EUROPEAN UNION

STRATEGIC TRAINING NEEDS ASSESSMENT

2019-2021

CEPOL European Union Agency for Law Enforcement Training

O utca 27, 1066 Budapest, Hungary
T +36 1 8038030
www.cepol.europa.eu

Budapest, October 2018

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 Member States and EU Agencies. Also, other European organisations, professional groups and networks contributed to it, and their assistance is hereby acknowledged with gratitude.

Table of Contents

Preface

One of the goals of the European Union is to offer its citizens an area of freedom, security and justice without internal frontiers, with respect for fundamental rights and the different legal systems and traditions of the Member States. In this area, the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration as well as measures to prevent and combat crime[1].

The European Union Agency for Law Enforcement Training (CEPOL) was established as an agency of the Union with the aim of training and facilitating cross-border cooperation between law enforcement officials. This, however, does not mean that CEPOL holds a monopoly over the area of law enforcement training. On the contrary, there are multiple EU entities operating in the area of law enforcement training: hence, cooperation and coordination are key, and particularly so in this historical moment, when the European Union is facing ever evolving security challenges both internally and externally.

The plurality of training providers and a wide training offer does not automatically guarantee that training is delivered in the areas where it is most needed. In general, the EU lacks a systematic process for identifying and addressing strategic training needs, which are constantly evolving[2].

The effectiveness of cooperation tools relies on law enforcement officials in Member States knowing how to use them, and thus training is essential to allow authorities on the ground to exploit the tools in operational situations[3].

To avoid duplication or overlap and to ensure better coordination of training activities for competent law enforcement officials carried out by EU agencies and other relevant bodies, CEPOL, on the basis of its founding Regulation, was mandated to assess strategic training needs.

To this end, CEPOL has conducted the first the 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. This shall help build the capacity of law enforcement officials, while seeking to avoid duplication of efforts and achieve better training coordination in a multiannual perspective.

As the Executive Director of CEPOL, I am glad to be able to present this Report to the EU decision makers and the wider public alike, and I am confident it will be recognised as a sound basis to orientate the EU's law enforcement training efforts in the years ahead.

The importance of the report lies primarily in the fact that for the very first time, comprehensive training needs at strategic EU level are clearly identified using a scientific approach, systematically presented, and explained in clear language.

Nevertheless, a series of themes constituting a common thread emerge from the analysis of the training needs in relation to 21 security threats and horizontal issues addressed in this report: differences in national legislations, under-developed cross-border exchange of information and investigative tools, and the lack of opportunity for multidisciplinary training are

[1] Treaty of Lisbon, 2007/C 306/01
[2] Commission Communication Establishing a European Law Enforcement Training Scheme, Brussels, 27.3.2013, COM (2013) 172 final
[3] Commission Communication, The European Agenda on Security, Strasbourg, 28.4.2015, COM (2015) 185 final

all factors that make the life of those meant to keep us safe and secure significantly harder, and conversely facilitates the work of those who mean to do us harm. The online dimension of crime- if indeed we can still distinguish the online and offline dimensions – a emerges from this report as some sort of new “wild west” where law enforcement confronts shapeshifting forms of criminality with a degree of success, but with resources nowhere near to what would be necessary. All in all, the report paints a picture of training needs in the context of fight against European criminality as an intertwined, borderless, compenetrated, and complex landscape.

It is difficult to disagree with the statement that Europe should do more, and not less, in this field. As the say goes, the only way to fight organised crime is through organised legality. This is where the role of agencies and bodies like CEPOL and the other partners in the Justice and Home Affairs policy area comes into play as a key element to better support a concerted response to the threats affecting European security. I am confident this report represents a ground-breaking development. Certainly, the reader will find relevant and at time even thought-provoking indications as to what experts and frontline practitioners believe security challenges are, and how training could help bridge gaps in law enforcement training.

Lastly, I would be remiss if I did not explicitly acknowledge the hard work done by my colleagues here at CEPOL, who have provided first-hand contributions to the drafting of this report: organising and moderating workshops, reading a large amount of documents, summarising outcomes of consultations, and so forth.

Acknowledgment also goes to excellent cooperation with our colleagues at the European Commission (DG HOME), whose help was crucial in developing the EU-STNA methodology.

Not least, of course, I have to express my personal gratitude to the 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.

Detlef Schröder

CEPOL Executive Director

EXECUTIVE SUMMARY

Aim of the Report

This EU-STNA Report is based on a structured methodology, which incorporates the examination of strategic and policy documents as well as consultations with practitioners, experts and stakeholders. Ultimately, the list of identified EU-level training needs has been prioritised by the Member States and shared with potential EU training providers.

It has to be noted that the priorities presented throughout the report refer only to the training dimension in particular areas of internal security. This report by no means intends to compare or weigh one crime or threat area, or a horizontal aspect, with another. In other words, the report only reflects the sensitivities of EU Member States as to what particular topic in should be given priority when planning EU level training for law enforcement officials.

Legal and Policy Background

The Law Enforcement Training Scheme[4] noted that the European Union lacks a systematic process for identifying and addressing strategic training needs, which are constantly evolving. The European Agenda on Security[5] identified training as one of the supporting cross-cutting actions to combat serious and organised cross-border crime and terrorism. As defined by the Preamble of the CEPOL Regulation[6], CEPOL should assess strategic training needs and address the Union's priorities in the area of internal security and its external aspects. Pursuant to the Article 4.1 of the Regulation, CEPOL is tasked to prepare multiannual strategic training needs analyses and multiannual learning programmes.

The EU-STNA was launched on 25 September 2017 at the Standing Committee on Operational Cooperation on Internal Security (COSI). Further updates were provided to COSI throughout the implementation phase of the EU-STNA, as well as other Council preparatory bodies were updated on the EU-STNA progress, i.e Law Enforcement Working Party and Customs Cooperation Working Party.

Key findings: Core capability gaps

It became clear during the assessment that more and more thematic categories are interlinked, partially overlapping, dependant on each other and cannot be treated in silos; hence a holistic and multidisciplinary approach to training shall be applied.

For example, *fundamental rights* is a cross-cutting element that should be integrated in each and every training. A similar situation is with *crime prevention* and *forensics*, which normally should form a part of a thematic training where relevant. Types of investigation that are mentioned as necessary to be involved in tackling a variety of crimes are *financial* and *cyber-investigation*.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a Law Enforcement Training Scheme.
[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions The European Agenda on Security.
[6] 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.

The following areas constitute the **core capability gaps of law enforcement officials** that can and shall be addressed by training[7]:

- **Cross-cutting thematic categories**:
  - Open Source Intelligence, data collection, analysis and application;
  - Financial investigations, money flows, alternative banking, etc.;
  - Elements of cyber-investigations, darknet and e-evidence;
  - Document fraud;
  - Fundamental and human rights;
  - Crime prevention;
  - Respective areas of forensics;
  - Links between different crime areas.

- **Related to information exchange and cross-border cooperation**:
  - Information exchange mechanisms, interoperability of the large scale IT systems, information exchange channels and procedures, including evidence handling, databases, Passenger Name Records (PNR), other, and with a special focus on the Schengen Information System, as well as other upcoming large scale IT systems (ETIAS and Entry-Exit System);
  - EU cooperation tools and mechanisms, including Joint Investigation Teams (JITs), the European Arrest Warrant (EAW), freezing order, etc.; and the role and possibilities of the respective EU agencies and other entities.

[7] No priority order

Findings on EU level thematic training areas

The list below indicates thematic areas, in order of priority identified by the EU Member States, in which EU-level training should be delivered to law enforcement officials in the upcoming three years (2019-2021) to support the EU response to serious and organised crime and other threats to internal security:

1. Facilitation of illegal immigration;
2. Counter-terrorism;
3. Trafficking in Human Beings;
4. Cyber-crime – Child Sexual Abuse and Sexual Exploitation;
5. Criminal Finances and Money laundering;
6. Cyber-crime – Attacks on Information Systems;
7. Illicit Trafficking, Distribution and Use of Firearms and Explosives;
8. Organised Property Crime;
9. Drugs – Production, Trafficking and Distribution of New Psychoactive Substances and Synthetic Drugs;
10. Cyber-crime – Non-cash Payment Fraud;
11. Document Fraud;
12. Drugs – Production, Trafficking and Distribution of Cannabis, Cocaine, Heroin;
13. Border Management and Maritime Security;
14. Crime Prevention;
15. Forensics;
16. Corruption;
17. Missing Trader Intra-Community Fraud;
18. Environmental Crime;
19. Excise Fraud;
20. Fundamental Rights;
21. CSDP Missions.

Each thematic category is reflected in a separate chapter of the report, which outlines the main challenges hindering the performance of law enforcement officials in the corresponding area. Furthermore, the EU-STNA distinguishes between environmental challenges and challenges that are related to knowledge, skills and competences of law enforcement officials. While the former category is determined by surrounding conditions in which law enforcement officials operate and cannot be solved by training (e.g. lack of technical equipment), the latter refers to capability, attitude and behaviour of the officials and can be addressed by training. It is important to note that each chapter also contains the advice and expert opinion of practitioners in the respective fields- hence, the report contains useful indications that go beyond the sheer ranking of training priorities but also provide a more comprehensive picture of challenges and their potential solutions.

Moreover, each thematic category was further scrutinized in order to identify more specific areas for training. This resulted in a list comprising main topics for training interventions in particular thematic categories, which is enclosed at the end of each chapter, with a consolidated list available at the end of the report (Annex 7). It is also important to mention that the list is indicative and shows the direction training should be channelled to, but it does not define particular training activities or their form, level, content, and target group. Therefore

a more detailed analysis of the mentioned elements will be necessary before designing specific training activities.

Other specific or cross cutting training needs

In addition to the 21 thematic categories as mentioned above, CEPOL has also identified a list of specific or cross-cutting training needs which, due to their nature were not allocated to any thematic category, but were offered to Member States for prioritisation. These to a great extent (but not limited to) originate from the strategic objectives of different LEWP networks and expert groups, and are listed below:

1. English language, specific professional terminology – cross-cutting;
2. Leadership training – specific;
3. Schengen Information System – cross-cutting;
4. Football Safety and Security – specific;
5. Intellectual Property Rights – specific;
6. Training on EU project and EU funds management – specific;
7. Stress Management, Conflict Management, Communication – cross-cutting;
8. Mafia Style Organised Crime – specific[8];
9. Protection of Public Figures – specific;
10. Training of Service Dog Handlers - specific.

Features of EU-level training

The consultation process reflected upon not just the content, but also the main features of EU-level training. It became clear that professional training should not only boost the knowledge, but also allow an exchange of experiences and practices between the practitioners and contribute to building trust. Training should:

- cover recent policies, operational (modus operandi), tactical, technology, research and scientific and other developments;
- bring together law enforcement officials, prosecution, judiciary, tax authorities, other officials, where possible to organise joint trainings;
- invite private parties (telecommunication companies, currier services, banking sector, NGOs, etc.) and academics as experts where relevant to provide better insight in various procedures;
- invite non-EU country participants and experts where admissible.

Considerations related to EMPACT priorities

As explained above, this EU STNA report seeks to identify training priorities, not to rank or priorities crime threats. It is understandable that the perceptions around whether a topic should be given priority over another may differ between investigators, criminal analysts, training operators and/or policy makers, and between specialists of different sectors. For this very reason, the preliminary list of identified training needs have been shared with the JHA and other relevant stakeholders to ensure consistency with overall crime priorities. To the great extent the thematic categorisation was acknowledged as covering the most imminent training needs, raising additional attention towards the importance of *Fundamental Rights* and the *Gender Perspective.* From Europol's perspective, *Mafia Style Organised Crime* should be moved to the top of the priority list. The non-recognition of the problem and the lack of capacity

[8] According to Europol, Mafia style organised crime should be given a more prominent position in the priority list.

building led to the current situation of national law enforcement structures significantly weakened and having insufficient resources and capabilities to fight against organised crime and Mafia structures, and against drugs production and trafficking in particular. It has been also pointed out by Europol that training in two priorities in the EU Policy Cycle (*Missing Trader Intra-Community Fraud* and *Environmental Crime*) should be prioritised together with *Crime Prevention*, *Forensics* and *Corruption*. For Frontex, *Border Management and Maritime Security* should remain a priority.

Coordination and delivery issues

Training in most cases is to some extent provided by different actors; nevertheless, the current offer is not sufficient either in terms of quantity, frequency, or is not accessible to potential trainees (no information, lack of seats, language barrier, ad hoc commitments, etc.). Therefore, training demand remains high, and the available training offer should be continued and reinforced. It is also important that the awareness and basic training is provided at national level ensuring that law enforcement officials are prepared for duty in general, including newcomers and first responders, and allowing practitioners from different areas to understand each other's work (e.g. basic cyber-language, etc.).

Consultation with the potential EU training providers (supporters)[9] was conducted to initiate potential training coordination. The table in the attachment (Annex 7) provides an overview of all training needs and consulted potential training providers who could support the training. It is worth raising attention to the fact that the majority indicated they would be able to provide content experts but not to organise training themselves. This is also in line with their mandates, hence the main training providers are CEPOL, the European Security and Defence College (ESDC) and the European Border and Coast Guard Agency (Frontex)[10]. These agencies already partially address the identified topics while implementing more detailed training needs analyses and addressing the specific thematic categories suitable for their respective target audiences and within their planning cycles.

Final considerations

The EU-STNA report has been shared with the European Commission and will be presented to the Council of the European Union and to the European Parliament with a view of establishing a structured policy for law enforcement training at the EU level. While awaiting an opinion from these EU institutions, the EU training providers are encouraged to coordinate their training provision with others and align it with the identified training priorities ensuring thus that the capability deficiencies of law enforcement officials are addressed.

The role of training should not be underestimated, in particular as training time is dedicated to preparing law enforcement officials to tackle different scenarios where internal security is at stake.

The first EU-STNA has to be understood as a pilot process that has been performed to identify law enforcement training priorities in a systemic way and to rank them in order of priority as expressed by the Member States. This was done to ensure that EU training resources can be allocated in a most efficient way and, where needed the most. This will support a coordinated

[9] EU Justice and Home Affairs agencies, the European Judicial Training Network, the Euopean Security and Defence College, the European Crime Prevention Network, and the European Union Intellectual Property Office.
[10] in alphabetic order

EU response in line with its priorities and safeguarding the EU values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights.

The first EU-STNA will be evaluated in order to assess its impact and to review the methodology before initiating the next full EU-STNA cycle (2022-2025). Future EU-STNAs should become a regular exercise which forms the foundation for further planning of training, thus contributing in a transparent manner to informing future decisions for the benefit of the European Union' law enforcement community- and ultimately, the security of the Union.

1. INTRODUCTION

1.1 Legal and policy background

Already in 2012/2013, it was noted that the European Union lacks a systematic process for identifying and addressing strategic training needs [11], which are constantly evolving. Furthermore, re-acknowledging this matter, this was included in the draft CEPOL regulation, which was finally adopted by the European Parliament and the Council of the EU in late 2015[12].

In the new CEPOL Regulation, co-legislators mandated CEPOL to assess the strategic training needs of the Union.

As defined by the Preamble of the Regulation, to avoid duplication or overlap and to ensure better coordination of training activities for law enforcement officials[13] carried out by the European Union agencies and other relevant bodies, CEPOL should assess strategic training needs and address the Union's priorities in the area of internal security and its external aspects. Pursuant to the Article 4.1 of the Regulation, CEPOL is tasked to prepare multiannual strategic training needs analyses and multiannual learning programmes.

At the same time, the European Agenda on Security[14] identified training as one of the supporting cross-cutting actions to combat serious and organised cross-border crime and terrorism. Training is essential to allow authorities on the ground to exploit the tools in an operational situation. Moreover, the Commission seeks to target this support in a strategic and cost-effective way.

The complex and rapidly evolving environment in which law enforcement officials operate as well as the presence of several training providers, and the lack of a systematic process to identify strategic EU training needs require a renewed approach to EU training.

The European Union Strategic Training Needs Assessment (EU-STNA), in accordance with the above-mentioned, aims at assessing strategic training needs and addressing EU priorities in the area of internal security and its external aspects, with a view to better coordinate training activities for law enforcement officials and avoid duplication of efforts among EU training providers.

1.2 EU-STNA methodology overview

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

The methodology behind the EU-STNA process was developed with the support of the European Commission and in close cooperation with the Member States as well as key stakeholders, like Europol and Frontex. It consists in a systematic analysis of strategic EU

[11] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a Law Enforcement Training Scheme
[12] 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
[13] Throughout the report the term "law enforcement officials" is used in line with the CEPOL regulation Art. 2 (1)
[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions The European Agenda on Security

documents detailing crime threats, which are then discussed in expert and focus groups by Member States' and EU specialists with a view to identify capability gaps and training needs that should be addressed by training activities implemented at EU level. Subsequently, these training needs are prioritised by the Member States at strategic level, and the outcomes are shared with the EU JHA agencies for their comments and for potential training coordination purposes. At the end of the analysis phase, an EU-STNA report (present document) is drafted and presented to the Council of the European Union for endorsement and to the European Parliament for information.

The EU-STNA shall suggest a distribution of tasks among EU level training providers and shall inform and facilitate planning. The project cycle will always be completed by an evaluation phase, during which lessons learned will be extracted for the improvement of the next EU-STNA cycle. Each EU-STNA cycle shall cover a four-year period aligned with the Policy Cycle.

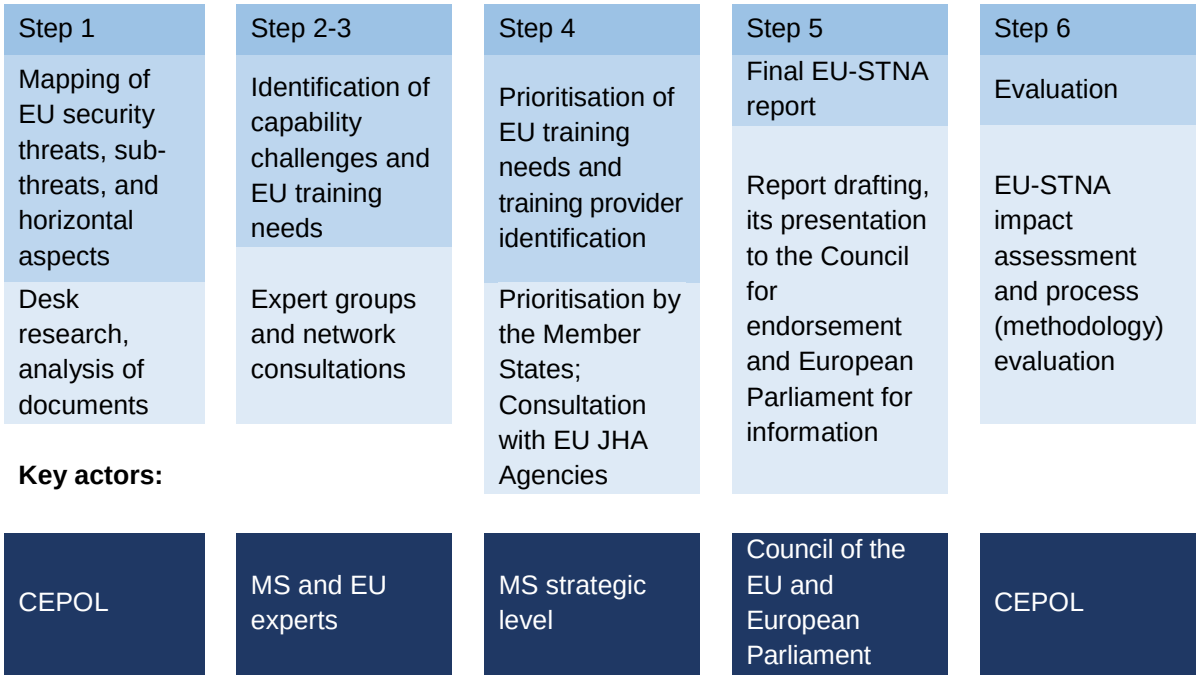


Fig.1 EU-STNA steps

EU-level training activities refer to strands 3 and 4 of the Law Enforcement Training Scheme (LETS) as identified in Commission Communication COM (2013)172, and namely 1) thematic policing specialism and 2) European Union civilian missions and capacity building in non-EU countries. The EU-STNA only looks at EU-level priorities, keeping national and bilateral/regional training outside of the scope of the exercise.

