relating to freedom, security and justice, more attention should be paid to interoperable law enforcement. The interoperability of information systems, which facilitate data exchange and information sharing, and the use of such systems continuously create new modes of law enforcement cooperation; therefore, they remain a core capability challenge to be addressed through training during the next cycle. Italy suggested sharing specific actions implemented in EMPACT groups to the benefit of the European law enforcement community.

Detailed list of training needs:

Cooperation, information exchange and interoperability
General overview of EU cooperation tools and instruments, including Police Code
Use of international cooperation tools for prevention and administrative proceedings
Joint operational activities and regional cooperation, joint investigation teams (JITs)
Cooperation with the United Kingdom
Cooperation with non-EU countries, including EMPACT mechanisms
Cross-border surveillance
Coordinated detection measures and investigations between the judiciary and police, including operational task forces aiming at identifying and arresting high-value targets
Coordinated prosecutions
Identification, collection and sharing of good practices on judicial cooperation
Use of special tactics, initiatives and practices such as witness protection programmes, European tracking solutions, EU most wanted list, undercover operations, controlled deliveries, etc.
Promoting a multidisciplinary/administrative approach
Promoting and raising awareness of information exchange instruments
Quality standards for storing data in EU information systems or interoperability components, general framework of data quality
Minimum standards for information exchange via Prüm framework in line with actual legal and technical developments

Cooperation, information exchange and interoperability
SIS: use and possibilities offered for investigations
SIRENE: new regulations, how to work with partners, enhancing the network; basic and advanced training
General single point of contact (SPOC) training including all existing and new systems, actual problems, sharing best practices
Passenger name record (PNR): exchanging best practices in diverse implementation of PNR and passenger information units (PIUs), awareness of national regulations and practices on cooperation among PIUs; PNR and data analysis
Sharing data with non-EU countries
How to access and combine EU funds (interoperability as a horizontal aspect)
Fingerprint scanning, including shared biometric matching service (sBMS), quality and fundamental rights including data protection
Biometric identification
Components of interoperability: how they work and how they can be used in investigations
Technical training for interoperability system operators
Safeguarding fundamental rights including data protection and data subject rights

In order to support taking action to stop crimes before they happen, the EU-STNA has uncovered numerous requirements for EU-level training on ***crime prevention***. Further efforts are required to raise awareness of the social, economic and political factors that influence today's crime scene and of the role that law enforcement can play in reducing and preventing disturbances and different forms of crime. It is important to raise awareness regarding the availability of European Crime Prevention Network (EUCPN) resources that can support law enforcement authorities in carrying out basic community policing functions competently and efficiently in close contact with residents. Since preventing local, national or international crime never follows a single-agency approach, sharing knowledge/data, collaborating with the relevant agencies and applying a multidisciplinary approach in crime prevention training have been highlighted as necessary. Furthermore, it is crucial to foster a relationship of trust between the police and society as a whole in all its diversity in today's EU; therefore, training provided in this area must focus on emphasising the principle of non-discrimination.

Detailed list of training needs:

Crime prevention
Role of crime prevention in tackling organised crime and role of law enforcement in crime prevention, e.g. training on community policing
Relevance of prevention, administrative measures
Prevention of crisis escalation
Use of AI solutions in prevention; proactive prevention/preventive prognostic procedures
Funding opportunities for prevention, EU fund management

Crime prevention
Approach of law enforcement to different target groups, reducing risk of discrimination (homeless, people in poverty, young criminals, religious background, ethnicity, migrants)
Using a domestic violence-informed approach in law enforcement interventions
Gender-based digital violence: how to obtain evidence, how to proceed, more efforts to detect crime related to social media
Perpetrator pattern-based approach: how perpetrators can manipulate the system, referral to perpetrator programmes
Agency and partnership approach (public and private) to be integrated into crime-specific training
Community policing, EUCPN toolbox
Evaluation of prevention activities

Being one of the fastest growing criminal industries in the world, ***document fraud*** is a central challenge for border security, internal security and migration management in the EU. It is often an essential element of other criminal activities, such as smuggling of drugs, firearms, and stolen vehicles, trafficking in human beings and migrant smuggling, not to mention its potential connections with terrorism. Expertise in tackling document fraud is becoming increasingly important because of the evolving, highly sophisticated methods and techniques used by criminal groups involved in document fraud. The EU-STNA has confirmed the need to further enhance general capacity in the prevention and detection of fraudulent documents, and to put a strong emphasis on understanding modern-day sophisticated document fraud, including the online trade in counterfeit documents, as well as on combining human expertise and advanced automated technology, such as AI, in order to detect fraud. The training offering in this area should also support cooperation and coordination among the authorities involved in the fight against document fraud.

Detailed list of training needs:

Document fraud
Link to other crime areas: clandestine movement of criminals and terrorists, drugs (new psychoactive substances), migrant smuggling, trafficking in human beings (identity, permits), trafficking in firearms and stolen vehicles, falsifying car registration documents and manipulating vehicle identification numbers
Modus operandi: sale of counterfeit or stolen documents on surface web and dark web; criminal use of technology for document fraud (face morphing, UV-curing ink, laser, engraving, nanographic printing, holographic stickers)
Detection of fraudulent documents (supporting/breeder documents, personal identification - comparing the person with the photo inside the document); collection of operational evidence when detecting fraudulent documents
Investigation: creating links between analysts and investigators, sharing relevant case studies; general trends and investigative techniques; dedicated databases for the law enforcement community

Tremendous change has also occurred in the field of ***forensics***, which explains why this has been identified by those involved in the EU-STNA as one of the core capability gaps that should be supported by EU-level training. Modern technology has developed forensic science considerably; however, the methods of criminals have also evolved with the advancement of technology. EU forensic experts must be aware of the latest changes affecting

current and future practices. Digital forensic experts must be skilled in extracting data from multiple sources without modifying them, enabling them to preserve the source of evidence for authenticity and integrity. With the latest technology updates, training in this area should have a strong focus on acquiring and using electronic evidence, e.g. in detecting cybercrime and seizing virtual currency.

Detailed list of training needs:

Forensics
Biometrics
Electronic evidence: securing, analysing, storing
Lawful hacking
Presentation of e-evidence, use of e-evidence in prosecution
Exchange of e-evidence, cross-border access to e-evidence, retrieval, judicial access to e-evidence; cross-border requests to online service providers
Collection of battlefield information and use of open source evidence to support war crime prosecution
Structuring mass data and information
Seizure of virtual currency and its use in the evidential chain
Data retention
Post-seizure analysis of high-value seizures (data can feed into the risk management framework)

The EU-STNA findings reiterate 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. Several new capability gaps have been identified: as a lesson learned from the global COVID-19 pandemic, there is an emerging need to pay increased attention to the protection of fundamental rights in extraordinary situations such as lockdowns, specifically considering the protection of vulnerable groups, in particular migrants and children as well as victims of domestic violence. A general introduction to fundamental rights is a training topic to be addressed for operational officials and managers. Further training topics cover the rights of children and minors, victims' rights, and hate crime and hate speech. New topics in the area of fundamental rights that need to be covered by specific training for law enforcement also include the procedural rights of non-EU citizens and the handling of gender/sexual violence. ***Data protection*** is a fundamental right stipulated by law at both national and EU level. As FRA highlighted during the EU-STNA consultations, the use of specific new technologies, such as AI and big data, is a comprehensive fundamental rights matter not only in terms of data protection but also considering the principles of non-discrimination and access to an effective remedy. Since law enforcement has already become largely data-driven and data plays a crucial role in the prevention, investigation, detection and prosecution of criminal offences, the use of personal data for these purposes raises multiple questions regarding the application of human rights principles, including how to regulate the investigatory powers of the state while respecting the essence of fundamental rights and freedoms. This situation creates a considerable number of training needs. Privacy and the use of new technologies go hand in hand, so law enforcement needs further support in developing skills, knowledge and solutions that enable them to reap the benefits of new technologies, information accessible online and turning personal data into analytical insights, while simultaneously ensuring the secure management of data in the course of any action taken by the authorities.

Detailed list of training needs:

Fundamental rights and data protection
General introduction to fundamental rights, especially online aspects
Fundamental rights knowledge in relation to receiving complaints from individuals belonging to vulnerable groups (complaints related to gender/sexual violence, hate crime); how to ensure fundamental rights for people with special needs and mental health issues, or for vulnerable groups, victims and suspects
Protection of fundamental rights in extraordinary situations such as pandemics, i.e. during lockdowns, notably for vulnerable groups (migrants, children, etc.), cooperation with NGOs
Impact of use of new devices on fundamental rights; victims' perspective
Raising awareness among police officers of standards applicable to police stops and of the damaging effect of discriminatory profiling practices on community relations and trust in law enforcement
Victims' rights: legal and psychological aspects, how to deal with traumatised victims; police officers as victims
Management and leadership training, zero tolerance towards non-respect of fundamental rights, handling and rights of whistleblowers, discriminative profiling
Handling gender during investigations, European Institute for Gender Equality (EIGE), Independent Police Complaints Authorities' Network (IPCAN)
Cooperation with judicial authorities
Fighting hate crime, racism and discrimination, how to deal with different -isms and unconscious bias towards underrepresented groups in society (elderly people, anti-ziganism, anti-semitism)
Procedural rights of suspects and the accused
Rights of persons deprived of their liberty
Rights of children as victims, perpetrators, witnesses; communication with children, interviewing techniques, processing children's data; interdisciplinary cooperation
Fundamental rights aspects of using datasets, predictive policing
Awareness of data protection principles during investigations, data protection impact assessment regarding data processing; fundamental rights and data protection when using different modern technologies (AI, facial recognition)
Use of data by police covering different areas of fundamental rights; legal requirement stemming from Directive; contact with data protection authorities, case studies, how to build investigations, mutual learning, what is legally non-compliant, etc.
Use of content by law enforcement officials when investigating (fight against terrorism, hate speech); how far legitimate interest of security can go; freedom of expression, freedom of information, legal content on the internet
Citizens' access rights to police data: data subject access requests, rights, how to process requests, time limit to respond, refusal grounds for police, privileges of law enforcement, freedom of information requests

Fundamental rights and data protection
Technical and organisational matters for protection of personal data within modern technologies
General Data Protection Regulation (GDPR) challenges for public–private partnerships for law enforcement
Access to e-evidence, linked to access to justice and victims' rights
Training for data protection officers
Protection of minors' personal data: how to process their data, how to record their data in police databases, application of extra data protection safeguards

3. EU TRAINING PRIORITIES

This chapter presents the training needs identified and prioritised by the Member States in the area of law enforcement that the European Union is recommended to address in the next 4-year cycle (2022-2025). The analysis in each subchapter reflects the outcomes of the consultation process with the relevant expert groups and networks as well as the input from European training providers; hence, it does not necessarily represent the official view of CEPOL.

The order of subchapters reflects the prioritisation of training needs carried out by the Member States and not that of crime threats. It shows where law enforcement officials across Member States consider capability gaps to be bigger and where they feel that more training is essential in order to increase effectiveness in tackling crime, without considering crime statistics.

Each thematic subchapter starts by presenting the major challenges that influence the efficiency and effectiveness of EU law enforcement. Challenges are divided into two categories:

- environmental challenges related to the conditions in which law enforcement officials operate, which have a substantial influence on their performance but cannot be solved through training;
- challenges concerning the knowledge, skills, responsibility and autonomy of law enforcement officials, which also have a substantial influence on their performance but can be addressed by training.

The thematic subchapters then present the training needs related to the capability challenges, providing the following:

- a short summary of training needs, followed by further details;
- the list of training needs in order of priority.

As regards environmental challenges, the ones that are most often mentioned include the lack of sufficient resources and differences in legislation across Member States. Although this Report focuses on challenges that can be addressed by training, it is important to note that efforts should also be made to tackle these major obstacles at EU level.

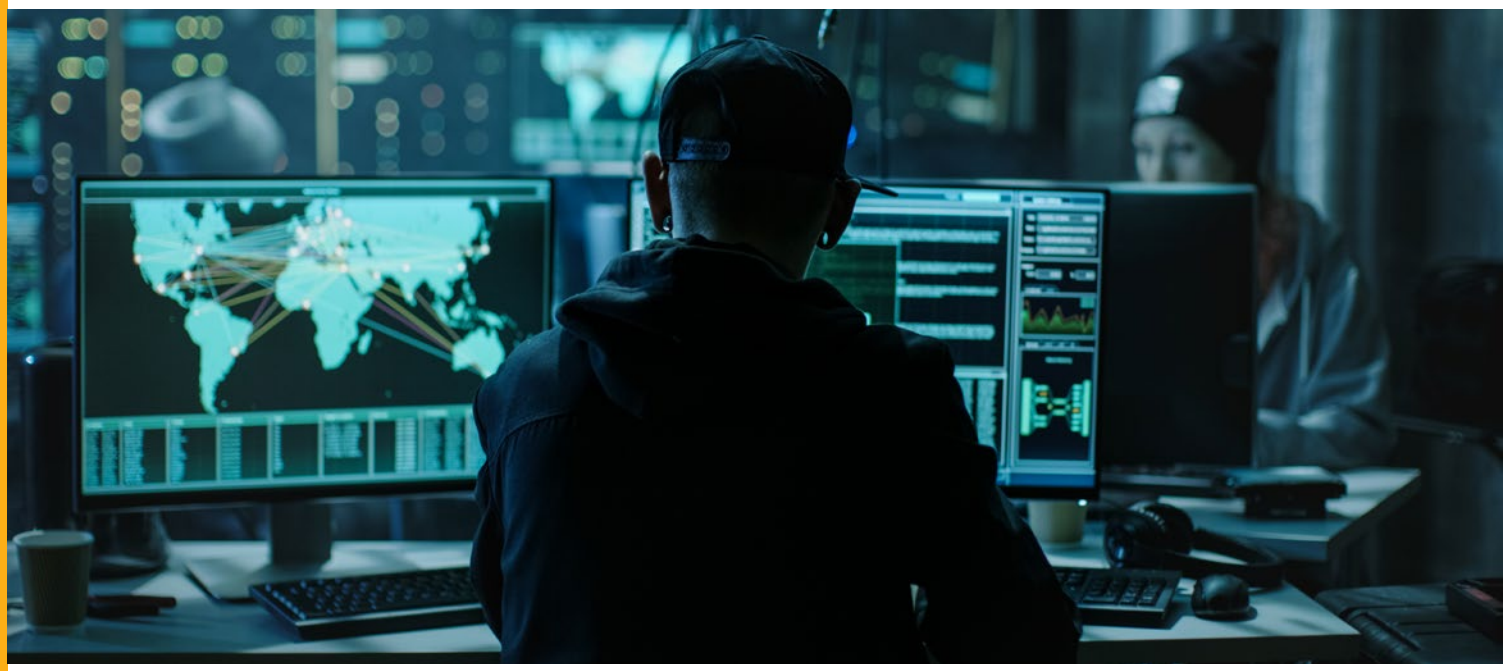
Looking at the training priorities, it becomes evident that the main trends identified during the first EU-STNA cycle are ongoing. The increasing combination and overlap of different types of crime require law enforcement officials to join forces and cooperate at both national and international level and urge for the provision of more multidisciplinary training. There remains a clear need to equip investigators working in a specific crime area with knowledge on the modi operandi of related crime areas as well as on investigation tools that can be used effectively in several crime areas (e.g. financial investigation, asset recovery, etc.).

The other trend identified in the previous EU-STNA cycle, namely the need for more joint training with other professional groups whose work is directly or indirectly related to that of law enforcement officials, is also still valid. The highest priority is given to the involvement of prosecutors and judges, but tax, labour and environmental inspectors and civil registrars are also among those who should participate in joint training where relevant. Furthermore, it is recommended that competent representatives of the private sector (in particular banks, IT and telecommunications companies, online service providers, shipping companies, postal and parcel delivery services, and intellectual property rights owners) as well as those of NGOs (e.g. organisations active in combatting trafficking in human beings or corruption, those engaged in providing support to victims of trafficking, etc.) are involved in joint training activities so as to gain a better insight into relevant processes and foster mutual cooperation.

What is definitely new compared to the findings of the previous EU-STNA is that, due to the COVID-19 pandemic, several criminal activities have shifted online, both to the surface web and to the dark web. It is enough to look at money laundering, the dissemination of terrorist content, child sexual exploitation, trade in illicit drugs, firearms and counterfeit goods, or document fraud. Crime-as-a-service is also increasingly offered online. At the same time, technological development (alternative payment methods, VPN services, encryption, storage of data on the cloud and servers outside the jurisdiction of the EU, etc.) creates new possibilities for perpetrators to conceal criminal activities.

The specific training needs presented in the subchapter on other thematic areas have remained stable since the first EU-STNA with one exception. Emergencies requiring law enforcement response constitute a new training topic, closely related to the sudden change in both the modi operandi of criminals and the work patterns of law enforcement due to the outbreak of the pandemic.

As regards topics where a wider transfer of knowledge is needed, train-the-trainers activities are proposed at EU level, followed by cascading the new knowledge to a broad range of officials at national level. In addition to being cost-effective, this approach facilitates the harmonisation of training content across the EU.



3.1. Cyber-attacks

3.1.1. Environmental challenges

Challenges identified in this area relate to existing differences in Member States' laws defining what constitutes a cyber-attack on information systems. These differences can obstruct the prevention, detection and sanctioning of cybercrime as well as of other serious and organised crime phenomena related to and enabled by cybercrime. Furthermore, judicial cooperation becomes more complicated and therefore less effective, with negative consequences on cyber security. The admissibility of e-evidence originating from another country is another legislative issue that needs improvement.

The private sector should be an ally of law enforcement authorities; however, there are several challenges hindering efficient cooperation. Private companies are in some cases reluctant to admit cyber-attacks, therefore criminal activities are largely underreported. Furthermore, private actors might face legal obstacles as regards sharing data with law enforcement or are unwilling to share them.

The number of cyber-attacks is growing while criminal methods are becoming more sophisticated. The rapidly increasing digitalisation of society and economy as well as the emergence of the Internet of Things create new vulnerabilities, which call for the strengthening of the capacity of law enforcement authorities. Unfortunately, high-cost forensic tools that could enhance the investigation of cyber-attacks remain unaffordable for law enforcement in many Member States.

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

(a) Challenges

Cybercrime services are increasingly offered online, being sold on the surface web and on the dark web, while criminals use cryptocurrencies to pay for them. The dark web also provides information on how to commit cybercrime. Since criminals use anonymisation, encryption and sophisticated techniques to cover digital traces, investigators of cyber-attacks should be aware of how to tackle these techniques.

The fact that criminal structures in this area are multifaceted, varying from organised groups and networks to lone offenders, developers, network administrators, intrusion specialists, mules or money launderers, poses a significant challenge in identifying and prosecuting offenders. Moreover, criminals quickly integrate technological developments into their operations, so law enforcement should have the capacity to keep pace.

The public and law enforcement officials not specialised in cyber-attacks lack situational awareness of the different types of cyber-attack, such as malware, web-based attacks, phishing, web application attacks, spam, distributed denial of service (DDoS), identity theft, data breach, insider threat, botnets, physical manipulation, damage, theft and loss, information leakage, ransomware, cyber-espionage, industrial espionage and cryptojacking. Therefore, the cybersecurity awareness of both law enforcement and the public needs substantial improvement.

The skills required by law enforcement agencies, prosecutors and the judiciary to combat cyber-enabled and cyber-dependent crime require significant development and adaptation to new technologies. Investigators of cyber-attack cases must have access to the latest online tools and develop alternative investigation techniques. It is imperative to develop the capacity of officials to perform big data and blockchain analyses, to deal with encryption, anonymisation and bulletproof hosting services, and to use new digital forensic tools.

Although the ability of law enforcement officials to properly manage digital evidence is key to the success of investigations, the capability gap related to identifying, handling, securing, preserving and analysing e-evidence remains a challenge.

Law enforcement should better understand and make use of the existing information exchange mechanisms as well as enhance its capacity to exchange e-evidence and use the SIRIUS platform. International cooperation among relevant law enforcement agencies and networks requires improvement. In addition, capacity building in non-EU countries experiencing rapid digital development seems highly necessary.

(b) Training needs

Summary

The key training priorities relate to the modi operandi and investigation techniques of cyber-attacks. Digital skills of law enforcement officials and the judiciary as well as their ability to deal with e-evidence need substantial improvement through training. Investigators should benefit from training on the operation of criminal networks and on national and international cooperation mechanisms. Besides investigators, cybercrime analysts should also be trained.

Awareness raising regarding cyber security, cyber-enabled and cyber-dependent crime, and cyber-attacks should target law enforcement, the judiciary and the public.

Member States indicated that 7 659 officials need training in this area.

Further details

Training covering the crime patterns and investigation techniques of cyber-attacks is imperative. It should focus primarily on the analysis of the latest cyber-attacks and the emergency response given by the EU as well as on how EU tools can be applied. Although ranked lower on the priority list, protocols to tackle large-scale cyber-attacks should also be included among the training topics.

Dealing with encryption, anonymisation and bulletproof hosting services is ranked high in terms of training priority. Furthermore, it is important to cover the management of e-evidence from detection through handling, securing, preserving, analysing and exchanging to presentation in court.

In addition, training is required on the operation of criminal networks and on how crime-as-a-service is used by them. Although given slightly lower priority, training on criminal profiling and motivation analysis is also required.

According to the Member States, law enforcement officials also need training on EU cooperation and information exchange tools, such as the Joint Cybercrime Action Taskforce (J-CAT), the European Union Agency for Cybersecurity (ENISA), the Computer Emergency Response Teams (CERTs), Europol's European Cybercrime Centre (EC3), the European Cybercrime Training and Education Group (ECTEG) and the Computer Security Incident Response Teams (CSIRTs).

Raising awareness of cyber-attacks, cyber-enabled and cyber-dependent crime, cyber threats and cybercrime investigation is ranked seventh in terms of training priority; it should target law enforcement, the judiciary and the public.

Training on big data and blockchain analyses and on the use of AI, machine learning and deep learning in cybercrime investigation also seems necessary.

Guidance on ensuring respect for fundamental rights such as human dignity, liberty, non-discrimination, gender equality, privacy and data protection should form part of all training activities.

List of identified and prioritised training needs

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

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
2.	Latest challenges for dealing with encryption, anonymisation and bulletproof hosting services
3.	Identifying, handling, securing, preserving, analysing and exchanging e-evidence
4.	Combatting crime-as-a-service used by criminals and criminal groups in illegal activities
5.	Effective international cooperation
6.	Protocols to tackle large-scale cyber-attacks
7.	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

8.	Big data analysis
9.	Blockchain analysis
10.	Using artificial intelligence, machine learning and deep learning in cybercrime investigation
11.	Cybercriminal profiling and motivation analysis
12.	Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection

3.2. Criminal finances, money laundering and asset recovery

3.2.1. Environmental challenges

Criminal finances, money laundering and asset recovery are linked to all areas of organised crime, since gaining financial benefits is one of the main motivations behind criminal activities. There are more opportunities to hide assets and criminal proceeds due to the rise of parallel financing systems, the exploitation of offshore structures, the complexity of trade-based money laundering schemes, and the use of cryptocurrencies. Transnational investigations remain resource-intensive and lengthy, and the widespread use of encryption technology by criminals further hinders operative efforts.

The implementation of the current legislation on anti-money laundering is lagging behind, while it appears necessary to develop a common legislative framework concerning emerging parallel financial systems and cryptocurrencies. Legislation on freezing and confiscating assets also needs improvement.

The capacities and tools of asset recovery offices, financial intelligence units and financial investigation bodies should be substantially reinforced.

The intelligence gap in criminal profits could be bridged by enhancing intelligence exchange between law enforcement organisations and tax authorities through a multidisciplinary approach accompanied by better data protection regulations. Besides making cooperation between different authorities cumbersome, the current data protection restrictions hinder financial big data analysis. Cooperation between the private sector and law enforcement agencies would be essential; however, investigators often face the challenge that the data received is incomplete or difficult to process. Ensuring the interconnection of national centralised bank registers could lead to major improvements.

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

(a) Challenges

The disruption of criminal networks could be enhanced by applying the "follow the money" approach, since criminals use varied financial schemes to hide and legalise criminal assets. Money laundering requires special financial and legal expertise; therefore, it is frequently offered under the form of crime-as-a-service by organised crime groups (OCGs) or specialised providers. Investigators in all crime areas should be aware of the possible financial schemes and methods used to hide criminal assets as well as of the importance of launching financial investigations and asset recovery in economically oriented criminal cases.

The knowledge of law enforcement services related to the use of artificial intelligence and on handling and analysing large amounts of data from different sources should be improved. Officials' capacity to use OSINT also needs development.

It is essential to make better use of existing EU instruments and institutions, with special regard to the new institutional landscape resulting from the establishment of the European Public Prosecutor's Office (EPPO). Cooperation with non-EU countries and the development of their financial investigation capacities should be enhanced as criminal assets are frequently hidden outside the EU.

(b) Training needs

Summary

Training in this area should target all law enforcement officials and provide a general introduction to criminal finances so that they are able to track the financial flows and assets behind any type of criminal activity. Training specifically designed for financial investigators should focus on the modus operandi of criminals and the methods of tracing, freezing and confiscating criminal assets. Special attention should be given to digital tools and new technologies to be used during investigation.

Member States indicated that 8 706 officials need training in this area.

Further details

The highest training priority is obtaining knowledge about the modus operandi of existing and emerging crime patterns. Officials need to improve their knowledge on criminal financing methods via normal financial systems and informal value systems as well as on different types of money laundering methods and fraud schemes. EU-level training should be complemented with national training activities.

Another priority is training on tracking, tracing, freezing and confiscating criminal assets, which should also involve judicial investigators. The technical aspects of investigation and the use of modern technologies, such as OSINT, AI and big data analysis, constitute the next topic in the ranking of training needs, accompanied by the respective data protection regulations. Investigations would benefit greatly from the capacity building of officials in the fields of financial analysis and financial forensics.

Being a core capability gap, the financial investigation capacity of general investigators should be developed through the provision of introductory training on financial investigations, asset recovery and cryptocurrencies. This is likely to contribute to the wider use of financial investigations in all crime areas.

In order to enhance law enforcement cooperation and information exchange, officials should have a good understanding of the roles of different EU institutions, whereby special attention should be paid to that of Europol and Eurojust (European Union Agency for Criminal Justice Cooperation) in operational and judicial cooperation and to the procedures related to the implementation of the EPPO Regulation. In this regard, cooperation methods and experience sharing with customs and tax authorities are required at both EU and Member State level. Cooperation mechanisms with private entities could be improved by providing training on the roles of financial institutions.