Within the framework of this project, an effort was made to include training activities on specific topics that are already being provided at EU level. This information was gathered via group discussions and some desk research, and is therefore not exhaustive. To a certain extent, participants were not aware of such ongoing training, which actually signals a need for a better promotion of training and for visibility actions. Therefore, this report does not claim to provide a full picture of the EU-level training landscape.

1.3 EU-STNA timeline and content

It has to be noted that the methodology was not tested before its actual implementation; hence the first EU-STNA constitutes a pilot exercise. The timeline of the EU-STNA is reflected in the Annex 6.

On 25 September 2017, CEPOL`S Acting Executive Director, supported by a brief introduction by the Director of the Directorate D "Security" of DG HOME, presented the features of the EU-STNA to the Standing Committee on Operational Cooperation on Internal Security (COSI); this marked the **official launch** of the pilot EU-STNA covering the period of 2018-2021.

In October 2017, CEPOL initiated **Step 1** (Desk research), which was supported by seven JHA agencies[15], the European Commission, the Council of the EU, the Secretariat of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in the European Parliament, the European External Action Service (EEAS), and the European Security and Defence College (ESDC) providing policy and strategic documents for analysis. In total, the desk research featured 265 documents (see Annex 2 for the complete list) and was concluded by the end of December 2017. The research helped extracting information on security threats, sub-threats, horizontal aspects and law enforcement capability challenges, which then served as a basis for further and more detailed discussions in the expert groups.

During the **first half of 2018**, CEPOL implemented **Step 2-3**, consulting all fourteen European Monitoring Platform against Crime Threats (EMPACT) groups, (See Annex 3 for a complete list of consulted expert groups), and convened seven additional expert group consultations on the following topics: Border Management, Coast Guard and Maritime Security; Corruption; Counter-terrorism; Crime Prevention; CSDP Missions; Forensics; and Fundamental Rights, Hate Crime and Genocide. Furthermore, to cover a broader area of law enforcement functions, CEPOL approached fourteen professional entities (networks/groups) (Annex 4) in the domain of law enforcement cooperation as their representatives had not been consulted previously via workshops.

All in all, during the workshop consultations, 495 representatives from fifty different countries and organisations were consulted (see Fig. 2).

Fig.2 Participation of countries and organisations in the EU-STNA consultations

In the framework of the consultations, participating experts highlighted and discussed the challenges faced by law enforcement officials specific fields, and they identified areas which

[15] EASO, EMCDDA, eu-LISA, Eurojust, Europol, FRA and Frontex.

should be addressed by training at EU level (for the decision tree guiding the discussions see Annex 5). Outcomes of the discussions, complemented by the results of the initial desk research and information gathered via written consultations, were analysed and resulted in a consolidated list of 184 EU-level training needs across 21 thematic categories and one category covering other training needs:

1	Facilitated Illegal Immigration	12	Drugs – Production, Trafficking and Distribution of Cannabis, Cocaine, Heroin	22	Other training needs:
2	Counter-terrorism	13	Border Management and Maritime Security	22.1	English Language
3	Trafficking in Human Beings	14	Crime Prevention	22.2	Leadership
4	Cyber-crime – Child Sexual Abuse and Sexual Exploitation	15	Forensics	22.3	Schengen Information System
5	Criminal Finances and Money Laundering	16	Corruption	22.4	Football Safety & Security
6	Cyber-crime – Attacks on Information Systems	17	MTIC Fraud	22.5	Intellectual Property Rights
7	Illicit Trafficking, distribution and use of Firearms and Explosives	18	Environmental Crime	22.6	EU Project and EU Funds Management
8	Organised Property Crime	19	Excise Fraud	22.7	Stress Management and Communication
9	Drugs – Production, Trafficking and Distribution of New Psychoactive Substances and Synthetic Drugs	20	Fundamental Rights	22.8	Mafia Style Organised Crime
10	Cyber-crime – Non-Cash Payment Fraud	21	CSDP Missions	22.9	Protection of Public Figures
11	Document Fraud			22.10	Training of Service Dog Handlers

In **June-July 2018**, as a part of **Step 4**, the outcomes were distributed among the EU Member States with a request to prioritise and rank the training needs. The EU Member States were approached via the contact points as communicated to CEPOL by the Law Enforcement Working Party nominating national representatives to express the Member States` official position. Twenty-five 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 JHA agencies, European Judicial Training Network (EJTN), the European Security and Defence College (ESDC), European Crime Prevention Network (EUCPN) and European Union Intellectual Property Office **(**EUIPO) for their opinion on prioritisation and potential training coordination. Lastly, both the results of the prioritisation and the draft report were shared with the European Commission.

At the same time, CEPOL initiated **Step 5,** the drafting of the EU-STNA report while listing the EU key training needs and indicating potential training providers. The report was finalised in **October 2018** and shared with DG HOME and tabled to the CEPOL Management Board for information in November. The final report will be presented to the Council of the European

Union 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 impact assessment of the EU-STNA (**Step 6**) will take place before the implementation of the next cycle in order to identify whether any adjustments need to be made to the methodology. CEPOL will commission this evaluation work in 2020 in order to allow sufficient time for its implementation, for possible methodology adjustments and for ensuring the alignment of the next EU-STNA with the next Policy cycle 2022-2025.

2. EU TRAINING PRIORITIES

The following section presents training needs on specific topics in the area of law enforcement that the European Union is recommended to address in the next three years (2019-2021). Even if not all thematic categories show the same number of training needs, none was given more attention than the other while examining the capability challenges together with the experts. The order of listing is the result of prioritisation done by the Member States. The analysis contained in the sub-chapter reflects the outcomes of the discussions held during the consultations with experts, hence do not necessarily reflect the official view of CEPOL.

Throughout the sub-chapters, a trend in law enforcement work of the recent years becomes visible: the increasing combination and overlap of different types of crime and of modi operandi of the perpetrators puts a demand on investigators and other specialists to join their expertise and efforts and to coordinate their work, both at national as at international level. This situation creates a number of horizontal issues that were mentioned for every individual thematic category described in the sub-chapters below evidencing a multidisciplinary character of the training needs expressed.

Most frequent mention was given to the fact that support by the cyber-crime investigation units for other investigation units is highly important, as the internet gives way to new modi operandi by OCGs. Also high on the list was training on cyber-crime issues for all investigators so that they could have a basic common understanding and can use tools in that area, e.g. Open Source Intelligence (OSINT), social media etc. The second most frequent topic is financial investigation techniques and different tools and elements related to financial crime, including cryptocurrencies, hawala, alterative banking etc., that are also relevant for crime investigations.

Further horizontal topics are crime prevention and fundamental rights, as well as respective elements of forensics, such as electronic evidence (e-evidence), as these are relevant within the framework. In addition, the support that can be offered by EU agencies are equally essential as the tools they put at the disposal of law enforcement in the Member States, and the EU information channels. Also, language training has been mentioned frequently, in particular English with a specific focus on law enforcement terminology.

Another trend becomes visible – linked with the need for a stronger multidisciplinary approach as described above –, and that is the request for more joint training with other professional groups, in particular prosecutors and judges but also where relevant other specialists whose duties are directly or indirectly linked to the law enforcement domain, e.g. tax authorities, municipal administration, environmental inspectors, etc. The private sector (banks, shipping companies, parcel delivery services etc.) and NGOs could also contribute to law enforcement training by their involvement as experts/trainers providing a better insight into the processes and fostering mutual cooperation.

Crime areas are interlinked, it is frequently hard to distinguish where one type of crime ends and another one begins. There is a clear need to prepare investigators in specific fields to obtain basic knowledge in other crime areas so that they can recognise related crime and have the opportunity to involve relevant experts.

And finally, on where it concerns a wider transfer of knowledge, there is a frequent demand for more EU Train-the-Trainers type of activities with a focus on the specific topics and consequent cascading of content at national level; this would also strengthen harmonisation

of training content across the EU. A further item that could contribute to and enhance a common understanding and cross-border cooperation is the exchange of good practice, for which online platforms can be a useful tool but also EU-level training activities and meetings.

The thematic chapters are listed in order of priority with regard to the need for training as indicated by the Member States. It seems important to emphasise that the prioritisation does not say anything about the importance or incidence of the specific type of crime in the EU. It merely refers to where law enforcement officials throughout different Member States consider more training is required in order to address capability challenges and to be able to tackle the particular crime area more effectively.

Each thematic chapter addresses challenges and training needs as well as recommended direction for EU-level training. The following distinction is made concerning the challenges encountered by law enforcement officials:

- Environmental challenges - relate to the aggregate of surrounding conditions that influence the performance, e.g. a lack of technical equipment and resources, different legislations etc., and cannot be directly tackled by training.
- Challenges related to knowledge, skills and competencies, which can be addressed by training aiming at the enhancement of the operational performance through boosting the capabilities of law enforcement.

The training subjects that would address shortcomings in the knowledge, skills and competencies and would influence the behaviour of law enforcement officials forming part of strategic response to security threats are reflected as follows:

- Narrative summary describing and detailing the training needs;
- List of training needs in priority order.

Where possible, examples of already existing EU-level training on specific subjects are pointed out.

In addition, CEPOL invited JHA agencies and other EU entities[16] active in the field of training and internal security to communicate their opinion on the prioritisation of training needs in general and to indicate their availability to address by training particular thematic.

2.1 Facilitation of Illegal Immigration

2.1.1 Environmental challenges

Illegal Immigration is a challenge that touches a high number of EU Member States, not only those on the external border. This topic has recently been subjected to a high number of new policies and regulation changes. One important related issue is the abuse of the asylum application system by migrants. On the one hand, this is a question for national authorities to take action on, but also the Dublin Agreement plays a role here. Migrants whose asylum application has been rejected in one country, still can apply in one or more other Member States. This can only be tackled by means of a political response in the form of a change of policy, and is hence out of the scope of this report.

[16] EJTN, ESDC, EUCPN and EUIPO.

Another problem concerns the different legislations. A particular legal problem is the returns to countries of origin or first entry countries, which is often quite cumbersome. Also here a solution must be sought at a political level, e.g. by means of bilateral agreements.

On a practical level, the absence of specialised regional units, a lack of experts and financial resources as well as the need and the difficulty to facilitate a speedy exchange of information, intelligence and evidence represent important challenges, which hamper cooperation. Also, the work with interpreters (at the border or in Hotspots) is not always easy. It requires trust and therefore a good work relationship. Possibly the registration of interpreters or the engagement of certified interpreters only should be considered.

2.1.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The inherent multinational character of this field of work makes cross-border cooperation imperative. For this, knowledge on the different legal systems with regard to returns and other issues is required; the speedy and reliable exchange of information is one of the pillars of this type of collaboration; and the foreign language capacities of border guards and other involved professionals (not only English) is another highly relevant issue.

In spite of all improved checking policies and procedures at the land, sea and air borders, there are still migrants, including minors, who manage to circumvent border control at entry or checkpoints on their transit route and to arrive at their destination whilst not having been registered at all.

Training can be a solution, or at least partly, to improve the work of the concerned professionals. Risk analysis, which in all EU countries must be done from different angles: entry, transit, and varying destination countries, can be practiced in interactive, hands-on training; links with other types of crime, e.g. Trafficking in Human Beings (THB) and in particular sham marriages, can be recognised by well-trained officials. There is a high turnover of staff, and therefore regular training is required to cover the gap in knowledge on other types of investigation and to promote mutual understanding and cooperation. Also, cooperation with the private sector can be enhanced by inviting representatives to law enforcement training or by having regular meetings for exchange of information.

b) Training needs

Summary

Next to the regular topics like investigation methods and techniques, modi operandi, the involvement of financial crime and cyber-methods in illegal immigration facilitation it is considered imperative that training is provided on other related areas and new issues. These involve investigation activities at Hotspots, document fraud with a focus on identity fraud, returns and PNR, and finally prevention and fundamental rights. Intercultural competencies, interviewing techniques against a certain cultural background and cooperation with interpreters was further mentioned.

Further details

The lack of familiarity of law enforcement officials with the type of support that can be requested from Europol and Frontex is often mentioned. The use of EU-level tools,

instruments and networks must therefore be part of regular training on investigation and cross-border cooperation.

Joint training with border guards, prosecution, customs and (financial) investigators could contribute to a better understanding of each other's work requirements and culture. Legal issues should be part of this, e.g. lawful interception, admissibility of evidence. On the other hand, the inclusion of private sector experts in order to enhance mutual familiarity and willingness to cooperate is recommended.

Training on EU Information Systems (SIS, VIS, Eurodac), and particularly on the coming changes, is highly important. At present, CEPOL in cooperation with eu-LISA and Frontex provide such training. Other professions in the multidisciplinary context could also benefit from training on this topic.

Looking at migrant smuggling, there seems to be a high training need of different professionals with the purpose to enhance cooperation with law enforcement officials. This involves the private sector as well as interpreters. Managers or unit leaders could enhance their understanding of the value and the means of cooperation. Training content for investigators should include an overview of the different legal frameworks about migrant smuggling as well as poly-criminality and a horizontal approach to organised crime. Exchange of good practice and experience would be beneficial.

Hotspot management is a "hot topic" as these are relatively new, and the knowledge is not widely spread nor is the way they function always perfect. There is a need for standardisation of procedures and for cooperation of different actors, including civil society. The identification and the handling of THB victims and unaccompanied minors is a challenge as well as detecting links to terrorism and recognising returnee foreign terrorist fighters.

EU-level training is available concerning subjects like combating organised crime facilitating illegal immigration by CEPOL and eu-LISA, financial crime in the context of this topic, Hotspots, and foreign fighters/returnees by CEPOL.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Facilitation of Illegal Immigration related training.

1	*Investigation of illegal immigration cases (techniques; modi operandi; poly-criminality; case studies; exchange of good practices; cooperation with prosecution; THB aspects, including sham marriages)*
2	*Document fraud with focus on identity fraud (impostors; profiling; debriefing; common risk indicators; detection of false documents; new technologies for detection; identification of forged and inappropriately issued breeder documents; document profiling; debriefing; common risk indicators; new modi operandi)*
3	*Returns and PNR (EU instruments; legislation; relevant information systems; in particular the PNR [data assessment]; smart borders; Frontex role in return; human rights)*
4	*Risk analysis and OSINT (OSINT techniques; tools; best practices (CIRAM) involving private parties; Vulnerability assessment; common risk indicators; intelligence used for the investigations; analysis of data on secondary movements; human rights)*
5	*Financial investigations in relation to illegal immigration cases (alternative banking solutions; hawala money transfer system; asset recovery; cryptocurrencies and cryptography; existing EU tools; instruments and networks (CARIN/FIU's/AROs/JITs/ EIO/ PCCC), data protection; cooperation with the private sector)*

6	*Prevention of illegal immigration (how to design and implement prevention campaigns from the law enforcement perspective; cooperation between private-public sectors; interagency and international cooperation; including work with the neighbouring non-EU countries)*
7	*Hotspots (evidence collection and THB identification; unaccompanied minors; human rights; identification of foreign terrorist fighters; profiling; common risk indicators; intercultural competencies; cultural mediation; interviewing techniques; use of interpreters)*

2.2 Counter-terrorism

2.2.1 Environmental Challenges

Counter-terrorism measures are to be seen as part of law enforcement interventions as well as of prevention. Both require cooperation between police and other actors. Investigators need the public and the private sector to support their work whilst community policing plays a very important role in prevention of radicalisation, e.g. links to certain communities, religious institutions, etc. Whilst for counter-terrorist experts cross-border cooperation is of the utmost importance, prevention work has a more local focus and demands cooperation with the municipalities, NGOs, the health sector, and social work.

A further challenge to be addressed is the need for the harmonisation of legal arrangements in the different Member States that hamper cross-border cooperation and access to e-evidence. In addition, the majority of the Member States has yet to address the potential future] threat of chemical terrorism. This can appear in form of attacks on individuals or large-scale actions. Governments must take CBRN defence measures that go beyond training of law enforcement.

2.2.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

In both cases described in the previous paragraph, officials need to be led by a thorough understanding of the phenomenon, including the background of the (potential) perpetrators. This requires an ability to read the signs and recognise terrorism indicators as well as cultural and regional aspects in this context. Officials in this field must have a wide view, not forgetting that terrorism is not only a phenomenon involving individuals from other cultures and countries but also national activists with extreme political views, and that the sources of recruitment are not only mosques but also frequently prisons.

Terrorism is deeply intertwined with financial crimes and document fraud whilst using the internet for their criminal business. Apart from cooperation with other specialists, some basic knowledge on these areas is required also for anti-terrorism experts.

Law enforcement exercising their duties may experience a dilemma when taking security measures whilst simultaneously aiming at respecting the rule of law, democratic principles and fundamental rights. This also concerns those situations where they need to establish whether a person is an autonomous terrorist or was forced to terrorist action.

b) Training needs

Summary

For counter-terrorist actions, both combat and prevention in the shape of de-radicalisation are highly relevant, which implies the need of a large set of skills for investigators, counter-terrorism specialists and community police. An understanding of the psychology of terrorists,

their political and religious motivations as well as their place in society, in the case of foreign terrorist fighters/returnees, needs to be understood for effective police interventions. Technical and legal issues around investigations as well as the financing of terrorism naturally require attention, and there, particularly OSINT, social network analysis and the use of EU databases are tools and methods of choice. The protection of critical infrastructure and soft targets requires scenario training as well as the development of threat assessment skills. In addition, international and interdepartmental cooperation and the links to other types of crime must be addressed.

Further details

The experts stressed that the need for transfer of fact- and evidence-based knowledge requires that content is nurtured by research findings.

Apart from a thorough knowledge on terrorism, its possibilities and threats as well as counter-strategies and methods, the exchange of good practice between EU Member States and beyond – as terrorism is a global threat – is imperative involving representatives of countries with a lot of counter-terrorism experience and proven and tested policies. Scenario training has been highly recommended, and it should include basic knowledge elements in order to ensure a common understanding, e.g. as the definition of terrorism.

Training should follow a multidisciplinary approach bringing together investigators in other crime areas, risk assessment and frontline officers, judges and prosecutors, customs and tax officers, and, where relevant, representatives of private companies, such as the banking sector, and other financial experts. The need of knowledge on CBRN defence issues implies the usefulness of inviting the expertise of specialised organisations such as the International Atomic Energy Agency (IAEA). Disaster Victim Identification (DVI) units must also receive training on this topic as they are often the first ones to be involved, even before an incident has been identified as a terrorist attack. First responders should receive regular refresher courses, even if there are no immediate threats. In both DVI staff and first responder training, awareness on terrorism, early signs, indicators, and cultural issues as well as cooperation options with other professionals must be part of the content.

Training on counter-terrorism is available being a regular element in CEPOL's Annual Programme, and it was stressed that this should be maintained and even reinforced.

EU-level training is available concerning subjects like fighting and preventing terrorism, identification and de-radicalisation of foreign fighters, links between terrorism and organised crime as well financial crime by CEPOL, whilst eu-LISA provides an important contribution by training on SIS, VIS and Eurodac as supportive tools in this fight.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Counter-terrorism related training.

1	*Terrorism prevention, de-radicalisation and disengagement ("Lone wolves": understanding the nature of the phenomenon; exchange of good practices; cooperation with the government and the private sector; local and community approach; stronger cooperation with experts from the private sector; terrorism with Islamic roots; extreme right wing; strategies/methods; exchange of experiences; community policing; understanding all the aspects of terrorism)*
2	*Foreign Terrorist Fighters and Returnees (sources of recruitment of Foreign Terrorist Fighters; how to deal with returnees: identification and profiling, risk assessment; strategic issues [EU policy]; how to use returnees for disengagement of potential FTFs; exchange of information; best practices; how to deal with returnees and their families; minors [FTFs and returnees]: how to deal with minors, age issues and how to establish their age; fundamental rights)*

3	*Radicalisation (ability to read the signs and recognise terrorism: basic knowledge on indicators, cultural, regional aspects; community policing: links to mosques, shops, communities, evidence of radicalisation; at senior Level: background knowledge on radicalisation theories; OSINT as a tool for evaluation and analysis of trends in society with regard to radicalisation etc.)*
4	*Investigations, encryption and e-evidence (raising awareness and promote the use of the existing tools and platforms to exchange information and encourage coordination at multilateral level; exchange best practices and modus operandi with governmental organisations, even broader than the EU; legal arrangements in the context of investigations; use of battlefield information as evidence; JITs and joint operations involving non-EU countries; alternatives to prosecution and conviction in terrorism cases)*
5	*Critical infrastructure protection and protection of soft targets (scenario training: distinction between hard targets and soft targets; threat assessment of most likely soft targets; data analysis; procedures – security measures; use of CCTV [what can be achieved with these – not the legal framework])*
6	*OSINT (use of modern resources [internet etc.] and social network analysis. Exchange of experiences; presentations by specialists [data mining, tools etc.]; importance and ways of sharing intelligence; databases (PNR), interoperability of systems [SIS, VIS, Eurodac, ETIAS, EES, ECRIS]; include experience gathering from private companies)*
7	*Terrorism financing (modi of money flows and alternative banking systems, incl. hawala, role of charities; crypto-currencies and new payment methods; money coming from other types of crime [THB, drug trafficking, cigarette smuggling] with the purpose of raising funds for terrorism [links to other serious crimes]; knowledge on each other's different frameworks at operational level; FATF 40 Recommendations, in particular 9 Special Recommendations on Terrorist Financing; include participants from the judiciary and prosecutors; involvement of the banking sector and other financial experts, customs and the tax office)*
8	*Chemical, biological, radiological and nuclear defence (CBRN or also CBRNE); (the reasons that could lie behind such an attack [psychological, legal, other issues]; the means used; does the means lead to an offender profile etc.)*
9	*Fundamental Rights (respect for the Rule of Law and democracy; chain: investigation, accusation, trial, conviction; human values; identification of victimhood of a person used for/forced to terrorist actions; dilemma between security measures and human rights; policies and practises for providing support to victims of terrorist attacks and alternatives to prosecution and conviction in terrorism cases)*

Europol`s European Counter Terrorism Centre`s (ECTC) proposed an alternative order of priorities as follows: 1.OSINT and Social Network Analysis 2. Investigations, Encryption and e-Evidence 3. Foreign Terrorist Fighters and Returnees 4. Terrorism Prevention, De-radicalisation and Disengagement 5. Radicalisation 6. Terrorism Financing 7. Critical Infrastructure Protection and Protection of Soft Targets 8. CBRN, CBRNE 9. Fundamental Rights.

ECTC's justification for favouring an alternative order of priorities is grounded in the fact to almost all terrorist attacks in the EU there is a strong internet dimension, and it is a real challenge for law enforcement agencies to address the technical hurdles of a highly volatile environment whilst striving to collect information in a constant changing landscape. The amount of digital data investigators are confronted with are huge, and the size, complexity, quality and diversity of these data sets require specialised investigation techniques and data processing applications. Handling digital evidence (e-evidence) needs special training and a certain level of understanding by both the investigators and the prosecutors/ judges.

2.3 Trafficking in Human Beings

2.3.1. Environmental Challenges

Human traffickers increasingly use the internet, including social media and the darknet, as a tool for recruitment monitoring and advertising the sexual services of victims. Still, cooperation between THB investigators and cyber-crime investigators is not yet everywhere part of standard procedures. Also, the lack of common tools for investigation and monitoring of social media together with legal constraints (different per Member State) hamper this type of investigative work. Whilst cooperation with labour inspectors is generally good, international cooperation is partially hindered by the fact that inspections on workplaces such as construction, agriculture, catering, etc. sites take place at different frequencies in the individual Member States and that the mandate on labour inspection lie with different bodies. The cooperation between law enforcement agencies and NGOs in the case of child victims requires improvement. Cooperation with private companies is important, and difficult as they are not always open to disclose information.

In the case of forced as well as sham marriages, national marriage laws differ, which can lead to problems for prosecution. At least a common definition and distinction of forced marriages from sham marriages would help as well as inclusion of the latter as a form of THB in relevant legislation in all countries. For gathering evidence, the investigators often focus on the victim's statement. In order to take the burden from the victim in this process, a change of the legal possibilities for obtaining other evidence should be made available, which would require a change of legislation.

The effectiveness of prevention campaigns is difficult to assess. A relevant question is whether THB investigators should be known in public and therefore participate in preventive information sessions, e.g. at schools.

2.3.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Typically, victims of labour exploitation are hard to identify as they are often not aware they are being exploited. A lack of knowledge of frontline officers and border guards on this phenomenon as well as on the cultural backgrounds and language of victims negatively impacts victim identification. With young children and minors, the communication and victim interviewing skills of law enforcement officials require improvement. Connections to other types of crimes also have relevance for victim identification, e.g. children and minors involved in petty theft instigated by groups engaged in Organised Property Crime. Cooperation with NGOs is lacking or sometimes completely absent.

The internet has become an important source of recruitment for all forms of exploitation, including sham marriages. A lack of qualified experts and of a common software tool for monitoring and investigating social media and other platforms is the great challenge here. Communication with cyber-experts is sometimes difficult due to the specific terminology they use and due to their separation from THB investigators in the organisational structures.. Furthermore, these often focus on child exploitation on the internet, not on THB.

Cooperation with financial investigators and Asset Recovery Offices (AROs) is not a common procedure everywhere, whilst with prosecutors and judges the problem is often that, where there is no relevant legislation or a clear definition distinguishing between THB and migrant smuggling, they tend not to recognise cases as THB. Finally, international cooperation implies the need for means to share intelligence and the support by EU Agencies. Knowledge on such possibilities is often lacking.

b) Training needs

Summary

THB is very multi-faceted involving a large variety of victims, links with other types of (organised) crime and requiring attention from a multidisciplinary group of professionals. Therefore, training needs include labour exploitation, forced and sham marriages, child exploitation as specific types of THB. Next, links with other types of crime and consequently the cooperation with other investigation units feature as an important element, (financial and cyber-investigation, document fraud). In addition, investigation tools and methods as well as intelligence analysis, cooperation with NGOs and civil societies, and victims' rights are considered elementary for training of investigators. Exchange of good practice at EU-level would be beneficial.

Further details

For this topic, contributors to the assessment place an emphasis on the importance of Train-the-Trainers' type of activity and training packages for THB experts on different sub-topics including victim identification, forced and sham marriages (including frontline officers), online investigation, financial investigation and asset recovery, links with other types of crime, and the difference between THB and human smuggling. Investigators working in other fields should be trained to recognise THB, in order to be able to identify victims and involve a THB expert.

The second issue highlighted is the need for a general EU-level training for prosecutors and judges, touching on the THB matters as listed below, or for joint THB courses aiming at investigators and prosecutors, with the purpose of strengthening cooperation. Other joint training was suggested with NGO staff, civil society (hospital staff, flight attendants etc.), labour inspectors, and cyber-crime and financial investigators.

Examples of existing training is the one-week theoretical and practical live exercise organised by the Organisation for Security and Cooperation in Europe (OSCE) in Italy in 2016 and 2017 which simulated practically all kinds of elements in such case work. Courses on labour exploitation are provided by CEPOL whilst Frontex offers training for border guards on labour exploitation indicators. Austria and Latvia have indicated that they organise training on this topic involving experts from private companies and labour inspectorates. Frontex is developing a child protection course for first and second line border guards. Courses on cooperation with financial investigators are part of CEPOL's annual programme, and Europol trains financial investigation skills. Webinars on victim identification could also be useful.

Europol pointed out that sexual exploitation should be explicitly mentioned as training priority area as still there are characteristics of the crime (for example the Voodoo method for Nigerians or the intra EU trafficking) that demand to continue the efforts on training and awareness. Furthermore, human smuggling should feature among links to other types of crime as migrants are a potential source for various forms of exploitation. European Institute for Gender Equality (EIGE) proposed to include the topic of victim protection among training priorities.

EU-level training is available concerning subjects like different types of THB, e.g. labour exploitation, child trafficking, links with other types of crime, like financial crime, cyber-crime, migrant smuggling and document falsification offered by CEPOL and Frontex, whilst Frontex and EASO also provide Train-the-Trainers activities in this domain.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Trafficking in Human Beings related training.

1	*Labour exploitation (training for frontline officers and border guards to identify potential labour exploitation victims; training on cultural differences; best practice for THB experts; involving labour inspectors.)*
2	*Child trafficking (training on communication with children, also for judges and prosecutors; identification of trafficked children; better cooperation with social NGOs, labour inspectorates; social media monitoring)*
3	*Victim identification (links and difference between THB and illegal immigration and human smuggling; evidence gathering, alternative evidence, victims' rights, also for prosecutors, judges and labour Inspectors; collecting evidence and interviewing techniques targeted at different forms of THB and different categories of victims; financial investigations/skills)*
4	*Intelligence analysis (joint training for the national points of contact in EU and international agencies; available tools; databases; services by international agencies; victim identification; awareness for THB as part of OCG crimes; connection with other crimes to which victims are forced)*
5	*Financial investigations and operations, and asset recovery (training on available EU tools; European Investigation Order; financial flows; dismantling of OCGs; banking; business models; behaviour patterns of OCGs; financial investigations and AROs; cross-border dimension on asset recovery; use of intelligence-led investigations including financial investigations, as this can provide a diversity of evidence to be used in addition to victims' testimonies; preferably Train-the-Trainers' type of activity.)*
6	*Rights of victims (need for training to ensure interests/rights of victims in criminal proceedings: interviewing techniques of victims [traumatised persons, children], victim identification and referral for support; finding alternative ways to evidence gathering instead of victims' testimony; need for national and EU-level training for law enforcement officials, prosecutors as well as judges as they safeguard victims' rights and interest during the proceedings)*
7	*Online and social media (Train-the-Trainers on online investigations; cyber-crime experts can be trained for THB indicators; available tools for internet monitoring and OSINT; cooperation with private companies, judges, prosecutors; communication with cyber-specialists; use of social media; prevention, awareness campaigns, exchange of practices. Information collection and exchange with non-EU countries, basic online investigative skills for THB investigators)*
8	*Prevention (exchange of good practices; common EU campaign; need to adapt campaign as traffickers' modus operandi changes; need to measure effectiveness; multi-agency/multidisciplinary approach)*
9	*Forced and sham marriages (general training , including for judges and prosecutors; establishment of indicators and specific methods for investigation focused on the features of sham and forced marriages and on social media in this context; general knowledge and understanding of the phenomena; how to raise awareness campaigns; how to teach social sectors; Train-the-Trainers to further conduct training in the national language at EU level for frontline officers; interlinkage with the topic of migrant smuggling is strongly needed as the method is also used for facilitated illegal immigration)*
10	*Document fraud (for frontline officers, prosecutors, investigators involved in THB)*
11	*Links to other crime types (drugs, firearms) for frontline officials (general training for frontline officers including indicators of other crime, in addition to victim identification; general/awareness training for investigators working in other crime areas)*

2.4 Cyber-Crime – Child Sexual Abuse and Sexual Exploitation

2.4.1 Environmental Challenges

Online Child Sexual Abuse and Sexual Exploitation (CSA/CSE) is a relatively recent topic. It requires high level of expertise that can deal with the rapid changes of tools and modi operandi. Number of cases is very high, especially compared to human and technical resources available. Member States should have adequate high-tech hardware and software at their disposal for the identification and extraction of e-evidence enabling their authorities to work and cooperate using comparable evidence of that nature.

Cross-border cooperation is an issue. On the one hand harmonisation of legislation with regard to cyber-investigation would be required to make the work of law enforcement officials as well as cross-border cooperation and sharing of e-evidence easier. Differences in data retention time per country, for instance, creates problems. On the other hand, more cases should be investigated on international level; for example live streaming of child sexual abuse, each country investigates the suspects mainly at national level. It was suggested to create a permanent task force at Europol who could try to understand the best way to investigate and to identify victims online. Another challenge is specifically the cooperation with South East Asia (e.g. Philippines), as there is either no cooperation partner in place or the cooperation is not functional.

Prevention in the context of CSA/CSE is a very specific challenge as it involves also parents and the need for age-related instruction of children. Furthermore, field officers lacking prevention expertise need to cooperate with specialised prevention officials, who sometimes have no knowledge of the topic. Law enforcement officials must also cooperate with NGOs.

2.4.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Due to the rapid development of this type of crime over the past few years, staff in some countries have multiplied, requiring high quality training that is not always readily available. Continuous challenges in relation to the rapid changes in modi operandi include constant updating, the encryption of hard drives and cloud services, anonymization, and the fight against person-to-person distribution of CSA/CSE material. The collection and exchange of data is made difficult by hidden IP addresses, unknown administrators, and the quantity of material. Another issue is that law enforcement officials should have proper understanding of the psychology of the offender for undercover activities. Cooperation with the private sector, in particular Internet Service Providers (ISP) and Email Service Providers (ESP) needs to be improved.

b) Training needs

Summary

Training should focus on darknet investigation and data collection techniques and tools, specifically, OSINT, e-evidence and social media analysis. Training should address the combat of live streaming of child sexual abuse and the removal or blocking CSA/CSE material. Offender psychology to use for undercover activities, and interviewing techniques are also mentioned as relevant training needs. Training could also help further cooperation with financial investigators, IT specialists, forensic experts and judicial staff. Prevention is mentioned as a highly important and sensitive issue, for which training of field officers and/together with prevention officials would be useful.

Further details

The tenor is that existing EU-level and national training is not enough, and that therefore an EU Train-the-Trainers' type of activity could lead to enhanced national training, e.g. on victim identification, removing and blocking CSA/CSE material, handling of perpetrators etc. EU-level courses on such topics are already provided by CEPOL but as they can only be attended by one person per Member State at the time, this does not fulfil the countries' need of well-trained staff. Training on OSINT, social media analysis, victim identification, psychology of offenders

as offered by Europol (COSEC[17] Course) should be more in-depth, e.g. a two-step course going from a beginner to a more advanced level. INTERPOL offers a course on victim identification that is similar to the CEPOL course, and some of this training also exists at regional level within the EU. It is specifically noted that the content of such training should include ways of cooperating with South East, e.g. by means of liaison officers from other countries, in case there is no liaison officer representing the investigator's own country. All this should include the exchange of good practices in the different countries, e.g. on the identification of victims in the context of live streaming as well as on securing, obtaining, handling and exchanging e-evidence. Experiences with workflow changes, the enhancement of technical skills and knowledge of investigators around these and other cyber-investigation matters should be addressed. Equally, sharing good practices on undercover operations is considered useful, not only EU-internally but also involving the USA. This type of training should include the legal frameworks in different countries as a topic, and prosecutors as participants. The same is valid for training on undercover operations and countering live streaming.

Cooperation with the private sector, in particular ISPs and ESPs needs to be improved by increasing the knowledge of law enforcement official on their activities. In addition, by means of the involvement of prosecutors and judges, training should provide opportunities for law enforcement officials to discuss methodologies to ensure that the gathering of e-evidence takes place pursuant to current legislation, so as to allow its admissibility in court proceedings

When speaking of prevention, a proposal was made for awareness training both for field officers, who could be involved in prevention campaigns and measures, as well as for prevention officials so they will understand more about CSA/CSE. Participation could be enhanced by doing this via webinars. Furthermore, EU-level training allowing an exchange of good prevention practice could lead to the development of an EU Prevention Package. Also, the higher administration levels could benefit from a more thorough understanding of the importance of prevention.

An overview of existing training on the diverse topics concerning CSA/CSE would be appreciated.

According to Europol, categorisation of training needs may lead to false expectations on behalf of the Member States, e.g. victim identification training identified under OSINT and social media analysis may attract the wrong type of student to the trainings.

EU-level training is available concerning subjects like methodologies to fight against child sexual exploitation on the internet and also victim identification, offered by Frontex and CEPOL, whilst Frontex organises training on child protection as well.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of sub-topics in the area of Child Sexual Abuse/Child Exploitation related training.

1	*Combating online violence, distant child abuse and live streaming (undercover operations online; tools and mechanisms, including the potential of EU agencies, in particular Europol; experiences from other countries; data protection; human rights)*
2	*Darknet (undercover operations on darknet and deep web; securing, obtaining and handling of e-evidence; anonymisation; new trends; removing material)*
3	*CSA/CSE investigations (behaviour of offenders; interviewing techniques; data encryption; international cooperation and information exchange; involving IT, forensic and psychology*

[17] Combating Online Sexual Exploitation of Children

	experts; data retention; intelligence gathering and analysis; sharing of operational best practices; involving the judicial community and the private sector; data protection; human rights).
4	*Prevention of CSA/CSE (countries with good prevention campaigns to share their experiences with others; EU prevention package; prevention campaigns for law enforcement agencies and judicial authorities; information exchange between law enforcement authorities and border control authorities)*
5	*OSINT and social media analysis for victim identification (in-depth training on OSINT and social media analysis; technical skills; best practices; cooperation with non-EU countries and the private sector; data protection; human rights)*
6	*Financial investigations in relation to CSA/CSE (money flows; cooperation with FIUs; financial intelligence)*

2.5 Criminal Finances and Money Laundering

2.5.1. Environmental Challenges

The different judicial systems between EU and non-EU countries create a problem that has a negative effect on investigation and cooperation. Setting up JITs that can include non-EU countries might create possibilities of enhanced collaboration.