Furthermore, in order to disrupt high-risk criminal networks, officials would benefit from training on the operation of mafia-style groups. Some solicitors, notaries, financial service providers, real estate agents and other professionals often knowingly and wittingly provide essential support to the money laundering process. Investigations must efficiently target these enablers of financial crime, which requires advanced training due to the complexities of evidencing.

Although prevention is not the primary task of law enforcement, joint training sessions with experts from the financial sector would be beneficial for reinforcing prevention mechanisms.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training for countering criminal finances and money laundering and facilitating asset recovery.

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 via normal financial system (electronic), offshore challenge to conceal beneficial ownership, informal value transfer systems (e.g. hawala), underground banking, international money laundering bolstered by fictitious contracts and invoices, bitcoin trading, 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; automatic launch of financial investigations; 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; automatic launch of financial investigations; 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 OSINT, technicality of virtual coins (seizures)
5.	Training on cryptocurrencies for general investigators
6.	Institutional training addressing a new landscape: implementation of EPPO Regulation, roles of EPPO, OLAF, Europol, Eurojust, European Judicial Cybercrime Network (EJCN) and national authorities. EU directives, tools available at Member State and EU level

7.	Financial analysis methods and financial forensics
8.	Investigation of crime enablers, lawyers, financial service providers and real estate agents who knowingly and wittingly provide services to facilitate criminal financial flows
9.	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)
10.	Roles of financial institutions in anti-money laundering, public–private partnership; roles of European Union Agency for Fundamental Rights, European Court of Justice and European Court of Human Rights 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

3.3. Counter-terrorism

3.3.1. Environmental challenges

The risk of terrorism and violent acts triggered by politically or ideologically motivated extremism remains an acute threat. Law enforcement plays a key role in combatting and preventing terrorism, both of which require cooperation with non-EU countries, different law enforcement authorities, NGOs and the private sector. Nevertheless, cooperation is often challenging because of the differences in legislation across Member States regarding the definition of terms and the exchange of evidence, including digital evidence.

Another challenge is the lack of sufficient human and technical resources, in particular to prevent the dissemination of terrorist content online, which is spreading faster than ever. The adoption of the regulation on addressing the dissemination of terrorist content online is a first step in laying down uniform rules across the EU in this respect; therefore, the implementation of this regulation is imperative in all Member States.

The EU has limited success in addressing terrorist financing, due partly to the lack of sufficient human and technical resources and partly to the lack of awareness of the financing aspect of terrorism when it comes to prevention and investigation.

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

(a) Challenges

Law enforcement capacities should be enhanced both in the field of prevention and in the fight against terrorism. Training should focus on more efficient detection and investigation of financing of terrorism and preventing the dissemination of terrorist content online, preventing and combatting the use of unmanned aerial vehicles (UAVs) and chemical, biological, radiological and nuclear (CBRN) weapons in terrorism, protection of public spaces, and the use of artificial intelligence for investigation.

Officials should be aware of the motivation of terrorists, in particular the cultural and religious aspects and the psychology of perpetrators, including that of foreign terrorist fighters and returnees. Community policing as well as cooperation with NGOs and religious communities are imperative.

Radicalisation in prisons and within the law enforcement system increasingly happens online. Officials should be acquainted with the signs of radicalisation and understand radicalisation indicators; furthermore, they should be aware of counter-radicalisation techniques and measures.

Cooperation at local and international level is essential. Emphasis should be placed on improving counter-terrorism officers' knowledge of the available EU databases, information systems and cooperation mechanisms, especially the use of the Schengen Information System (SIS) and the Supplementary Information Request at the National Entries (SIRENE). The EU has limited authority to combat terrorism in non-EU countries. It can help to develop capacity to prevent and combat terrorism in non-EU countries by providing technical assistance and training on countering terrorism and violent extremism.

In order to enhance the preparedness of law enforcement to respond to attacks in public spaces, it would be necessary to improve collaboration between the competent public authorities or services and private actors (e. g. crisis management and civil protection authorities, fire brigades, regulatory agencies, emergency health services and private security companies, operators of entertainment venues/festivals, hospitality, shopping malls, sport events, tourist sites, places of worship).

Since it is very difficult to follow the money related to terrorism, the capacity of law enforcement to detect, investigate and combat the financing of terrorism should be strengthened, which requires cooperation with the private sector, especially financial institutions.

(b) Training needs

Summary

Training is most needed on preventing, detecting and combatting different forms of radicalisation. The training priority ranked second is the enhancement of investigation capacity, with a focus on the improvement of digital skills, which are needed for the handling of electronic evidence, and on investigation methods used in related crime areas such as financial crime, notably financing of terrorism. Furthermore, officials should receive training on how to stop the dissemination of terrorist content online and on how to deal with foreign terrorist fighters and their families.

Joint training activities are expected to enhance cooperation and information exchange at local and international levels. Training is also necessary on the resilience of critical infrastructure, particularly the role that law enforcement needs to play in case of complex scenarios, such as hybrid threats. Another highly relevant area is the protection of public spaces (such as the protection of places of worship) against terrorist attacks and other forms of serious violent acts. This should be complemented with providing expert knowledge to law enforcement on the use of UAVs and that of AI.

Member States indicated that 5 375 officials need training in this area.

Further details

According to the Member States, the highest priority is training on preventing and countering radicalisation that leads to violent extremism and terrorism, radicalisation in prisons, insider threats, and new forms of radicalisation, including digital trends, as well as training on respecting fundamental rights while countering radicalisation. Community policing and knowledge on the psychological and cultural background of terrorists play a key role in this field.

The next priority is training on the use of OSINT in counter-terrorism and on the identification, collection, acquisition, preservation, exchange and presentation of digital evidence and the use of AI and big data analysis. Consideration should also be given to lawful interception techniques.

Officials dealing with counter-terrorism should be familiar with the techniques used in financial investigations (financial analysis and forensics) so that they can trace the financial flows related to terrorist activities. Officials should also have a good understanding of national data protection regulations. Training should be delivered in cooperation with financial institutions and cover emerging threats and the financial links to other types of crime, such as tax fraud, money laundering, illicit trafficking in cultural goods, drugs, small arms and misuse of non-profit organisations.

Preventing the dissemination of terrorist content online, in the context of emerging digital trends, and the implementation of the new regulation are ranked fourth in the list of training needs.

Furthermore, training is necessary on the identification of foreign terrorist fighters and returnees and on how their family members should be dealt with by law enforcement. Again, consideration should be given to providing knowledge on fundamental rights and on cultural and religious aspects.

As mentioned earlier, cooperation is essential both at local level with NGOs and religious communities and at international level with law enforcement agencies. Training, especially joint training activities, could enhance cooperation among stakeholders. Regional and cross-border cooperation in specific terrorism cases could be enhanced by sharing best practices and implementing cross-border exercises.

Moreover, training is needed on the protection of public spaces and on the resilience of critical entities, with a focus on sharing views and best practices for handling attacks and testing different prevention and response measures.

Hybrid threats are a combination of different actions against protected state and non-state domains, frequently involving elements of cybercrime; therefore, training should cover countering hybrid threats and include aspects related to cybersecurity. In fact, there is a need for raising awareness of hybrid threats and the role which law enforcement plays in responding to them at EU level.

In addition, officials need training on the use of Unmanned Aerial Vehicles (UAVs), with an emphasis on both the related threats posed by terrorists and the opportunities for law enforcement. This should be complemented with training on the use of AI to combat terrorism.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training on counter-terrorism.

1.	Radicalisation: preventing and countering radicalisation that leads to violent extremism and terrorism; new forms of radicalisation; fundamental rights and data protection, including non-discrimination
2.	Use of OSINT in counter-terrorism; value of digital evidence; methods of lawful interception
3.	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 public-private 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.
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
5.	Foreign terrorist fighters, travelling terrorists and returnees; law enforcement approach to family members of foreign terrorist fighters
6.	Use of information systems and cooperation mechanisms in the fight against terrorism
7.	Protection of public spaces and resilience of critical entities; sharing best practices on handling attacks
8.	Regional and cross-border cooperation on specific terrorism cases
9.	Unmanned aerial vehicles: threats and opportunities for law enforcement
10.	Use of AI by law enforcement
11.	Tackling document fraud

3.4. Trafficking in human beings

3.4.1. Environmental challenges

Criminals involved in any type of trafficking in human beings increasingly use online surfaces for different purposes. For investigators, it is a challenge to follow social media and internet sources in the framework of cross-border cooperation because of the existing differences in legislation across Member States. At the same time, criminals often distance themselves from the place of exploitation; therefore, cooperation in investigating open sources is essential.

Trafficking in human beings is increasingly carried out by criminal networks based on family ties. Being based on trust and loyalty, these networks are more stable and thus more difficult to disrupt. Criminal networks infiltrating legal business structures makes it challenging to trace and prosecute offenders.

Because of the growing demand for low-wage, low-skilled or seasonal workers in the EU, labour exploitation is on the rise. Cooperation with labour inspectorates is essential; however, as they are usually not part of law enforcement, information exchange with these authorities is often burdensome.

Cooperation with NGOs engaged in combatting child trafficking is also essential in order to ensure multi-agency support and provide adequate protection and assistance to child victims of trafficking, with a special focus on interviewing children and placing them in shelters dedicated to child victims.

Differences in legislation across Member States as well as the existing gaps in cooperation between law enforcement and the judiciary hinder the successful prosecution of cross-border human trafficking cases.

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

(a) Challenges

Trafficking in human beings has become easier as services are available throughout the trafficking chain and information can be increasingly shared online via encrypted communication. In order to detect criminal networks, investigators should be aware of the structure and operation of these networks and of the different techniques used by them to hide or legalise criminal proceeds, including the infiltration of legal businesses. Besides, investigators lack adequate ability to use the digital tools available for identifying IP addresses, service providers, users, potential victims and suspects of trafficking as well as for detecting online recruitment and exploitation.

Victim identification is a key challenge, which requires different skills depending on the type of criminal act. In order to identify victims of human trafficking at the borders, within hotspots or in camps, frontline officials' capabilities, including their familiarity with the language and cultural background of potential victims, should be improved. In particular, victims of labour exploitation are difficult to identify as they are not always aware that they are being exploited and there is a lack of strong and efficient cooperation between law enforcement and labour inspectorates. Identifying and working with child or minor victims requires special psychological and interviewing skills.

Since trafficking in human beings is linked to other crime areas such as migrant smuggling, document fraud and organised property crime, officials investigating these types of crime need to be aware of the potential appearance of human trafficking cases.

It is difficult to investigate and prosecute criminals as they increasingly use digital technology (e.g. encrypted communication, online banking, digital wallets, etc.) for online recruitment and advertisement, monitoring victims' movements, moving criminal profits, and forging identity documents and work permits. The digital skills of law enforcement officials should be improved so that they can identify victims on the internet, trace criminals and their assets on online surfaces, analyse big data and use AI.

Cooperation among different authorities at national and international level is challenging, especially when it comes to the judiciary and to information exchange between labour authorities and law enforcement. Cooperation with non-EU countries should also be improved.

Understanding the psychology of victims and establishing efficient collaboration with them poses another major challenge. Victims are often traumatised, since criminals frequently use psychological and physical violence and drugs to coerce them. In order to enhance the effectiveness of collaboration with victims, which is key to the successful investigation and prosecution of criminals, a multidisciplinary and victim-centred approach should be applied in cooperation with NGOs and institutions providing victim support. It is also challenging to ensure effective protection and assistance for vulnerable victims of trafficking, including their reintegration into society, particularly in the case of unaccompanied minors.

(b) Training needs

Summary

The EU Strategy on Combatting Trafficking in Human Beings 2021-2025, presented in April 2021, also highlights that systematic training of law enforcement and justice practitioners on specific elements of the crime as well as with multi-stakeholder, simulation-based practical exercises to test procedures in handling trafficking cases will increase professionalism and coordination in dealing with the cases and will ensure appropriate follow-up. The Strategy encourages such training activities to focus on the specific features of trafficking for different forms of exploitation (sexual, forced labour, forced criminality, forced begging, child trafficking), the complex dynamics between trafficking in human beings and other illicit activities, methods for detecting the crime and its financial aspects, the role and use of internet and social media, as well as on developing skills in managing investigations and moving them towards prosecutions (evidence gathering, interviewing victims, victim protection, transnational cooperation). In addition to specialised training for law enforcement working on trafficking cases, training other law enforcement officers working in other crime areas as well as training for the judiciary is necessary to increase the detection, reporting and to improve handling of trafficking cases.

Acquiring knowledge about the crime patterns of human trafficking for the purposes of sexual exploitation, labour exploitation and forced criminality constitutes the highest training priority. The modus operandi of child trafficking is also considered an important topic to be addressed. In order to be effective, law enforcement officials need training on the use of digital tools and new technology for investigation.

Training on offline and online victim identification is necessary for various target groups, including border guards and frontline officials. This should be complemented with training activities on collaborating with victims, cultural aspects, and victims' psychology.

The need for training on trends in related crime areas, such as organised property crime, migrant smuggling, document fraud and criminal finances, is also highlighted.

Since cross-border cooperation is paramount, more training is required on EU and international cooperation tools and mechanisms. In order to enhance cooperation at national level, especially with labour authorities, training for law enforcement officials should also involve labour inspectors and civil registrars.

Member States indicated that 5 665 officials need training in this area.

Further details

The top training priority is acquiring knowledge about the modus operandi of trafficking in human beings, particularly human trafficking for the purposes of sexual exploitation, labour exploitation and forced criminality, with a special focus on how criminals apply different forms of violence to coerce victims and on how they use digital tools to their advantage.

Furthermore, law enforcement officials need dedicated training sessions on the structure and operation of criminal networks, covering crime-as-a-service, the infiltration and use of legal business structures and the profiling of persons undertaking different roles in the trafficking chain. In addition, it is necessary to address the possible links with non-EU migrant smuggling networks involved in trafficking in vulnerable persons such as women and unaccompanied minors.

The next topic on the list of priorities is the modus operandi of human trafficking for the purpose of sexual exploitation, with a focus on detection, victim identification, safeguards, support and referral. The improvement of the capacity to combat child trafficking is also considered important. Moreover, training should be provided on the use of digital technology by criminals at the different stages of trafficking, particularly on encrypted communication, document fraud and moving assets, as well as on improving the digital skills of law enforcement officials and their use of new technologies.

In addition, there is a need for training on victim identification at the borders, by first responders and online. It should cover, inter alia, the use of open source intelligence and the darknet, identifying and dealing with vulnerable victims such as children and women, and the victim referral system.

Although ranked slightly lower, training dedicated to a multidisciplinary approach concerning victims is also considered important, with a focus on working with victims of human trafficking for forced criminality, tackling cultural differences, and understanding how the psychological harm suffered by victims influences their behaviour during investigation. As Ireland indicated, training should also provide knowledge on how to manage the physical and psychological trauma symptoms manifested by victims of human trafficking (e.g. post-traumatic stress disorder, depression, anxiety, etc.) during the investigation and litigation process.

The next priority on the list is training on the link between criminal finances and money laundering and on tracing, seizing and confiscating criminal proceeds and recovering assets. This would enable law enforcement officials to disrupt criminal networks by following the money.

In order to enhance international cooperation, training is required on the use of the existing information channels, the setting up and operation of joint investigation teams, the use of large-scale IT systems and interoperability. Investigators also need training on international cooperation tools, cooperation with the United Nations (UN), the International Organization for Migration (IOM) and non-EU countries, and cooperation with NGOs and institutions providing victim support.

As the prevention and detection of criminal activities are key elements, dedicated training activities should be organised.

During the consultation process with training providers, FRA noted that supporting victims' access to justice could be accentuated, whereby special emphasis is placed on women and children. Regarding unaccompanied children/minors, especially third-country nationals in need of special protection and entitled to have a person appointed to assist them throughout the proceedings, FRA highlighted that topics related to guardianship, the rights of the child and the best interests of the child should be integrated into the training curriculum, where applicable.

The EU Strategy on Combatting Trafficking in Human Beings 2021-2025 also contains a key action on enhancing capacity building, sharing of best practices for the identification of victims of trafficking, in particular among vulnerable groups, including through dedicated funding for training of police, social workers, inspector services, border guards and encourages Member States to promote gender sensitive and child rights based training for officers and all practitioners likely to come into contact with victims.

List of identified and prioritised training needs

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

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.	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
3.	Trafficking for sexual exploitation: modus operandi including online; detection, victim identification, safeguards, support and referral, with a focus on women and children
4.	Investigations on the increasing use of digital technology at different stages of trafficking, particularly on encrypted communication and moving assets
5.	Child trafficking
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, Interpol); how to start a JIT; use of large-scale IT systems
9.	International cooperation with the UN and IOM, cooperation with non-EU countries, cooperation with NGOs/institutions providing victim support; referral of victims
10.	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
11.	Prevention of human trafficking
12.	Detection of criminal forms of labour exploitation in workplaces
13.	Forensics

3.5. Drug trafficking

3.5.1. Environmental challenges

Following the changing behavioural trends regarding drug consumption, the modi operandi of drug production and trafficking have also altered. Criminals increasingly use innovative technological solutions and shift their operations to online surfaces. Violence in drug cases is on the rise, with firearms and explosives acting as enablers of violent attacks. Criminal networks engaged in drug production and trafficking are well organised and use diverse methods to legalise or hide criminal assets, including widespread corruption and the infiltration of legal business structures.

The existing differences in legislation across Member States and the legal challenges in prosecuting cases related to new psychoactive substances (NPS), (pre-)precursors, essential chemicals, equipment and materials hinder the prosecution of criminals, who are well aware of the countermeasures of law enforcement.

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

(a) Challenges

Criminals use sophisticated equipment and digital technology for drug production allowing them to produce drugs on a large scale. Trends in availability and types of NPS change rapidly, as do the methods of drug smuggling that take advantage of digital technologies, the darknet, encryption services, and postal and parcel delivery services. The capabilities needed for tackling all forms of drug trafficking should be enhanced together with the skills required to use open source intelligence and artificial intelligence. Furthermore, the capacity of first responders to identify NPS needs improvement.

Investigators should be aware of the modi operandi of highly organised criminal networks engaged in drug production and trafficking. There is a great need to expand the knowledge of law enforcement officials on financial investigation related to drug cases, including tracking, tracing, freezing and confiscating criminal assets.

In order to increase the effectiveness of investigation and prosecution, cooperation should be fostered with EU and non-EU countries as well as with relevant EU agencies and the European Multidisciplinary Platform against Criminal Threats (EMPACT) structure. Improved exchange of information and closer cooperation between customs and police authorities have been identified as critical in the fight against drug smuggling.

(b) Training needs

Summary

The EU Agenda and Action Plan on Drugs 2021-2025 foresees training activities for law enforcement officials in different fields such as forensics, financial investigations and training for prison staff. Training on EU level is provided by different players, in cooperation with EMCDDA.

Corresponding to the challenges mentioned above, the highest priority in terms of training is acquiring knowledge about the changing crime patterns of drug trafficking, both offline and online. Furthermore, the training of law enforcement should focus on new digital tools and technologies for investigation and on enhancing the use of national and international cooperation mechanisms.

Member States indicated that 8 774 officials need training in this area.

Further details

The most relevant training topic for law enforcement officials is related to the changing methods of drug smuggling, including offline trafficking through container ports and online trade at retail level. Officials would also benefit from training on innovations and the use of digital technologies in drug trafficking as well as on the use of different drug distribution channels (the darknet, postal and parcel delivery services, fishing and pleasure vessels, etc.). Although ranked slightly lower in terms of priority, investigators also need training on the latest trends and developments in drug production, on innovative technological solutions and on the changing behavioural trends regarding drug supply and consumption.

Training on the use of digital investigation tools, such as open source intelligence, artificial intelligence, decryption and operational intelligence analysis, would improve the effectiveness of law enforcement.

In order to disrupt and dismantle highly sophisticated criminal networks, investigators need training on the business models and modi operandi of such networks as well as on their methods for hiding or legalising criminal profits, such as the use of cryptocurrencies and parallel financial systems.

Furthermore, it is essential to provide training on the existing tools for cooperation between law enforcement and the judiciary, such as joint investigation teams, on global tools for drug monitoring, and on international information exchange mechanisms. Cooperation with non-EU countries should also be a training topic. In order to enhance the prosecution of criminal cases, it is necessary to organise joint training activities with the judiciary, covering legal challenges and solutions in prosecuting cases related to drugs, precursors and NPS.

Another dimension of training should focus on how to recognise the mislabelling practices used in the case of NPS, (pre-)precursors, essential chemicals, equipment and materials, and how to conduct forensic analysis. First responders also need training on identifying and responding to the use of NPS as well as on the risks associated with occupational exposure to potent and highly toxic NPS or their adulterants and contaminants.

In order to facilitate the investigation of drug trafficking via aircrafts, training should also focus on general aviation, passenger data such as advance passenger information (API) and passenger name records (PNR), and flight monitoring tools.

Given that law enforcement is responsible for a share of prevention activities, training is also needed on detecting drugs and providing adequate responses to drug use in the prison environment.

All training activities should have a component regarding the application of fundamental rights and data protection regulations throughout the investigation and prosecution of drug cases.

During the consultation with training providers, Europol suggested adding the topic of dismantling illicit synthetic drug laboratories. While a separate training course is dedicated to this at EU level, in terms of training needs, it is covered under the topic of tackling drug production (the sixth priority) in the list below.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat drug trafficking.

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.	Investigation: use of digital investigation tools, OSINT, darknet, decryption, AI, social networks, operational intelligence analysis; training of first responders on synthetic opioid poisoning
3.	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)
4.	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; changing behavioural trends regarding drug supply and consumption
5.	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
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.	Legal challenges and solutions in prosecuting cases related to drugs, precursors and NPS
9.	Tackling document fraud, including mislabelling of (pre-)precursors and NPS
10.	Forensics
11.	General aviation: definition and legal framework, types of aircraft and characteristics, flight basics, API and PNR, and available monitoring tools
12.	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
13.	Fundamental rights and data protection

3.6. Migrant smuggling

3.6.1. Environmental challenges

Smuggling of migrants into the EU affects many EU Member States, not only the ones with external borders; however, the challenges faced vary from country to country. Issues such as how to respond to migrant flows and how to deal with migrants applying for asylum in different countries should be addressed at political level.

The New Pact on Migration and Asylum (COM(2020)609 of 23 September 2020) offers solutions and should be considered when designing educational products at EU level, especially in relation to migrant smuggling EMPACT Priority.

With The New Pact, Commission presents a new, durable European framework to manage the interdependence between Member States' policies and decisions and to offer a proper response to the opportunities and challenges in normal times, in situations of pressure and in crisis situations: one that can provide certainty, clarity and decent conditions for the men, women and children arriving in the EU, and that can also allow Europeans to trust that migration is managed in an effective and humane way, fully in line with our values.

With the New Pact on Migration and Asylum, the Commission proposes common European solutions to European challenges. The challenges outlined below are also identified by the renewed EU action plan against migrant smuggling (2021-2025) (COM(2021)591 of 29 September 2021). The renewed EU action plan against migrant smuggling should also be a key factor when designing the educational products in the area of migrant smuggling EMPACT priority.

Despite EU Commission and national efforts, Member States' asylum, reception and return systems remain partially unharmonized, resulting in a number of loopholes.

More effective control at the external borders is hampered by the lack of sufficient human resources that also hinders investigations, which are scarce. The absence of adequate technological tools available for law enforcement further hampers effectiveness. Limited resources result in fewer reports regarding secondary clues that might lead to further relevant information. It is particularly difficult to find expertise in financial investigation related to migrant smuggling cases.

The increasing use of digital tools and encrypted communication channels by irregular migrants and criminal networks makes the detection and investigation of migrant smuggling cases more challenging. In addition, secondary movements have become more diverse, complex and multidirectional, with significant differences across nationalities. In order to tackle these challenges, efficient cross-border cooperation and information exchange are imperative.

Migrant smuggling is dominated by flexible and highly adaptable criminal networks in which the managerial level distances itself from the criminal activities, resulting in the fact that most detected suspects are low-level criminals.

The work with the private sector, especially with interpreters, can be cumbersome. Even though it is a position of trust, there is no unified quality assurance system for employing certified interpreters at the borders.

In addition, to effectively counter the transnational nature of migrant smuggling beyond EU borders, closer cooperation is needed with key partner countries of origin and transit, both at bilateral and at regional level.

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

(a) Challenges

Migrant smuggling involves a wide variety of modi operandi including sham marriages, bogus paternity, false employment contracts, fake invitation letters, false medical visas, and false claims of being victims of trafficking or refugees. Law enforcement officials should also be aware of and make links to the methods and techniques used to investigate other crime areas such as trafficking in human beings, firearms trafficking, drug trafficking, document fraud and excise fraud. This rarely happens as limited resources do not allow for the employment of professionals for each aspect of the process, although conducting interviews or behavioural analyses during the interview process requires completely different expertise than using biometrics or detecting fraudulent documents, visas, and supporting documents. The screening capacities of border guards should also be strengthened.

Criminals take advantage of digital platforms, encryption and drones throughout the chain of migrant smuggling activities, including for the monitoring of law enforcement movements. The limited success in prosecuting offenders is due partly to the lack of adequate skills among law enforcement officials to respond to the use of digital platforms, social media and mobile applications by criminals, and partly to the limited capacity to use open source intelligence, gather intelligence and perform decryption.

Law enforcement officials' knowledge on financial models including hawala and money service bureaux, and on cryptocurrencies, financial investigations and asset recovery should be substantially improved.

Since there is a growing demand for services facilitating secondary movements, these are readily available and offered as crime-as-a-service. In order to tackle the organised crime groups involved, cross-border cooperation is essential.

Tackling migrant smuggling requires a comprehensive approach involving consulates, travel companies and civil registries as well as optimal networking among specific entities. Partnerships and cooperation with public and private sectors should be improved both within the EU and with non-EU countries. Joint investigation teams are increasingly set up to facilitate information exchange and evidence sharing but not to the extent necessary. The level of information exchange is expected to increase with the implementation of the framework for interoperability of large-scale IT systems, which should be a priority at both political and technical level. The implementation of the PNR Directive is of key importance, particularly as regards the upcoming review of the current approach on PNR data transfer to third countries. International judicial cooperation remains a challenge as there is still a need to increase the mutual understanding of and interaction among the different judicial systems in the Member States. Staff deployed in Common Security and Defence Policy (CSDP) missions face specific challenges linked to their unique contexts and work environment. Training could allow civilian CSDP missions to be faster, more flexible and more efficient in tackling migration.