In some cases, there is even a lack of a legal framework, mainly due to rapid technology developments, e.g. virtual currencies. Also, the legislation on crime enablers such as money mules and cash collectors could benefit from harmonisation between EU countries.

Data protection and retention naturally is an important and often problematic issue in this context, it being subject to national legislation. This affects the sharing of information between law enforcement authorities.

2.5.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Combating financial crime implies the need for a multidisciplinary approach. Unfortunately, the exchange of information between the different stakeholders, in particular of financial data is problematic. Also, the cooperation with non-EU countries is often difficult but highly necessary.

Checking potentially false documents of cash carriers and the authenticity of a company cannot be done fast. Excellent knowledge, including the fact that non-fraudulent documents can contain false data, as well as rapid exchange of information is required to reveal document fraud cases.

As it is inherent in financial crime and money laundering that they are linked with other types of organised crime, cooperation with other investigation units or other types of law enforcement sectors, e.g. customs, is imperative.

b) Training needs

Summary

The training needs mainly encompass investigation methods and techniques including undercover operations, intelligence collection and analysis, etc. as well as new technologies including cyber-investigation. Also training on the tracing and recovery of proceeds of crime are mentioned here. Further important issues are trade-based money laundering, modi operandi, crime enablers, hawala, and new online payment methods. International cooperation is considered a must, and in particular the use of JITs and the knowledge of the

type of support EU agencies can offer. On the level of prevention of money laundering, the sharing of good practice could be effective.

Further details

In order to improve cooperation between different professional sectors involved, joint multidisciplinary training, including law enforcement, judiciary staff, the tax and the banking sector, could help. This, however, might not be sufficient as, in fact, more exchange of information and of good practice would be required, even involving the enhancement of communication with heads of unit and prosecutors. Joint training would also be beneficial for law enforcement officials investigating other types of crime and prosecutors so they gain a more thorough understanding of financial investigation and asset recovery.

Changes in the types of organised crime groups (OCGs) and a need for OCG mapping as well as developing an understanding of their cross-border links represent a challenge whilst at the same time their modi operandi evolve in line with modern day technologies. This is particularly valid for different types of fraud, like investment fraud and mass marketing fraud, where the methods of OCGs are manifold and highly sophisticated and where a high number of countries is involved.

For investigators, there is a need for specialised training on different topics, but also for basic training on new technologies (including evidence gathering) and virtual currencies, involving IT specialists. A Train-the-Trainers' type of activity could help cascading this type of knowledge more rapidly at national level. The same is valid for training on crime enablers and money laundering syndicates. The lack of knowledge on money mules can be solved by training.

Generally, the exchange of good practice, tools and trends is considered useful, and in particular for investigative practices and intelligence collection.

CEPOL already provides a series of EU-level training activities on this topic, including financial investigation and asset recovery, money laundering, following the money, alternative banking and payment methods, etc., however more EU-level training would be needed.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Criminal Finances and Money Laundering related training.

1	*Tracing and recovery of proceeds from crime (freezing and confiscation of criminal assets; international cooperation)*
2	*Financial investigations (specialised training for investigators and prosecutors on financial investigations and cryptocurrencies; new technologies; darkweb; virtual currencies; anonymous payment methods; cooperation with private sector)*
3	*Joint Investigation Teams addressing criminal finances (international legal assistance; role of EU agencies; cooperation with non-EU countries; funding possibilities)*
4	*Money mules and crime enablers (modi operandi, mutual legal assistance; different typologies; cooperation with private entities; alternative banking, hawala; cooperation with non-EU countries)*
5	*Intelligence analysis (trends and new developments; collect, share and exploit relevant data and knowledge)*
6	*Document and identity fraud (mainly for first responders, how to detect and identify, best practices; forged non-ID documents [invoices etc.]; investment fraud; financial instruments; cooperation with private sector)*
7	*Prevention of money laundering (awareness raising campaigns to law enforcement, the judiciary, the public and private sector; identification and sharing of good practices including case studies from investigations and prosecutions, trade-based money laundering; gold and precious metals as means of money laundering)*
8	*Undercover operations (recruiting and handling of, dealing with informants; intelligence collection and sharing abroad; good practices)*

2.6 Cyber-Crime – Attacks on Information Systems

2.6.1 Environmental Challenges

Identified challenges in this subject area concern issues like differences in national legislations – in particular in the area of data protection and of admissibility of e-evidence obtained from another country –, awareness of the public sector of network attacks, and better coordination, for instance, between the Joint Cyber-crime Action Taskforce (J-CAT) and law enforcement. For the latter, it would be necessary to first identify the best procedural practices and draft corresponding guidelines.

For cyber-incidents, and in particular for major cyber-attacks, cooperation with the press for public communication would be highly important. In this context, also a common cyber-incident response protocol would be beneficial for better cooperation and a more efficient and coherent response by officers throughout the EU. In support of this, a network as well as a contact list of first responders would be useful.

Further mentioned is the lack of a common approach when investigating criminal networks as well as the need for the creation of efficient communication channels, including common methodologies in the area of intelligence gathering and processing.

In the domain of cyber-security and hybrid threats as well as cyber-espionage, cooperation with the private security companies must be improved: many companies lack the willingness to share information.

Prevention requires cooperation with prevention specialists, and public/private prevention partnerships would be useful. Public awareness and knowledge on data protection requires reinforcement.

It would be important to ensure access to suitable high-tech hardware and software for the identification and extraction of e-evidence.

2.6.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

A global framework for the incident response process between the law enforcement agencies would be very beneficial especially via virtual simulations. For technical reporting law enforcement officials would require special forensic expertise and the capability to extract, handle and share e-evidence and data whilst coordinating their work with other actors involved (private sector, prosecution, judiciary, victims); for tactical reporting, law enforcement officials with coordination capabilities would be necessary. Coordination with European Union Agency for Network and Information Security (ENISA) and Computer Emergency Response Teams (CERTs) is considered important.

When dealing with cryptoware and ransomware using encryption, officers often lack knowledge on malware detection and analysis. A common analysis framework is missing, which also affects other types of crime. More knowledge on en- and decryption is required, and there is a strong need for high-level technicians in the area of cyber-investigations.

Collaboration between Critical Information experts amongst themselves and with the public sector could be reinforced by live exercises at EU level involving the different actors in cyber-attack investigations.

For digital forensics and e-evidence, highly specialised forensic tools and techniques are used and they enable law enforcement staff to investigate criminal networks. This implies a strong need for forensic capacities with knowledge on the latest technologies used by such criminal networks.

b) Training needs

Summary

Identified training needs focus on cyber-investigation techniques and tools as well as undercover operations in the darknet, analytical tools, techniques in the area of digital forensics and e-evidence, and of the investigation of network attacks, DDoS attacks and encryption. Furthermore, cyber-intelligence handling, malware detection and analysis, intelligence gathering and analysis in the context of the protection of critical infrastructure as well as in the case of cyber-security and hybrid threats are listed. Cooperation of law enforcement with Europol (EC3), European Cyber-crime Training and Education Group (ECTEG) and J-CAT should be addressed in training as well as information exchange channels at EU level. Prevention as a training subject is considered relevant in the context of cooperation with and awareness-raising of the private sector and the public, e.g. by cooperation with the press and other campaigns.

Further details

Cooperation with the public and private sector and the Computer Security Incident Response Teams (CSIRT) as part of EU live exercise training focusing on the use of methods could involve the following levels:

a. Tactical training: using cyber-simulators to set different cyber-scenarios;
b. Technical training: cyber-expertise, digital forensics expertise;
c. Management level/judiciary level/prosecution office: basic knowledge for better coordination of cooperation with law enforcement;
d. Cooperation with public and private sector in cyber-incident aspects.

EU-level 2-step training in the area of cryptoware and ransomware using encryption is considered useful:

- Step 1: First Responders – law enforcement responding to a call from private sector;
- Step 2: Cyber-investigators – identification of OCGs.

A Train-the-Trainers' type of activity on different topics at EU level is also considered useful and necessary for cascading of knowledge at national level.

Where intelligence and operational aspects are addressed in EU-level training, this should be done in a way that facilitates advanced learning. For digital forensics a live forensic analysis exercise would be beneficial. This could be preceded by preparatory training by means of e-learning modules whilst intermediate and advanced level training would be done in residential activities. Also, advanced data extraction should be taught by means of EU training.

Joint training with prosecutors and judges would ensure that e-evidence is gathered pursuant to current legislation and is therefore admissible in court proceedings. And finally, cyber-investigation is a horizontal issue and should therefore be included in all training on other types of crime investigation.

In this area CEPOL, in joint efforts with Europol, already provides EU-level training activities on OSINT and IT-solutions, operational intelligence analysis, advanced Windows file systems, cyber-crime and cyber-investigations, cyber-security, cyber-forensics and social media implications. This however does not cover the high demand of training. The Training

Governance Model developed by entities taking part in cyber-crime related training will provide a systemic approach of training with the European Union.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Cyber-crime – Attacks on Information Systems related training.

1	*Cyber-investigations in general (Information exchange mechanisms, SIENA, role of EU agencies, data analysis, crime-as-a-service, investigation of criminal networks, modus operandi, crime-as-a-service, information collection and exchange with non-EU countries, multidisciplinary approach, cooperation with prosecution and judiciary, JITs, data protection)*
2	*Digital forensics and e-evidence (analysis in different operating systems, in cloud, data extraction, data protection, data retention, new technologies: cloud computing, cryptocurrencies, block chains, encryption, Big-data, Internet of things, autonomous systems, evidence securing, connections between machines, cooperation with private parties)*
3	*Investigation of Network attacks, DDoS attacks (use of methods and not oriented to the use of tools (avoid dependence of tools), tactical - using cyber-simulators with the capacity to set different cyber-scenarios, technical, digital forensics, EU 'live-exercises' to promote closer cooperation and coordination process between public-private sector and "Computer Security Incident Response Team's.)*
4	*Cyber-intelligence (analytical tools and intelligence packages, how to interpret data, best practices exchange, cooperation with J-CAT and European Cyber-crime Centre, crime-as-a-service, data protection)*
5	*Protection of critical infrastructure (first responders, intelligence gathering, analysis, cooperation channels and entities, sharing of best practices, common cyber-incident response protocol, data protection)*
6	*Cyber-security and Hybrid threats (intelligence gathering ad analysis, international information exchange channels and tools, Cyber-espionage, new technologies, cooperation with private sector and different intelligence entities, cyber-security cases studies)*
7	*High level OSINT and social media analysis (techniques and tools, 'Free-tools' software, use of existing EU tools and information exchange mechanisms, cooperation with Europol and ECTEG, public communication of Cyber-Incidents)*
8	*Undercover operations on darknet (techniques, cooperation with Europol and ECTEG, best practices)*
9	*Prevention, cyber-awareness (community policing training in the area of cyber-and cyber-awareness, communication with private sector, media, showman capabilities, EU prevention campaigns, best practices)*
10	*Malware investigations (first responders, different scenarios, malware detection and analysis, identification of organised criminal groups who are behind, 'Block chain' investigations, financial investigation elements, cryptocurrencies, data protection)*

2.7 Illicit Trafficking, Distribution and Use of Firearms and Explosives

2.7.1 Environmental Challenges

Cooperation between competent authorities leaves room for improvement. One of the reasons for difficulties here is the difference in national legislations and a wide spectrum of national authorities dealing with this phenomenon. Due to the plurality of actors involved, like forensics, investigators, intelligence, and licencing authorities, the existing knowledge is quite dispersed and applied practices differ, which does not foster cooperation.

In addition to the above, on the political level there is a strong lobby pressure from the private sector, which did not support the new Directive. This results in private companies not being

willing to cooperate with the law enforcement or making cooperation lengthy and not sufficiently productive.

More challenges relate to the legislative aspects, e.g. the situation around precursors and control of chemicals is complicated due to the fact that not all Member States implemented the relevant regulation, and there are different loopholes in licencing systems. Related to this, not all Member States have set up Focal Points to ensure better communication when receiving information and answering requests.

Finally, it was also noted that there are several EU initiatives that support fight against firearms trafficking, but the level of bureaucratic procedures does not always allow to apply for and/or to benefit from the projects.

2.7.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Combating firearms trafficking requires a multidisciplinary approach. Unfortunately, the exchange of information between the different actors is not flawless. Knowledge on available cooperation instruments and opportunities, especially towards non-EU countries, is often not sufficient and slows down the investigations. Moreover, understanding trafficking routes, modus operandi and reasons and being able to link them with other crime areas is essential in combating serious and organised crime in general and firearms trafficking in particular.

It is equally important for law enforcement officials to possess an adequate level of knowledge in the domains of cyber-, false documents and criminal finances, and to be able to relate this to and apply it on the daily basis whilst investigating firearms trafficking.

b) Training Needs

Summary

Training needs to encompass general aspects of firearms trafficking, detection methods and investigation techniques, including undercover operations, false document detection and open source intelligence. International cooperation is a further topic, starting from a general knowledge of the type of support the EU agencies can offer, e.g. cooperation instruments like JITs, and especially their application in relation to non-EU countries. Firearms-specific elements have to be included in first responder training as further success of the investigation strongly depends on the quality of work at the crime scene. Also, ballistic experts should be sufficiently equipped with the most recent tools and knowledge allowing to use them. On the level of prevention, sharing of good practices would be effective to foster inter-institutional cooperation and decrease the crime.

Further details

Consulted experts acknowledged the need for training and underlined that efforts have to be made at both national and EU-level. EU-level training should feature new policy and operational developments including changed modi operandi and new EU legislative instruments, i.e. the new Firearms Directive (on the control of the acquisition and possession of weapons), newly established deactivation standards, but also tracing mechanism as derived from the United Nations (UN) Protocol. Joint training with border/coast guard and customs authorities, forensic experts as well as judiciary and prosecution would be beneficial to better understand the procedures and each other's role and requirements.

Taking into account the external dimension of the phenomenon, relevant Policy Cycle elements in general and firearms trafficking in particular should be covered in pre-deployment training of CSDP mission personnel.

Training on JITs, with a particular focus on cooperation with Western Balkan countries, and support by Eurojust is deemed important. Similar but insufficient training already exists supported by Eurojust, Europol, CEPOL, EJTN, and European Academy of Law. Accessibility and frequency of such training should be reinforced. A Train-the-Trainers' type of activity and subsequent sharing of knowledge to the national level would be useful here. This could also be valid for training on OSINT and darknet as in spite of available EU courses by Europol and CEPOL such courses still are high in demand.

Some further aspects such as tracing mechanism, recognition of weapons, particularly firearms as well as its parts and the ammunition if eligible, forbidden, under control measures, duly deactivated, etc. should be included among training needs according to Frontex.

Ballistic experts need to have an opportunity to exchange experiences and best practices with colleagues from other Member States, as well as to learn about new developments, enhancing the awareness about the different automated ballistic systems, their potential and data protection. Forensic workshops with the purpose to set up a technology watch at EU level, to identify manufacturers, import circuits outside the EU etc., giving an update of state of play of the situation at EU level and involving forensic experts, are important.

In addition, more information and potentially training on EU project and EU funds management would improve project implementation and boost operational performance.

Finally, such a self-explanatory aspect of danger of weapons in general, should not be neglected, and covered by all law enforcement training initiatives as legal weapons also lead to crime.

EU-level training activities on this issue seem to be mainly provided by CEPOL and Frontex, including cross-border investigations and strategic aspects in this context, firearms trafficking at external borders, firearms trafficking in the darknet, improvised explosives as well as explosives in different environments, and the European Explosive Ordnance Disposal.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Illicit Trafficking, Distribution and Use of Firearms and Explosives related training.

1	*General aspects and changes in the modus operandi (New developments; involvement of non-EU countries; information exchange channels and mechanisms; role and potential of the EU agencies [Europol, Eurojust, Frontex: EUROSUR Fusion Services, PNR, SIENA]; new legislative initiatives and their implications and application, practical use of Europol`s tools)*
2	*Firearms trafficking investigations, incl. financial investigations (investigation and information exchange; inclusion of financial investigations and asset recovery offices; seizures; role of CARIN and EFE; joint training with border/coast guard and customs authorities)*
3	*Darknet and undercover operations (new payment methods, e.g. cryptocurrencies; alternative banking; potential links to terrorism financing; online trade)*
4	*OSINT (digital investigation techniques on open web; online trade, focus on sellers and buyers; intelligence picture on social platforms)*
5	*First responders training (detection; forensic techniques; crime scene investigation; securing of evidence; exchange of best practices and experiences)*
6	*JITs in relation to firearms trafficking (cooperation elements; role of Eurojust and Europol; cooperation with Western Balkans other non-EU countries)*
7	*Detection and investigation of document fraud in relation to firearms trafficking (new technologies for detection; identification of forged and inappropriately issued breeder documents)*

8	*Prevention (Enhancing existing projects; stronger cooperation with private sector; exchange of best practices in national campaigns related to safety and legal use of firearms)*

2.8 Organised Property Crime

2.8.1 Environmental Challenges

Organised Property Crime (OPC) is not treated as a priority in every Member State, which consequently leads to a lack of experts and financial resources assigned to its investigation. This is generally true, but also in particular for art theft and metal theft. The latter has now shifted to the southern Member States, therefore requiring a regional approach. In the area of stolen motor vehicles, a high turnover of staff and therefore loss of the required expertise is reported as a challenge. This type of theft requires highly technically qualified staff, who can establish relationships of trust with private companies (manufacturers). In many cases the support of Financial Investigation Units and AROs would be necessary. OPC experts in the EU-STNA workshop emphasised that asset recovery should be made compulsory in High Value Target (HVT) cases. For these cases a problem is identified in the fact that criminals can very easily change their identity in some non-EU countries, which implies a need of enhanced cooperation with these countries. An additional challenge is the different interpretations of the term in different countries.

When investigating online markets, the usual problem is the legislation, which differs per country and therefore hampers cross-border cooperation. It is also not conducive that only part of the Member States has ratified the Prüm Convention on the exchange of data, fingerprints and vehicle registration.

2.8.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

A challenge that could be countered by well-trained officers is the identification of OCGs and Mobile OCGs (MOCGs) involved in this type of crime, e.g. petty theft and domestic burglary, and in poly-criminality, specifically forcing trafficked minors to pickpocketing. This is, for example, highly relevant for determining the minors' status as victims and for ensuring their rights. In the context of domestic burglary, the recognition of involvement of an OCG would imply the need for cross-border checks and intelligence exchange with other countries.

The transportation sector, and consequently cargo theft, is increasingly targeted by followers of the crime-as-a-service business model, and will require qualified law enforcement experts. At present this is realised in the realm of cyber-crime but will increasingly affect traditional organised crime. A search tool for investigating online markets would be useful, and consequently also training on such investigation techniques including, undercover investigations in online markets. Also fencing should be part of training on criminal activities in the context of OPC.

Other types of OPC face different challenges. With ATM attacks, prevention is a highly important issue and a catalogue of good practice would be helpful, including cooperation with the private sector and preventive measures. Different profiles, risk of violence and lack of security in non-EU Member States are also mentioned. The difficulties with motor vehicle theft, on the other hand, lie in the lack of knowledge on modi operandi, the detection of stolen parts, and the need to use networks to reach car producers as individually that is very challenging.

HVTs usually are linked with MOCG, which have very specific cultural backgrounds; law enforcement officials need to understand these cultures in order to be able to identify them.

b) Training needs

Summary

For this type of crime, training needs are centred on (cyber-) investigation procedures and tools, including OSINT, and on modi operandi by MOCGs. Cooperation with financial investigators and AROs plays an important role generally. Joint training with financial investigators as well as prosecutors could foster trust and promote cooperation between the different units. Some training on this issue is provided by the CARIN[18]. Europol proposed that training should include alternative approaches to money laundering investigations in OPC cases, such as asset seizure and confiscation by equivalent value, multidisciplinary approach and use of civil liability.

Further details

Links with other types of crime, in particular the exploitations of minors in the context of THB and document fraud should be a training subject as well as measures against theft of cultural goods. Administrative measures and prevention to support the fight against OPC and targeted prevention were mentioned as training on this sub-topic is already a new initiative foreseen in the Operational Action Plan of the EMPACT Group on OPC. For training on investigation of HVT, it is also considered useful to involve prosecutors and magistrates via Eurojust and the EJTN as well as law enforcement officials from non-EU countries in order to ensure that linked OPC incidents are identified as such and are consolidated in one investigation and prosecution, not separately as isolated property crime incidents.

Training on MOCGs and their changing and most recent modi operandi, e.g. the use of drones, is considered highly useful the way it is already provided by CEPOL, as cross-border cooperation is very important here.

The international dimension should cover instruments for obtaining information on foreign criminal records (ECRIS), on the exchange of DNA and biometric data, on the application of supervision measures in the country of residence of the perpetrators (as an alternative to provisional detention), as well as on transfer of proceedings and of sentenced persons. The exchange of good practices when applying the Prüm Convention/Swedish Initiative in the different ratifying Member States is also considered as potentially helpful. Planned interoperability of the large scale IT systems (SIS, VIS, Eurodac, EES, ETIAS and ECRIS) will facilitate the work of law enforcement officials in this domain providing faster, more reliable and more complete access to information necessary to prevent, investigate, detect and prosecute criminal offences.

Furthermore, according to Eurojust's comments, training should include an introduction to the national legislation of the MOCGs source countries, particularly in relation to concrete investigative measures, as well as competent authorities to request those measures, e.g. controlled delivery, undercover investigation, cross-border surveillance, house searches, wiretapping, obtaining bank data and information on revenues and properties, obtaining DNA

[18] www.http://carin-network.org

and biometric data, criminal records, summoning and hearing witnesses/experts, temporary transfer of detainees.

EU-level training provided by CEPOL covers OPC committed by MOCGs and domestic burglaries. Every year the focus is on a different type of OPC. More training would certainly be appreciated.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Organised Property Crime related training.

1	*OPC investigations and phenomena in general (new changing modus operandi; use of drones; fencing; mobile organised criminal groups and their structure; intelligence of the use of on-line platforms; statistics; administrative measures; poly-criminality; specialist training on cargo theft; pickpocketing and the links to THB; ATM attacks; domestic burglary; different investigative strategies; information exchange on perpetrators; HVTs; Prüm and other instruments; best practice to ensure that linked OPC incidents are identified as such and are consolidated in one investigation and prosecution; obtaining information on foreign criminal records [ECRIS]; application of supervision measures in the country of residence of the perpetrators; transfer of proceedings and of sentenced persons.; introduction to the national legislation of the MOCGs source countries; competent authorities to request measures [controlled delivery; undercover investigation; cross-border surveillance; house search; wiretapping; obtaining bank data; obtaining information on revenues and properties; obtaining DNA and biometric data; criminal records; summoning and hearing witnesses/experts; temporary transfer of detainees])*
2	*Financial investigations and asset recovery in OPC cases (International cooperation; cooperation with prosecution and the judiciary; confiscating proceeds of crime; asset recovery; freezing orders; HVTs; involvement of non-EU countries; alternative approaches to money laundering investigations: asset seizure and confiscation by equivalent value; multidisciplinary approach and use of civil liability.)*
3	*Motor vehicle crime (modi operandi; cooperation with the industry; technical and forensic possibilities; cooperation instruments and channels)*
4	*Crime against cultural goods (identification and recognition of the restricted cultural objects; recognise potential risk objects; involving customs officers; data collection and analysis; identification of and information exchange on looted material; counterfeiting; fake and forged cultural goods; alert and train judicial and cultural authorities to the importance and scale of the phenomenon of illicit trade in archaeological objects; lessons learnt; successful prosecutions; information about the EU directives; better understanding of relevant laws in other countries; EIO; MLAs; International Letters of Request; SIENA; international cooperation and tools: ICOM and UNESCO; good practices; cross-border cooperation; new trends; online trafficking; investigating with IT tools; how to harness technological progresses against traffickers; deep web; OSINT; social media analysis; online sale platforms; financing of organised crime through the illegal trafficking of cultural goods)*
5	*OSINT (undercover investigations online; online markets; fencing; best practices; tools and techniques)*
6	*Administrative approach and prevention in OPC (administrative measures to support the fight against OPC; targeted prevention [potential victims]; including cooperation with private sector; new modus operandi; exchange of best practices)*
7	*Minors and links to THB (Identification of THB cases; interviewing techniques; age assessment; human rights; involvement of psychologists; minor victims or offenders)*
8	*Document fraud in OPC (develop the knowledge and expertise on the link between document fraud and OPC as well as on OCGs producing and providing fraudulent and false documents)*

2.9 Drugs – Production, Trafficking and Distribution of New Psychoactive Substances and Synthetic Drugs

2.9.1 Environmental Challenges

In the area of synthetic drugs, a huge challenge is created by the differences in legislation in the different countries. Legislators cannot keep up with the rapid pace with which, for example, New Psychoactive Substances (NPS) are brought onto the market. Some countries now have a procedure that includes new drugs immediately as they appear, others do not. A further issue, as with many other topics, is the difficulty in exchanging data against the background of data protection laws, which also differ per Member State. On the level of cross-border cooperation, the exchange of forensic data is also difficult.

Prevention requires a focus on schools and parents, and some thoughts must be given to the question how to raise awareness without increasing interest for experimenting with drugs. Law enforcement can be involved, but also medical staff and (former) drug users.

Cooperation with other sectors can meet with difficulties, e.g. with the private sector, e.g. shipping and freight companies, glassware producers, airlines, fast package companies (like UPS) etc. as they are not always willing to provide support. A further problem characteristic for international cooperation is the selection of HVT, when the priorities of the Member States differ due to the available capacities in smaller and larger countries. As for cyber-crime support in investigations, only some countries have darknet specialists in each team.

2.9.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The difficult cooperation with China for countering drug smuggling could be tackled by organising joint training activities with Chinese law enforcement officials. Other types of collaboration, e.g. interdepartmental with FIUs and cyber-crime units, are not yet standard procedure. Also, the support by private companies as mentioned under 2.9.1 and can be positively influenced, if representatives were invited to law enforcement training or through regular information sessions and meetings.

The lack of common databases, which are accessible by different types of law enforcement, and the knowledge on those that are indeed available, is a challenge in all types of crime. In this context the lack of regular feeding data into the common database with reference pictures that could help with the identification of mislabelling hampers investigations.

In the workflow of drug investigators, a problem arises when forensic examinations take a very long time. Forensics experts might become able to work faster, if their knowledge on synthetic drugs would be enhanced.

b) Training needs

Summary

Cooperation with financial investigators and the use of their tools are part of the training needs mentioned as well as profiling and identification of psychoactive substances and precursors. Furthermore, prevention and links to other types of crime, e.g. document fraud, are mentioned, but also more specialised training needs in the area of detecting illicit drug manufacturing and the dismantling of illicit laboratories. Safety and security procedures as well as data entry are important topics here. Cooperation with FIUs and AROs including the latest financial trends like cryptocurrencies and alternative banking deserve attention. Criminal profiling courses should focus on container and cargo shipments, profiling of companies and natural persons and facilitator recognition.

Further details

Suggestions were made to invite representatives from private companies as experts in law enforcement training with the purpose of improving cooperation with them. The same is valid for investigators of other types of crime, e.g. financial crime and cyber-crime, as they could obtain a general understanding of drug crimes. Also the reverse is valid: drug investigators should learn at least the basics or even a bit more details concerning financial and cyber-investigation. Estonia, Latvia, Poland as well as the Scottish Police College have started such training activities on financial investigations already, which can be used for benchmarking. INTERPOL and Europol have organised similar training activities. Darknet investigation is addressed in some national training (Austria, Belgium, Latvia).

The CEPOL 3-step training on the dismantling of illicit laboratories, in cooperation with Europol, is highly valued but should also include lab detection. Trainers, not just experts, should be engaged who first have completed a Train-the-Trainers' type of activity. Special Weapons and Tactics (SWAT) Teams training should include precaution measures. Furthermore, an annual webinar on the latest trends and data sharing via SIENA would be welcomed.

Practical training supported by a webinar on the detection of mislabelling practices would help law enforcement officials, in particular customs officers and border guards, to perform better threat assessment. There are initiatives within the OAP of the related EMPACT group, Sweden offers training on this matter and the webinar delivered by CEPOL on this topic in 2018 was successful and should be regularly repeated. Training on profiling of shipments should engage experts from source countries like China.

Prevention training could focus on personal safety of officers when dismantling an illicit lab including protection measures and first aid. Besides the joint 3-step training of CEPOL and Europol, mentioned above, Poland provides such training, and in some countries the Ministry of Health is in charge of this.

Apart from CEPOL and Europol's joint 3-step training activity on dismantling illicit laboratories, at EU level also training on synthetic drugs and precursors, drug markets and strategic analysis in this domain, the latter in cooperation with the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of the Production, Trafficking and Distribution of New Psychoactive Substances and Synthetic Drugs related training.

1	*Intelligence, analysis and operations, incl. trafficking methods and routes (intelligence gathering and analysis; sharing cross-border; modus operandi; intelligence-led operational planning; cross-border surveillance; controlled delivery; multidisciplinary approach, i.e. links to other crime areas))*
2	*Profiling and identification of new psychoactive substances/precursors (detection; profiling of shipments; techniques and equipment; international cooperation and cooperation with judiciary and private partners (chemical industry, pharmaceutical companies, post); cooperation with non-EU countries; darknet sales; involve customs and border authorities; profiling regarding natural persons; financial transactions; ways of payment; recognition of and approaching of facilitators)*
3	*Detection and dismantling of illicit synthetic drugs labs (latest trends and developments; production methods, production of precursors, instruments and tools; role and potential of the EU agencies; personal safety measures; evidence collection; criminal facilitators; OCGs*
4	*OSINT and darknet (online investigations and investigations on the deepweb and darknet, tools and techniques, role of EU agencies and their potential, best practices, cryptocurrency investigations, identification of high value vendors)*

5	*Investigations, incl. financial investigations (modus operandi; financial flows; money mules; alternative banking systems; hawala; cryptocurrencies; offshore heavens; cooperation with FIUs and AROs; international cooperation and asset recovery)*
6	*Prevention of drug crime (train-the-trainer on social prevention methods; best practices; personal safety; guidelines and standards; involvement of private sector)*
7	*Document fraud, mislabelling practices and detection (mislabelling practices; cooperation with industry; risk created by mislabelling; exchange of experiences; cooperation with non-EU countries; detection equipment; container shipment controls)*

2.10 Cyber-Crime – Non-Cash Payment Fraud

2.10.1 Environmental Challenges

The continuous rise and spread of online shopping have been cited as contributing factor in the increase of card-not-present fraud. Investigations are prolonged in their work due to the absence of a physically present perpetrator. A lack of staff then reinforces the problem as there is a high turnover with experts leaving for better paid employment. This also implies that staff can often not be sent for training as there is nobody to perform their duties. High-tech hardware and software for the identification and extraction of e-evidence is not sufficiently available in all Member States.

Another aspect that makes investigation difficult is the different data protection and cyber-legislations as well as data retention policies versus the Budapest Convention on Cyber-crime. Both international and national cooperation are hampered by a lack of a common approach and of interagency reporting as well as intelligence sharing. Moreover, data protection regulations change continuously as do payment methods and modi operandi, in particular in the area of airline fraud. Common regulations throughout the EU would prevent criminals having a free field to play.

A further challenge is the lack of cooperation with civil society actors and the unawareness of the public concerning self-protection measures. Many victims are not even reporting the crime. A general awareness campaign on these types of crime, including phishing and social engineering, would be necessary.

Finally, cooperation with banks is crucial; however, it is a fact that banks also tolerate a certain level of fraud with regard to e-commerce. It would be imperative for proper investigation to enhance exchange of information between banks and law enforcement and that the fraud is reported and confirmed very quickly.

2.10.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

On the level of knowledge and skills, the challenges consist in the need for expertise with regard to recognising of fraudulent documents and card fraud, and for cooperation with shops and airlines as well as potential victims from vulnerable groups. Furthermore, Card-Not-Present (CNP) fraud is a facilitator crime, and therefore investigators must recognise links with other types of crime and the need for cooperation with other investigation units. Reporting should be regular element in this type of work, and it often is lacking. Common definitions and indicators would be helpful for cross-border cooperation. Also, new regulations require to be explained for the sake of proper and coherent application.

Technically, the greatest challenges are the recognition and disruption of cardable websites and the identification of criminals resorting to phishing and social engineering. The lack of knowledge on methods used by criminals, available tools and software in the area of cyber-forensics and on encryption, as well as on methodologies for gathering, securing, handling and sharing of electronic evidence also hamper investigations. Changes in this domain come at a very rapid pace, both concerning modi operandi and the technological level.

The topic is also a horizontal one as it covers different areas of the digital and financial world. Anonymization plays a role as well as the creation of fake identities and companies online, the increased use of cryptocurrencies etc. Training on these issues should not only focus on teaching investigators specific skills but also on making them look forward. It should also bring tactical investigators and technical experts together.

b) Training needs

Summary

Training on Non-Cash Payment Fraud should include card present and card-not-present transactions for forensic experts and investigators including new threats and technologies and cooperation with private partners and non-EU countries. Judicial staff could also benefit from an introduction to online investigation. Further needs comprise the identification, investigation and disruption of social engineering/phishing and cooperation with the civil society in this domain. Further topics are darknet, cyber-forensics and e-evidence. In the financial domain, topics to be addressed include logical attacks on ATMs, in particular for first responders, new payment methods, including cryptocurrencies. Data protection and e-privacy including EU and national regulations as well as conventions are highly relevant, and finally document fraud with a focus on the recognition of fake documents and cooperation with other departments in this context.

Further details

There is current training (e.g. Avila, Spain) on card present fraud that is lauded by the experts, including training for forensic experts on malware. Furthermore, ECTEG, in cooperation with Europol's EC3 and CEPOL provides courses on Cyber-forensics. Also EU funded FREETOOL project was mentioned as good initiative among others. Where it concerns responses to cyber-incidents, the International Council of E-Commerce Consultants is providing high quality training.

The experts contributing to this analysis consider some training subjects in this area to be essentially a national responsibility, e.g. on financial investigation and the use of OSINT, however, they also see the benefit for advanced courses at EU level.

Live exercises would be welcomed and should include cases involving the darknet as practical training is highly relevant in this context. It was mentioned in addition that training on evidence gathering and handling should be reinforced.

To ensure that e-evidence gathering takes place pursuant to current legislation so as to allow its admissibility in court proceedings, joint training with prosecutors and judges would be beneficial.

EU-level training is available concerning subjects like combating payment card fraud investigations and forensics, organised by CEPOL and Frontex, but more activities on the subject would be beneficial.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Non-Cash-Payment Fraud related training.

1	*Investigations (new modus operandi used by the OCGs; exchange of good practices; case studies; witness protection; European tracking systems; the EU most-wanted list; undercover operations; controlled deliveries)*
2	*Online investigations, darknet, OSINT (advanced EU-level training; detection and investigation, gathering and securing evidence; live-exercises on darknet cases, e-evidence gathering, securing, handling, and validation; common concept of darknet; darknet and other crimes [Firearms, Drugs, CSA/CSE]); basic training on darknet; second step: platform for the tools; bring together tactical investigators and technical experts to share experiences and to better understand each other's work; exchange of good practices; detection, monitoring and investigations online; how to work on the deep web and the darknet; advanced training for specialists; basic for judicial staff)*
3	*Cyber-forensic, e-evidence (basic training on the use of tools and software and on encryption; available tools; software; data encryption; evidence; different devices; advanced training on digital forensics, tools and techniques for specialists, including new developments, use of artificial intelligence, big data analysis; analysis of the devices [e.g. amazon drones] and cryptography)*
4	*Financial investigation, intelligence and operational aspects (financial investigations; new technologies and developments; tools; modi operandi; sharing good practices; trigger thinking; OSINT; available tools; case studies from different countries to be shared at EU level; capacities of different EU tools and instruments; agencies (e.g. Europol); cooperation mechanisms; undercover operations online; common concept; new intelligence sources; investigation of cryptocurrencies; how to follow the money; online investigations tools; data retention; fake companies)*
5	*Social engineering/phishing (recognition and investigation of social engineering and phishing cases; disruption of the criminal industry and crime enablers; darknet for investigators; business email fraud; information exchange; social media analysis; general awareness campaigns for the civil society)*
6	*Data protection (practical training on very specific topics; GDPR; training of DPO, [national and EU], information exchange, information protection; new legislation/regulations [e.g. e-Privacy, Police Directive, GDPR, PSD2], application of data protection [when, how and under which conditions] data protection will be applied; the consequences; possibilities of cooperation between law enforcement and the private sector; constraints, limitations, requirements, etc.; implementation of the legal framework in practice; cooperation; communication between experts; data exchange channels; the Budapest Convention; the Convention on Cyber-crime of the Council of Europe)*
7	*Prevention (law enforcement officials should be trained on how to communicate with the society on preventive matters [locally and at EU level]; EU-level training to include information on recent modi operandi as a standard; research should be strengthened)*
8	*Card present fraud (training for specialists for forensics and investigators; new trends and threats; new rapidly developing technologies (NFC); vulnerabilities; cooperation with private partners and non-EU countries; card fraud recognition; flight purchases)*
9	*Card-not-present fraud (specialised training on detection and investigation of CNP fraud; cooperation with private companies and non-EU countries; EU cooperation mechanism, information exchange tools; new technologies; new payment methods; how to work with private companies [DHL, UPC})*
10	*Logical attacks on ATMs (for first responders: technical challenges and available services and tools; exchange of good practices; detection; common definition; common understanding; malware analysis; psychical check of the ATMs offenders; including the private sector experts, e.g. the security industry, especially on incident handling)*
11	*Document fraud (recognition of fake documents using different technologies; cooperation between different investigation departments; digitalisation; facial recognition; block chains; smart documents; emerging documents; cooperation with investigators and with document fraud departments; modi operandi of the OCGs)*
12	*Airline fraud; e-commerce (new payment methods; cryptocurrencies; investigation of those; cooperation with different entities, customs etc.; sharing good practices and case studies; modi operandi; detection and confirmation of the incident for first responders: stakeholders; payments methods applied by providers; new payment methods; basic on national level and more advanced training at EU level)* *Comment from Frontex: links to various cross border crime such as migrants smuggling, THB, drugs trafficking, etc. should be addressed.*

2.11 Document Fraud

2.11.1 Environmental Challenges

To start with, a common definition distinguishing document fraud from identity fraud as well as a common terminology would be required, specifically for court procedures. Moreover, it would be useful, if evidence hidden in mobile phones and laptops of criminals could be collected and used in court in a more effective way.