Law enforcement officials should fully respect fundamental rights during the detection, investigation and prosecution of migrant smuggling cases; for this reason, their knowledge on how to comply with fundamental rights throughout the process should be improved. High turnover of police staff might lead to those who are not properly trained dealing with migrant smuggling.

Dealing with requests concerning unaccompanied minors is an additional challenge due to growing pressure on national migration management and child protection systems and as a result of insufficient cooperation among various institutions such as police, asylum, social and child protection authorities. These institutions do not always have protocols for working together in case a child goes missing, which prevents a proper and swift response if this situation arises.

(b) Training needs

Summary

To enhance the investigative capabilities of law enforcement, training is needed on the use of digital platforms and new technological tools. Obviously, officials should be aware of the multifaceted crime patterns of migrant smuggling and able to use financial investigation techniques. Training on linked crime areas such as trafficking in human beings and document fraud is also necessary.

Cross-border cooperation should be enhanced through training on information exchange systems, interoperability, EU cooperation tools and mechanisms, and cooperation with non-EU countries, including the role of CSDP missions.

Moreover, training activities should address fundamental rights compliance, particularly as regards gender equality.

Member States indicated that 6 149 officials need training in this area.

Further details

Law enforcement officials primarily need training on investigation tools, with a focus on the application of digital instruments, open source intelligence, the use of social media and mobile applications, intelligence gathering and decryption.

Training regarding the varied modi operandi of migrant smuggling cases is also high on the priority list. It should cover crime patterns such as sham marriages, bogus paternity, false employment contracts, fake invitation letters, false medical visas (including vaccination certificates), and false claims of being victims of trafficking or refugees. Furthermore, the use of digital platforms by criminals for all phases of migrant smuggling, mass mobilisation for migration, arranging secondary movements, and monitoring law enforcement movements should also be addressed during training activities. The next priority in the ranking is to better understand the operation of criminal networks, their structure and their organisation.

Training on the existing information exchange systems and the framework for interoperability of large-scale IT systems is considered essential for the enhancement of cross-border cooperation among law enforcement officials. Although ranked somewhat lower, cooperation mechanisms with non-EU countries should also be addressed by implementing a comprehensive approach that involves consulates, civil registries and travel companies. Training on EU cooperation tools and mechanisms, such as joint investigation teams, and on cooperation between administrative and law enforcement units and the judicial sector (prosecutors, lawyers and judges) would also enhance the effectiveness of investigation and prosecution.

Furthermore, law enforcement officials need training on the methods and techniques used to investigate linked crime areas, primarily on financial investigation and asset recovery, then on the nexus between migrant smuggling and trafficking in human beings, and last but not least, on tackling document fraud (including imposters).

In addition, it is necessary to provide training on compliance with fundamental rights and gender equality in the process of detecting, investigating and prosecuting migrant smuggling cases, and on dealing with unaccompanied minors.

Training activities should aim to improve the existing knowledge and skills of officials and to develop further knowledge and skills in order to achieve the required job competencies.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat migrant smuggling.

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
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), SIS II, role of large-scale IT systems in combatting migrant smuggling under the EMPACT framework
5.	Improving knowledge on financial models including hawala and money service bureaux, cryptocurrencies, financial investigations and asset recovery
6.	Nexus between migrant smuggling and trafficking in human beings: exploitation of migrants after arrival in the EU
7.	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.)
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, JITs; cooperation between administrative and law enforcement units and the judicial sector (prosecutors, lawyers and judges)
10.	Dealing with requests concerning unaccompanied minors
11.	Detecting secondary movements
12.	Procedures and tools used in migration crisis situations
13.	Fundamental rights, including access to international protection, non-discrimination and data protection

3.7. Child sexual exploitation

3.7.1. Environmental challenges

Online child sexual exploitation has been on the rise over the past few years and the COVID-19 outbreak has led to a considerable increase in criminal activity due to children's increased use of the internet, often without parental supervision. It is imperative to strengthen the investigative capacity of law enforcement in this crime area, as at present the number of cases far surpasses the resources available. On top of this, the overburdening of officials tends to result in early burnout, since it is difficult to cope with the psychological aspects of cases. Besides human capacity, Member States need adequate equipment, such as high-tech software and hardware, in order to detect criminal activities and manage e-evidence so that it can be presented in court.

Furthermore, legislative differences hinder efficient cross-border cooperation. There are gaps in national laws and regulations on web hosting and data retention. Legislation also needs improvement in the area of protecting children against sexual exploitation and abuse, including as regards the requirement for relevant online service providers to detect online child sexual exploitation and report it to authorities.

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

(a) Challenges

Law enforcement officials face difficulties in identifying and working with child victims of sexual abuse and exploitation. This is partly because offenders frequently use grooming techniques and blackmail children.

Child sexual offenders are problematic to detect and to prosecute, due to various factors. They often use fake identities, encryption and anonymous VPN services, proxy servers and the dark web, which makes it easier to hide criminal activities. Furthermore, they opt for password protected storage services, where the hosting providers are not necessarily aware of the content stored. To pay for different services along the criminal chain, offenders use online payment methods and virtual currencies.

In order to tackle child sexual abuse and exploitation, investigators should be equipped with high-tech software and hardware as well as an excellent ability to use digital investigation tools and methods, including online undercover operations and digital forensics. Moreover, law enforcement must also be trained in the specificities of investigations dealing with child sexual abuse. In reality, the capacity of law enforcement remains low; there is a considerable lack of sufficiently trained investigators. Detecting child sexual abuse material, analysing big data and combatting anonymisation are skills that need improvement. The use of digital tools and new technology by the judiciary should also be enhanced.

Cooperation at national and international level is an issue. Besides the legislative obstacles described above, officials are not always aware of the international nature of the crime area and thus limit their focus to national investigation. Law enforcement and the judiciary should be better acquainted with existing international cooperation mechanisms, such as joint investigation teams and information and evidence exchange tools. Cooperation with the judiciary as well as with NGOs needs improvement at national level.

Given that child sexual abuse involves harassment, systematic abuse, and verbal, psychological and physical violence towards children, it can be psychologically challenging for law enforcement officials. Investigators need regular mental health and psychological support while in this job. In addition, they should be familiar with child-friendly investigation techniques to deal with traumatised children, and have solid knowledge of children's rights and children's welfare.

Law enforcement officials should be aware of their role in preventing child sexual exploitation as well as their role in supporting the design and implementation of prevention programmes targeting parents, children, teachers and offenders.

(b) Training needs

Summary

The highest priority in terms of training is related to victim identification and the detection of child sexual abuse and exploitation material. Training is also needed on online investigation tools, alternative investigation techniques, the management of e-evidence, and the use of digital forensic tools.

Cooperation at national and international level can be enhanced through joint training activities with the participation of law enforcement officials and the judiciary as well as through sharing best practices. In addition, training on financial investigation techniques and on the identification of high-risk criminal networks is also necessary.

Furthermore, officials need training related to the fundamental rights aspects of investigating child sexual abuse and exploitation cases, with a special focus on dealing with children and children's rights. In addition, as cases are psychologically challenging, investigators should receive training on the support tools available to preserve their mental health.

Awareness raising is key to preventing child sexual exploitation. Training should focus on the full concept of prevention, more precisely on how to design and carry out effective prevention activities from idea to execution (planning, clear and structured messages, the inclusion of stakeholders, the use of communication channels, types of audience, risk and change management, measuring impact and outreach) as well as on the protection of children's rights.

Member States indicated that 6 192 officials need training in this area.

Further details

The most relevant topics in terms of training include the identification of victims of child sexual abuse and exploitation (including, inter alia, the analysis of big data, videos and images for the purpose of victim identification) and the detection of child sexual abuse and exploitation material.

In addition, officials need training on developing and applying innovative investigation methods, including online investigation tools, the use of open source intelligence and online undercover investigations, as well as on digital forensics. This latter topic should cover the management of digital evidence throughout the entire process of investigating and prosecuting, including the presentation of e-evidence in court and the international dimensions of admissibility of e-evidence. Dealing with the challenges posed by encryption and anonymisation services used by offenders, such as VPNs, proxy servers and Tor, should also be among the training topics. As for the development and application of innovative investigation approaches, training courses such as Combatting the Online Sexual Exploitation of Children (COSEC) should be used.

Furthermore, training on international cooperation tools and mechanisms, such as joint investigation teams, is necessary. In general, it should raise awareness of the importance of cross-border cooperation and focus on sharing best practices of successful international investigation. Training should also touch upon good cooperation

mechanisms at national level, with a special focus on those operating between the judiciary and law enforcement. It would be advisable to organise joint training activities for law enforcement and the judiciary.

Officials investigating child sexual abuse and exploitation cases should also receive training on how offenders use online payment methods including virtual currencies. In addition, training on the structure and operation of high-risk criminal networks would be helpful.

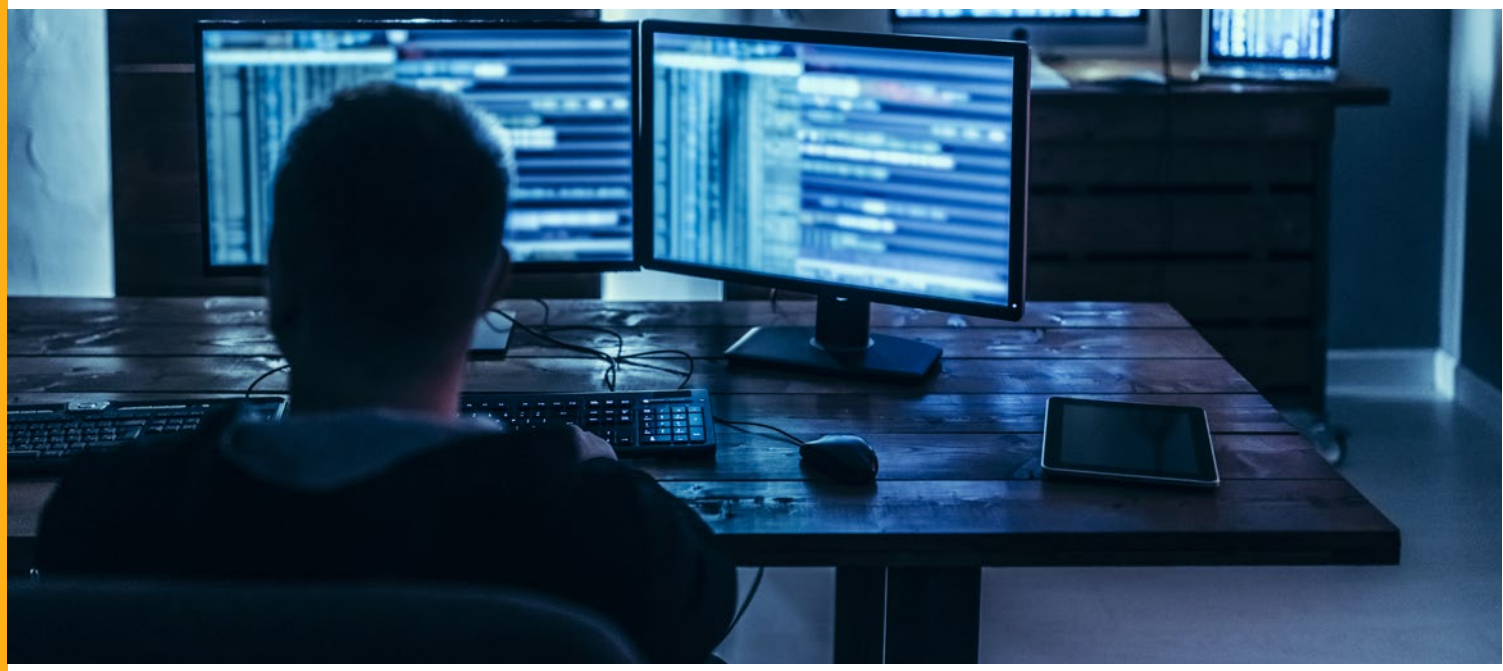
Law enforcement officials' knowledge on gender-related cyber violence against women and girls as well as on the rights of victims, suspects and offenders also requires improvement through training. In addition, officials need to learn about the psychological tools and techniques that can support their mental health while they are dealing with child sexual abuse and exploitation.

Training on offender management is also considered a priority, with a focus on the difficulties encountered in handling offenders, ways of overcoming legal, procedural and other obstacles, and relapse risk assessment. Training should provide an opportunity to share best practices and experiences related to offender management, including maintaining registries, disclosure policies, monitoring for relapse, risk assessment, managing cross-border travel, and working with other agencies.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat child sexual exploitation.

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.	Handling encryption and anonymisation services in online child sexual abuse (VPNs, proxy servers, Tor)
6.	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
7.	Financial investigations related to child sexual exploitation cases (online payment methods including virtual currencies)
8.	Identification of high-risk criminal networks involved in child sexual abuse and exploitation
9.	Tackling gender-related cyber violence against women and girls
10.	Tools and techniques for mental health/psychological support for law enforcement officers dealing with child sexual abuse and sexual exploitation
11.	Child victims` rights, offenders' rights, suspects' rights
12.	International offender management



3.8. Online fraud schemes

3.8.1. Environmental challenges

Online fraud covers different types of fraud schemes that are constantly evolving in line with technological development. Due to its multifaceted nature, investigators dealing with this crime area should be competent in tackling the varied forms of fraud. The pandemic has given an impetus to online fraudsters while law enforcement is lagging behind in terms of investigative resources. Furthermore, investigations are lengthy and require additional capacity for well-trained law enforcement officials. However, those individuals possessing the knowledge needed for these types of investigation are better paid in the private sector, which again raises capacity issues within law enforcement.

Differences in Member States' approaches to and legislation on data protection, data retention and cybercrime hinder cross-border cooperation. The same is true for judicial cooperation: there is no proper legal framework in place to follow when it comes to information and intelligence exchange.

Cooperation with the private sector is essential; however, companies are reluctant to share data and information with law enforcement. As companies seek to protect their brand name and reputation, and insurance companies might not compensate for fraud-related losses, fraud cases remain underreported.

The adequate management of digital evidence is imperative for ensuring the effectiveness of investigations. Member States should invest more resources in high-tech software and hardware that can be efficiently used for the detection and management of digital evidence. The admissibility of digital evidence in different countries is another legislative issue that obstructs the cross-border prosecution of cases.

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

(a) Challenges

Online fraud schemes are perpetrated in many forms and law enforcement should be aware of the crime patterns in each type of fraud and their combinations. Officials investigating other crime areas should also improve

their knowledge on fraud schemes as the latter can be linked to many crimes. However, it is important to maintain the balance between the training side and the operational side so that the time dedicated by law enforcement officials to training at EU or national level does not result in even more prolonged investigations and pending cases.

New fraud typologies are related to emerging online tools and digital techniques for committing crimes; therefore, investigators should be acquainted with digital investigation tools and tackle the criminal use of encryption, anonymisation, bulletproof hosting services and the darknet. In practice, law enforcement has a lack of trained investigators and a lack of digital and technical skills. Even though part of this capacity building requires EU-level support, it is also a national responsibility. The expert group suggested that each police force should be responsible for developing digital skills within their units.

While criminals use virtual currencies, virtual tokens and online payment methods for online fraud, investigators lack the capacity to apply financial investigation and disruption techniques. Furthermore, the use of deepfakes created with artificial intelligence makes fraud detection challenging.

Criminal networks engaged in online fraud are highly collaborative, providing criminal services to one another in a chain, distancing themselves in this way from the crime and rendering the identification of suspects by law enforcement more difficult. There is a need for providers with expertise in taxation, banking, law, finance, IT and combatting money laundering, but also for low-skilled collaborators such as money mules, call centre operators and cash carriers.

Inter-agency cooperation is not strong enough at international level, and the same can be said for the cross-border exchange of e-evidence. According to the respondents, it is difficult to obtain data from foreign countries and apply data protection regulations throughout investigations. Law enforcement lacks information from the private sector, even though well-functioning public–private partnerships are needed in order to disrupt criminality. Cumbersome cooperation with banks and with international partners leads to offences often being investigated as stand-alone smaller cases without revealing the international fraud schemes behind them.

Although there is a great need to inform the public about the crime patterns of online fraud, there are insufficient awareness-raising campaigns in this field.

(b) Training needs

Summary

Training is needed on the different aspects of fraud schemes, on their modi operandi, and on effective investigation methods. This should cover the broad range of fraud types including investment fraud, CEO fraud, business email compromise fraud, non-delivery fraud, bank fraud, social benefit fraud, subsidy fraud, romance fraud and fake invoice fraud, and other fraud methods such as helpdesk fraud and online system fraud.

Furthermore, officials need training on digital investigation techniques, digital forensics, and cooperation tools and mechanisms at national and international level.

Member States indicated that 6 285 officials need training in this area.

Further details

The most relevant training topic is related to online payment fraud including carding platforms, internet and mobile banking fraud, online payment requests, fraudulent near-field communication (NFC) transactions, SIM swapping, smishing, phishing, vishing, and e-commerce fraud.

Ranked as the second priority, training is required on the modi operandi of cyber scams such as online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud and helpdesk fraud.

Training on crime patterns related to card-present fraud, such as skimming, contactless card fraud, and mobile payment and mobile-app payment fraud, is slightly lower on the priority list, but still considered necessary. The same is true of training on tackling intrusions into transaction networks, such as banking malware/POS malware, logical attacks against ATMs, and the use of malware to intercept login details for online banking services.

In addition, training should focus on improving the knowledge of law enforcement officials on tools and techniques that facilitate cybercrime, and cover cryptocurrencies, encryption, anonymisation, online forgery, the use of deepfakes created with artificial intelligence and money muling. In order to enhance the digital skills of law enforcement, training should also cover cyber threat intelligence and the use of the darknet and open source intelligence.

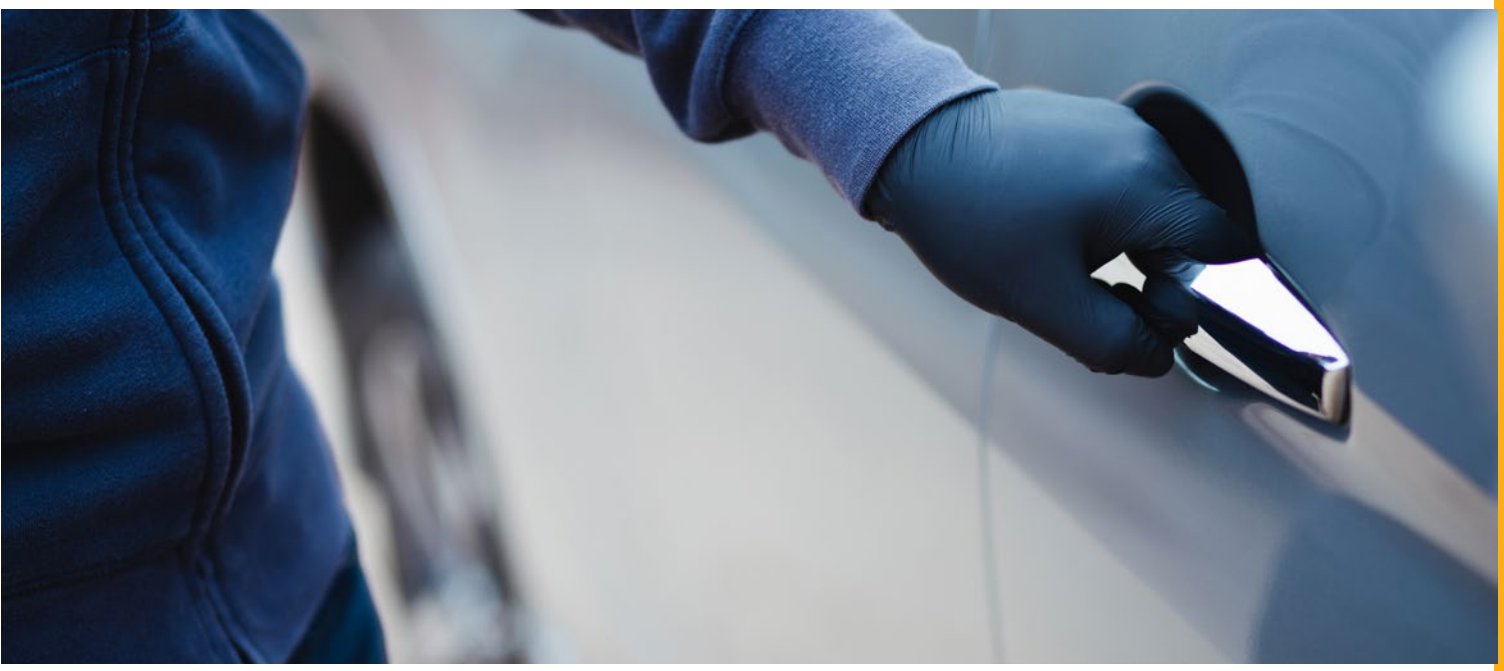
As there is a lack of human capacity for investigation and for attending training sessions, it is suggested that with regard to technological developments and investigation tools, train-the-trainers activities are organised at EU level with the aim of cascading the new knowledge to a broad range of officials at national level.

In addition, training should also focus on mechanisms for national and international cooperation between law enforcement agencies and on cooperation with the private sector. Joint training activities with the involvement of private-sector actors could enhance relations between law enforcement and the public sector.

List of identified and prioritised training needs

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

1.	Card-not-present fraud: compromise online payments, e-skimming, mobile banking fraud, online payment requests, SIM swapping, smishing, phishing and vishing, e-commerce fraud, carding platforms and darknet marketplaces
2.	Cyber scams: online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud, mimic and voice fraud, helpdesk fraud, social engineering
3.	Cybercrime facilitators: cryptocurrencies, 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.	Intrusions into system networks of financial institutions: banking malware/POS malware, logical attacks against ATMs, use of malware to intercept login details for online banking services
7.	International law enforcement cooperation, public–private partnership, inter-agency cooperation (cooperation with financial institutions, internet service providers and online platforms)
8.	Information exchange and cross-border exchange of evidence
9.	Legal challenges in non-cash payment methods
10.	High-risk criminal networks
11.	Crime prevention
12.	Fundamental rights and data protection



3.9. Organised property crime

3.9.1. Environmental challenges

Organised property crime (OPC) is a complex phenomenon, with crime patterns changing even across different parts of the same country. Nevertheless, tackling OPC is not considered a key priority in all Member States. As a result, the human resources allocated for investigation in this crime area are insufficient as are the essential investigation tools, such as GPS and new technological devices. Consequently, the processes and networks behind fencing remain underinvestigated and there is an intelligence gap regarding key locations and routes of stolen goods.

Differences in legislation across Member States hamper the investigation of online markets. Efficient cooperation and information exchange are necessary in cross-border investigations; however, they are hindered by the lack of adequate instant messaging systems. While most EU Member States have adopted the Prüm Convention on the exchange of data, fingerprints and vehicle registrations, its implementation is lagging behind. As reported by CARPOL, the network of EU law enforcement contact points for tackling cross-border vehicle crime, cooperation in investigating cross-border vehicle crime could be enhanced by providing more financial resources to this working group.

When working with the private sector, data protection regulations present a challenge in that they often do not allow private actors to collect personal information that is useful from an operational point of view during criminal investigations.

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

(a) Challenges

OPC is committed by extremely flexible criminal networks with a high level of mobility, such as mobile organised crime groups (MOCGs) and outlaw motorcycle gangs. Unlike the legislation at national and EU level, criminal networks adapt easily to new circumstances and react quickly to technological developments. Obviously, new crime phenomena require rapid response from the authorities.

The increased use of violence in OPC cases indicates that investigators need knowledge on new trends in the illicit production and use of firearms and explosives. Furthermore, OPC is linked to other crime areas such as document fraud and financial crime, but the highly-specialised investigators in a certain field sometimes lack knowledge about other crime areas. In addition, law enforcement should be better equipped with digital investigation tools, especially in cases which involve the use of cyber-based instruments to break into smart homes.

Fast and secure communication channels should be ensured for law enforcement without the linguistic barriers that currently constitute an obstacle for investigators speaking different languages. Cross-border cooperation could be enhanced through better information exchange mechanisms and joint training activities with the involvement of different actors, including private companies.

(b) Training needs

Summary

Training is needed on all the specific types of OPC, including the crime patterns and modi operandi of organised burglaries, robberies and thefts, vehicle crime, attacks against ATMs, illegal trafficking in cultural goods, and fencing. Investigators should be well aware of how criminal networks operate in general and in changing circumstances. This should be complemented with training on mechanisms for national and international cooperation and information exchange.

Digital investigation tools and technologies should also feature in law enforcement training. Moreover, officials should receive training on the trends in crime areas linked to OPC, such as financial crime, illicit firearms and document fraud, and on specific methods, e.g. financial investigation and asset recovery.

Member States indicated that 5 017 officials need training in this area.

Further details

Training is most needed on the modi operandi of organised burglaries, robberies and thefts, the latter covering cargo crime, organised pickpocketing and distraction thefts, and metal theft. Tackling the use of firearms and violence should be included in the training topics.

Cross-border cooperation and information exchange are imperative for the efficient investigation of OPC cases. Training on JITs, online secure databases and information exchange mechanisms provided by Europol and Interpol (e.g. the I-24/7 system for secure exchange of information), with attention being paid to respecting data protection regulations, would greatly enhance the work of investigators. Training should also focus on the communication channels used by criminals, such as SKY ECC.

The third priority in terms of training is related to criminal networks, their structures and operation, high-value targets and mafia-style organised crime.

Training on the patterns of vehicle crime is next in the ranking. As CARPOL indicated, country-level training should be complemented with EU-level training activities focusing on the transit and export of stolen vehicles and parts, illicit trade in stolen vehicle parts, lease and rental fraud, and the geolocation of vehicles that are of interest to law enforcement agencies. Training should target police, customs and border guard officials, with the additional involvement of private actors.

The way in which trafficking in cultural goods is tackled could be enhanced through training provided to law enforcement officials from different institutions (police officers, border guards, customs officers, etc.) and through capacity building among cultural heritage experts.

The crime patterns of thefts and attacks on ATMs should also be included in the training topics, with special attention being paid to the use of firearms and explosives in these criminal cases.