At the operational level, challenges reside in the lack of knowledge and use of a common and interoperable database, which would enable investigators, border guards and customs officers to easily access intelligence, to store or compare data, to cross-check at border check points and to support the exchange of data. This would require legislative changes.

The absence of security features on other fraudulent documents, e.g. invoices, cargo rights documents etc. is a problem particularly for customs officers. In addition, the non-inclusion of an intelligence officer in the investigation units and a lack of intelligence in strategic reports frequently hamper the investigation. Structural problems concerning the end-responsibility of intelligence makes cooperation with Europol sometimes difficult.

Highly relevant synergies with (public) administration and the private sector, in particular with alcohol and tobacco producers, and IT companies, are not functioning as they should.

Prevention is connected with the controlling of documents due to the nature of document fraud aiding other types of crime. Time pressure is an issue here.

2.11.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Cyber-investigation involving the darknet, face-recognition tools and biometrics authentication become increasingly important as well as modi operandi like face morphing. A lack of qualified staff leads to available tools not always being used.

Officers trained in recognising very professionally forged, counterfeited and pseudo-documents, both from the EU Member States and from non-EU countries, would be able to successfully deal with the time pressure. One of the huge and chronic challenges is the practice of mislabelling and the lack of knowledge on this issue.

The outcomes of some research on this issue implemented by Europol may help improve this, and training will be required. However, there exists a lack of knowledge in the area of specific documents, e.g. Middle East countries. And finally, language is an issue.

Improvement of cooperation with prosecutors and investigators has become more urgent due to terrorist attacks, and multidisciplinary cooperation would benefit from joint training activities.

b) Training needs

Summary

EU-level training on document fraud should focus on the identification of fraudulent documents using the most up-to-date methods, specifically at IT and cyber-investigation level, as well the use of EU tools and instruments for investigation and international cooperation. Early detection of fraudulent documents as a means of prevention of other crimes stands in the focus here as well as database interoperability for enhanced international cooperation.

Further details

While many sub-topics can be covered by national training, EU-level training on this horizontal issue needs to focus on specialists and those working at the external borders of the EU as well as on A Train-the-Trainers' type of activity. Quite some content could be transferred by means of webinars or e-learning modules, followed by classroom training and refresher courses in order to secure continuity. The inclusion of the topic Document Fraud in CEPOL's Exchange Programme is considered useful as well.

EU-level training should provide an opportunity for exchange of good practice. Document fraud is also a horizontal issue and should therefore be integrated in training activities by CEPOL and Europol on other related topics, e.g. THB, counterfeiting; cooperation with EMPACT Drivers could be useful here. Even though this type of training is not considered urgent, it could help improve cross-border cooperation and building up networks.

The detection of document fraud has the potential to prevent other types of crime. Therefore, specialist training on this topic can have a wider effect. Also, a Train-the-Trainers' type of activity would be required. Furthermore, a webinar for specialists could be beneficial on detection methods, modi operandi, e-documents, trends and developments.

The lack of awareness of existing databases, e.g. FADO[19], require training after this having been made available and standardised; in particular awareness of the existence of databases in the Member States and the planned interoperability of the large scale IT systems (SIS, VIS, Eurodac, EES, ETIAS, ECRIS) of the EU requires to be addressed. The Law Enforcement Working Party (LEWP) Report could serve as training input.

EU-level training on the detection of document fraud has been implemented already by Frontex, CEPOL, OSCE, and International Centre for Migration Policy Development (ICMPD). A course on identity expertise including reference to identity management, chip technology, biometrics and means to detect digital fraud was provided by Frontex in 2017 and 2018. In cooperation with the Commission, Frontex has organised workshops for EU-consular officials at key locations on the detection of fake documents submitted for visa applications. The Commission recognises that the existing training structure on documents fraud[20] might need revision on both document security and document fraud.

The experts contributing to the EU-STNA have pointed out that EU-level training should be made accessible for a wider target group and reach more participants. They also suggested the drafting of an EU-level common curriculum for national implementation addressing a broad multidisciplinary target group.

EU-level training is available, even if insufficient, concerning subjects like the detection, investigation and forensics of false documents and how they facilitate other types of crime; also prevention is addressed. As organisers CEPOL and Frontex are to be mentioned.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Document Fraud related training.

1	*Identity fraud (Impostors; modus operandi; identity registration process in different countries; documents requested online; facial recognition)*

[19] False and Authentic Documents Online database in 24 languages.

[20] This structure is based on the 2004 Council document 12356/1/04/REV 11 on the "Framework for harmonised programmes for the training of document examiners in three levels", last updated under the Italian Presidency in 2014.

2	*Fraudulent ID and travel documents (detection of document fraud; modus operandi; e-documents; trends, developments; training for border guards; new areas of document fraud; new techniques in document verification; security features; involvement of private sector (airlines, hotels, banks); exchange of best practices on biometrics enrolment; document granting and issuing procedures)*
3	*Document fraud investigations (modus operandi; exchange of best practices; tools, databases and information channels including SIENA; Counterfeiting Monitoring System (CMS); database interoperability; links to other crimes; cooperation with prosecution)*
4	*Online markets and darknet for document fraud investigators (modus operandi; specific characteristics of the internet; how to monitor the network; future developments; criminal activities on darknet; international cooperation; digital manipulation; security management; involving private sector; risk analysis)*

2.12 Drugs – Production, Trafficking and Distribution of Cannabis, Cocaine, Heroin

2.12.1 Environmental Challenges

For this specific topic, most environmental challenges identified were found in the area of legislation as well as the logistics or structuring of investigations. On the one hand there are different definitions of drug crime in national jurisdictions, on the other, there is a lack of common standards or even common terminology. This also reflects itself in problems in the context of international cooperation, which at the beginning would require a better exchange about mutual requirements for securing evidence than is often the case now. Cooperation with other investigative areas, e.g. financial crime, cyber-crime, is not yet everywhere a regular procedure; and collaboration with NGOs also requires reinforcement. Finally, similarly to other areas, a lack of time and human resources is mentioned having a negative impact on performance.

2.12.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

As in many other investigation areas, cooperation with cyber-crime investigators becomes increasingly necessary; however, drug investigators feel insecure to contact them due to a lack of understanding of the cyber-language and cyber-basics.

Where it concerns the detection of illicit manufacturing of drugs and dismantling labs the challenges are mainly seen at the operational level, involving health and safety issues and technical skills. Also links with other areas, like container shipments, glassware companies, chemical companies, DHL etc. as well as with other types of crime, e.g. financial crime, document fraud etc., are relevant and not always explored sufficiently. There is, however, a lack of demonstration labs for training purposes in the EU.

International cooperation is elementary but frequently suffers from the lack of knowledge on the international instruments available.

b) Training needs

Summary

Investigation of drug crimes involving cannabis, cocaine and heroin is considered a highly operational topic. Therefore, on the one hand, training needs in this area are related to poly-drug trafficking and poly-criminality as the major issue identified by Serious and Organised Crime Threat Assessment (SOCTA). On the other hand, training needs are very much focused

on practical issues like cooperation with other investigative areas, including cyber-crime, financial crime, forensics, but also with bodies outside the law enforcement sector, including glassware companies, chemical industry, shipment and parcel services etc. Topics like modi operandi of OCGs, cyber- and financial investigation tools and methods, risk assessment and health and safety in the context of lab dismantling, profiling and detection of concealment methods, and the basics of document fraud are some examples of the content required.

Further details

It is considered highly relevant for every drug investigator to receive some basic training on cyber-investigation whilst more specialised officers could then be trained more in-depth on these matters. This will help improve their communication capacities with cyber-crime investigators and their understanding of what they can expect from them. The same goes for cooperation with financial investigators and training on financial crime. As for availability of training at present, Germany and Ireland have informed that they offer training for first responders on online markets and the darknet.

Document fraud and prevention as horizontal issues deserve specific attention. In particular the first issue is rather vast, and it will only be possible to include elements of this in topic-related training, e.g. freight and air documents, mislabelling, false declarations. For more specialised training, customs officers should be the target group. Prevention on the other hand is considered more a national issue but exchange of good practice could be an element in EU-level training. Training on prevention is also the only topic that is not considered as urgent as the others. At present, The Netherlands has indicated that they offer regular training on prevention, and EMCDDA has prevention specialists.

International cooperation requires training on EU tools and instruments, e.g. support by Europol and Eurojust, JITs, SIENA etc. Here, the importance of participation of managers as well as prosecutors in such training is highlighted in order for them to gain more awareness of the possibilities and requirements, when their staff embark on cross-border cooperation endeavours. Frontex suggested that cooperation with customs and border or coast guard should be reflected in training activities.

Topics like the profiling of shipments, transportation routes and means, including vessels, as well as the use of modern technologies and services or tools, also those used for analysis, should be added to the training needs.

It was generally pointed out that every police official should receive some national basic training on OCGs and their modi operandi, and any EU-level training on such matters can only be attended as a next step towards higher specialisation. Also, this type of training, it being largely operational, always needs to provide the latest trends and updates on the modi operandi and investigation methods.

As EU-level training can be mentioned activities on the smuggling of cocaine and heroin offered by CEPOL; European reporting on illicit cannabis production by Frontex; and contributions by EMCDDA on monitoring drug supply indicators and drug seizures, recent trends, etc.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of the Production, Trafficking and Distribution of Cannabis, Cocaine and Heroin related training.

1	*Online markets and darknet (cooperation and communication between drug investigation units and specialised cyber-crime units; cyber-crime, darknet, cryptocurrency, open net and social networks, OSINT; new methods, tools and techniques; manual on darknet; good practices; information exchange and cooperation with non-EU countries; multidisciplinary approach)*
2	*Illicit manufacturing of drugs, detection (specialised training for first responders and new officers on risk assessment; indicators; chemical substances; production of chemicals; risk assessment of the infrastructure: travel, user facilities, surveillance; interpretation of data; identification of modi operandi; precursors: new modi operandi methods, current trends and concealment methods; intelligence through INCB and international cooperation)*
3	*Detection and dismantling of illicit laboratories (personal protection; suspicious indicators [smell, products], also for prosecutors; data entry: information on modi operandi and new trends should be entered in a database with most recent examples of daily operations; exchange of good practices)*
4	*Links to other types of crimes (firearms; THB; migrant smuggling; OPC; exchange of good practices at EU level about OCGs and their way of working; links to other crimes; organised motorcycle gangs, etc.)*
5	*Prevention (training for prevention officials on communication methods and how to reach people on social media; good practices exchange with other countries; joint prevention campaigns; Train-the-Trainers: basic prevention elements of the drug use; cooperation with NGOs; profiling of parcels by DHL other postal services; prevention of cannabis cultivation)*
6	*Criminal profiling regarding legal and national entities (drugs; container shipments; profiling; company profiling [wittingly and unwittingly exploited] and cargo shipments; profiling regarding natural persons; financial transactions; ways of payment; recognition of facilitators and how to approach them)*
7	*Investigations, incl. financial investigations (exposure techniques; concealment methods; new tools and methods for investigations; overview of legislation in different countries concerning financial investigations; cryptocurrencies and alternative banking; trends, modi operandi)*
8	*Document fraud (specialised training for investigators and prosecutors; identification and sharing of knowledge and good practices)*

2.13 Border Management and Maritime Security

2.13.1 Environmental Challenges

The border management experts focused to a minor extent on environmental challenges, and more on training, but a very important one is the management of Hotspots. A lengthy set-up of and failing logistics in the Hotspots, which are meant to improve the countries' capacity to receive and register migrants and strengthen the coordination between the involved agencies, the channelling of migrants into appropriate procedures frequently turns out to end up in a bottleneck, leading to overcrowded reception facilities that are not always adequate. Cooperation depends on the willingness of Member States and can only be improved by political means.

2.13.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

National border management strategies are linked to national and to EU security strategies as well as to the Frontex regulation, which implies an obligation for implementation by the Member States. A European Integrated Border Management (IBM) strategy is under development. Therefore, training is highly relevant to ensure adequate implementation. Coordination with Frontex and cross-border cooperation is one of the important challenges, e.g. with regard to situational monitoring and risk analysis, as well as cooperation with

economic and political experts. Also the exchange of information with legal experts requires improvement, which could be achieved by means of training.

An important issue is the external dimension. Border management content and the maritime dimension should also be divulged within CSDP missions. It is recommended to consider establishing links with ESDC and CEPOL training and other mission-related available training and include high sea risks, external borders and migration as topics.

b) Training Needs

Summary

Training on Border Management and Maritime Security should cover a whole variety of topics as this law enforcement area plays a strongly preventive role in the fight against a whole range of crime types. Prevention and detection of document fraud and identity fraud is one of the first subjects to be mentioned but also OCGs, particularly in the context of migrant smuggling cases and THB, and consequently also the identification of victims and vulnerable groups. Prevention of serious and organised crime and terrorism should be looked at from the border/coast management perspective. Furthermore, maritime surveillance and operational preparedness as well as fighting maritime security threats must be subject of training. Training on search and rescue operations must be practice-oriented including tabletop exercises. Situational monitoring and risk analysis are further important topics, and one of the most urgent ones considering recent developments is the management of Hotspots. Fundamental rights were also mentioned as needing to be addressed as a horizontal topic.

Further details

Frontex asked to place more emphasis on situational monitoring and risk analysis under border management and maritime security by removing PNR. According to Europol, PNR would be better suited and more relevant than systems like European Travel Information and Authorisation System (ETIAS) and the Entry-Exit System (EES). Furthermore, Frontex suggested that there should be a reference to capabilities and services related to the European Border Surveillance system (EUROSUR), especially in terms of surveillance and situational awareness. Furthermore, they recommended to widen the risk analysis portfolio by including items such as the establishment and management of risk analysis systems, including the creation and improvement of specialised risk analysis units at national, regional and local level; the Common Integrated Risk Analysis Model (CIRAM); and the development of operational and tactical risk analysis products for border surveillance and check activities.

Exchange of good practice in a variety of domains is required, including tackling of illegal activities at the border, evidence handling, search and rescue operations, THB investigation and the fight against smuggling of migrants; also, the management of Hotspots for the sake of harmonisation of procedures. Joint training with prosecutors conducting investigations in this area is considered important. In particular for THB and migrant smuggling, study visits in the regions combined with workshops from the perspective of border management and maritime security would be beneficial.

In many cases, joint training with or the involvement of experts from shipping companies, travel agents and other private partners is considered highly relevant in the fight against terrorism, piracy and other maritime security threats as well as serious and organised crime, in particular where it concerns prevention by means of security checks, passenger registration and the recognition of falsified documents. Representatives of agencies (e.g. International Maritime Bureau (IMB) Piracy Centre) from EU and non-EU countries and of ship agents, and agencies

that determine security measures for ships sailing to dangerous areas could be invited. This is also valid for training on risk assessment and situational monitoring. Relevant topics are, amongst others, the protection of critical infrastructure at sea, physical coercion as well as the International Ship and Port Facility Security Code (ISPS). At present this is part of pre-deployment training, e.g. EUCAP mission Somalia and Operation Sophia.

Where it concerns the prevention of serious and organised crime and terrorism from the perspective of border and coast guard management, an emphasis is put on the need for behaviour analysis; for this a connection with the training initiatives of Aquapol and ESDC on maritime security is considered beneficial. CEPOL training activities for operational analysts as well as the CEPOL course on Counter-terrorism are mentioned as a positive example.

In order to train operational preparedness, in particular for search and rescue operations, practice-oriented, interactive training including tabletop exercises is required, also to improve coordination between authorities. Furthermore, refresher courses at EU level as well as proficiency training with a maritime security focus and workshops aiding to harmonise standard operational procedures are mentioned.

Document fraud is already addressed in quite a number of training initiatives by Frontex, International Organisation on Migration (IOM), UN and other international organisations, and this should be streamlined in order to save resources, and to harmonise and update the content. This could be combined with teaching a common English terminology at advanced level. Aquapol and Frontex also offer training on falsified documents including transportation documents, health declarations, certificates, etc. Meetings of Immigration Liaison Officers (ILOs) are used for the exchange of knowledge as well.

Frontex is developing a tool for first line border checks for the identification of victims and vulnerable groups. In this domain, some language training other than English (Arabic, African languages) is mentioned as potentially useful.

Generally, the frequency of Frontex' training on IBM should be enhanced, and this type of training should also be directed at the management level. Study visits would enhance mutual learning and improve cooperation.

Frontex is the main provider on EU-level training on border management, whilst CEPOL also provides some activities in this domain, e.g. on Hotspots, PNR, and other related subjects.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Border Management and Maritime Security related training.

1	*Prevention and detection of document fraud and identity fraud (fraud recognition; procedures, protocol; tools and equipment; risk analysis; cooperation with border/police operators, customs, forensic experts, consulate/embassies, document issuing authorities, also private sector/airlines; transport document control; specific falsified documents; English course on specific terminology; sharing good practices; identification of the nationality of the person; exchange of information [also with non-EU authorities]; EUCAPS, military and police cooperation)*
2	*Prevention of serious and organised crime and terrorism from the border/coast management perspective (EU Maritime Security Strategy 2014 and implementation reports; risk analysis at an early stage [before the vessel arrives in the port]; common procedures and definition for ferries, cruises, postal vessels, pleasures vessels, cargos; harmonised approach to check*

	persons and cars; maritime customs activities; PNR in maritime security; joint training of border guards and police and other services to foster mutual trust and information and intelligence exchange and improving communication; cooperation with the private sector)
3	*Maritime surveillance and operational preparedness (interagency cooperation; exchange of practice; practical training; operation of different assets in different situations in dangerous, out-of-the-ordinary meteorological conditions; operational preparedness 24/7: need for unified guidelines and training on the common procedures; refresher training courses at EU level as well as proficiency training within the maritime aspect; link to the external dimension (ECDS); Standard operational procedures concerning fundamental rights)*
4	*Border management and organised criminal groups (European Integrated Border Management strategy for different targets groups at all levels; study visits for mutual learning [technical possibilities]; OCGs: new trends, phenomena, modi operandi; cyber-crime: good practice exchange; basic knowledge to use cyber-investigation tools; cooperation with cyber-specialists; for first responders: awareness raising on exchange systems and tools, (Schengen information system) and their functioning; emphasis on data quality; screening the mixed flows; unregistered migrants; fingerprinting, evolution of the SIS AFIS; standard operational procedures concerning fundamental rights)*
5	*Situational monitoring and risk analysis (risk analysis; interoperability with the involvement of Frontex; identification of high risk travellers; PNR; security control of ships; Common Control Centres; involving private partners and shipping companies)*
6	*Hotspots (THB, vulnerable groups, asylum seekers; managing (securing) of Hotspots; harmonising approaches; dealing with falsified documents; Fast Intervention Teams; specific English language for de-briefers; psychological profiling (e.g. Foreign Terrorist Fighters); cooperation with NGOs; prevention)*
7	*Internal borders, secondary movements (biometric data for the detection of multiple identities; protection on unaccompanied minors and separated children; behaviour analysis; interoperability of systems, SIS, VIS, Eurodac, ETIAS, EES, ECRIS)*
8	*Ensuring freedom of movement, fundamental rights (ensuring rights of travellers; data protection and privacy issues; interoperability of systems; SIS, VIS, Eurodac, ETIAS, EES, ECRIS)*
9	*Search and Rescue Operations (cooperation between Member States and non-EU countries in order to enhance efficiency and efficacy; procedures under adverse conditions; specialised medical treatment and first aid included in training on SROs; exchange of good and established practice)*
10	*Identification of victims and vulnerable groups (Behaviour analysis techniques supporting identification, body language, facial expression, micro-mimics, level of vulnerability; interviewing techniques; cultural, religious aspects; indicators)*
11	*Migrant smuggling cases and THB (other crimes: firearms trafficking, drugs trafficking, etc.; EU Policy Cycle in general; latest trends in smuggling of migrants, THB, including modi operandi, trends; exchange of good practice; connection with OCGs subject; information on the available and upcoming legislative initiatives, modifications at EU level; new technologies and interoperability of systems; risk analysis methods and profiling of vessel behaviour; behaviour analysis; cultural awareness, mediation and interview techniques; implementation of the return decisions to the SIS; EU Maritime Security Strategy 2014 and implementation reports; maritime cross-border criminality; Maritime Threat Analysis including all types of documents concerning persons and goods; Aquapol cooperation)*

12	*Environmental crime from the border management perspective (detection; technologies; protected species; illegal trafficking)*
13	*Maritime security threats (piracy, armed robbery; training for relevant law enforcement officials on maritime security threats; ship security; joint operations)*

2.14 Crime Prevention

2.14.1 Environmental Challenges

The experts involved in the EU-STNA workshops identified a general and overall lack of knowledge on the administrative approach in this context about crime prevention measures, a challenge which they considered as not to be overcome by means of training. Coordinated interventions using administrative tools to supplement actions under criminal law in order to prevent, counter, disrupt and suppress serious and organised crime would be required. Some countries need to change legal regulation in order to be able to improve the administrative approach.

2.14.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

On the level of privacy and data protection, a lack of knowledge on the internal procedures for sharing information leads to insecurity and low-level cooperation between different entities. Particularly for fundamental rights there is a lot of training but it still does not suffice. Training needs to follow a harmonised approach and be based on practice including real examples and study court cases as well as an exchange of good practice so people can learn from each other. Also the rights and protection of law enforcement officials (duty of care) must be an integral part of all training, including research results and practical examples.

Management might benefit of gaining a more thorough understanding of the importance of crime prevention measures, as they can have a positive effect reducing crime and therefore police work and financial resources.

With regard to radicalisation, officials need to be aware that there is a potential infiltration in the military where people with the intention to become terrorists take advantage of military training.

Where it concerns the cross-border exchange of information for administrative purposes in the fight against crime, an information gap was identified between field officers and case officers as well as between law enforcement and administrative bodies.

A further challenge that was identified is on the level of sharing and cascading of gained knowledge: there is no system that allows to assess whether and how this takes place and there exists no formal obligation.

b) Training needs

Summary

Management and officials must be made aware of the importance and potential of crime prevention measures. Highly relevant is here a multidisciplinary approach, involving in

particular border guards and administrative staff, and developing trust by understanding each other's tasks. Knowledge on intercultural competencies and national legislations play a role in the context of efforts to convince non-EU countries of the importance of preventive measures (CSDP Missions). Information exchange and knowledge on EU information exchange channels, mechanisms and tools is necessary as well as a knowledge on socio-economic factors, with a special focus on minors and offenders. Cooperation with civil society and other partners also must be a topic. Terrorism prevention is closely related to prevention of radicalisation. And finally, the prevention of misuse of legal frameworks, corruption and intra-organisational abuse of power is an issue to address.

Further details

Safety is written with capital letters for everybody where it concerns crime prevention. A dynamic approach is required due to the fast developments and changes in the criminal world, as well as an understanding of the background: prevention measures must be based on root cause analysis.

Offender prevention would require looking into socio-economic factors: how can recruitment be prevented, which reasons can someone have to become involved in criminal activities, and such. A special focus should be directed at prevention work with young people and with victims. The civil sector, social partners and industries must be included here as well. Training for the management level is also recommended in order to obtain an understanding of how to create a good and effective crime prevention policy and that it takes time to achieve good outcomes. Using research outcomes here would be elementary.

Early warning indicators need to be recognised in order to be able to prevent crime. Multidisciplinary cooperation and the sharing of information as well as risk assessment are further elements that can contribute to crime prevention. This requires knowledge on the different types of terrorism and the potential crime prevention steps.

As border guards and police play a pivotal role in prevention, they must be trained to heighten their vigilance and enhance their skills, and at best together with police and other services to foster mutual trust and information and intelligence exchange and improving communication. Training should focus on the EU information exchange channels, mechanisms and tools, and the roles of different agencies.

Another issue is the potential misuse of legal frameworks: misconduct by law enforcement staff will damage the trust in their work and their representatives at national and EU level. This requires more than training but dealing with this at the educational level is one step in the right direction. The same goes for intra-organisational misuse of power.

Prevention in the context of missions to non-EU countries is a challenging issue. Making those countries aware of the added value of crime prevention and offer learning from one's own experiences is an element for CSDP missions and should therefore be part of pre-deployment training.

Crime prevention is a horizontal issue and must be part of training activities on all kinds of topics in the law enforcement area. A Train-the-Trainers' type of activity is considered necessary with a focus on terrorist prevention.

European Crime Prevention Network (EUCPN) connects local, national and European level and promotes and disseminates crime prevention knowledge and practices among the EU Member States. CEPOL provides EU-level training on crime prevention in a general sense, e.g. new crime prevention trends and methods, but also in specific contexts, like terrorism (de-

radicalisation and attack prevention). This being a horizontal issue, it is addressed in training on other topics where relevant.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Crime Prevention related training.

1	*Prevention of terrorism (recognition of early warning indicators; multidisciplinary cooperation; sharing information between Member States; good practices; common understanding of the crime prevention; risk assessment; knowledge on the different types of terrorism and related crime prevention steps; private sector; awareness on radicalisation, including aspects of potential infiltration in the military training; identification, profiling)*
2	*Cross-border information exchange for administrative purposes (between field officers and case officers; between law enforcement and administrative bodies; administrative approach; EU information exchange channels, mechanisms, tools, like SIENA, SIS, VIS, EURODAC, ETIAS, EES, etc.; role of different agencies)*
3	*Prevention of SOC (including cyber-crime; administrative tools to prevent, counter, disrupt and suppress SOC; backgrounds, modus operandi, root; for management level: change the view / perception of prevention (particularly at senior level); show that crime prevention is effective; different elements and steps in crime prevention; creation of a good and effective crime prevention policy; offender prevention: socio-economic factors; recruitment; reasons for involving in criminal activities; special focus on minors, victims, offenders, how to work with them; cooperation with the civil sector, social partners, and industries; cyber-: new tools, developments; role of EU agencies)*
4	*Multidisciplinary preventive approach and cooperation (awareness of investigators and middle management of the opportunities and importance of crime prevention; administrative approach; cooperation with private sector; building trust; mutual understanding; working in network; prevention and external dimensions: intercultural competencies, different cultures, standards and legislation, cooperation mechanisms with international organisations, private sector etc.)*
5	*Prevention of the misuse of legal frameworks, corruption (misconduct and trust to police; for top managers: corruption and crime prevention; definition; policy documents; indicators; building culture of and respect the legality; threats against employees as well as decision-makers; rights of law enforcement)*

2.15 Forensics

2.15.1 Environmental Challenges

Standardisation of case work methods throughout the EU Member States is an issue. Attention would need to be paid to establishing and following a common forensic case management process and use a unified lay-out for the forensic reports. Harmonisation of the legal framework would also be helpful.

Member States should have at their disposal adequate high-tech hardware and software for the identification and extraction of e-evidence enabling their authorities to work and cooperate using comparable e-evidence. Such hardware and software, however, are at times not sufficiently available in all Member States.

2.15.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The fast development of new digital technologies, media and hardware, the use of the internet, represent a challenge for digital forensics and the gathering of e-evidence. Electrical vehicles forensic, drones forensic, Internet of Things forensics, smart home and social media and instant messaging forensics are examples of those new trends where training must catch up with the new developments. Specialists must know what to recover and how at the crime scene, how to handle it, how to interpret and present this evidence in court. Judicial staff needs to be trained as well in order to enhance their understanding of the technology.

Fundamental rights are an issue here as in many other topics, and in particular where it concerns data protection, the retention and destruction of physical and electronic items, the right to be forgotten, secure access solutions on biometrics, and also interviewing children; the complexity of these issues requires training to be provided regularly, if not continuously.

The experts pointed at a problem which consists in the general lack of understanding of the strands of evidence by different professionals involved, such as likelihood ratio (LR) and interpretation methods, intelligence to approach accuracy, etc.

And finally, the evidence management systems are widely varied throughout the Member States, and harmonisation is imperative. Compliance of evidence with the chain of custody must be assured (ISO 21043).

b) Training needs

Summary

Training on this topic should be offered to a variety of target groups, including forensic and ballistic experts, forensic auditors, judiciary staff, first response officers, and investigators. Topics should focus on examination and documentation techniques, gathering, securing and processing evidence, old and new tools, the technical/scientific interpretation of facts, and the requirements for digital forensics and e-evidence as well as the new challenges coming with this. The collection, handling, processing, use and reporting of forensic data requires special attention as well as presenting these in legal proceedings. Standardisation of case work methods requires training on the use of compatible databases. Further subjects to address concern fundamental rights in the context of forensics, including data protection, interviewing children, retention and destruction of items etc. The exchange of good practices, latest developments and experiences is elementary for cross-border cooperation.

Further details

Training can contribute to the standardisation of the case work methods by means of knowledge transfer concerning the use of compatible databases. A common forensic terminology and common definitions would need to be determined and used in training, and an exchange of good practice manuals and a sharing of ideas would be useful.

One of the most relevant areas is the collection, handling, processing, use and reporting of forensic data as well as gathering evidence (incl. digital evidence) from a crime scene. This also involves the formulation of reports, understanding the submitted data and reports, data sharing in a centralised way, the P2P system etc. Professionals outside the forensics area should also be trained, including judges, investigators and first response officers, in order to have a basic understanding why specific data and substances are collected. Training for

middle management about the ISO Standard and to what extent it facilitates standardisation and uniformity is also recommended.

In training, the forensic disciplines need to be related to specific crime areas and related forensic disciplines. Some basic knowledge on and understanding of each other's work will enhance the quality of cooperation. This also is valid for the interpretation of results and the formulation of conclusions. Here, harmonisation throughout the EU would be very important.

Forensics training must involve new areas of research, e.g. cyber-, cyber enables crime, CBRN, online violence, distribution of fake information, fraud etc. It also must be practice-oriented; a Train-the-Trainers approach is highly favoured.

Where it concerns the use of forensic science techniques in legal proceedings and pre-trial investigations, training can promote the acceptance of these new developments by the judiciary. Joint CEPOL and EJTN training activities as already in place can support this.

Examples of EU-level training activities include topics like quality control and assurance in crime scene investigation, open source IT forensics, advanced Windows file systems forensics and unmanned aerial vehicles (drones), at times in cooperation with ENFSI; Frontex provides training on Forensic and analytical training for law enforcement agencies, nevertheless, more activities on the subject would be beneficial.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Forensics related training.

1	*Securing and processing evidence (crime scene recovery: what to recover and how; assurance that the evidence complies with the chain of custody; ISO Standard 21043; evidence management system [high level of variation between Member States])*
2	*Collection, handling, processing, use and reporting of forensic data (formulating reports and understanding submitted data and reports [for forensic experts and professionals outside of the forensic area]; P2P network, data sharing in a centralised way; validation and update of the databases; Present data evidence to court: understanding of the technology; combination of different types of data [physical and digital]; training at judiciary level in terms of acceptance of new forensic developments in the use within the legal system; use of forensic science developments in legal proceedings and pre-trial investigations, digital forensic science; chain of custody and evidence strength and resistance; evolution of the SIS AFIS)*
3	*Gathering evidence from a crime scene, CSI (police, forensic practitioners, judiciary staff and first attending officers and Investigators should be involved at different levels in this activity: good practice and cooperation; specific data and substances collected; knowledge required; quality assurance by the technical staff; training for middle management: ISO Standard and to what extent it facilitates standardisation and uniformity; documentation techniques from good enough until excellent; good practices on Crime Scene Examination, the technical/scientific interpretation of the facts (Volume Crimes versus Major Crimes); cross-border crime scene and united evidence management)*
4	*Digital forensics and e-evidence, cyber-enabled crimes (continuous training on digital market and digital media; how to interpret what you have and how to present it; fake news; new challenges: electric vehicles forensic, drones forensic [the examination of drones to recover GSP data and its subsequent interpretation]; internet of things' forensics; social media and instant messaging forensics; digital evidence on digital traces; way to gather information and to treat it; e-discovery methodology and utilising this for intelligence gathering)*

5	*Interpretation of results, (transparent) formulation of conclusions and case assessment and interpretation (opinion-based vs. factual results; DNA interpretation. Potential or limitation of Likelihood Ratio (LR) calculations; [common understanding of] fingerprints; factual evidence plus indirect evidence interpretation in conjunction; strands of evidence such as likelihood ratio and interpretation methods, investigation, intelligence to approach accuracy; awareness raising; target group: forensic professionals; common methodology in the EU Member States)*
6	*Standardisation of case work methods (legal framework on EU and national level; use of compatible databases; exchange of good practice manuals and sharing ideas through expert meetings; forensic case management process harmonisation at EU; unified EU forensic report layout)*
7	*Document examinations (document examination techniques, high tech crime experts, document fraud)*
8	*Financial forensics (training of forensic auditors; analysis and financial investigations)*
9	*Technology Watch and forensics in relation to firearms (new tools, approaches, solutions; involving researchers and academia)*
10	*Training for ballistic experts (best practices; new developments; experiences of other countries; different automated ballistic systems; data protection)*
11	*Specific crime areas and related forensic disciplines (e.g. drugs, other; knowledge on NPS and precursors; explosives; trafficking; nanoparticles and nanomaterial; involving expertise from academic; training of technical assessors with SOC knowledge (accreditation); identification of incoming refugees; cross-border fraud in money flows, alternative banking systems, cryptocurrencies; CBRN; Smuggling of goods and persons; online violence)*
12	*Fundamental rights in forensics (data protection, the right to be forgotten [GDPR, CCTV, imagery in general terms; collection of evidence; interviewing children; retention and destruction of items, physical and electronic; secure access solutions on biometrics)*

2.16 Corruption

2.16.1 Environmental Challenges

Corruption is a threat to democracy as it does not only concern the criminal world but also the private and public sector, even reaching up to political parties and the government. This makes it a matter of particular concern for law enforcement and the judicial area due to their duty to protect the rule of law and the democratic governance.

What makes the fight against corruption so challenging for those who are assigned to detect, investigate and combat this phenomenon is the fact that it can concern their own professional environment. This makes some people blind for it as it is too close to home, or puts them into a dilemma of loyalty versus duty.

Investigating corruption might stop on the situational level due to the above-mentioned blindness or due to political pressure. It requires substantial human resources with independent power to depart from the situational level and address structural corruption, which is frequently interlinked with other organised crime areas.

Public procurement can be mentioned as a special topic where the challenges lie in the fact that there usually is a lack of transparency and often also of intelligence. Cooperation with whistle-blowers and witnesses is difficult due to the lack of protection that can be offered to

these. A potential link with the financing political parties here adds to the complexity of the issue.

For investigators, the challenge lies in the huge amount of data they have to process in corruption investigation, and in the lack of resources. This also concerns CSDP missions, as they frequently suffer from a limited number of anti-corruption specialists. Analysis software could help investigators to deal with the data processing in their anti-corruption work.

2.16.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

A general lack of anti-corruption training was identified by the experts involved, particularly in the area of public administration. Officials often do not understand in what way a conflict of interest may impact their work, or they do not include enough details in their asset declarations. In addition, the detection of corruption in their own work environment is often a challenge. This also involves public procurement, an area on which the knowledge of law enforcement officers requires enhancement.

The absence of guidance on the criminal and procedural codes and on modi operandi was mentioned by the experts involved as something that could improve the work of anti-corruption specialists, also at EU level. It was suggested that an EU-led survey could contribute to establishment of such a guide.

b) Training Needs

Summary

Here the training needs focus on sensitisation for and prevention of corruption as well on different contexts where corruption can happen. Ethics and integrity, awareness and recognition, risk assessment and vulnerabilities need to be addressed, as well as the duty to report and the recognition of conflicts of interest. Contexts are public administration including the judiciary, prosecution and public procurement processes, but also in sports and involving organised criminals. In the latter contexts, corruption detection, evidence collection and reporting techniques and the use of informants and witnesses are relevant. Also modi operandi, financial investigation techniques and the use of information sharing channels at EU level should be mentioned here, and of course international cooperation.

Further details

Sensitisation for corruption and suspicious transactions is one of the goals that can be achieved by means of raising awareness and enhancing knowledge about indicators. This should be combined with providing guidelines how to report about this and to whom, and with risk analysis as a prevention tool.

Apart from specific topics that relate to corruption in individual areas there are quite a few issues that are considered important to be covered generally and at EU level. These involve risk assessment, cooperation with the private sector partners, interagency and cross-border cooperation, interviewing witnesses and whistle-blowers. Training aiming at investigators should include content on analytical tools to help the detection or investigation of corruption, ways of gathering evidence, reporting techniques and how to present data in court as well as the use of SIENA and other information sharing channels.

At a more specialised level, training on corruption in the context of organised crime should include financial tools and transactions like cryptocurrencies, hawala etc., and the international flow schemes in the private sector. Furthermore, criminal law, modi operandi, criminal and procedural codes are as important as strategic planning for the disruption of criminal structures. With regard to corruption in the private or public sector, training must address tax evasion techniques, informal or secret ways of illegal financing of political parties, and bribery. Also training on cyber-investigation elements (e.g. e-sport games) comes into the picture here. Furthermore, pre-deployment training for CSDP missions should include anti-corruption as a topic with a focus on governance and oversights within rule of law institutions in post conflict countries. This could be included in training in the area of the Security Sector Reform.

Intelligence analysis, and as a tool for this also social network analysis and special geographic information analysis, as well as the use of analysis software tools could be the red thread running through a lot of topics listed.

For judges training on the assessment of corruption evidence is suggested, but otherwise joint training for judicial and law enforcement staff is generally recommended. Also representatives of the public sector should be invited.