Furthermore, law enforcement officials should receive training on financial investigation and asset recovery related to OPC as well as on digital investigation tools, with a focus on the use of GPS for tracking and monitoring and on the use of open source intelligence.

Although ranked lower on the priority list, training on the crime patterns and modus operandi of fencing is also important, as it is related to all types of OPC. Focus should be placed on the online surfaces and offline routes used for fencing as well as on the interconnection of criminal networks and actors throughout the chain.

As regards training on prevention, special attention should be paid to the European barrier model and the administrative approach to OPC. The European Crime Prevention Network (EUCPN) should be involved in training activities so as to provide information on best practices in prevention.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat organised property crime.

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, MOCGs, 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 EUCARIS; geolocation of vehicles; cooperation with manufacturers to localise vehicles
5.	Tackling trafficking in cultural goods (police, border guards and customs)
6.	Financial investigation and asset recovery related to organised property crime cases
7.	Tackling theft and attacks on ATMs
8.	OSINT focused on organised property crime
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 Member States could use within the EMPACT framework
11.	Forensics
12.	Prevention: using the European barrier model for organised property crime; administrative approach
13.	Tackling document fraud
14.	Fundamental rights and data protection

3.10. Border management and maritime security

3.10.1. Environmental challenges

Most challenges in this area can be addressed through training. The establishment and management of hotspots is an exception: capacities dedicated to hotspots are never sufficient to receive the wave of migrants and ensure the smooth processing of individual cases.

Border management would benefit from the creation and improvement of risk analysis units at local, national and regional level as well as from the development of strategic and operational risk analysis products for border control activities. Furthermore, border guards should be equipped with new, 3D digital technology for border management.

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

(a) Challenges

Border guards and customs officials are responsible for checking the passengers and goods entering/exiting the European Union. Their capacity to screen and detect false documents and breeder documents remains limited, while criminals tend to use sophisticated new technology for document fraud.

Officials should be aware of the modi operandi, signs and risks of all organised crime areas and terrorism so that they are able to identify victims of human trafficking, foreign terrorist fighters and illegal migrants. The same is true of illegal trafficking in goods: border guards are expected to be able to detect illegal drugs, cultural goods, firearms, explosives, animals and plants. Respect for fundamental rights is an issue due to lack of awareness.

The continuous updating of large-scale IT systems requires the constant improvement of border guards' ability to use these systems. Emerging technologies such as the Internet of Things, biometrics, and artificial intelligence are creating new challenges that call for fast and innovative response from law enforcement.

It is essential that there is effective cooperation in border management and maritime security between Member States and EU Agencies, as well as between EU agencies with CSDP missions and with non-EU countries.

(b) Training needs

Summary

Training is essential for the implementation of the Integrated Border Management Strategy. Frontex is the training hub on border management and maritime security in the European Union and its cooperation with the Member States is essential in order to make the best use of the available training resources. Training should cover cross-border crime patterns in organised crime areas and terrorism, identity management, fraud and risk analysis as long as it is covered by the Frontex mandate in accordance with the Regulation (EU) 2019/1896.

Information and intelligence exchange mechanisms, the use of new digital technologies at the borders and risk analysis should be among the training topics. Furthermore, safeguarding fundamental rights should also be reflected in the training portfolio.

Member States indicated that 7 201 officials need training in this area.

Further details

Training is most needed on identifying cross-border crime and security threats, such as drug trafficking, the smuggling of goods, foreign terrorist fighters, and human trafficking, whereby a special focus is placed on victims of trafficking. In the area of maritime security, officials need training on fighting environmental crime, including the pollution of waters and land, and illegal waste dumping into seas and on land.

As capacities are limited, training should also touch upon situational monitoring, strategic and operational risk analysis, the implementation of the Common Integrated Risk Analysis Model (CIRAM), the use of the information and intelligence exchange systems available at EU level, and the use of new, 3D digital technologies for border management. Although ranked slightly lower, training is also necessary on tackling high-risk criminal networks.

In terms of cooperation, which is imperative in border management, the highest priority is given to enhancing cooperation with CSDP missions in non-EU countries. This is followed by cooperation with Member States and training academies in order to best explore the training opportunities offered by Frontex. Capabilities and services related to the European Border Surveillance System (EUROSUR), especially in terms of surveillance and situational awareness, should be included in the training topics.

In addition, training on safeguarding fundamental rights is highly necessary in this area, with a special focus on the dignified treatment of persons at the border, in compliance with the principles of non-discrimination, the right to liberty, respect for privacy, and the use of force. Furthermore, although ranked lower on the priority list, training should also cover access to international protection, the prohibition of refoulement, the prohibition of collective expulsion and push-backs, and procedural safeguards related to decisions taken at the border.

In order to ensure efficient responses when interacting with persons crossing the borders, communication barriers should be lifted; therefore, it is considered important to provide border guards with training on communication and relevant language skills.

In addition, training activities should focus on operational preparedness for maritime surveillance as well as for fighting maritime security threats.

During the process of consultation with training providers, Frontex indicated that the topic of integrated border management should be added to the list of training priorities.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training related to border management and maritime security.

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
3.	Common as well as new digitalisation practices (three dimensions: border security, information exchange and humanitarianism)
4.	Document fraud detection at border crossing points
5.	Cross-border criminal networks
6.	Border management in non-EU countries with shared external borders; experience sharing with CSDP missions mandated with border management aspects
7.	Dignified treatment of persons at the border in compliance with principles of non-discrimination, right to liberty, respect for privacy and use of force
8.	Communication and language skills needed for interactions with those crossing the border
9.	Cooperation with Member States and training academies
10.	Screening and debriefing
11.	Access to international protection, prohibition of refoulement, prohibition of collective expulsion and push-backs
12.	Procedural safeguards related to decisions taken at the border
13.	Improving capacity to implement coast guard functions

3.11. Firearms trafficking

3.11.1. Environmental challenges

Differences in legislation across Member States result in burdensome bureaucratic processes when it comes to information exchange and obstruct efficient international cooperation among law enforcement authorities.

Due to deficiencies in cooperation, even among National Firearms Focal Points, there are gaps in the intelligence picture on the routes of firearms trafficking. Meanwhile, the detected routes have become resilient despite the efforts of the law enforcement units engaged in tackling firearms trafficking. In order to enhance cooperation, better equipment and clearer processes are needed.

Obviously, the increased illicit use of firearms and explosives leads to growing violence in other crime areas such as drug trafficking and terrorism. The fact that information on the construction methods of crude firearms is easily accessible via online platforms creates further opportunities for criminals.

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

(a) Challenges

Firearms and explosives are key enablers for other criminal activities such as drug trafficking, ATM attacks and terrorism; still, officers working in linked crime areas lack sufficient knowledge on how to tackle the firearms threat. Therefore, Member States should dramatically develop the expertise of their law enforcement authorities in this respect, along with the legal framework.

International cooperation during investigation is essential in view of the need to improve the online and offline traceability of weapons and to ensure information exchange between law enforcement and licensing authorities. To this end, coordination and cooperation both within the EU and with international partners, particularly Interpol, should be reinforced.

At national level, there is a need to enhance cooperation among law enforcement authorities such as customs, police and border guards as well as with prosecutors and forensic specialists in order to tackle the principal sources and routes of illicit firearms, drawing inspiration from the South-East Europe Firearms Experts Network.

Last but not least, it is necessary to improve forensic and ballistic expertise.

(b) Training needs

Summary

Law enforcement training should focus primarily on the modus operandi of this crime area as well as on the online and offline investigation methods that can be used effectively. This should be complemented with training on cooperation mechanisms at national and international level, with the additional involvement of judicial authorities and non-EU countries.

Using train-the-trainers activities to raise the awareness of a broad range of law enforcement officials concerning the increasing firearms threat would be beneficial. At the same time, investigators of illicit firearms cases should receive training on firearms forensics and the basics of financial investigation.

Member States indicated that 4 995 officials need training in this area.

Further details

Training is most needed on the modus operandi of firearms related criminal cases, focusing on the illicit diversion of firearms from legal supply chains, the reactivation of deactivated firearms, the conversion of alarm and signal weapons into lethal weapons, and the smuggling of firearms and parts of firearms into the EU.

Furthermore, law enforcement officials should receive training on the methods of online trading in illicit firearms via the surface web and the dark web as well as on the offline trading methods via postal and parcel delivery services. This should be complemented with online investigation methods, such as the use of open source intelligence, the darknet and other communication platforms.

In addition, law enforcement training is required on the operation of high-risk criminal networks engaged in the illicit production of and trade in firearms both within and outside the EU. In order to enable the disruption of criminal networks, financial investigation tools should also be included in the training topics.

Firearms forensics is ranked next in terms of priority, including training on the use of the automated biometric identification system (ABIS) and similar systems as well as on the collection of forensic evidence.

Moreover, training should be provided on tools and mechanisms for cooperation within the EU, with non-EU countries and with relevant international organisations. In this respect, training activities should target police, customs and border guards. It is important to also include ways of cooperating with the private sector, with a focus on sharing best practices. Representatives of judicial authorities and of non-EU countries should also be involved in training activities.

Since the illicit production of and trafficking in firearms influences other criminal areas, train-the-trainers courses appear beneficial so as to cascade knowledge to the broadest community of law enforcement officials. These awareness-raising training activities should focus on the firearms threat and initiatives to counter illicit firearms production and trafficking as well as on discrepancies in the relevant national and international legislation.

The prevention of illicit firearms production and trafficking could be enhanced through tactical, individual prevention activities such as intelligence build-up and preparedness for quick international cooperation as well as through sharing best practices for prevention campaigns.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat firearms trafficking.

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
2.	Illicit trafficking in firearms linked to organised crime and terrorism; supplying OCGs with firearms and ammunition from an illegal market
3.	Online aspects of firearms trafficking: OSINT, dark web, open web, other communication platforms, etc.
4.	Financial investigations related to firearms trafficking
5.	Cooperation with Member States, non-EU countries, international organisations and the private sector
6.	Firearms forensics: use of ABIS and different systems, forensic evidence
7.	Raising awareness of the firearms threat and initiatives to counter illicit firearms production and trafficking; national and international firearms legislation
8.	HUMINT management in illicit firearms related crime
9.	Best practices for prevention campaigns
10.	Fundamental rights and data protection

3.12. Missing trader intra-community fraud

3.12.1. Environmental challenges

Missing trader intra-community (MTIC) fraud is an area consisting of many forms of crime that abuse the differences in the tax and legal systems across Member States. Cooperation at national level among the different types of authorities is essential; however, tax authorities, which play a leading role in investigations in this area, are not part of law enforcement in many Member States.

At international level, there are few strategic and operational agreements to facilitate joint investigation and information exchange. Investigators face difficulties when accessing foreign business registries. The setting up of a centralised bank account register at European level with a single access point might improve international cooperation in the near future. Furthermore, an EU-level enforcement strategy is under discussion, but yet to be accepted.

Another major challenge in this crime area is that criminals have a high level of legal and accounting expertise. At the same time, good professionals working in the private sector are usually put off by the lower salaries in the public sector; thus, law enforcement lacks adequate and sufficient human resources to tackle MTIC fraud.

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

(a) Challenges

There is insufficient public understanding of the fact that MTIC fraud is a serious crime and of the scale of proceeds generated by criminal organisations.

MTIC fraud is strongly linked to other crime areas such as document fraud, which is facilitated by the availability of free software that can be used to issue fake invoices and bank statements. Criminals involved in MTIC fraud frequently play a role in other fraud schemes too. To hide or legalise criminal assets, criminal networks engaged

in MTIC fraud apply money laundering methods using virtual currencies and online bank accounts. Investigators have insufficient awareness of and knowledge on how MTIC fraud is financed and do not know what financial investigation techniques to apply. There is insufficient analysis in relation to the financial flows in MTIC fraud cases and a lack of capacity to analyse the large amounts of data seized from suspects.

Technology and digital infrastructure are essential components in concealing criminal activities. Technological development allows criminals to set up complex fraud schemes from one single device, store data in the cloud and on servers outside the jurisdiction of the EU, and use alternative payment methods, VPN services, encryption and VoIP. Law enforcement officials should be aware of the modus operandi of these schemes and of the relevant investigation techniques.

Criminal networks engaged in this crime area are highly sophisticated and work with a complex set of legal and illegal businesses and experts. The focus on transnational organised crime groups through intelligence-led investigation is insufficient. Investigators should be able to tackle those private sector professionals on whose services the fraud schemes are based.

Furthermore, there is insufficient cooperation and information exchange between national and international authorities and agencies, e.g. police, customs, prosecutors, judicial authorities, Europol, Interpol, and administrative authorities. Information sharing between tax authorities and law enforcement agencies is highly desirable at national and international level. Cooperation with key non-EU countries in which organised crime groups operate should be enhanced. In order to efficiently tackle MTIC fraud cases, a special focus is required on regional level cooperation covering joint operational activities. Law enforcement should make better use of the existing networks and cooperation instruments such as JITs, FIUs, European Investigation Orders (EIOs), European Arrest Warrants (EAWs), and information sharing via the Secure Information Exchange Network Application (SIENA). In addition to public sector agencies and authorities, cooperation with the private sector is essential. As regards information exchange and the sharing of data, it is a challenge to observe data protection regulations, especially during the intelligence gathering stage preceding investigation.

In order to further enhance the capacity to combat MTIC fraud, it is necessary to develop analytical products such as threat and risk assessments, early warnings, lists of high-value targets, scenarios and future trends.

(b) Training needs

Summary

First and foremost, law enforcement officials need training on the diverse modi operandi within the area of MTIC fraud, digital investigation methods and the intelligence-led investigation approach. Furthermore, training is required on the tools and methods used to combat related crime areas, such as document fraud, other fraud schemes and financial crime. The analytical skills of law enforcement should also be reinforced through training, with a focus on data and risk analysis and the relevant data protection regulations.

As cooperation is a key element in combatting MTIC fraud, joint training activities should be organised at national, EU and international level, involving different types of authorities and agencies, and non-EU countries.

Member States indicated that 4 657 officials need training in this area.

Further details

Law enforcement officials need training on the multifaceted modus operandi of MTIC fraud, including the operation of criminal networks, OCGs specialised in offering fake invoices, financial flows and schemes used for MTIC fraud, the exploitation of legal structures, versatility, adaptability to new trends and specialised advising.

There are insufficient investigative, prosecutorial and judicial proactive and intelligence-led approaches at national level; therefore, training is essential on intelligence-led investigation focusing on transnational organised

crime as well as on operational cooperation and sharing best practices.

Financial investigation techniques used to reveal money laundering methods such as the use of online banking and cryptocurrencies should be included in the training topics. The next priority is training to improve the use of digital technology by law enforcement officials. In addition, investigators working in the area of MTIC fraud need training on the tools and methods used to combat other related crime areas such as document fraud and other fraud schemes.

In order to enhance cooperation between the relevant agencies at national and international level, it would be desirable to organise joint training activities with the participation of the different actors along the enforcement chain, such as tax inspectors, police and customs officers, prosecutors and judges. Covering tax confidentiality issues at EU level would have an added value when it comes to information exchange.

Training on data and risk analysis, which is required, inter alia, for the detection of companies that might be used for MTIC fraud, should be accompanied by training on data protection regulations.

As several training providers, such as CEPOL, Europol, Eurojust, EJTN and EPPO, deliver EU-level training on tackling different aspects of MTIC fraud to various target groups, cooperation should be enhanced in order to harmonise these activities.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat missing trader intra-community fraud.

1.	Modus operandi: organised crime groups specialised in offering fake invoices; financial flows and schemes used for MTIC fraud; 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
4.	Technology and digital infrastructure as essential components in concealing and facilitating criminal activities (data storage, alternative payment methods, VPN services, encryption, 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.	Forensics
10.	Tackling document fraud
11.	Crime prevention

3.13. Corruption

3.13.1. Environmental challenges

Corruption is a complex, multifaceted and multidimensional phenomenon ranging from low-level petty bribery to state capture, where organised crime groups infiltrate and conquer all or part of the state institutional system. The political and institutional set-up, culture and tradition of a country largely influence the level of corruption, the tolerance of society towards corruption and the opportunities for law enforcement officials to efficiently investigate and prosecute cases.

Detection is challenging, as corruption is a hidden, largely underreported phenomenon, where in most cases all parties involved benefit from the transaction. The capacity of law enforcement to investigate petty corruption targeting public servants should be increased. When it comes to the investigation of systemic, grand corruption cases, the main challenge is to cope with the political pressure.

Legislation is in place in most Member States, but its implementation depends on political will. Many Member States report that the emergency ruling during the pandemic has given new opportunities for governments to allocate public funds via procurements and subsidies with less transparency and control.

The protection of whistleblowers and witnesses is an issue in most Member States due to loose, partially-implemented legislation and an improper institutional framework.

By setting up the European Public Prosecutor's Office (EPPO), the EU has taken further steps to ensure the backbone of an efficient institutional structure for investigating and prosecuting corruption cases. However, the national implementation of integrity systems and independent control mechanisms is lagging behind in some Member States. It is necessary to reinforce national authorities' capacity to address highly complex corruption cases related to organised crime, in particular by setting up specialised anti-corruption structures and by increasing the capacity of relevant police units.

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

(a) Challenges

Corruption is strongly linked to criminal finances; therefore, the capacities of investigation authorities to analyse large sets of data, follow the money and recover state assets should be improved. The complexity of money laundering typologies and multi-jurisdictional judiciary processes requires law enforcement personnel to possess special knowledge and skills. New phenomena such as the use of cryptocurrencies by criminals require regular knowledge updates. Corruption is one of the main crime enablers used by criminal networks as part of their criminal business model. It is prevalent in all crime areas and implemented in a variety of forms ranging from bribery through nepotism, match-fixing, extortion and embezzlement to grand corruption linking political and business interests. It is challenging for law enforcement officials to be aware of all types of corruption and have up-to-date information on the changing trends due to the digitalisation of public administration.

Since corruption is an underreported phenomenon, it is essential for investigators to be able to deal with witnesses and whistleblowers and analyse their motivation for reporting.

The development of a culture of integrity and good risk management practices within public administration and law enforcement would be beneficial, particularly as regards awareness and the proper management of conflicts of interest.

Cooperation between the police and the judiciary is imperative so as to ensure that the evidence gathered during investigations can be adequately presented in court. Furthermore, international cooperation and information exchange should be improved, with a special emphasis on available cooperation mechanisms and the roles of different institutions at EU level. With regard to non-EU countries, the anti-corruption element of change management in CSDP missions could be reinforced.

(b) Training needs

Summary

Though corruption is recognised as one of the major challenges to democracy and the prosperity of citizens, training opportunities at national and international level remain insufficient.

Training topics should primarily include the crime patterns of corruption, the different forms of its manifestation, and investigation techniques, with a special emphasis on financial investigation methods.

Another aspect that requires attention is cooperation with the judiciary, between EU institutions, and with non-EU countries, which can and should be enhanced through joint training activities involving representatives from the relevant fields.

Moreover, it is essential to provide training on the prevention of corruption, focusing on integrity and anti-corruption strategies as well as on vulnerability and risk assessment.

Member States indicated that 6 127 officials need training in this area.

Further details

The highest priority in terms of training is financial investigation related to corruption cases. Training should focus on the recovery of state assets, corrupt payments in the financial system, cash-based corruption, offshore structures, and cryptocurrencies used for making payments to corrupt officials and for money laundering purposes.

The next priority in the ranking is training on the existing cooperation mechanisms at EU level, the roles of OLAF and EPPO, the information and intelligence exchange tools available to investigators, such as SIENA, SPOC, liaison offices and other information sharing channels. Cooperation with the judiciary, ranked slightly lower, should be enhanced through joint training activities focusing on presenting data and evidence in court. Representatives of the public sector and those of anti-corruption NGOs should be invited to multidisciplinary training activities focusing on anti-corruption strategies and tactics.

Furthermore, law enforcement officials need training on the different corruption methods related to the allocation of state funds, such as public procurements and state subsidies, and their relation to party financing. In addition, the manipulation of digital processes in public administration and the forms of corruption related to the health and sport industries, in particular match-fixing, should also be included in the training topics.

With regard to crime patterns, training is needed on investigation techniques, including analytical tools to facilitate the detection or investigation of corruption, evidence collection, intelligence analysis, big data analysis, reporting techniques, sharing best practices and dealing with witnesses and whistleblowers.

Training on prevention should focus mainly on integrity and risk assessment. To develop a culture of integrity, it is necessary to put emphasis on anti-corruption and integrity strategies within public administration and law enforcement, the proper management of conflicts of interest and respect for the rule of law. In addition, it is also crucial to have an overview and understanding of the risks and threats caused by corruption before they materialise into corruption-related crime.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat corruption.

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.	Cooperation between national, EU and international agencies and with judicial professionals, roles of EPPO and OLAF
3.	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)
4.	Investigation and intelligence practices
5.	Corruption as a crime enabler
6.	Sharing expertise, best practices, data and information between Member States 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
10.	Internal investigations
11.	Protecting and handling whistleblowers and witnesses
10.	Police ethics
11.	Tackling document fraud

3.14. Excise fraud

3.14.1. Environmental challenges

International cooperation is of key importance in tackling excise fraud cases; however, the culture of spontaneous information exchange between countries and law enforcement agencies needs to be further strengthened. The current shortcomings are due partly to the lack of awareness among officials of the available information exchange tools, and partly to the lack of harmonised legislation. At the same time, criminal networks operating in this crime area are highly flexible and easily adapt to new circumstances, which means that effective data and information sharing between countries and law enforcement agencies is imperative for enhancing investigations.

With regard to investigations and conducting operational actions or physical checks, the major challenge seems to be the lack of sufficient human resources in customs and police agencies. Besides border management and risk-analysis based customs control, the inspection of small parcels is also an aspect that needs attention in view of the rapid growth in the volume of this form of illegal commerce. Law enforcement operations must be backed up with effective operational, tactical and strategic analysis capabilities. Wiretapping and surveillance are hindered by legal constraints and technical obstacles, such as encrypted messages and phone calls via encrypted apps.

In order to efficiently tackle excise fraud cases, it is necessary to enhance cooperation with industry so as to identify synergies and effectively use its expertise and gathered intelligence.

As regards the prevention of excise fraud, effective systems should be in place and accompanied by effective control mechanisms. The lack of adequate and sufficient resources slows down the efforts to adapt the existing systems to the rapid changes and emerging challenges or to establish new control and cooperation mechanisms. The Excise Movement Control System (EMCS), the backbone of excise control in the EU, is designed to facilitate trade and not to detect offences.

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

(a) Challenges

One of the main challenges for law enforcement is keeping up with the changing crime patterns in excise fraud. For illicit tobacco production, criminals use modern technology to boost production capacity, hide from detection and ensure the protection of production sites. In the case of oil fraud, there is an increasing shift to non-fossil fuels and the criminal abuse of biofuels in fraudulent biodiesel trading. In the fight against alcohol fraud, Brexit has changed the landscape and the possibilities of law enforcement cooperation. Similarly, the business models and modi operandi of criminal networks evolve rapidly, and thus investigators' knowledge in this area should be enhanced.

The use of online investigation tools, such as open source intelligence and undercover operations on the darknet, needs improvement. The capacity of law enforcement to conduct big data analysis and use artificial intelligence should also be strengthened.

Furthermore, the experience and knowledge of law enforcement officials regarding how to investigate the financial aspects of criminal activities should be greatly reinforced in areas such as the identification of proceeds of crime, money laundering techniques, and the tracking, tracing and freezing of criminal assets.

The detection and investigation of cases is often hindered by a lack of capacity to recognise the fraudulent documents used in the different phases of excise fraud, from renting premises to presenting documents at customs controls.

Proper cross-border operational collaboration requires more effective use of EU and international cooperation tools and mechanisms, including joint investigation teams, and familiarity with the roles of different EU institutions. Law enforcement's cooperation with the private sector and with non-EU countries should also be enhanced.

(b) Training needs

Summary

Law enforcement officials primarily need training on the crime patterns and investigation methods of excise fraud. This is followed, in terms of priority, by training on cooperation mechanisms at national and international level, sharing best practices and case studies. Furthermore, officials would also benefit from training on the use of online investigation tools and on criminal and risk analysis methods.

Training on how to incorporate financial investigation into excise fraud investigation is in high demand together with training activities targeting a common approach to legislation.

Member States indicated that 7 423 officials need training in this area.

Further details

According to the respondents, training should primarily focus on the crime patterns and investigation methods of tobacco and mineral oil fraud cases. Regarding the illegal tobacco trade, investigators would benefit from training providing in-depth knowledge on illegal cigarette production methods, manufacturing equipment, new products, raw tobacco and different smuggling methods as well as on tackling the contraband of cheap whites, the smuggling of counterfeit products and the illegal use of waterpipe tobacco. In the case of mineral oil fraud, training should focus on combatting designer fuel fraud and fuel laundering as well as on offences with missing traders. Training on crime analysis methods could also support the work of investigators.

The next broad topic in terms of training priority, as ranked by the Member States, relates to cooperation tools and mechanisms. On the one hand, training should cover bilateral and international cooperation mechanisms, how to build trust among law enforcement officials, EU cooperation tools and cooperation with non-EU countries. On the other hand, it should focus on national level cooperation mechanisms, such as sharing best practices on cooperation between law enforcement, fiscal bodies and customs authorities as well as with private actors in the industry.

Furthermore, law enforcement officials need training on how to integrate financial investigation into excise fraud investigation, with a focus on financial investigation methods, enhanced asset recovery and big data analysis.

Training should also be provided on the effective use of both online and offline investigation tools, such as open source intelligence, online undercover operations on darknet markets, decryption, covert surveillance, GPS, covert investigations, informant handling practice and interviewing techniques. In addition, training on customs risk analysis and mobile control units could enhance the work of law enforcement officials performing border or inland controls.

The fight against transnational excise fraud is hindered by the fact that cross-border fraud is often committed only in the final phase, in the country of destination, whereby no offence takes place in the country of origin or the countries of transshipment. In such cases, criminals deliberately move excise products through as many jurisdictions as possible to block law enforcement efforts. Therefore, organised cross-border fraud can be tackled only via effective cooperation between law enforcement authorities.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat excise fraud.

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.	Use of crime analysis methods
4.	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
5.	Integration of financial investigation methods into excise fraud investigation accompanied by enhanced asset recovery and big data analysis
6.	Crime patterns, intelligence and investigation methods, techniques and tools in the area of alcohol fraud
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.	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
11.	EU legislation and international agreements, Framework Convention on Tobacco Control
12.	Covert surveillance, GPS, covert investigation, informant handling practice, interviewing techniques
13.	External Union transit procedure (T1), transit fraud, abuse of the 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

3.15. Intellectual property crime, counterfeiting of goods and currencies

3.15.1. Environmental challenges

The production and import of counterfeit goods is on the rise within the EU in many industries and trading has shifted online, both to the surface web and to the dark web. The highest increase has been seen in pharmaceutical crime due to the huge demand for medical supplies as a consequence of the COVID-19 pandemic. Human and technological capacities to detect falsified documents and counterfeit products need improving. Law enforcement should be equipped with adequate technological tools to detect counterfeit products and properly manage digital evidence. Since customers are often not aware that they are purchasing counterfeit products, the reporting of cases is limited. Thus, cooperation with industry players and supervisory authorities is essential at national, European and international level.

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

(a) Challenges

One of the challenges in this area comes from the fact that counterfeit products are traded in a broad variety of industries and law enforcement should have knowledge of them all. Products are mostly sold online using encrypted communication channels, which makes investigations lengthy and difficult. There is clear awareness among officials of document fraud being a linked crime area due to the use of falsified labels and forged origin and travel documents. However, the potential link to environmental crime is not yet widely recognised.

The detection of counterfeit products at the borders is challenging due to the semi-finished products entering the EU (i.e. trademarks, labels, logos, etc. are added on imported 'blank' products and packaging). The prosecution of cases is hindered by the use of legal business structures for trading in counterfeit products and whitewashing criminal profits.

In order to ensure more effective information exchange, cooperation with health and environmental protection authorities, consumer protection agencies and industry players should be significantly improved.

(b) Training needs

Summary

Training in this area should focus on the modi operandi of criminal networks, the use of digital tools for investigation, the preservation of evidence, and the investigation methods used in linked crime areas, particularly in document fraud and financial crime. This should be complemented with training on the protection of intellectual property rights.

Cooperation tools and information exchange mechanisms should be addressed during joint training activities involving representatives of industry players, such as right holders and online and offline intermediaries (e.g. e-commerce marketplaces, social media platforms, mobile app stores, domain name registries and registrars, transport and logistics service providers, payment industry), customs, the police, market surveillance authorities the judiciary, and non-EU countries.

Member States indicated that 4 648 officials need training in this area.

Further details

Training is most needed on the crime patterns of counterfeiting: how criminals use legal business structures, online platforms, fraudulent documents and virtual currencies. The second training priority is the protection of intellectual property rights in different business areas. Since trade in counterfeit products and piracy mostly happen online, training on digital investigation techniques and cyber patrolling is also ranked high on the list. In terms of investigation, although ranked relatively low, officials need training on financial investigations related to this crime area.

Further training topics include the different forms of counterfeiting and infringement of intellectual property rights (IPR), such as pharmaceutical crime, currency counterfeiting, fraud in commercial items and copyright protection.

Joint training activities are expected to enhance cooperation between customs, the police, market surveillance authorities and the judiciary as well as cooperation with non-EU countries. Training should cover the use of databases, information exchange platforms and the tools provided by the European Union Intellectual Property Office (EUIPO). Furthermore, it is suggested that joint training activities with IPR owners as well as with online/offline intermediaries, could enhance cooperation between law enforcement and industry players.

Training on customs risk-analysis tools/systems and processes is expected to help prevent counterfeit goods from entering the EU.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat intellectual property crime, counterfeiting of goods and currencies.

1.	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
2.	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)
3.	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.	Tackling currency counterfeiting
7.	Issues related to fraud in commercial items, e.g. food, drinks, textiles, etc.
8.	Cooperation between customs, the police (including border police), and market surveillance authorities and the judiciary
9.	Customs risk analysis related to (trade in) counterfeit goods
10.	Financial investigations
11.	Cooperation with IPR holders , as well as with online/offline intermediaries
12.	Forensics
13.	Fundamental rights and data protection

3.16. Environmental crime

3.16.1. Environmental challenges

The main issue regarding this crime area used to be the lack of awareness of decision-makers, law enforcement officials and the general public of environment-related criminal activities. Since the launch of the European Green Deal in 2019, more attention has been paid to the protection of the environment and to illicit activities against the environment. Despite the rapidly growing interest in the area at public and political level, the lack of awareness of the details on environmental crime and of its costs to society remains one of the key challenges. Unfortunately, this lack of awareness results in a lack of resources for investigating environmental crime. Obviously, if the area receives less attention from law enforcement, criminals have more chance of avoiding detection and prosecution.

Much like the categorisation and classification of crimes, legislation on environmental crime is different in all Member States. The differences in legislation combined with the transnational nature of environmental crime make cross-border cooperation in investigation imperative, as criminals take advantage of legal gaps and inconsistencies. Although restrictive data protection regulations hinder the exchange of information among different authorities to a certain extent, cooperation between national authorities as well as with the private sector could still be improved.

Despite the challenges mentioned above, environmental crime is receiving increasing attention in the European and global political scene and it doesn't seem like this trend is going to change in future.

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

(a) Challenges

The awareness of decision-makers regarding the significant implications of environmental crime should be enhanced. The general public's awareness of the costs of environment-related criminal activities to society should be raised.

Environmental crime is multifaceted including, inter alia, hazardous and non-hazardous waste crime, wildlife crime, maritime exploitation, crime related to the use of renewable energy and recycling, illegal, unreported and unregulated fishing, pollution of air and waters, and ozone depletion. Investigators' knowledge about the varied modi operandi in all areas should be improved alongside the enhancement of their digital investigation skills. As environmental issues gain importance at European level, the number of environmental crime investigators is expected to grow, which requires significant investment in international training, especially in view of the rapid changes in crime patterns.

Corruption constitutes an integral part of environmental crime, be it petty corruption involving bribery of public officials or grand corruption involving criminal infiltration of legal business structures. In order to disrupt the corrupt practices applied by criminal networks, there is a great need to improve investigators' ability to use financial and economic crime investigation techniques such as national and international asset recovery to seize the proceeds derived from environmental crime.

Better cooperation and information exchange between Member States' law enforcement and with non-EU countries, including CSDP missions, are necessary. Networking among different agencies dealing with environmental crime issues should also be enhanced. Cooperation between law enforcement, judiciary authorities and environmental inspectorates is vital for success, the latter possessing expertise and critically important knowledge on environment management.

(b) Training needs

Summary

Investigation techniques and modi operandi in the different areas of environmental crime must be among the training topics. The highest ranked area is waste crime, followed by wildlife crime, maritime exploitation, and pollution. All investigators would benefit from training on specific online and offline investigation techniques as well as from training focusing on related crime areas such as financial crime, corruption and document fraud. Cooperation at national and international level should be enhanced through joint training activities. The emerging legislative trends related to the circular economy and the administrative steps to counter environmental crime constitute new training topics.

Member States indicated that 5 861 officials need training in this area.

Further details

The ranking of training needs varies across the different areas of environmental crime. The highest priority is given to training on the modus operandi of waste crime including waste trafficking, dumping at sea, landfills, mixture of waste, disposal, dismantling and waste fires as well as to training on effective investigation techniques. Training on combatting wildlife crime, including timber trade, is ranked sixth in terms of priority. Tackling maritime exploitation is the ninth training priority, covering topics such as pollution and illegal, unreported and unauthorised fishing. This is followed by the need for training on combatting air pollution and ozone depletion.

The second highest training priority according to the Member States is related to specific investigation techniques for environmental crime cases. Focus should be placed on improving the digital skills of law enforcement, including the use of open source intelligence and darknet investigation, as well as on intelligence collection, dealing with whistleblowers, undercover operations and wiretapping.

Law enforcement officials need to be familiar with the peculiar operation of high-risk criminal networks active in the area of environmental crime. The infiltration of legal business structures by organised crime is an existing threat. Special attention should be paid to the criminal infiltration of the recycling and renewable energy systems, as these industries receive heavy state subsidies. At the same time, the transnational trade of quotas, due to its complex nature and lack of transparency, offers possibilities for criminal exploitation. Criminals also use legal and technical experts as crime enablers. In order to disrupt criminal networks, it is essential for investigators to be well-trained on financial investigation techniques as well as on tracing, tracking and freezing assets originating from environmental crime. In addition, training is required on combatting document fraud and corruption related to environmental crime.

International cooperation could be enhanced by training law enforcement officials on how to use the existing EU cooperation instruments and networks as well as global cooperation tools and mechanisms, and on how to implement best practices of cooperation with non-EU countries. Training focusing on cooperation between different agencies dealing with environmental issues would boost both national and international cooperation.

The new legislative trends related to the circular economy should be covered in training, as such knowledge would help in the process of identifying crime enablers.

In order to enhance prevention activities, it is important to provide training on administrative tools to combat environmental crime as well as training for the personnel of CSDP missions on how to spread good enforcement practices and standards in host countries.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat environmental crime.

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, darknet; collection of intelligence, dealing with whistleblowers; undercover actions, surveillance, wiretapping as part of environmental crime investigation
3.	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
4.	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
5.	Cooperation: interagency cooperation between different agencies dealing with environmental issues; EU cooperation instruments and networks; cooperation with non-EU countries, global cooperation tools

6.	Wildlife crime: emerging patterns, trends, crime groups. Wildlife crime shall cover crime against flora and fauna in line with CITES (Convention on International Trade in Endangered Species of Wild Fauna and Flora), including illegal logging and timber trade (modus operandi, investigation techniques), trafficking protected species (glass eels, reptiles, mammals, birds), illicit pet trade, etc.
7.	New legislative trends related to the circular economy to help in identifying crime enablers
8.	Related crime areas such as document fraud and corruption
9.	Maritime exploitation and pollution; illegal, unreported and unauthorised fishing (modus operandi, investigation techniques)
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

3.17. External dimensions of European security

3.17.1. Environmental challenges

The stability of the EU's neighbourhood is crucial for its internal security. When discussing the external dimensions of European security, two main, strongly-interrelated directions should be covered, namely the capability challenges and training needs related to CSDP missions' personnel, and capacity building in – and in cooperation with – non-EU countries. CSDP missions have been on the agenda of strategic-level training priorities for a long time, but are traditionally ranked low on the priority list. Capacity building in non-EU countries is a relatively new topic, although there is a lower level of awareness in Member States of its relevance and importance in preventing organised crime and terrorism within the EU. Meanwhile, the EU invests increasingly in capacity-building activities in non-EU countries in order to enhance the safety of the European community.

In the case of CSDP missions, it is challenging to find the right personnel. Officials should be able to cover different fields, flexible enough to work with military, law enforcement and civilian colleagues and able to face the hostility towards the EU's presence that is sometimes encountered. The ratio of women employed in CSDP missions is still very low. As staff turnover is high in CSDP missions, there should be proper systems in place to preserve institutional knowledge and memory.

In terms of capacity building in non-EU countries, the challenges are manifold, including political, economic and budgetary aspects ranging from language barriers and political tensions between states participating in the same capacity-building project to the low level of digitalisation of counterparts and reluctance to cooperate with the EU.

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

(a) Challenges

The cooperation concept needs to change in order to develop Member States' and non-EU countries' national and generic capabilities as national systems of coordination, communication and management. This can be achieved through deployment and career path development of officials, the improvement of the legal framework, budget development and strategic communication, which will support increased contribution to CSDP missions and operations.

A more integrated, strategic approach is needed for the management of CSDP missions, focusing on local ownership, evaluation, analysis, benchmarking techniques, operational impact assessments, the identification of best practices and the use of lessons learned in the missions' planning, management and review. The analytical, planning and decision-making structures and procedures in CSDP missions need substantial improvement.

In CSDP missions, it is necessary to deepen knowledge about the rule of law, criminal justice, anti-corruption, gender equality, cultural diversity, an enabling environment for civil society, non-discrimination, freedoms of association, assembly and speech, and taking action against hate speech.

Furthermore, there is a need for capacity building in partner states, particularly in neighbouring and enlargement countries, which will support operational cooperation with EU Member States and agencies. Capacity building should also aim to provide partners with the necessary tools, such as digital ecosystems, and with information on how to adopt national legislative reforms and adhere to international standards.

In order to support the capacity-building efforts related to the external dimensions of European security, strong cooperation among stakeholders is fundamental. Civil-military cooperation and its conceptual development should be enhanced. In addition, synergies between CSDP structures, Commission services and Justice and Home Affairs actors should be improved and best practices should be disseminated. It is crucial to ensure that non-EU countries are involved in EMPACT and in counter-terrorism activities.

(b) Training needs

Summary

Training should start by building capacity to better organise CSDP missions, with a focus on increasing leadership effectiveness and improving analytical, benchmarking and operational skills. The need for pre-deployment training covering a wide range of topics is next in the ranking.

Awareness should be raised in Member States of how the external actions of the EU contribute to safeguarding the rule of law and internal security.

Officials working with non-EU countries need English and French-language training. Digital skills and the use of new technology should be improved both within CSDP missions and in non-EU countries. In addition, respect for human rights and gender mainstreaming should be included in the training topics. The same is true of cooperation with stakeholders.

In order to ensure the effectiveness of training activities, cooperation and synergies between the relevant training providers should be streamlined.

Member States indicated that 3 937 officials need training in this area.

Further details

The highest priority in terms of training is to increase leadership effectiveness in CSDP missions. In this respect, the focus needs to be on enhancing the capacity to better organise the missions as well as on change management in the host country.

Pre-deployment training is essential for CSDP missions and should cover topics such as the rule of law, criminal justice, anti-corruption, policing in line with international human rights standards, differences in legislation on the use of force, duty of care, and cooperation between civilian and military missions. Training on the improvement of the efficiency, consistency, transparency, oversight and accountability of CSDP missions is also needed as part of an integrated approach, focusing on analytical, planning and decision-making structures and procedures.

There is a need to raise awareness of the EU's role as a security provider through its CSDP missions and of how this relates to safeguarding the rule of law within the EU and to its internal security. Awareness raising should target both law enforcement and the public in the Member States.

Language training is also considered a priority, with a focus on English communication skills and French as a foreign language. In addition, digital skills should be improved both within CSDP missions and in non-EU countries.

Furthermore, the political, economic and budgetary aspects of cooperative projects in defence and security within the framework of CSDP should be included in the training topics.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training focusing on the external dimensions of European security.

1.	Leadership in CSDP missions, planning and command, change management in host country
2.	Pre-deployment training
3.	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
4.	The EU's role as a security provider through CSDP, including CSDP policy on strategic ambitions and capability limitations
5.	Analytical, planning and decision-making structures and procedures
6.	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
7.	Role of CSDP missions in supporting EU internal security (external dimension of internal security)
8.	Building advisory capacity of CSDP missions

9.	Language training: English communication skills; French as a foreign language
10.	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)
11.	Civil-military cooperation and its conceptual development
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.	Cooperation: synergies between CSDP structures, Commission services and 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
16.	High-risk criminal networks
17.	Tackling document fraud
18.	Crime prevention

3.18. Other thematic areas

This chapter covers specific training needs that fall outside the scope of the 17 thematic areas presented in the previous subchapters and derive from various sources. English language training is a horizontal topic that is not related to one specific crime area. The need for training on tackling core international crimes was identified through the desk research conducted, as was the importance of providing training in the area of emergencies requiring law enforcement response. Meanwhile, the other topics were indicated during the written consultation with law enforcement professional networks. The training needs are listed in order of priority, as ranked by the Member States.

Management and leadership training for law enforcement officials has long been on the agenda; therefore, CEPOL has already introduced a broad offer of onsite and online resources. Besides the improvement of leadership and managerial skills, sharing best practices on the reorganisation of law enforcement work and operations as a result of the pandemic would be appreciated. Furthermore, as several experts indicated, law enforcement leaders need awareness-raising training in areas that are less in the focus of everyday investigations, such as zero tolerance towards the non-respect of fundamental rights and better allocation of resources within the organisation.

The main language of law enforcement international cooperation is English. Although training is provided at national level in all Member States and the English competence of law enforcement is improving, **English language** courses are still in demand so as to enhance both general language skills and knowledge of specific law enforcement terminology.

Policing of football events has a unique character with an international dimension. Officials working in this field have to face several challenges resulting from the various interpretations of the European standards and the differences in national legal frameworks and available resources across Member States. The Pan-European Think Tank of Football Safety and Security Experts indicated that it is necessary to develop effective partnerships with foreign colleagues and to fully comprehend and implement the EU legal framework. The training of officials should cover raising awareness of international football dynamics and of the variability in national experiences and perspectives, legal frameworks, policing structures and strategies, and cultural factors. Training would provide an opportunity to share established good practices and crowd management techniques and to discuss issues such as the importance of adopting a proportionate and targeted approach, effective communication at the planning and operational stages and early intervention to prevent and limit public order risks. Furthermore, training should also address international information exchange and cooperation mechanisms on policing football events and highlight the role of visiting police delegations in informing visiting supporters about policing tactics. In order to maximise the sharing of experiences, challenges and remedial actions, it is advisable to complement explanatory sessions with interactive ones. Training should target the law enforcement practitioners responsible for policing international football events such as match commanders, spotters and the personnel of national football information points (NFIPs).

In its response to the written consultation, the European Network for the **Protection of Public Figures** (ENPPF) indicated several training needs of protection officials, emphasising the importance of risk assessment and harm prevention, and addressing the issue of interference with the privacy of the protected person. The training of protection officers should be delivered while maintaining the highest domestic and international standards, and should apply a two-tier approach comprised of addressing team leaders with a full programme and decision-makers with a short activity.

In order to efficiently protect public figures, preventive protection officials need training on threat and risk assessment for a particular venue or programme. Training should include the exchange of information on the use of case studies to detect those posing a serious risk, the joint development of responses to the same types of problems, and the use of information processing software. Furthermore, emphasis should be placed on how to filter out serious threats from the set of threats using elaborated analytical programmes, the transfer of knowledge, and the aspects and characteristics of reliable assessment.

Venue security officers, close protection officers and security drivers would benefit from training on preparation, venue security, selecting and securing transport routes, responding to frequently changing programmes and needs depending on the security situation, and addressing unexpected situations. Training would enhance the provision of complete protection at events organised with the participation of VIPs that attract crowds.

CBRN experts of personal protection services need training on CBRN supervision and defence for the permanent residence of VIPs, for the transport routes used by the protected persons and for public programme venues, in particular mass events. Training should focus on CBRN protection of premises, CBRN security of events, the scope of possible national partner services that can be involved in providing CBRN defence, and the performance of CBRN security tasks. Close protection officials would benefit from training on emerging and asymmetric threats and non-conventional weapons. A major challenge that cannot be addressed through training but that needs

considerable attention is ensuring that the equipment of protection officials is adequate for the constantly changing threats.

As identified by the EU-STNA desk research, capability challenges in the area of **emergencies requiring law enforcement response** are related to the rapidly changing environment and crime patterns. The refugee crisis of 2015 exposed weaknesses and gaps in EU and national crisis management systems as well as a lack of capacity and available tools in the Member States most under pressure. The outbreak of COVID-19 was another example of a sudden change not only in the modi operandi of criminals but also in the work patterns of law enforcement agencies. The implications that pandemics and public health emergencies can have on policing should be assessed and acknowledged. The upcoming economic recession will generate further emergencies in Member States, for which law enforcement should be prepared. Tackling these challenges requires an integrated and coordinated law enforcement approach at national and international level.

There is a need to build capacities for the prevention or early detection of emergency situations and for adequate rapid response to crises. Therefore, it is important to provide training on EU crisis management, including the role of agencies and Member State law enforcement authorities, and on inter-agency cooperation, preferably as joint courses across EU institutions and agencies. First responders would benefit from sharing best practices of fellow organisations and colleagues regarding how to react to crisis situations.

The need to understand the financial opportunities provided to law enforcement authorities by the EU arose during the desk research and was brought up in some of the expert group discussions. In this respect, training should focus on the **EU funding opportunities** available to law enforcement, the preparation of project proposals and EU project management.

Core international crimes (genocide, crimes against humanity, war crimes, and sexual and gender-based violence by the Islamic State of Iraq and the Levant) are largely committed in conflict zones where ongoing conflicts reduce investigative opportunities. While the conflicts largely take place outside the EU, they also have an impact on the Member States; therefore, the nexus between internal and external security should be explored. In order to bring perpetrators to justice and close the impunity gap, it is necessary to improve information exchange and cooperation mechanisms and enhance national investigations and prosecutions.

Training on the investigation of core international crimes should be developed in cooperation with Eurojust, CEPOL and the European Judicial Training Network and should cover the review of case-law on the use of open source evidence in prosecution, measures to strengthen information exchange, combatting racism and xenophobia, and investigating foreign terrorist fighters as potential war criminals. Military officials would benefit from training on evidence collection and transmission.

As the Disaster Victim Identification Network indicated in its response to the written consultation, training in the area of **disaster victim identification** should focus on the identification of disrupted human remains, the management of disaster victim identification activities during mass fatality incidents, and deployment abroad due to mass fatality incidents taking place in other countries. Moreover, it is essential to increase the efficiency of international collaboration, which is hampered by the insufficient harmonisation of identification procedures for individual cases.

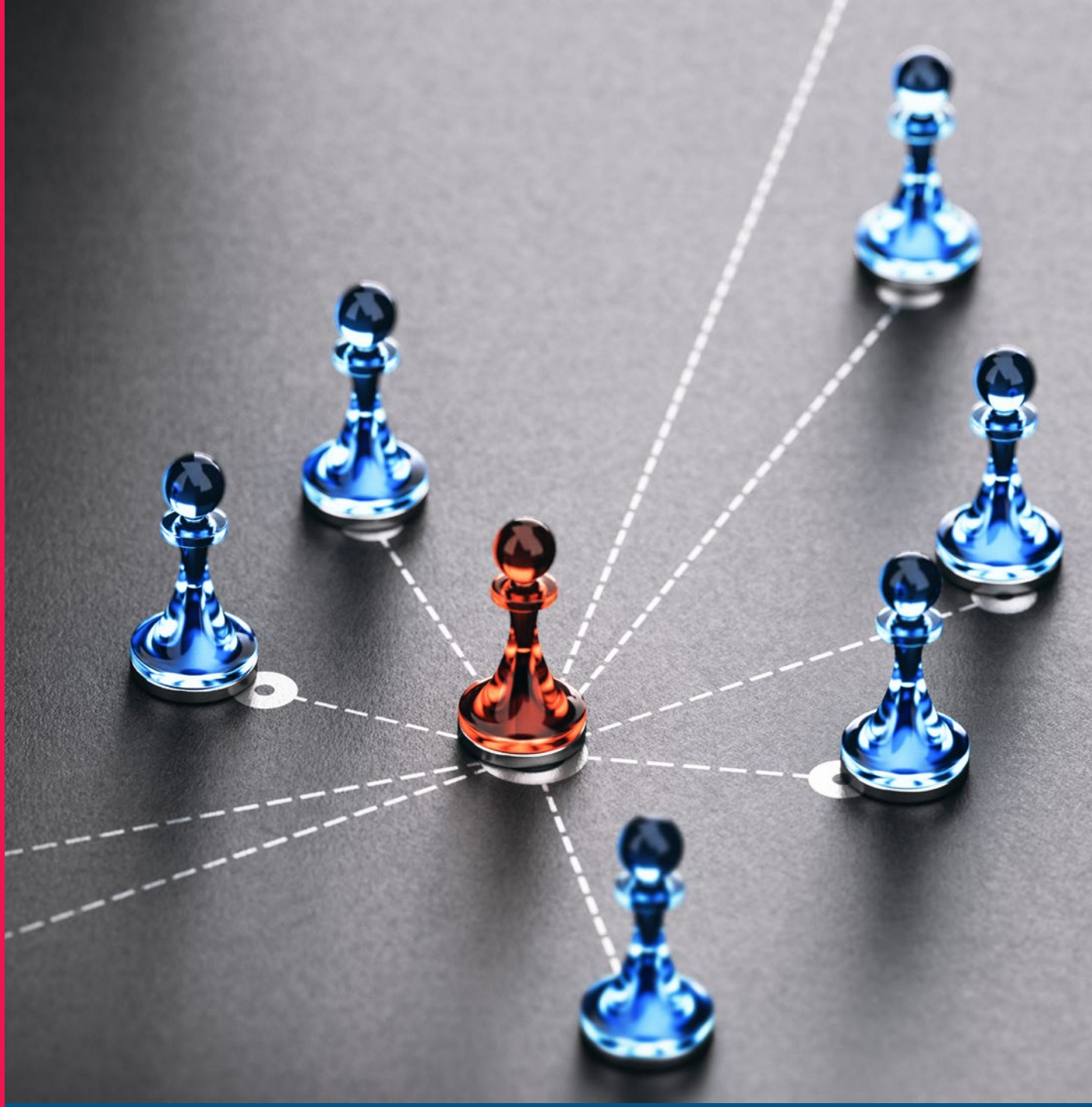
In its response, the Police Network for Law Enforcement Dog Professionals (Kynopol) specified that dog handlers need upskilling on how to train service dogs for new scents and for new disciplines, including searching for different objects such as computer parts, memory sticks and mobile phones. Furthermore, in order to support counter-terrorism, methods should be developed for training service dogs to search for improvised explosive devices. Besides training, a significant challenge that needs to be addressed in this area is the procurement of good quality dogs.

Member States indicated that 5 797 officials need training in this area.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of other thematic areas where training for law enforcement is needed.

1.	Leadership and management
2.	English language
3.	Public order
4.	Emergencies requiring law enforcement response
5.	EU funding and EU project management
6.	Core international crimes
7.	Stress management, conflict management and communication
8.	Disaster victim identification
9.	Training of service dog handlers



4. CONSULTATION WITH TRAINING PROVIDERS

Following the contribution of several law enforcement expert groups and networks to the process of the EU-STNA (see Annexes 4 and 5 for the list of contributors), CEPOL invited European agencies and other entities particularly active in the field of internal security and in related training initiatives to join the round of consultations, share their opinions on the prioritisation of training needs and indicate their availability to support the training efforts in the thematic areas identified. In total, 15 training providers were contacted in this respect and feedback was received from the following parties:

- European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA),
- European Asylum Support Office (EASO),
- European Border and Coast Guard Agency (Frontex),
- European Commission,
- European Crime Prevention Network (EUCPN),
- European Institute for Gender Equality (EIGE),
- European Judicial Training Network (EJTN),
- European Monitoring Centre for Drugs and Drug Addiction (EMCDDA),
- European Public Prosecutor's Office (EPPO),
- European Union Agency for Criminal Justice Cooperation (Eurojust),
- European Union Agency for Law Enforcement Cooperation (Europol), and
- European Union Agency for Fundamental Rights (FRA).