In addition, the sharing of good practice, also on legal frameworks and resulting possibilities in countries (e.g. the use of *agents provocateurs*; the use of full transcriptions in court, etc.) is considered an opportunity for mutual learning. An idea was to create international expert platforms specialised on anti-corruption for continuous information sharing (workshops and online) as a follow-up after a (series of) training activity(ies).

Corruption is addressed at EU level in activities provided by CEPOL including the investigation and prevention of corruption tackling corruption in the context of missions to non-EU countries.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Corruption related training.

1	*Financing and facilitating organised crime, anonymous payments and corruption, cross-border cooperation (criminal and procedural codes; modi operandi; sharing of good practice; legal frameworks: use of agents provocateurs; the use of full transcriptions in court; training on cryptocurrencies: modi operandi; tracking financial transactions; tactics; cooperation with banks; anonymous bank accounts; long money flow to enhance the understanding of criminal transactions; financial criminal analysis for analysts; strategies to disrupt criminal structures; cooperation with the private sector; detection of informal and secret ways of financing political parties; tracking financial transactions in relation to public procurement; seizures of tax declarations, financial transactions, process of tax declaration, use of hawala; interagency and cross-border cooperation with a specific focus on anti-corruption: use of SIENA, and other information sharing channels at EU level; collaboration between Member States in the gathering of evidence; knowledge on collaboration possibilities; involve judiciary, prosecution, and private sector)*
2	*Ethics and integrity in public administration (assessment of risks and vulnerabilities related to corruption; horizontal issue in the context of corruption: sensitisation by means of training, prevention; conflict of interests; state capture; risk assessment in the context of large public projects; corruption in the public procurement process; how to recognise the possibility of corruption; obligation to report about suspicious transactions; best practices on verification of persons; anti-corruption assessments of legislation. Involve judiciary, prosecution, and private sector)*

3	*Evidence collection and reporting techniques (uniform way of gathering and presenting data; use of data in court [law enforcement officials and prosecutors]; assessment of evidence for judges; training for judiciary and prosecution)*
4	*Informants and witnesses (witness protection; how to attract informants; interviewing techniques in relation to informants; protection of whistle-blowers; involve judiciary and prosecution)*
5	*Corruption in sports, suspicious money transfers (use of analytical tools to detect corruption; joint training with the private sector; social network analysis; use of IT tools in the context of investigations; geographic special information analysis; techniques to retrieve information from different websites in connection with sports [e-sports]; use of e-sport games to pay bribery and gathering evidence in this context; darkweb, also in the context of online sport games; involve judiciary, prosecution and private sector)*

2.17 Missing Trader Intra-Community Fraud

2.17.1 Environmental Challenges

The diversity of this type of crime is a challenge for investigation and (inter-)national cooperation. An important characteristic of Missing Trader Intra-Community Fraud (MTIC) is that it requires a strongly multidisciplinary approach, with tax administration – not in all Member States part of law enforcement – being the core group. The departure of highly skilled professionals to or the difficult recruitment of, mainly, forensic analysts from the private sector due to non-competitive public salaries is therefore a huge problem. In a high number of Member States there are no analytical tools and software available. A lack of analysts and forensic auditors deteriorates the situation. Furthermore, the many different departments in some Member State make national and international cooperation difficult. Investigation overlaps are frequent and would require coordination. Cooperation with non-EU countries is also mentioned as being problematic, and also cooperation with prosecutors and judges should be better than it is now.

In the cross-border combat of this type or crime, the difference in regulations and procedures creates difficulties, e.g. with intangibles like gas and electricity. Moreover, certain industrial traditions, for instance the fact that computer parts, discs and other electronic products have no serial numbers, hamper investigations. There is no harmonised approach to data protection and bank secrecy, which has provided challenges for the establishment and operation of a European Bank Account Registry. Finally, not all Member States experience the same type of MTIC Fraud.

Investigations suffer from a lack of information exchange and cooperation mechanisms concerning import and customs databases. Mutual database access between police and customs should be more systemic and improved substantially. MTIC investigators also often lack time to follow the money, which in fact is at the core of the criminal activities. It is imperative to also involve non-EU countries in the investigations, which is not always the case at present. Although a VAT Reverse Charge and Quick Response mechanism have been published by the European Commission, reverse charge is not introduced by all Member States at the same time.

2.17.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The challenges for cooperation, whether international or inter-disciplinary, are manifold. It starts with the fact that cooperation between law enforcement bodies and sharing information and data is crucial. An understanding of each other's responsibilities and possibilities as well as of procedures and legislation in other countries is elementary. Knowledge on the support options and available tools at EU level is highly relevant for cross-border cooperation as is on channels like SIENA for sharing data.

One of the big problems consists in the fact that there is a large variety of topics and forms of crime, while simultaneously many officials involved have no proper overview over the different types of crime, e.g. customs procedures in general, the abuse of customs procedures, the fictitious export to a non-EU country etc.

The challenge for law enforcement officials is how to find the money and the master minds behind the crime. Experts involved have to deal with a reality that has changed completely in a short period of time due to use of the internet for fraud crimes, the introduction of alternative payment methods, mobile devices etc.

At the level of prevention, international initiatives frequently do not comply with the national agendas and are therefore not taken on board by the Member States. There is no one-size-fits-all training: flexibility is required and local and regional needs must be met.

b) Training Needs

Summary

What is very specific for MTIC Fraud is the multidisciplinary element, the huge variety of different forms of fraud and the ways how to exchange data in a reality where official databases are not mutually accessible, data protection and bank secrecy and rapid changing payment methods. The needs for MTIC training focus on the general topics that are also relevant for other types of organised crime, like online investigations including OSINT, criminal investigation techniques and international cooperation tools like JIT and SIENA, intelligence collection and analysis and the use of databases, financial investigations, modi operandi as well as prevention.

Further details

The following points are considered useful

1) A general training activity for judges and prosecutors to enhance their understanding;
2) An EU-level Train-the-Trainers' type of activity to promote national cascading;
3) Up-to-date webinars on current trends and modi operandi to share good practices;
4) Tax administrators should be included in relevant law enforcement training;
5) EU-level training for big data analysts, specifically on the exchange of data and practice to understand each other's systems better;
6) EU-level training for forensic auditors, as national authorities cannot afford it.

Training at national and EU level is available, however, law enforcement officials are not always aware, for example of CEPOL training on alternative payment methods; or it may not be enough, like training by the European Anti-Fraud Office (OLAF) on digital evidence and computer forensics, or Europol's on cryptocurrencies. The Academy for European Law is offering training for prosecutors and judges. Training on informant handling is offered by CEPOL in cooperation with Europol. CEPOL also provides a training activity on MTIC as a stand-alone topic.

Training should naturally be up-to-date and include modern techniques. When it comes to the link between MTIC fraud and money laundering, training on cryptocurrencies and alternative banking platforms would be necessary. Some of this training is provided by Europol but it is not considered to be sufficient.

Europol proposed giving higher priority to MTIC fraud, the topic being an EMPACT priority.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Missing Trader Intra-Community Fraud related training.

1	*Criminal investigations, innovative techniques (training on JITs, general and advanced level is required; access official databases [customs have no access to police databases and vice versa]; tax authorities/administrations to be invited for training)*
2	*Carousel fraud crime patterns (General training on the fraud patterns; general overview of the phenomena; custom procedures; information exchange; cooperation mechanism re import and customs data bases.; training also for judges and prosecutors to understand the phenomena; tax authorities/administrations to be invited as well; info on investigation, incl. administrative investigation practices)*
3	*MTIC fraud in economic sectors (clothing, products from China, Turkey etc.; introduction to MTIC for customs officers; food: acquisition fraud; electricity and gas plus different legislations on gas and electricity; e-Commerce; tax authorities/ administrations to be invited for training)*
4	*Financial investigations, anti-money laundering, financial crime enablers (specialised training on financial investigations for investigators and prosecutors in MTIC; exchange of intervention strategies against facilitators in criminal finances; sharing knowledge, trends and modi operandi; modern techniques enabling investigators to follow the criminals and their developments; hawala; cryptocurrencies; alternative banking platforms; money laundering syndicates; underground banking/Informal Value Transfer Systems (IVTS); money mules; asset recovery: asset tracing, identification, valuation, management; non-conviction-based confiscation; cooperation with non-EU countries; collecting evidence for first responders; what to do on the crime scene; how to keep digital evidence admissible later; include prosecutors and judges, and tax authorities/administrations)*
5	*Online investigations, OSINT, darknet (Informant handling; OSINT; identification of OCGs on deep web and darkweb; social media; digital evidence and computer forensics; OCG systems and methods; including tax authorities/administrations)*
6	*Intelligence collection and analysis (operational, tactical strategic level; information channels and tools; how to gain access to data; exchange of good practices among authorities from the same country and among Member States; big data analysis, control of movement of goods and related money moves; data protection, banking secrecy; information exchange; analytical tools and software; big data analysis; exchange of data and practice to understand each other's systems and products better; including tax authorities/administrations)*
7	*Prevention (awareness raising campaigns for law enforcement, the judiciary and the public; training of relevant actors; identify and share good practice from investigations and prosecutions; including tax authorities/administrations)*

2.18 Environmental Crime

2.18.1 Environmental Challenges

A very specific problem here in this area is that some national authorities do not consider environmental crime to be a priority, which leads to a lack of resources dedicated to the fight against this phenomenon compared to the large scale of the problem. Simultaneously, Environmental crime is an established EMPACT priority as determined by the Council of Ministers. There is consequently also little support by managers and leaders for the investigation of environmental crime. For criminals, on the other hand, it is a crime with low risk and high reward.

It has in common with the majority of the other topics that the legislation is different per country as well as the categorisation and classification of this type of crime. Problems even occur when trying to determine whether specific actions that have a negative impact on the environment are illegal or not; and there are no checklists or guidelines. These factors also contribute to the difficulty of setting up and conducting interagency and international cooperation. Another challenge, brought about by the rapid changing technologies and new types of waste, is the high amount of legislative changes, which are hard to keep up with.

In order to overcome these obstacles, a change of attitude is required, which can then contribute to the amendment of policies in all EU Member States and consequent prioritisation, with more resources.

2.18.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The environmental crime area involves waste and wildlife trafficking, large-scale unlicensed fishing, damaging protected areas and buildings, destroying habitats and removing protected plants as well as trade in ozone depleting substances. Many of these topics are very country-specific, which makes EU-level training difficult to conceptualise.

Environmental crime is complex as it involves a huge amount of data and information. Also links with other types of crime are always there, e.g. document fraud (licenses). This, and the importance of multidisciplinary cooperation (customs, border control and environmental officials), makes the coordination of this work highly necessary.

As in many cases, corruption is behind environmental crime cases, and therefore cooperation with financial investigation units is imperative. Still, in many countries this is not yet part of the regular procedures.

International cooperation is not initiated often enough, partly due to the low priority these cases receive but also due to lack of knowledge of law enforcement officials about the possibilities. Training on EU support, tools and instruments seems to be absolutely necessary, and here is also mentioned awareness training for unit leaders and managers.

On the practical level of the immediate work, the identification of protected species represents a challenge as well sampling and evidence gathering. The information held by specialised NGOs in this crime domain should be analysed and evaluated by law enforcement. Also, document fraud presents difficulties where decisions are to be made whether the items presented are second-hand or waste. Here, in particular border guards are in demand requiring knowledge on the legal background, administrative issues, and the identification of

waste. As a follow-up phase, intelligence should be gathered, including financial information, on the criminal pattern. This type of investigation, often on cross-border scale, should be done on a more regular basis.

b) Training needs

Summary

For the fight against environmental crime, specialised training is needed on illicit waste trafficking, including waste dumping and vessel trafficking, as well as wildlife trafficking. The more general topics concern modi operandi, OCGs as service providers, new trends and EU agencies, tools and instruments (e.g. JITs, SIENA); collaboration with customs and border control authorities and non-EU countries; data collection and analysis methods, and evidence for court procedures. On the level of cooperation with other crime investigation units, financial investigation (FIUs and AROs) is mentioned including sub-topics like cryptocurrencies, money flows. Also, cyber-investigation touching on OSINT and light net, open web,, online trade, and sellers and buyers should be addressed. Document fraud is a further issue with regard to import/export certificates or fraudulent declarations, or misclassification of documents. On the level of prevention, training is considered useful where it concerns the use of new technologies, cooperation with the media and with academics as well as NGOs. Involvement of prosecutors and judges as well as high-level officials would be beneficial.

Further details

One of the big issues here certainly is the fact that the level of tolerance towards environmental crime is still very high. Unfortunately, there exists a general idea within law enforcement that this is not part of their mandate. A change of attitude is needed, and training is considered one area with potential to achieve this, at least partly. A further suggestion is to have an EU-level large-scale event including law enforcement and academics where the latest research findings can be presented. EU–level training on document fraud in this context is considered useful, however, mainly in form a Train-the-Trainers' type of activity which would then facilitate cascading of knowledge at national level.

Whilst officials specialised in environmental crime investigation need to learn about financial and digital investigation techniques, they also see a need for those investigators to learn some basics about environmental crime.

France and Germany provide training on wildlife trafficking. The European Union Network for the Implementation and Enforcement of Environmental Law (IMPEL) and EnviCrimeNet provide opportunities for the exchange of good practices but no training. There is also a network of practitioners in the fight against wildlife trafficking where this type of exchanges is possible. Contacts with Eurojust would be welcomed. At EU level there are CEPOL training activities on environmental crime and wildlife trafficking. And yet law enforcement could benefit from more EU-Level training considering the fact that this topic is relatively new.

Europol proposed giving a higher priority to environmental crime, it being an EMPACT priority, whilst Eurojust suggested training on the services and tools provided by Europol, Eurojust and other bodies supporting the fight against this type of crime.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Environmental Crime related training.

1	*Illicit waste trafficking (tools; methods for data collection and analysis; good practices; document border controls; cooperation with non-EU countries and environmental authorities; waste dumping; role and potential of the EU agencies; vessel trafficking; damage evaluation and provide proof to the court)*
2	*Investigations, including financial investigations (modus operandi; latest trends; new developments, illegal profits; cryptocurrencies; money flows; evidence collection; JITs; good practices; cooperation with judges and prosecutors; FIUs and AROs; international cooperation; cooperation possibilities provided by Eurojust, Europol and the existing international networks of practitioners dealing with environmental crime)*
3	*Environmental crime in general aspects (modus operandi, new trends; exchange of best practices; role, support and potential of EU agencies [Europol, Frontex: EUROSUR, EFCA] and other relevant authorities; criminal actors and legal businesses; origin, transit and destination countries)*
4	*Prevention of environmental crime (use of new technologies; cooperation elements with Eurojust, Europol, Frontex, others; cooperation with media, communication techniques; stronger cooperation with academics, NGOs; exchange of good practices)*
5	*OSINT and darknet, focus on environmental crime (online trade; identification of endangered species; information collection tools and methods; analysis of data; sellers and buyers)*
6	*Wildlife trafficking (identification of protected species; better collaboration between customs and border control authorities; role and potential of the EU agencies; intelligence on trafficking routs; good practices)*
7	*Document fraud, focus on environmental crime (organised criminal groups involved in document fraud; import/export certificates or fraudulent declarations; misclassification of documents; cooperation with relevant authorities; exchange of good practices; cooperation with prosecutors and other relevant stakeholders)*

2.19 Excise Fraud

2.19.1 Environmental Challenges

To combat this type of crime, many actors from different services are involved, which makes harmonised cooperation essential. Countering smuggling via sea, land or air requires well-coordinated cooperation efforts as well as the exchange of information and intelligence between the Member States. However, the sharing of intelligence is subject to different legislations in the EU Member States, and coordination is frequently not effectuated, in some cases due to a lack of understanding of management for this need.

There is often a lack of human resources; for example, of specialists both at operational as well as at tactical and strategic level. Also, for the control of small parcels there are simply not enough human resources available. Even the number of service dogs and tools like x-rays, scanners, etc. does not always suffice.

Cooperation with private companies, is frequently difficult. Organised meetings with this sector could be helpful. Also, prevention would be an important issue here as cooperation would be useful.

2.19.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The use of EU instruments and tools is highly relevant for cross-border cooperation and successful tackling of this type of crime. Unfortunately, the level of knowledge on how to apply these is not the same everywhere. The use of JITs could be much better.

One of the big challenges mentioned is the cross-border trade in cigarettes, an important matter for external border control.

The lack of capacity to recognise fraudulent declarations and to use certain equipment in the fight against cross-border smuggling is a further problem. Also risk analysis and profiling are challenging tasks requiring a lot of work effort. Training on these issues would be highly relevant and provide a forum for a multidisciplinary exchange of experience. The knowledge on the use of information and intelligence exchange tools, e.g. diverse systems for criminal analysis, in the context of containers, and how to use them for criminal analysis should be strengthened, and cooperation with non-EU countries could be improved.

To enhance the understanding of criminal infiltration into legal business structure would also be imperative for law enforcement to formulate a law enforcement response. Understanding the criminal business model is crucial to target law enforcement actions on the vulnerable points of OCG activity.

On the level of (international) investigations, the challenges are manifold. It usually starts with the fact that international cooperation is often seen as prolonging the investigation phase, for which resources are not available. On the other hand, often no international cooperation is initiated due to a lack of knowledge on the potential support and tools at EU level.

The public needs to be made aware of the amount of money EU states are losing due to excise fraud. Health campaigns combined with such information could be beneficial for raising intolerance towards illicit products.

b) Training Needs

Summary

For training, the focus is first on certain types of excise fraud including illicit manufacturing and trade of cigarettes, the movement of raw materials, and precursors. Then topics like skilled workers, uncontrolled trade of manufacturing machinery, mineral oil fraud schemes and tax evasion are listed, and T1 fraud as well as the control of external borders in the framework of excise fraud. In the context of these topics, databases for sharing of intelligence and information, OCGs, the integrated use of financial investigative tools in excise investigations, international asset tracing (e.g. role of AROs, asset recovery networks) and recovery, JITs, external border control, modi operandi etc. are mentioned, in addition to other more specialised sub-topics. Finally, the more general issues like criminal investigation, collection of analysis of intelligence, evidence gathering, and cooperation with financial and cyber-crime investigators (e-Commerce, OSINT) as well as prevention are included.

Further details

For the enhancement of cooperation, at national level between administration and law enforcement and at international level between Member States, the exchange of good practice but also participation of officials in CEPOL's Exchange Programme would be considered useful. Furthermore, the support for investigators by EU Agencies, e.g. Frontex and OLAF, and which information or intelligence can be shared should be subject of training. The cooperation with prosecutors is also relevant for investigators; joint training of these two target

groups is therefore highly favoured. EU training on “Crime Enablers” should particularly involve the private sector, e.g. banks, warehouses.

Cigarette and oil fraud enjoy higher priority when it comes to training compared to alcohol fraud however as alcohol fraud is one of the main forms of excise fraud and of a cross-border nature, it should also feature among training needs where relevant.

For the enhancement of cooperation, joint training could be useful in particular with judges and prosecutors.

In general, the exchange of good practice is held high. It would be useful to learn from other countries about their methods, tools, equipment, legislation and procedures.

CEPOL’s annual