4.1. General remarks

While the training providers largely agreed with the prioritisation of the training needs carried out by the Member States, they also expressed complementary views in those areas where their opinions differed from the list. The participants noted that more importantly than taking a stand on the priorities as set by the Member States, the consultation should focus on how each EU-level training provider could contribute to covering the needs, and on the cooperation methods available to those ultimately implementing the training programme to be designed based on the EU-STNA findings. Frontex put forward a proposal to review the EU-STNA methodology so that the relevant training providers would be allowed to share their opinions and make suggestions, in particular regarding needs related to their own areas, at an earlier stage, before the phase of prioritisation. As all training providers were involved in the expert group meetings preceding the prioritisation process, Frontex's proposal might be addressed by asking training providers for input regarding the composition of the expert groups.

4.2. Thematic observations

In relation to ***the use of new technologies***, ECTC observed that, given the increased use of AI in all areas of life, including law enforcement, it should be given more priority. FRA noted that all training activities addressing AI and big data should make reference not only to data protection but also to other fundamental rights, in particular non-discrimination and access to an effective remedy. Europol also brought attention to a gap in generic training on topics related to mass data, data protection, machine learning, law enforcement cooperation and EU cooperation tools.

Views concerning ***data protection and fundamental rights*** were strongly supported by FRA, which pointed out the importance of integrating fundamental rights awareness into training in all thematic areas, with a focus on purpose limitation, necessity and proportionality, data quality and access rules in the case of large-scale databases, interoperability and information exchange. While fundamental rights considerations are of particular importance in ***combatting radicalisation***, they are equally essential when it comes to the collection of digital evidence and lawful interception, addressing terrorist content online and foreign terrorist fighters (including the return of their families from conflict zones), the interoperability of large scale IT systems and the use of AI by law

enforcement. Therefore, FRA suggested that special emphasis should be placed on the principle of non-discrimination, to be complemented with a more general reference to fundamental rights across all areas.

Europol highlighted the need to raise awareness of ***EMPACT*** as an EU flagship initiative in the fight against organised crime. It suggested the development of a training package for EU law enforcement and beyond with a view to deepening understanding of how EMPACT works and how Member States can engage or become action leaders. Considering the launch of the new EMPACT cycle 2022–2025, Europol also sees a need to design more in-depth, advanced training targeted at EMPACT Drivers and Co-drivers.

The importance of maintaining ***high-risk criminal networks*** as a key priority was acknowledged by the Commission's representatives involved in the consultation. They are confident that training based on the current EU-STNA findings will benefit Member States' authorities and other relevant audiences, since focus on this area is well justified and the related training efforts are needs-based.

As regards the ***fight against drug-related crime***, Europol noted that the detection and dismantling of illicit synthetic drugs laboratories had been left off the priority list. While the topic is a stand-alone training activity at EU level, in this Report the dismantling of illicit laboratories is addressed under the priority of tackling drug production. Europol also stressed the importance of being familiar with encryption applications, and of acquiring decryption skills, due to the fact that encryption services had emerged as the primary means of communication among criminals involved in large-scale drug trafficking. The decryption skills of law enforcement will be addressed through training related to the horizontal capability gap 'Digital skills and use of new technologies'.

In the area of ***criminal justice***, Eurojust confirmed its commitment to contribute to training delivery covering judicial cooperation, the use of judicial instruments, or other topics related to its operational activities, such as cross-border investigations, joint investigation teams, electronic evidence, casework reports and the Counter-Terrorism Register. Furthermore, Eurojust proposed that, together with its close networks, namely the European Network for investigation and prosecution of genocide, crimes against humanity and war crimes (Genocide Network), the European Judicial Network (EJN), the Network of National Experts on Joint Investigation Teams (JITs Network) and the European Judicial Cybercrime Network (EJCN), it could assist with raising awareness of these courses in order to increase attendance by judicial authorities. In relation to ***criminal proceedings***, FRA brought up the importance of considering procedural rights when referring to fundamental rights in different areas such as cyber-attacks, criminal finances, money laundering, asset recovery and terrorism. This suggestion has been incorporated into this Report since the horizontal aspect of fundamental rights and data protection makes reference to procedural rights.

Frontex pointed out that, although they are relevant to EU wider security, the final list of training priorities contains only a limited number of areas covered by the agency, such as ***integrated border management***. In relation to ***border control and maritime security***, FRA noted that training in this area should cover not only procedural safeguards related to decisions taken at the border but also the treatment of third-country nationals, in particular aspects such as human dignity, right to liberty, right to private and family life, data protection, non-discrimination, the rights of the child, and the right to an effective remedy. Although the Report has already addressed these issues, their importance is further highlighted here.

With regard to ***trafficking in human beings and migrant smuggling***, FRA commented that supporting victims' access to justice could be accentuated, with a special emphasis on women and children. Regarding unaccompanied children/minors, especially third-country nationals in need of special protection and entitled to have a person appointed to assist them throughout the proceedings, FRA highlighted that topics related to guardianship, the rights of the child and the best interests of the child should be integrated into the training curriculum, where applicable.

In terms of ***fundamental rights*** in a wider sense, FRA suggested that CEPOL should also consider developing specific training courses on topics such as victims' rights, illegal hate speech online and violence against women and girls. In relation to the latter, EIGE mentioned that it was exploring the possibility of providing training on cyber violence against women and girls.

In conclusion, it can be stated that this round of consultations has endorsed the list of identified training needs. The vast majority of the additional topics raised by EU training providers have also been included in this Report. Furthermore, the consultation has provided a good overview of the training courses that the agencies are already offering, planning to add to their portfolios or willing to design. Since the implementation of the EU-STNA findings requires a split of tasks among EU-level training providers, the exchange of views and information is absolutely crucial for coordination and for the identification of potential cooperation methods.

5. CONCLUSIONS

The outcomes of the second EU-STNA provide an overview of the core capacity-building needs of European law enforcement officials operating in a continuously evolving environment. While law enforcement has always had to cope with change, the pace of transformation is accelerating, with new challenges arising on every front. Technology is the most rapidly developing area, which is impacting the very foundations of police work and requiring law enforcement to constantly integrate and mobilise digital tools in its operations. At the same time, crime patterns are becoming more complex and criminals are often among the earliest adopters of new technology, as they are continuously piloting, iterating and expanding their methods. This is the paradigm reflected by the findings of the second EU-STNA, which show that, in general, the core capability gaps and the related training needs have remained stable since the previous cycle, and digitalisation has resulted in highly accentuated needs. Furthermore, the COVID-19 pandemic has recently created a range of unforeseen and unprecedented challenges in the context of European security, which are urging law enforcement to be even better prepared for coping with and resolving crisis situations effectively.

Based on the findings of the second EU-STNA, the core capability gaps of law enforcement officials and the related thematic training areas are as follows:

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

Table 3. Core capability gaps and main thematic training areas

21st century law enforcement must be equipped with comprehensive expertise in order to successfully provide quality public safety services to the community. It is only through adequate expert skills and knowledge that law enforcement is able to confront and tackle current challenges in a professional and effective manner and thus there is a need for continuous professional development.

In order to address the training needs expressed by the Member States, the EU should allocate further financial and human resources to EU-level training providers. The resources currently available to CEPOL can ensure the training of 30 000 law enforcement officials per year, while the need is almost four times greater.

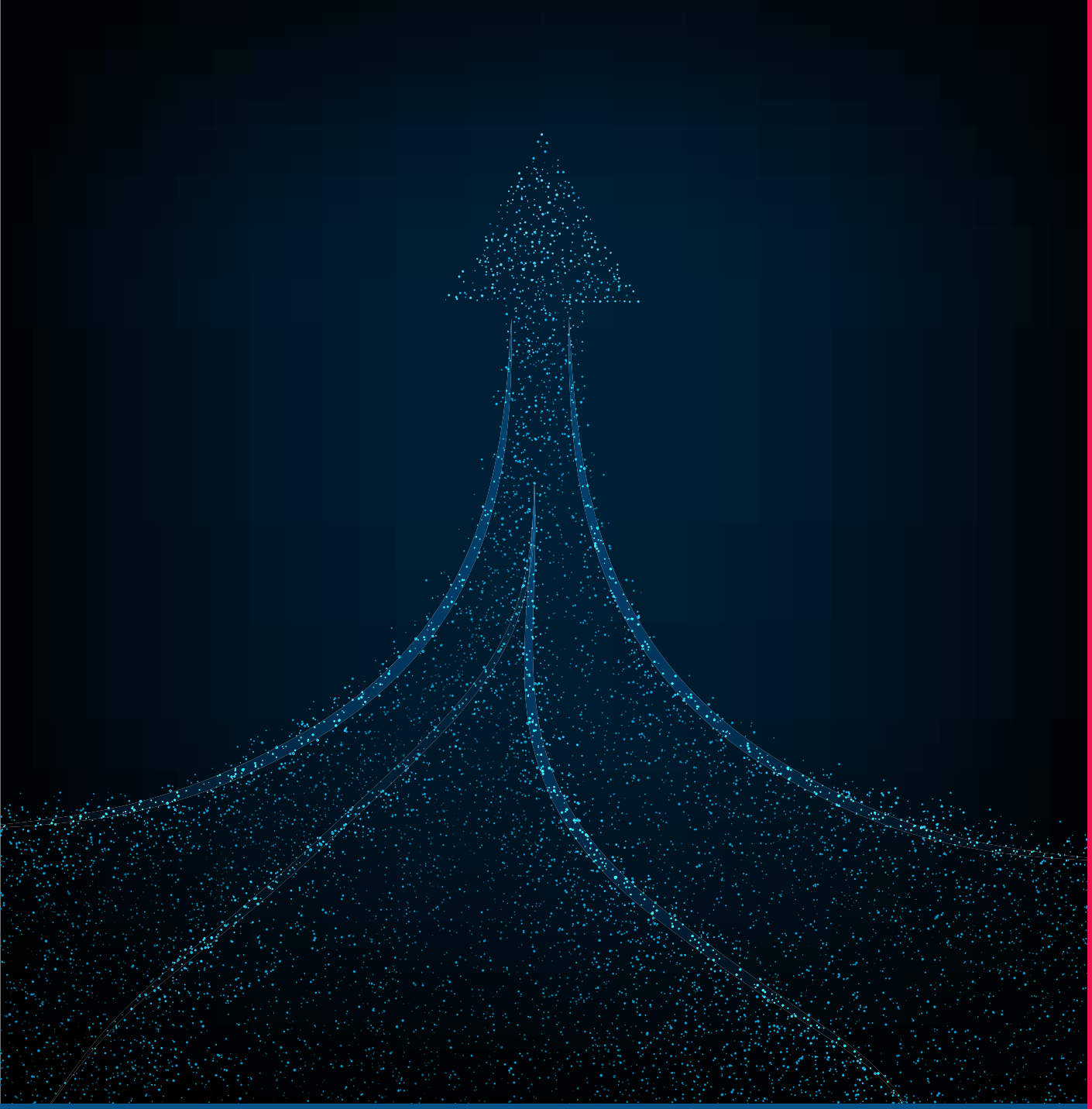
Cross-border multidisciplinary and interdepartmental cooperation and training are key to a successful fight against serious and organised crime and terrorism. The EU-STNA findings suggest a high demand for the joint training of professionals from different backgrounds, particularly in order to further strengthen cooperation along the justice chain, which is vital for the reduction of crime. Involving financial and tax authorities, and prosecution and judiciary staff in joint training as participants or lecturers is considered important. In order to reach the different target groups and bring professionals together, training providers across the EU must step up in terms of joint operations and establish advanced mechanisms for improving cooperation and coordination.

Furthermore, the EU-STNA highlights the importance of deepening cooperation with the private and academic sectors. Public–private partnerships create an opportunity to combine the competencies of multiple actors and generate new solutions and services that are relevant to many areas of law enforcement, especially when it comes to the increased use of the machine simulation of human intelligence processes, e.g. artificial intelligence. In addition, closer cooperation must be actively developed with academia and relevant research institutes in terms of training, research and innovation.

In the light of the increasing interconnection between internal and external security, we must continue to reinforce cooperation with partners outside the EU. The EU-STNA has highlighted the need to train law enforcement officials in non-EU countries and/or invite them to participate in joint training, where relevant and admissible. Education and training for law enforcement, judicial authorities and other relevant agencies contribute to building up trust, common understanding and networks with the Member States' authorities, resulting in intensified cross-border cooperation between the EU and its external partners, and thus a more effective fight against cross-border crime.

Training is available on most of the topics and subtopics identified in this Report without overlaps. New training should be developed in some areas, such as the use of new technology, artificial intelligence, cryptocurrencies, and the emergency response of law enforcement.

Considering the rapid changes in modern-day society, mentioned in this Report several times, training provided to law enforcement officials during the EMPACT 2022-2025 cycle must always focus on the latest criminal trends, techniques and modi operandi as well as on policy, operational and technological developments.



6. WAY FORWARD

The second EU-STNA process has reiterated the ongoing need for training in the area of law enforcement as well as for a coordinated approach taken by the relevant EU-level training providers. Based on the findings, in order to build an efficient and coordinated training portfolio that addresses the threats to EU internal security, the following actions are recommended:

- Coordination and cooperation between EU training providers should be continuously improved. Hence, it is necessary to establish advanced cooperation mechanisms that lead to synergies and coordinated training delivery.

- While Member States have the primary responsibility for delivering awareness training, due to the volume of emerging challenges in the area of law enforcement, this should also be complemented at EU level. Thus, EU training providers will have more tasks relating to delivering awareness training regarding new trends and developments.

- EU training providers, backed up by the policy makers, must be prepared to deliver what is needed to ensure that competency is a foundational principle across European law enforcement.

- In order to fully exploit the comprehensive EU-STNA, which has been found useful as a strategic guideline and lookup tool in efforts to align the planning of law enforcement training and as a baseline for the work programmes of JHA agencies, training providers at EU level should increasingly rely on the EU-STNA findings when designing their training portfolios. Furthermore, the EU-STNA can also benefit national-level training providers, including those engaged in upskilling law enforcement and other professionals who work in fields related to the external dimensions of European internal security.

- Since there is no other designated platform bringing together all EU-level training offerings and self-learning materials for law enforcement practitioners, CEPOL is to continue investing in and promoting its new e-learning platform, LEEd. In addition to offering thematically-grouped training activities, and research and science resources relevant to law enforcement, LEEd facilitates communication between its users.

- In order to obtain the desired training results and make an impact on the ground, it is necessary to continue designing training programmes based on detailed analyses in each particular area, such as the operational-level analyses already conducted by CEPOL and several other EU-level training providers in line with their planning cycles and target groups.

- The EU-STNA, which started as a pilot in 2017 and was evaluated in 2020 in order to assess its impact and review the methodology used, should continue as a regular exercise. Now based on an established but continuously reviewed and improved methodology, it forms the foundation for further training planning, thus contributing in a transparent manner to informing future decisions that benefit the European Union's law enforcement community, and ultimately, the security of the EU. However, to fully utilise the potential of the EU-STNA as guidance for evidence and needs-based law enforcement training at EU level, in line with the recommendations resulting from the external evaluation of the pilot EU-STNA, more political backing and formal approval should be sought at EU level. The endorsement of the EU-STNA Report by the Standing Committee on Operational Cooperation on Internal Security would raise awareness of the purpose and process of the EU-STNA, support more diligent stakeholder input during consultations, and reinforce the importance and further usage of this comprehensive exercise.

This Report will be presented to the European Commission (DG HOME), the Standing Committee on Operational Cooperation on Internal Security and the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), which are invited to provide strategic guidance and set up law enforcement training priorities for 2022-2025.

ANNEXES

Annex 1 List Of Acronyms

@ON	Operational Network to Counter Mafia-style Serious and Organised Crime Groups
ABIS	automated biometric identification system
AI	artificial intelligence
AIRPOL	Law enforcement network of police and border guard units at European airports
ALEFA	Association of Law Enforcement Forensic Accountants
AMON	Anti-Money Laundering Operational Network
API	Advance passenger information
ATLAS	Network of European Special Intervention Units combatting terrorism and violent crime
ATM	automated teller machine
CARIN	Camden Asset Recovery Inter-agency Network
CARPOL	Network of EU law enforcement contact points for tackling cross-border vehicle crime
CBRN	chemical, biological, radiological and nuclear
CEO	chief executive officer
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CIRAM	Common Integrated Risk Analysis Model
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
COSEC	Combatting the Online Sexual Exploitation of Children
COSI	Standing Committee on Operational Cooperation on Internal Security
COVID-19	Coronavirus disease 2019
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
CTI	cyber threat intelligence
DDoS	distributed denial of service
DG Home	European Commission Directorate-General for Migration and Home Affairs
DVI	Disaster Victim Identification
EASO	European Asylum Support Office
EAW	European Arrest Warrant
EC3	European Cybercrime Centre
ECDC	European Centre for Disease Prevention and Control
ECTC	European Counter Terrorism Centre
ECTEG	European Cybercrime Training and Education Group
EEAS	European External Action Service
EFE	European Firearms Experts
EIGE	European Institute for Gender Equality
EIO	European Investigation Order
EJCN	European Judicial Cybercrime Network

EJN	European Judicial Network
EJTN	European Judicial Training Network
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMCS	Excise Movement Control System
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EMPEN	European Medical and Psychological Experts Network for Law Enforcement
ENAA	European Network on the Administrative Approach tackling serious and organised crime
ENFAST	European Network of Fugitive Active Search Teams
ENISA	European Union Agency for Cybersecurity
ENLETS	European Network of Law Enforcement Technology Services
ENPPF	European Network for the Protection of Public Figures
ENVICRIMENET	Network of European law enforcement agencies against environmental crime
EPPO	European Public Prosecutor's Office
ESDC	European Security and Defence College
EU	European Union
EUCARIS	European car and driving licence information system
EUCPN	European Crime Prevention Network
EU CULTNET	Informal network of law enforcement authorities and experts competent in the field of cultural goods
EUIPO	European Union Intellectual Property Office
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	European Asylum Dactyloscopy Database
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EUROSUR	European Border Surveillance System
EU-STNA	European Union Strategic Training Needs Assessment
F-gas	fluorinated greenhouse gas
FIU	financial intelligence unit
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
GPS	global positioning system
HUMINT	human intelligence
ICT	information and communications technology
IOM	International Organization for Migration
IP	internet protocol
IPCAN	Independent Police Complaints Authorities' Network
IPR	intellectual property rights
IT	information technology
J-CAT	Joint Cybercrime Action Taskforce
JHA	Justice and Home Affairs
JIT	joint investigation team

JRC	Joint Research Centre
Kynopol	Police Network for Law Enforcement Dog Professionals
LEEd	Law Enforcement Education Platform
LETS	Law Enforcement Training Scheme
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
LO	liaison officer
MOCG	mobile organised crime group
MSE	experts for Major Sports Events
MTIC	missing trader intra-community
NEC	National EMPACT Coordinator
NFC	near-field communication
NFIP	national football information points
NGO	non-governmental organisation
NPS	new psychoactive substances
OCG	organised crime group
OLAF	European Anti-Fraud Office
OPC	organised property crime
OSINT	open source intelligence
PERCI	EU platform to combat illegal content online
PIU	passenger information unit
PNR	passenger name record
POS	point of sale
RCEG	Radio Communication Expert Group
sBMS	shared biometric matching service
SIENA	Secure Information Exchange Network Application
SIM	subscriber identity module
SIRENE	Supplementary Information Request at the National Entries
SIRIUS	platform for cross-border access to electronic evidence
SIS	Schengen Information System
SKY ECC	end-to-end encrypted messaging application
SOCTA	Serious and Organised Crime Threat Assessment
SPOC	single point of contact
T1	external Union transit procedure
TISPOL	European Traffic Police Network
UAV	unmanned aerial vehicle
UN	United Nations
UV	Ultraviolet
VIP	very important person
VoIP	voice over internet protocol
VPN	virtual private network
Wi-Fi	wireless networking technology

Annex 2 Glossary of terms

EU Strategic Training Needs Assessment (EU-STNA)	Detailed examination and identification, among EU priorities in the area of internal security, of those priorities with a training dimension that should be tackled through training activities at EU level. It results from the practical implementation of the EU-STNA Methodology and its different steps. The question to be answered by the EU-STNA is: What training should be delivered at EU level to address LE capability challenges?
EU-STNA Methodology	The step-by-step process to be followed to assess training-related EU priorities in the area of internal security and its external aspects, in line with the relevant policy cycles.
Security threats and sub-threats	Security threats refer to areas of serious and organised crime and other threat areas (e.g. terrorism) that pose security risks within the EU. Sub-threats refer to the more detailed sub-categories of those threats.
Core capability gaps	1. Tools or activities that, although not necessarily crime as such, are facilitating the commission of various crimes (for example, the use of the darknet, the financing of organised crime or terrorist financing); 2. Aspects relating to the combatting and prevention of crime that are common to various crime areas (for example law enforcement information exchange); 3. Societal challenges, for example migration flows or the use of the internet.
Capability challenge	Deficiencies related to the performance of law enforcement officials, i.e. related to their environment, awareness, knowledge, skills or responsibility and autonomy. – The **environment** is the aggregate of surroundings, conditions or influences. When environmental deficiencies form an obstacle to performance, it is clear that the desired result cannot be obtained by influencing (personal) characteristics of the official. Rather, the conditions in which the official operates are causing the issue. An example of this could be when the technical tools for examining travel documents in order to identify document fraud are missing. – **Awareness** is the knowledge that something exists, or the understanding of a situation or subject at the present time based on information or experience. Awareness is an important element in change management, where it is seen as a prerequisite for change. Recognising a problem, deficiency or expectation can be sufficient for establishing the desired change, without the need for increased knowledge, skills or competences. – **Knowledge** is the result of an interaction between intelligence (capacity to learn) and situation (opportunity to learn), and is therefore more socially-constructed than intelligence alone. Knowledge includes theory and concepts and tacit knowledge gained as a result of the experience of performing certain tasks. Understanding refers to more holistic knowledge of processes and contexts and may be distinguished as know-why, as opposed to know-that. – **Skills** reflect the practical application of knowledge and are measurable through testing and observation. They refer to the proficient manual, verbal or mental manipulation of data or things. Skills can be readily measured by a performance test where the quantity and quality of performance are tested, usually within an established time limit. An example of the proficient manipulation of things is vehicle-operation skills. An example of the proficient manipulation of data or evidence is investigation skills.

Capability challenge	–	**Responsibility and autonomy** refer to the ability of the learner to apply knowledge and skills autonomously and with responsibility. The main difference from skills is that responsibility and autonomy are the capacity to perform, whereas a skill is the actual manipulation of things or data. Acting with responsibility and autonomy implies an ability to demonstrate substantial authority, innovation, autonomy, scholarly and professional integrity and sustained commitment to the development of new ideas or processes in work or study contexts, including research. Examples are problem solving, strategic thinking, coaching and mentoring, etc.
Training	Activities aimed at increasing law enforcement officials' awareness, knowledge, skills, responsibility and autonomy, etc., in order to ensure the correct performance of their tasks.	

Annex 3 List of documents consulted

	AUTHOR	TITLE	DATE
1	Council of the European Union	Artificial Intelligence as an Opportunity for Security in Europe – Follow-up	21/09/2020
2	Council of the European Union	COUNCIL CONCLUSIONS ON CIVILIAN CSDP COMPACT	07/12/2020
3	Council of the European Union	Council Conclusions on Eastern Partnership policy beyond 2020	11/05/2020
4	Council of the European Union	Council Conclusions on Internal Security and European Police Partnership	24/11/2020
5	Council of the European Union	Council conclusions on the New European Research Area	01/12/2020
6	Council of the European Union	COUNCIL DECISION (CFSP) 2020/1515 of 19 October 2020 establishing a European Security and Defence College, and repealing Decision (CFSP) 2016/2382	20/10/2020
7	Council of the European Union	COUNCIL DECISION 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)	12/06/2007
8	Council of the European Union	COUNCIL REGULATION (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen	07/10/2013
9	Council of the European Union	Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")	07/06/2017
10	Council of the European Union	EU Drugs Strategy 2021-2025 (Approved)	18/12/2020
11	Council of the European Union	EU Policy on Training for CSDP	03/04/2017
12	Council of the European Union	PRESS release on VIS	08/12/2020
13	Council of the European Union	REGULATION (EC) No 1987/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System	28/12/2006
14	Council of the European Union	Report on the review of the EU PNR Directive (995420) ADD1	28/07/2020
15	Council of the European Union	The new EU Security Union Strategy	21/09/2020
16	Council of the European Union	Situational Awareness Paper drafted under the auspices of the CCWP (doc. 11234/19 - LIMITE),	24/07/2019
17	European Commission	Meeting on EU Strategy on Organised Crime	10/02/2020
18	EASO	EASO ANNUAL TRAINING REPORT 2019	2019

	AUTHOR	TITLE	DATE
19	EASO	EASO Asylum Report 2020 Annual Report on the Situation of Asylum in the European Union	2020
20	EEAS	Civilian Capability Development Plan 2020 (EEAS(2020)1242)	02/08/2018
21	EEAS	Civilian CSDP Compact (Doc Ref. 14305/18, 19 November 2018)	18/11/2018
22	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES FOR MISSION MANAGEMENT AND STAFF ON GENDER MAINSTREAMING	29/06/2018
23	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON ANTI-CORRUPTION	23/11/2020
24	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON BORDER MANAGEMENT	09/02/2017
25	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON CRIMINAL INVESTIGATION	23/11/2020
26	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON LEGISLATIVE DRAFTING	04/03/2020
27	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON MARITIME SECURITY	09/02/2017
28	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON POLICE-PROSECUTOR COOPERATION	23/11/2020
29	EEAS	CIVILIAN OPERATIONS COMMANDER OPERATIONAL GUIDELINES ON PUBLIC ORDER POLICING (“Crowd and Riot Control”)	09/02/2017
30	EEAS	CivOpsCdr Operational Guidelines for Monitoring, Mentoring and Advising in Civilian CSDP Missions	07/11/2014
31	EEAS	EEAS-Commission services Joint Action Plan (Doc. Ref. SWD(2019) 173, 30 April 2019)	30/04/2019
32	EEAS	Mini concept on border management and maritime security (WK 11845 2020 INIT)	14/05/2020
33	EEAS	Mini concept on cyber security and cyber-crime (still under consultation, EEAS(2020)1084)	01/10/2020
34	EEAS	Mini concept on hybrid threats (still under consultation, WK 11851 2020 INIT)	14/05/2020
35	EEAS	Mini concept on organised crime (EEAS(2019) 617)	29/05/2019
36	EEAS	Mini concept on possible civilian CSDP efforts to address security challenges related to irregular migration (still under consultation, EEAS(2020)1268)	07/10/2020
37	EEAS	Reports on security situation, dialogue and needs of CT/PVE LE Agencies (on a case-by-case basis and if specifically demanded by CEPOL)	n/a
38	EIGE	A guide to risk assessment and risk management of intimate partner violence against women for police	18/11/2019
39	EIGE	Cyber violence against women and girls	13/06/2017
40	EIGE	Estimation of girls at risk of female genital mutilation in the European Union: Step-by-step guide (2nd edition)	11/01/2019
41	EIGE	Estimation of women and girls at risk of FGM	not yet published

	AUTHOR	TITLE	DATE
42	EIGE	Gender-specific measures in anti-trafficking actions: report	17/10/2018
43	EIGE	Indicators on intimate partner violence and rape for the police and justice sectors	24/07/2018
44	EIGE	Intimate partner violence and witness intervention: what are the deciding factors?	12/11/2020
45	EIGE	Police and justice sector data on intimate partner violence against women in the European Union	12/06/2019
46	EIGE	PROTECTING VICTIMS: AN ANALYSIS OF THE ANTI-TRAFFICKING DIRECTIVE FROM THE PERSPECTIVE OF A VICTIM OF GENDER-BASED VIOLENCE	2017
47	EIGE	Recommendations for the EU to improve data collection on intimate partner violence	01/06/2018
48	EIGE	Risk assessment and management of intimate partner violence in the EU	18/11/2019
49	EIGE	Study on the implications of COVID-19 for women victims of intimate partner violence	not yet published
50	EIGE	Understanding intimate partner violence in the EU: the role of data	12/06/2019
51	EMCDDA	EMCDDA SPECIAL REPORT COVID-19 and drugs - Drug supply via darknet markets	05/2020
52	EMCDDA	EU Drug Markets - Impact of COVID-19	05/2020
53	EMCDDA	EU Drug Markets Report 2019	11/2019
54	EMCDDA	EU4MD SPECIAL REPORT - Emerging evidence of Afghanistan's role as a producer and supplier of ephedrine and methamphetamine	11/2020
55	EMCDDA	European Drug Report 2020 - Trends and Developments	09/2020
56	EMCDDA (European Monitoring Centre for Drugs and Drug Addictions)	European Drug Report – Key Issues	22/09/2020
57	EMCDDA (European Monitoring Centre for Drugs and Drug Addictions)	European Drug Report: Trends and Developments 2020	22/09/2020
58	eu-LISA	ANNUAL REPORT ON THE 2019 ACTIVITIES OF EURODAC - FACTSHEET	07/2020
59	eu-LISA	Artificial Intelligence in the Operational Management of Large-scale IT Systems: perspectives for eu-LISA Research and Technology Monitoring Report	07/2020
60	eu-LISA	Distributed Ledger Technologies and Blockchain: Perspectives for eu-LISA and the Large-scale IT Systems Research and Technology Monitoring Report 2019	2019
61	eu-LISA	ECRIS TCN (in development phase) LEAFLET	07/2019
62	eu-LISA	EES (in development phase) LEAFLET	07/2019
63	eu-LISA	ETIAS (in development phase) LEAFLET	07/2019
64	eu-LISA	eu-LISA Consolidated Annual Activity Report 2019	30/06/2020
65	eu-LISA	Eurodac 2019 Annual Report	07/2020

	AUTHOR	TITLE	DATE
66	eu-LISA	Eurodac 2019 statistics	03/2020
67	eu-LISA	Eurodac 2019 statistics - FACTSHEET	03/2020
68	eu-LISA	European Asylum Dactyloscopy Database (Eurodac) LEAFLET	07/2019
69	eu-LISA	Interoperability (in development phase) LEAFLET	07/2019
70	eu-LISA	Report on the technical functioning of central SIS II 2017-2018	10/2019
71	eu-LISA	Report on the technical functioning of the Visa Information System (VIS)	08/2020
72	eu-LISA	Schengen Information System (SIS) LEAFLET	07/2019
73	eu-LISA	SIS II - 2019 ANNUAL STATISTICS FACTSHEET	03/2020
74	eu-LISA	SIS II 2019 Statistics	03/2020
75	eu-LISA	VIS TECHNICAL REPORT 2017-2019 - FACTSHEET	08/2020
76	eu-LISA	Visa Information System (VIS) LEAFLET	07/2019
77	Eurojust	2018 Eurojust Report on Counter-Terrorism	2019
78	Eurojust	2019 Eurojust Report on Counter-Terrorism	2020
79	Eurojust	Annual Report 2017	2018
80	Eurojust	Annual Report 2018	2019
81	Eurojust	Annual Report 2019	2020
82	Eurojust	Case-law by the Court of Justice of the European Union on the European Arrest Warrant	2018
83	Eurojust	Case-law by the Court of Justice of the European Union on the European Arrest Warrant	2020
84	Eurojust	Case-law by the Court of Justice of the European Union on the principle of ne bis in idem in criminal matters	2020
85	Eurojust	Challenges and best practices from Eurojust's casework in the area of cybercrime	2020
86	Eurojust	Conclusions of the 14th Annual Meeting of National Experts on Joint Investigation Teams (JITs)	2019
87	Eurojust	Conclusions of the 23rd meeting of the Genocide Network, 25-27 October 2017	2017
88	Eurojust	Conclusions of the 24th meeting of the Genocide Network, 24-25 May 2018	2018
89	Eurojust	Conclusions of the 25th Meeting of the Genocide Network, 14-15 November 2018	2019
90	Eurojust	Conclusions of the 26th meeting of the Genocide Network, 22-23 May 2019	2019
91	Eurojust	Consolidated Annual Activity Report 2018	2019
92	Eurojust	Consolidated Annual Activity Report 2019	2020
93	Eurojust	Country profile for Finland	2019
94	Eurojust	Cumulative prosecution of foreign terrorist fighters for core international crimes and terrorism-related offences	2020
95	Eurojust	Current situation in judicial cooperation in new psychoactive substance and (pre-)precursor cases	2018
96	Eurojust	Cybercrime Judicial Monitor (Nr. 4, Nr. 5)	2019

	AUTHOR	TITLE	DATE
97	Eurojust	Cybercrime Judicial Monitor issue 5	2020
98	Eurojust	Digest of the European Court of Human Rights jurisprudence on core international crimes	2017
99	Eurojust	Digital Evidence Situation Report	2020
100	Eurojust	EJN Videoconference on COVID-19 measures – Summary of discussions	2020
101	Eurojust	Eurojust and the Western Balkans region	2020
102	Eurojust	Eurojust casework in asset recovery at a glance	2019
103	Eurojust	Eurojust Guidelines for deciding on competing EAWs	2018
104	Eurojust	Eurojust Guidelines for deciding on competing EAWs	01/10/2019
105	Eurojust	Eurojust Meeting on Counter-Terrorism, 19-20 June 2019, Summary of Discussions	2020
106	Eurojust	Eurojust Memorandum on Battlefield Evidence	2020
107	Eurojust	Eurojust Memorandum on Battlefield Evidence	2018
108	Eurojust	Eurojust newsletter	2019
109	Eurojust	Eurojust newsletter (Q1 2019)	2020
110	Eurojust	Eurojust Report on the Criminal Justice Response to Foreign Terrorist Fighters	2018
111	Eurojust	Eurojust Report on the Criminal Justice Response to Foreign Terrorist Fighters	n/a
112	Eurojust	Eurojust Report on Trafficking in Human Beings	23/02/2021
113	Eurojust	Eurojust: The European Union Agency for Criminal Justice Cooperation	2020
114	Eurojust	First report of the observatory function on encryption (joint Europol-Eurojust report)	2019
115	Eurojust	Guidelines for deciding on competing requests for surrender and extradition	2019
116	Eurojust	Guidelines for Joint Investigation Teams	2018
117	Eurojust	Guidelines on Joint Investigation Teams involving third States	2019
118	Eurojust	Joint EE and MT Presidencies – Conclusions of CF meeting of 06-10-2017	2018
119	Eurojust	Joint Eurojust-Europol Annual Report 2017 to the Council of the European Union and the European Commission - PDF document	2018
120	Eurojust	Joint Eurojust–Europol Annual Report 2018	2019
121	Eurojust	Joint Eurojust–Europol Annual Report 2019	2020
122	Eurojust	Joint Note of Eurojust and the European Judicial Network on the practical application of the European Investigation Order	2019
123	Eurojust	Joint report of Eurojust and Europol on Common challenges in combating cybercrime	2019
124	Eurojust	Judicial analysis of trafficking in human beings case-law	2018
125	Eurojust	Note on Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders	2020
126	Eurojust	Outcome report of Eurojust meeting on the European Investigation Order	2018

	AUTHOR	TITLE	DATE
127	Eurojust	Outcome report of the meeting on migrant smuggling	2018
128	Eurojust	Overview of European case-law on the European Arrest Warrant	2018
129	Eurojust	Presidency report of the 5th EU Day Against Impunity for genocide, crimes against humanity and war crimes	2020
130	Eurojust	Prosecuting war crimes of outrage upon personal dignity based on evidence from open sources – Legal framework and recent developments in the Member States of the European Union	2018
131	Eurojust	QUESTIONNAIRE ON THE IMPACT OF THE CJEU JUDGMENTS IN JOINED CASES OG (C-508/18) AND PI (C-82/19 PPU) AND CASE PF (C-509/18)	2019
132	Eurojust	Report of Eurojust's casework experience in the field of prevention and resolution of conflicts of jurisdiction	2018
133	Eurojust	Report on Eurojust's casework in asset recovery	2019
134	Eurojust	Report on Eurojust' s Casework in the field of Asset Recovery, including Freezing and Confiscation	12/02/2019
135	Eurojust	Report on Eurojust's Casework in the field of Asset Recovery, including Freezing and Confiscation	2018
136	Eurojust	Report on Eurojust's Casework in the field of the European Investigation Order	2020
137	Eurojust	Report on Eurojust's Casework on Environmental Crime	2020
138	Eurojust	Report on national legislation and Eurojust casework analysis on sham marriages	2020
139	Eurojust	Report on the functioning of the European Judicial Cybercrime Network	2019
140	Eurojust	Second JIT Evaluation Report	2018
141	Eurojust	Second report of the observatory function on encryption	2020
142	Eurojust	Supporting judicial authorities in the fight against core international crimes	2020
143	Eurojust	Supporting judicial authorities in the fight against terrorism	2019
144	Eurojust	Supporting judicial authorities in the use of joint investigation teams	2020
145	Eurojust	Terrorism Convictions Monitor	2019
146	Eurojust	The impact of COVID-19 on judicial cooperation in criminal matters – Executive summary	2020
147	Eurojust	The principle of Ne Bis in Idem in criminal matters in the case-law of the Court of Justice of the EU	2017
148	Eurojust	The prosecution at national level of sexual and gender-based violence committed by ISIL	2017
149	Eurojust	Third JIT Evaluation Report: Evaluations received between November 2017 and November 2019	2020
150	EUROPEAN COMMISSION	EU Security Union Strategy	24/07/2020
151	EUROPEAN COMMISSION	"REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA"	13/09/2017

	AUTHOR	TITLE	DATE
152	EUROPEAN COMMISSION	2020-2025 EU action plan on firearms trafficking	24/07/2020
153	EUROPEAN COMMISSION	Counter-Terrorism Agenda for the EU	09/12/2020
154	EUROPEAN COMMISSION	A credible enlargement perspective for and enhanced EU engagement with the Western Balkans	06/02/2018
155	EUROPEAN COMMISSION	A European strategy for data	19/02/2020
156	EUROPEAN COMMISSION	A Union of equality: EU anti-racism action plan 2020-2025	18/09/2020
157	EUROPEAN COMMISSION	A Union of Equality: Gender Equality Strategy 2020-2025	05/03/2020
158	EUROPEAN COMMISSION	Accompanying the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND TO THE COUNCIL Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims	20/10/2020
159	EUROPEAN COMMISSION	Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing	07/05/2020
160	EUROPEAN COMMISSION	Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818	23/09/2020
161	EUROPEAN COMMISSION	ANNEX New Pact on Migration and Asylum	23/09/2020
162	EUROPEAN COMMISSION	ANNEX to the Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818	23/09/2020
163	EUROPEAN COMMISSION	ANNEX to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL introducing a screening of third country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817	23/09/2020
164	EUROPEAN COMMISSION	ANNEXES 1-4 to the 2020-2025 EU action plan on firearms trafficking	24/07/2020

	AUTHOR	TITLE	DATE
165	EUROPEAN COMMISSION	ANNEXES to Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund]	23/09/2020
166	EUROPEAN COMMISSION	COMMISSION IMPLEMENTING DECISION (EU) 2017/1528 of 31 August 2017 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II)	07/09/2017
167	EUROPEAN COMMISSION	Commission Recommendation – Cybersecurity of 5G networks	29/03/2019
168	EUROPEAN COMMISSION	COMMISSION RECOMMENDATION of 23.9.2020 on an EU mechanism for Preparedness and Management of Crises related to Migration (Migration Preparedness and Crisis Blueprint)	23/09/2020
169	EUROPEAN COMMISSION	COMMISSION RECOMMENDATION of 23.9.2020 on cooperation among Member States concerning operations carried out by vessels owned or operated by private entities for the purpose of search and rescue activities	23/09/2020
170	EUROPEAN COMMISSION	COMMISSION RECOMMENDATION of 23.9.2020 on legal pathways to protection in the EU: promoting resettlement, humanitarian admission and other complementary pathways	23/09/2020
171	EUROPEAN COMMISSION	COMMISSION STAFF WORKING DOCUMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU)XXX/XXX [Asylum and Migration Fund]	23/09/2020
172	EUROPEAN COMMISSION	COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL	20/12/2017
173	EUROPEAN COMMISSION	COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL SECOND REPORT UNDER THE VISA SUSPENSION MECHANISM	19/12/2018
174	EUROPEAN COMMISSION	COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL THIRD REPORT UNDER THE VISA SUSPENSION MECHANISM	10/07/2020
175	EUROPEAN COMMISSION	COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation	09/12/2020
176	EUROPEAN COMMISSION	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation	09/12/2020
177	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION Guidance on the implementation of EU rules on definition and prevention of the facilitation of unauthorised entry, transit and residence	23/09/2020

	AUTHOR	TITLE	DATE
178	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL First Progress Report on the EU Security Union Strategy	09/12/2020
179	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL First Progress Report on the EU Security Union Strategy	09/12/2020
180	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL First Progress Report on the EU Security Union Strategy	09/12/2020
181	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2020 Communication on EU enlargement policy	06/10/2020
182	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Commission Work Programme 2021 A Union of vitality in a world of fragility	19/10/2020
183	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Enhancing the accession process – A credible EU perspective for the Western Balkans	05/02/2020
184	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union	20/04/2016
185	EUROPEAN COMMISSION	Communication on Secure 5G deployment in the EU – Implementing the EU toolbox	29/01/2020
186	EUROPEAN COMMISSION	Communication on the Global EU response to COVID-19	08/04/2020
187	EUROPEAN COMMISSION	Contribution submitted in July 2020 by COM (HOME.D5) to Europol in the framework of the data collection exercise for the upcoming EU SOCTA 2021.	n/a
188	EUROPEAN COMMISSION	Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – 2 years of application of the General Data Protection Regulation	24/06/2020
189	EUROPEAN COMMISSION	EMN Inform on Missing Unaccompanied Minors – April 2020	08/04/2020
190	EUROPEAN COMMISSION	Establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU	23/09/2020
191	EUROPEAN COMMISSION	EU Agenda and Action Plan on Drugs 2021-2025	24/07/2020
192	EUROPEAN COMMISSION	EU Agenda and Action Plan on Drugs 2021-2025 ADD 1	24/07/2020
193	EUROPEAN COMMISSION	EU Agenda to tackle Organised Crime 2021-2025, 10 February 2021, Enhancing Law Enforcement Capacity in the area of Digital Investigations	10/02/2020
194	EUROPEAN COMMISSION	EU mechanism for Preparedness and Management of Crises related to Migration (Migration Preparedness and Crisis Blueprint)	23/09/2020
195	EUROPEAN COMMISSION	EU strategy for a more effective fight against child sexual abuse	24/07/2020

	AUTHOR	TITLE	DATE
196	EUROPEAN COMMISSION	EU Strategy on victims' rights (2020-2025)	24/06/2020
197	EUROPEAN COMMISSION	EUROPEAN COMMISSION HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY Brussels, 18.3.2020 JOIN(2020) 7 final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Eastern Partnership policy beyond 2020 Reinforcing Resilience – an Eastern Partnership that delivers for all	18/03/2020
198	EUROPEAN COMMISSION	Evaluation of EU Drug Strategy 2013-2020 and EU Action Plan on Drugs 2017-2020	24/07/2020
199	EUROPEAN COMMISSION	EXECUTIVE SUMMARY OF THE EVALUATION of the EU Drugs Strategy 2013-2020 and the EU Action Plan on Drugs 2017-2020	27/07/2020
200	EUROPEAN COMMISSION	Factsheet: 20 Deliverables for 2020: Bringing tangible results for citizens	11/2020
201	EUROPEAN COMMISSION	Factsheet: A EUROPE THAT PROTECTS EU Crisis Protocol: responding to terrorist content online	07/10/2019
202	EUROPEAN COMMISSION	Factsheet: Countering illegal hate speech online 5th evaluation of the Code of Conduct	22/06/2020
203	EUROPEAN COMMISSION	Factsheet: THE EU AND ITS NEIGHBOURS: Tackling Security Challenges Together	11/2020
204	EUROPEAN COMMISSION	Increasing resilience and bolstering capabilities to address hybrid threats	13/06/2018
205	EUROPEAN COMMISSION	Joint Action Plan on Counter-Terrorism for the Western Balkans	10/05/2018
206	EUROPEAN COMMISSION	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU's Cybersecurity Strategy for the Digital Decade	16/12/2020
207	EUROPEAN COMMISSION	Joint Framework on countering hybrid threats - a European Union response	06/04/2016
208	EUROPEAN COMMISSION	Judicial training strategy 2021-2024	02/12/2020
209	EUROPEAN COMMISSION	Mapping of measures related to enhancing resilience and countering hybrid threats	24/07/2020
210	EUROPEAN COMMISSION	New Pact on Migration and Asylum	23/09/2020
211	EUROPEAN COMMISSION	Orientations towards the first Strategic Plan for Horizon Europe	12/2019
212	EUROPEAN COMMISSION	Progress report on the Implementation of the European Agenda on Migration	16/10/2019
213	EUROPEAN COMMISSION	PROPOSAL FOR A COUNCIL REGULATION amending Regulation (EC) No 168/2007 establishing a European Union Agency for Fundamental Rights	05/06/2020

	AUTHOR	TITLE	DATE
214	EUROPEAN COMMISSION	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL addressing situations of crisis and force majeure in the field of migration and asylum	23/09/2020
215	EUROPEAN COMMISSION	PROPOSAL for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation	09/12/2020
216	EUROPEAN COMMISSION	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL introducing a screening of third country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817	23/09/2020
217	EUROPEAN COMMISSION	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund]	23/09/2020
218	EUROPEAN COMMISSION	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online	12/09/2018
219	EUROPEAN COMMISSION	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters	17/04/2018
220	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography	16/12/2016
221	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography	16/12/2016
222	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL First Report under the Visa Suspension Mechanism	20/12/2017
223	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL On the review of Directive 2016/681 on the use of passenger name record (PNR) data	24/07/2020
224	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL SECOND REPORT UNDER THE VISA SUSPENSION MECHANISM	19/12/2018
225	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims	20/10/2020
226	EUROPEAN COMMISSION	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL THIRD REPORT UNDER THE VISA SUSPENSION MECHANISM	10/07/2020
227	EUROPEAN COMMISSION	Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims	03/12/2018
228	EUROPEAN COMMISSION	Shaping Europe's digital future	19/02/2020

	AUTHOR	TITLE	DATE
229	EUROPEAN COMMISSION	Study on Data collection on trafficking in human beings in the EU	09/2020
230	EUROPEAN COMMISSION	Study on reviewing the functioning of Member States' National and Transnational Referral Mechanisms	16/10/2020
231	EUROPEAN COMMISSION	Study on the economic, social and human costs of trafficking in human beings	09/2020
232	EUROPEAN COMMISSION	The European Agenda on Security	28/04/2015
233	EUROPEAN COMMISSION	The protection of children in migration	12/04/2017
234	EUROPEAN COMMISSION	Third progress report factsheet	10/2020
235	EUROPEAN COMMISSION	Western Balkans: An Economic and Investment Plan to support the economic recovery and convergence	06/10/2020
236	EUROPEAN COMMISSION	WHITE PAPER On Artificial Intelligence – A European approach to excellence and trust	19/02/2020
237	EUROPEAN COMMISSION STAFF WORKING DOCUMENT	Implementation of Home Affairs legislation in the field of internal security – 2017-2020/Part 1.	09/07/2020
238	EUROPEAN COMMISSION STAFF WORKING DOCUMENT	Implementation of Home Affairs legislation in the field of internal security – 2017-2020/Part 2.	09/07/2020
239	EUROPEAN COMMISSION	Amendment to Commission Implementing Decision (EU) 2017/1528 (SIRENE Manual) – draft (to be adopted Q1 2021)	n/a
240	EUROPEAN COMMISSION	Commission Implementing Decision laying down the technical rules necessary for entering, updating, deleting and searching data in SIS and other implementing measures in the field of police cooperation/ borders – draft (to be adopted in 2021)	n/a
241	EUROPEAN COMMISSION	Commission Implementing Decision on laying down rules as regards the minimum data quality standards and technical specifications for entering photographs, DNA profiles and dactyloscopic data in the SIS in the field of police/borders – draft (to be adopted in 2021)	13/01/2021
242	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy to Tackle Organised Crime 2021-2025	14/04/2021
243	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025	14/04/2021
244	EUROPEAN COMMISSION	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience	25/11/2020
245	EUROPEAN COMMISSION	EU Child Rights Strategy	n/a
246	EUROPEAN COMMISSION	Final report of the evaluation study on the EU Policy Cycle for organised and serious international crime/EMPACT 2018-2021	19/10/2020

	AUTHOR	TITLE	DATE
247	EUROPEAN COMMISSION	New Commission Implementing Decision – New SIRENE Manual (Police and Borders) – draft (to be adopted in 2021)	n/a
248	EUROPEAN COMMISSION	SIRENE Handbook – (to be drafted in 2021)	n/a
249	EUROPEAN COMMISSION	The operational action plans for the 2 drug priorities	n/a
250	EUROPEAN COMMISSION	The soon-to-be-adopted Work Programme on Civil Security for Society Cluster of Horizon Europe for period 2021-2022,	15/06/2021
251	Council of the European Union	Draft Council conclusion on possible continuation	14/01/2021
252	Council of the European Union	Draft timeline – EMPACT 2022-2025	14/01/2021
253	European Parliament	The fight against terrorism	6/2019
254	European Parliament Council of the European Union	DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime	04/05/2016
255	European Parliament Council of the European Union	DIRECTIVE (EU) 2019/713 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA	10/05/2019
256	European Parliament Council of the European Union	Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography	13/12/2011
257	European Parliament Council of the European Union	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems	12/08/2013
258	European Parliament Council of the European Union	REGULATION (EU) 2017/371 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 1 March 2017 amending Council Regulation (EC) No 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (revision of the suspension mechanism)	08/03/2017
259	European Parliament Council of the European Union	REGULATION (EU) 2018/1860 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals	07/12/2018
260	European Parliament Council of the European Union	REGULATION (EU) 2018/1861 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006	07/12/2018
261	European Parliament Council of the European Union	REGULATION (EU) 2018/1862 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU	07/12/2018

	AUTHOR	TITLE	DATE
262	European Parliament Council of the European Union	REGULATION (EU) 2019/1896 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624	14/11/2019
263	ENISA	ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends	01/01/2019
264	EUROPOL	A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism	12/07/2019
265	EUROPOL	Beyond the pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU	30/04/2020
266	Europol	European Union Serious and Organised Crime Assessment A corrupting influence: the infiltration and undermining of Europe`s economy and society by organised crime	2021
267	Europol	EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT Crime in the age of technology 2017	2017
268	Europol	EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2020	2020
269	EUROPOL	Europol's preliminary input to the EU Commission meeting on the Organised Crime Agenda	n/a
270	Europol	INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020	2020
271	EUROPOL	Malicious Uses and Abuses of Artificial Intelligence	19/11/2020
272	EUROPOL	EU Serious and Organised Crime Threat Assessment (EU SOCTA), to be published in March 2021	12/04/2021
273	FRA	OVERVIEW OF ANTISEMITIC INCIDENTS RECORDED IN THE EUROPEAN UNION 2009–2019	10/09/2020
274	FRA	Your rights matter: Security concerns and experiences	22/07/2020
275	FRA	Antisemitism: Overview of antisemitic incidents recorded in the European Union 2009-2019	10/09/2020
276	FRA	Children's rights and justice Minimum age requirements in the EU	23/04/2018
277	FRA	Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 3	30/06/2020
278	FRA	Criminal detention conditions in the European Union: rules and reality	12/12/2019
279	FRA	Experiences and perceptions of antisemitism Second survey on discrimination and hate crime against Jews in the EU – Summary	10/09/2019
280	FRA	Experiences and perceptions of antisemitism Second survey on discrimination and hate crime against Jews in the EU	10/12/2018
281	FRA	Fundamental Rights Report 2019	06/06/2019
282	FRA	Handbook on European law relating to access to justice	23/09/2019
283	FRA	Handbook on European non-discrimination law – 2018 edition	21/03/2018
284	FRA	Hate crime recording and data collection practice across the EU	21/06/2018
285	FRA	Integration of young refugees in the EU: good practices and challenges	19/11/2019
286	FRA	Justice for victims of violent crime Sanctions that do justice Part III	24/04/2019
287	FRA	Proceedings that do justice Justice for victims of violent crime Part II	24/04/2019
288	FRA	Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications	12/02/2019

	AUTHOR	TITLE	DATE
289	FRA	Protecting migrant workers from exploitation in the EU: boosting workplace inspections	22/08/2018
290	FRA	Protecting migrant workers from exploitation in the EU: boosting workplace inspections Annex 1: Institutional set up (monitoring) for combating labour exploitation at national level	22/08/2018
291	FRA	Protecting migrant workers from exploitation in the EU: boosting workplace inspections Annex 2: Risk management systems to detect labour exploitation at national level	22/08/2019
292	FRA	Relocating unaccompanied children: applying good practices to future schemes	11/05/2020
293	FRA	Rights in practice: access to a lawyer and procedural rights in criminal and European arrest warrant proceedings	13/09/2019
294	FRA	Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union – Volume II	09/05/2018
295	FRA	Victims' rights as standards of criminal justice Justice for victims of violent crime Part I	25/04/2019
296	FRA	Women as victims of partner violence Justice for victims of violent crime Part IV	24/04/2019
297	FRA	YOUR RIGHTS MATTER: SECURITY CONCERNS AND EXPERIENCES Fundamental rights survey	2020
298	FRONTEX	Risk Analysis for 2020	2020
299	FRONTEX	Vulnerability Assessment Main Vulnerabilities Related to Training for Border Control Briefing Note	2020
300	IOM (International Organization for Migration)	World Migration report	2020
301	LIBE	A comprehensive Union policy on preventing money laundering and terrorist financing	2020
302	LIBE	Anti-racism protests following the death of George Floyd (2020/2685(RSP)	2020
303	LIBE	Combating sexual harassment and abuse in the EU (2017/2897(RSP))	2017
304	LIBE	Cutting the sources of income for jihadists – targeting the financing of terrorism (2017/2203(INI)), Rapporteur ALDE NART Javier	2017
305	LIBE	DRAFT REPORT on the implementation of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims (2020/2029(INI))	2020
306	LIBE	DRAFT REPORT on the implementation of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (2015/2129(INI))	2017
307	LIBE	EU accession to the Istanbul Convention and other measures to combat gender-based violence (2019/2855(RSP)	2019
308	LIBE	Findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)) Rapporteurs: HOHLMEIER Monika, STEVENS Helga	2018

	AUTHOR	TITLE	DATE
309	LIBE	Motion for resolution on the EU Security Union Strategy (2020/2791(RSP)) (scheduled for plenary adoption in December 2020)	2020
310	LIBE	Report on financial crimes, tax evasion and tax avoidance (2018/2121(INI)) Rapporteurs NIEDERMAYER Luděk, KOFOD Jeppe	2018
311	LIBE	Rise of neo-fascist violence in Europe (2018/2869)(RSP))	2018
312	LIBE	Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP))	2019
313	LIBE	Situation of rule of law and fight against corruption in the EU, specifically in Malta and Slovakia (2018/2965(RSP)	2018
314	LIBE	State of implementation of the Union's anti-money laundering legislation (2019/2820(RSP)	2019
315	LIBE	The Cum Ex Scandal: financial crime and the loopholes in the current legal framework (2018/2900(RSP))	2018
316	LIBE	Zero Tolerance for female genital mutilation (2017/2936(RSP))	2017

Annex 4 Law enforcement groups contributing to EU-STNA

(In alphabetical order)

EMPACT groups 2018-2021

1. Cannabis, Cocaine and Heroin
2. Criminal Finances, Money Laundering and Facilitated Asset Recovery
3. Cybercrime – Attacks against Information Systems
4. Cybercrime – Child Sexual Abuse and Child Sexual Exploitation
5. Cybercrime – Fraud and Counterfeiting of Non-cash Means of Payment
6. Document Fraud
7. Environmental Crime
8. Excise Fraud
9. Facilitation of Illegal Immigration
10. Illicit Firearms Tracking
11. Missing Trader Intra-Community Fraud
12. Organised Property Crime
13. Synthetic Drugs, New Psychoactive Substances
14. Trafficking in Human Beings

Other thematic Expert Groups convened

1. Border Management and Maritime Security
2. CEPOL Knowledge Centre on Counter Terrorism
3. Crime Prevention
4. External Dimensions of European Security
5. Forensics
6. CEPOL Expert Group on Fundamental Rights
7. CEPOL Knowledge Centre on Law Enforcement Cooperation, Information Exchange and Interoperability

Summary table of expert consultations

FORMAT	NUMBER	DATE	NUMBER OF INDIVIDUALS/ ORGANISATIONS REPRESENTED	NUMBER OF COUNTRIES REPRESENTED
Online focus group meetings	20	March-May 2021	225	27
Written consultation with professional groups	1	April-May 2021	24	n/a
Written consultation with National EMPACT Coordinators	1	May-June 2021	n/a	27

Annex 5 Other professional groups/networks consulted

(In alphabetical order)

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

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

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
Cyber-attacks		
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	CEPOL ECTEG
2	Latest challenges for dealing with encryption, anonymisation and bullet-proof hosting services	CEPOL
3	Identifying, handling, securing, preserving, analysing and exchanging e-evidence	CEPOL EJTN
4	Combatting crime-as-a-service used by criminals and criminal groups in illegal activities	CEPOL Europol EC3
5	Effective international cooperation	CEPOL Europol Eurojust[2] CEPOL (to non-EU countries) eu-LISA
6	Protocols to tackle large-scale cyber-attacks	n/a
7	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	Europol EC3
8	Big data analysis	n/a
9	Blockchain analysis	CEPOL
10	Using artificial intelligence, machine learning and deep learning in cyber-crime investigation	n/a
11	Cybercriminal profiling and motivation analysis	n/a
12	Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection	CEPOL EUCPN
Criminal finances, money laundering and asset recovery (Fraud, economic and financial crimes)		
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 via normal financial system (electronic), offshore challenge to conceal beneficial ownership, informal value transfer systems (e.g. hawala), underground banking, international money laundering bolstered by fictitious contracts and invoices, bitcoin trading, 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)	CEPOL CCA[3] EPPO

(2) SIRIUS E-Evidence Series developed by Europol and Eurojust and integrated in LEEd by CEPOL

(3) for CEO Fraud and ML as a service

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
2	Tracking, tracing, freezing and confiscating assets, opportunities to hide assets quickly, intelligence on criminal turnovers and profits, including training for judicial investigators; automatic launch of financial investigations; pre-seizure planning; importance of interlocutory sales	CEPOL EPPO
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; automatic launch of financial investigations; pre-seizure planning; importance of interlocutory sales; management of confiscated assets and social reuse of criminal assets	CEPOL EPPO EJTN
4	Technicalities and information priorities, technical aspects of investigation, modern technologies, use of AI, big data analysis and OSINT, technicality of virtual coins (seizures)	CEPOL
5	Training on cryptocurrencies for general investigators	CEPOL
6	Institutional training addressing a new landscape: implementation of EPPO Regulation, roles of EPPO, OLAF, Europol, Eurojust, European Judicial Cybercrime Network (EJCN) and national authorities. EU directives, tools available at Member State and EU level	CEPOL EPPO EJTN
7	Financial analysis methods and financial forensics	CEPOL EPPO
8	Investigation of crime enablers, lawyers, financial service providers and real estate agents who knowingly and wittingly provide services to facilitate criminal financial flows	CEPOL
9	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)	CEPOL EPPO
10	Roles of financial institutions in anti-money laundering, public–private partnership; roles of Fundamental Rights Agency, European Court of Justice and European Court of Human Rights in anti-money laundering; case studies on fundamental rights and data protection issues in criminal investigations	CEPOL EPPO EJTN
11	Roles of the police, tax and customs agencies and the financial sector in prevention/control mechanisms	CEPOL EPPO
12	Fundamental rights and data protection	CEPOL EPPO
Counter-terrorism		
1	Radicalisation: preventing and countering radicalisation that leads to violent extremism and terrorism; new forms of radicalisation; fundamental rights and data protection, including non-discrimination	CEPOL Europol EJTN
2	Use of OSINT in counter-terrorism; value of digital evidence; methods of lawful interception	CEPOL (TC) Europol

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
3	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.	CEPOL (to non-EU countries) Europol
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	Europol
5	Foreign terrorist fighters, travelling terrorists and returnees; law enforcement approach to family members of foreign terrorist fighters	CEPOL (to non-EU countries) Europol
6	Use of information systems and cooperation mechanisms in the fight against terrorism	eu-LISA Europol
7	Protection of public spaces and resilience of critical entities; sharing best practices on handling attacks	CEPOL (to non-EU countries) EU COMMISSION (JRC/HOME D.2)
8	Regional and cross-border cooperation on specific terrorism cases	CEPOL (to non-EU countries)
9	Unmanned aerial vehicles: threats and opportunities for law enforcement	EU COMMISSION (DG HOME D.2)
10	Use of AI by law enforcement	Europol
11	Tackling document fraud	CEPOL (to non-EU countries)
Trafficking in human beings		
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	CEPOL EUCPN Europol Frontex EJTN
2	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	Europol Frontex
3	Trafficking for sexual exploitation: modus operandi including online; detection, victim identification, safeguards, support and referral, with a focus on women and children	EASO Europol Frontex
4	Investigations on the increasing use of digital technology at different stages of trafficking, particularly on encrypted communication and moving assets	CEPOL Europol
5	Child trafficking	EASO Europol Frontex
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	CEPOL EASO Europol Frontex
7	Links to criminal finances and money laundering; financial investigations: tracing, seizing and confiscating criminal proceeds, asset recovery.	Europol EJTN
8	Use of existing information and cooperation channels (e.g. Europol, Interpol); how to start a JIT; use of large-scale IT systems	Europol

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
9	International cooperation with the UN and IOM, cooperation with non-EU countries, cooperation with NGOs/institutions providing victim support; referral of victims	Europol
10	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	CEPOL EASO Europol EJTN
11	Prevention of human trafficking	EUCPN Europol Frontex
12	Detection of criminal forms of labour exploitation in workplaces	Europol
13	Forensics	Europol
Drug trafficking		
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	CEPOL EMCDDA EUCPN Europol
2	Investigation: use of digital investigation tools, OSINT, darknet, decryption, AI, social networks, operational intelligence analysis; training of first responders on synthetic opioid poisoning	CEPOL
3	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)	Europol
4	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; changing behavioural trends regarding drug supply and consumption	CEPOL EMCDDA
5	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	CEPOL
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	CEPOL EMCDDA
7	Law enforcement cooperation: global tools for drug monitoring linked to international cooperation, cooperation with non-EU countries	CEPOL Europol
8	Legal challenges and solutions in prosecuting cases related to drugs, precursors and NPS	CEPOL
9	Tackling document fraud, including mislabelling of (pre-)precursors and NPS	CEPOL Europol
10	Forensics	CEPOL
11	General aviation: definition and legal framework, types of aircraft and characteristics, flight basics, API and PNR, and available monitoring tools	n/a
12	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	EMCDDA
13	Fundamental rights and data protection	CEPOL

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
Migrant smuggling		
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	CEPOL Europol
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	CEPOL Europol
3	Understanding the operation of organised crime groups	CEPOL Europol
4	Information exchange: European Asylum Dactyloscopy Database (Eurodac), SIS II, role of large-scale IT systems in combatting migrant smuggling under the EMPACT framework	CEPOL eu-LISA Europol
5	Improving knowledge on financial models including hawala and money service bureaux, cryptocurrencies, financial investigations and asset recovery	CEPOL Europol
6	Nexus between migrant smuggling and trafficking in human beings: exploitation of migrants after arrival in the EU	Europol
7	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.)	CEPOL Europol
8	Document and identity fraud with a focus on visa fraud and forged supporting documents; biometrics; networking and support	CEPOL Europol Frontex
9	EU cooperation tools and mechanisms, JITs; cooperation between administrative and law enforcement units and the judicial sector (prosecutors, lawyers and judges)	CEPOL Eurojust Europol EJTN
10	Dealing with requests concerning unaccompanied minors	CEPOL EASO Europol Frontex
11	Detecting secondary movements	CEPOL Europol
12	Procedures and tools used in migration crisis situations	CEPOL Europol Frontex
13	Fundamental rights, including access to international protection, non-discrimination and data protection	CEPOL Europol EASO Frontex
Child sexual exploitation		
1	Identifying victims of sexual abuse and exploitation, analysis of big data, images and videos for victim identification purposes; detecting child abuse material	CEPOL Europol
2	Investigation: detecting child abuse material; use of new forensic tools; online undercover operations	CEPOL (to non-EU countries)
3	Use of OSINT and the dark web	CEPOL

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
4	Developing and applying innovative investigation methods	n/a
5	Handling encryption and anonymisation services in online child sexual abuse (VPNs, proxy servers, Tor)	n/a
6	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	Eurojust Europol
7	Financial investigations related to child sexual exploitation cases (online payment methods including virtual currencies)	Europol
8	Identification of high-risk criminal networks involved in child sexual abuse and exploitation	Europol
9	Tackling gender-related cyber violence against women and girls	CEPOL (planned) EIGE (planned) EUCPN
10	Tools and techniques for mental health/psychological support for law enforcement officers dealing with child abuse	CEPOL
11	Victims' rights, offenders' rights, suspects' rights	CEPOL
12	International offender management	CEPOL
Online fraud schemes (Fraud, economic and financial crimes)		
1	Card-not-present fraud: compromise online payments, e-skimming, mobile banking fraud, online payment requests, SIM swapping, smishing, phishing and vishing, e-commerce fraud, carding platforms and darknet marketplaces	CEPOL
2	Cyber scams: online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud, mimic and voice fraud, helpdesk fraud, social engineering	CEPOL
3	Cybercrime facilitators: cryptocurrencies, encryption, anonymisation, online forgery, new online tools and digital techniques, use of deepfakes created with AI, money muling	CEPOL
4	Card-present fraud: skimming, contactless card fraud, mobile payment fraud	CEPOL
5	Cyber threat intelligence, dark web and OSINT	CEPOL
6	Intrusions into system networks of financial institutions: banking malware/POS malware, logical attacks against ATMs, use of malware to intercept login details for online banking services	CEPOL
7	International law enforcement cooperation, public–private partnership, inter-agency cooperation (cooperation with financial institutions, internet service providers and online platforms)	CEPOL (to non-EU countries)
8	Information exchange and cross-border exchange of evidence	CEPOL
9	Legal challenges in non-cash payment methods	CEPOL
10	High-risk criminal networks	n/a
11	Crime prevention	EUCPN
12	Fundamental rights and data protection	n/a
Organised property crime		
1	Organised burglaries, robberies and thefts and new trends in modus operandi	CEPOL EUCPN
2	International investigation, operational cooperation, cross-border observation, best practices, joint investigation teams; communication channels used by criminals (e.g. SKY ECC)	EUCPN
3	Criminal networks, OCGs, MOCGs, clans and different roles of members	CEPOL

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
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	n/a
5	Tackling trafficking in cultural goods (police, border guards and customs)	n/a
6	Financial investigation and asset recovery related to organised property crime cases	n/a
7	Tackling theft and attacks on ATMs	CEPOL EUCPN
8	OSINT focused on organised property crime	n/a
9	Fencing, online activities, processes, networks and routes used for stolen goods	n/a
10	Capacity building among cultural heritage experts, including a network of experts that Member States could use within the EMPACT framework	n/a
11	Forensics	n/a
12	Prevention: using the European barrier model for organised property crime; administrative approach	ENAA
13	Tackling document fraud	n/a
14	Fundamental rights and data protection	CEPOL
Border management and maritime security		
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	Europol Frontex
2	EU-level intelligence analysis and information exchange systems	Europol eu-LISA Frontex
3	Common as well as new digitalisation practices (three dimensions: border security, information exchange and humanitarianism)	Europol
4	Document fraud detection at border crossing points	Europol Frontex
5	Cross-border criminal networks	Europol
6	Border management in non-EU countries with shared external borders; experience sharing with CSDP missions mandated with border management aspects	Europol
7	Dignified treatment of persons at the border in compliance with principles of non-discrimination, right to liberty, respect for privacy and use of force	CEPOL EASO Europol Frontex
8	Communication and language skills needed for interactions with those crossing the border	EASO Europol
9	Cooperation with Member States and training academies	Europol Frontex
10	Screening and debriefing	Europol Frontex
11	Access to international protection, prohibition of refoulement, prohibition of collective expulsion and push-backs	EASO Europol

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
12	Procedural safeguards related to decisions taken at the border	CEPOL EASO Europol Frontex
13	Improving capacity to implement coast guard functions	Europol Frontex
Firearms trafficking		
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	CEPOL Frontex
2	Illicit trafficking in firearms linked to organised crime and terrorism; supplying OCGs with firearms and ammunition from an illegal market	CEPOL
3	Online aspects of firearms trafficking: OSINT, dark web, open web, other communication platforms, etc.	CEPOL
4	Financial investigations related to firearms trafficking	n/a
5	Cooperation with Member States, non-EU countries, international organisations and the private sector	CEPOL eu-LISA
6	Firearms forensics: use of ABIS and different systems, forensic evidence	n/a
7	Raising awareness of the firearms threat and initiatives to counter illicit firearms production and trafficking; national and international firearms legislation	n/a
8	HUMINT management in illicit firearms related crime	n/a
9	Best practices for prevention campaigns	EUCPN
10	Fundamental rights and data protection	n/a
Missing trader intra-community fraud (Fraud, economic and financial crimes)		
1	Modus operandi: organised crime groups specialised in offering fake invoices; financial flows and schemes used for MTIC fraud; exploitation of legal structures, versatility, adaptability to new trends and specialised advising	CEPOL EPPO
2	Investigation: intelligence-led investigation focusing on transnational organised crime; operational cooperation; sharing best practices	CEPOL EPPO
3	Financial investigations to detect money laundering	CEPOL EPPO
4	Technology and digital infrastructure as essential components in concealing and facilitating criminal activities (data storage, alternative payment methods, VPN services, encryption, VoIP fraud)	EPPO
5	Links to other crime areas	CEPOL EPPO
6	Tax confidentiality issues at EU level in the context of information exchange	EPPO
7	Raising awareness of MTIC fraud among the judiciary and the public	EPPO
8	Data analysis and data protection	EPPO
9	Forensics	EPPO
10	Tackling document fraud	EPPO
11	Crime prevention	EPPO

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
Corruption		
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	CEPOL EPPO
2	Cooperation between national, EU and international agencies and with judicial professionals, roles of EPPO and OLAF	CEPOL EPPO EJTN
3	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)	CEPOL EPPO
4	Investigation and intelligence practices	CEPOL EPPO
5	Corruption as a crime enabler	CEPOL EPPO
6	Sharing expertise, best practices, data and information between Member States and with civil society	CEPOL EPPO EJTN
7	Understanding the risks and threats caused by corruption before they materialise into corruption-related crime	CEPOL EPPO EJTN
8	Digital skills of law enforcement	EPPO
9	Promoting anti-corruption strategies, culture of integrity and integrity testing	CEPOL EPPO
10	Internal investigations	CEPOL EPPO
11	Protecting and handling whistleblowers and witnesses	CEPOL EPPO EJTN
12	Police ethics	CEPOL EPPO
13	Tackling document fraud	CEPOL EPPO
Excise fraud (Fraud, economic and financial crimes)		
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	CEPOL EPPO
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	CEPOL EPPO
3	Use of crime analysis methods	CEPOL EPPO
4	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	CEPOL EPPO

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
5	Integration of financial investigation methods into excise fraud investigation accompanied by enhanced asset recovery and big data analysis	CEPOL EPPO
6	Crime patterns, intelligence and investigation methods, techniques and tools in the area of alcohol fraud	CEPOL EPPO
7	Border control, mobile unit control, customs risk analysis	CEPOL EPPO
8	Means of transport/smuggling: road/land border crossing points, sea, railway, green border	CEPOL EPPO
9	OSINT, online undercover operations on darknet markets, decryption	CEPOL EPPO
10	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	CEPOL EPPO
11	EU legislation and international agreements, Framework Convention on Tobacco Control	CEPOL EPPO
12	Covert surveillance, GPS, covert investigation, informant handling practice, interviewing techniques	CEPOL EPPO
13	External Union transit procedure (T1), transit fraud, abuse of EMCS (doubling/mirroring legal consignments)	CEPOL EPPO
14	High-risk criminal networks	CEPOL EPPO
15	Tackling document fraud	CEPOL EPPO
16	Good practices on prevention, closely related to control mechanisms	CEPOL EPPO
17	Forensics	CEPOL EPPO
Intellectual property crime, counterfeiting of goods and currencies (Fraud, economic and financial crimes)		
1	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	CEPOL
2	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)	CEPOL
3	Digital investigation techniques, cyber patrolling	CEPOL
4	Pharmaceutical crime: falsified medicines, counterfeit medical products, including COVID-19 related vaccines and products	CEPOL
5	Copyright protection: piracy of digital content, literary works, artistic works	CEPOL
6	Tackling currency counterfeiting	CEPOL
7	Issues related to fraud in commercial items, e.g. food, drinks, textiles, etc.	CEPOL
8	Cooperation between customs, the police (including border police), and market surveillance authorities and the judiciary	CEPOL
9	Customs risk analysis related to (trade in) counterfeit goods	CEPOL
10	Financial investigations	CEPOL
11	Cooperation with IPR holders , as well as with online/offline intermediaries	CEPOL
12	Forensics	CEPOL

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
13	Fundamental rights and data protection	CEPOL
Environmental crime		
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	CEPOL EJTN
2	Investigation: digitalisation, OSINT, darknet; collection of intelligence, dealing with whistleblowers; undercover actions, surveillance, wiretapping as part of environmental crime investigation	CEPOL
3	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	CEPOL
4	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	CEPOL EJTN
5	Cooperation: interagency cooperation between different agencies dealing with environmental issues; EU cooperation instruments and networks; cooperation with non-EU countries, global cooperation tools	CEPOL EJTN
6	Wildlife crime: emerging patterns, trends, crime groups. Wildlife crime shall cover crime against flora and fauna in line with CITES (Convention on International Trade in Endangered Species of Wild Fauna and Flora), including illegal logging and timber trade (modus operandi, investigation techniques), trafficking protected species (glass eels, reptiles, mammals, birds), illicit pet trade, etc.	CEPOL
7	New legislative trends related to the circular economy to help in identifying crime enablers	CEPOL EJTN
8	Related crime areas such as document fraud and corruption	CEPOL
9	Maritime exploitation and pollution; illegal, unreported and unauthorised fishing (modus operandi, investigation techniques)	CEPOL
10	Pollution or illegal exploitation of air, ozone depletion; F-gas Regulation	CEPOL
11	Administrative tools to combat environmental crime	CEPOL
12	Raising general public awareness of the costs of environmental crime to society	CEPOL EUCPN (in 2023)
13	Role of CSDP missions in spreading good practices and standards in host countries (training for mission personnel as part of pre-deployment training)	n/a
14	Fundamental rights and data protection	CEPOL
External dimensions of European security		
1	Leadership in CSDP missions, planning and command, change management in host country	CEPOL Europol
2	Pre-deployment training	CEPOL Europol Frontex
3	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	Europol
4	The EU's role as a security provider through CSDP, including CSDP policy on strategic ambitions and capability limitations	CEPOL Europol
5	Analytical, planning and decision-making structures and procedures	CEPOL Europol

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
6	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	CEPOL Europol
7	Role of CSDP missions in supporting EU internal security (external dimension of internal security)	CEPOL Europol
8	Building advisory capacity of CSDP missions	CEPOL Europol
9	Language training: English communication skills; French as a foreign language	Europol Frontex
10	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)	Europol
11	Civil-military cooperation and its conceptual development	Europol
12	Political, economic and budgetary aspects of cooperative projects in defence and security within the framework of CSDP	Europol
13	Digital skills of law enforcement	Europol
14	Duty of care in CSDP missions	Europol
15	Cooperation: synergies between CSDP structures, Commission services and 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	Europol
16	High-risk criminal networks	Europol
17	Tackling document fraud	Europol Frontex
18	Crime prevention	Europol
Other thematic areas		
1	Leadership and management	Frontex
2	English language	n/a
3	Public order: community policing; 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, managing crowd events with VIP participation, CBRN supervision and defence, sharing best practices, case studies, quality assurance for an EU model for training protection officers; protection of public spaces	EUCPN EU COMMISSION (DG HOME D.2)
4	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	n/a
5	EU funding and EU project management	n/a

	TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
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; 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	EASO
7	Stress management, conflict management and communication	EASO Frontex
8	Disaster victim identification: international collaboration; harmonisation of identification procedures for individual cases; identification of deceased persons in non-disaster contexts	n/a
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	Frontex

Annex 7 Estimated volume of training

(In order of training priority)

THEMATIC AREA	NUMBER OF PARTICIPANTS
Cyber-attacks	7 659
Criminal finances, money laundering and asset recovery	8 706
Counter-terrorism	5 375
Trafficking in human beings	5 665
Drug trafficking	8 774
Migrant smuggling	6 149
Child sexual exploitation	6 192
Online fraud schemes	6 285
Organised property crime	5 017
Border management and maritime security	7 201
Firearms trafficking	4 995
Missing trader intra-community fraud	4 657
Corruption	6 127
Excise fraud	7 423
Intellectual property crime, counterfeiting of goods and currencies	4 648
Environmental crime	5 861
External dimensions of European security	3 937
Other thematic areas	5 797
Total	**110 368**

By thematic area, in descending order as indicated by the Member States.

THEMATIC AREA	NUMBER OF PARTICIPANTS
Drug trafficking	8 774
Criminal finances, money laundering and asset recovery	8 706
Cyber-attacks	7 659
Excise fraud	7 423
Border management and maritime security	7 201
Online fraud schemes	6 285
Child sexual exploitation	6 192
Migrant smuggling	6 149
Corruption	6 127
Environmental crime	5 861
Other thematic areas	5 797
Trafficking in human beings	5 665
Counter-terrorism	5 375
Organised property crime	5 017

THEMATIC AREA	NUMBER OF PARTICIPANTS
Firearms trafficking	4 995
Missing trader intra-community fraud	4 657
Intellectual property crime, counterfeiting of goods and currencies	4 648
External dimensions of European security	3 937
Total	**110 368**

QR-09-22-117-EN-C

EU Strategic Training Needs Assessment 2022-2025

Publications Office
of the European Union

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, Ó utca 27, Hungary •
Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu •
www.cepol.europa.eu

Find CEPOL on: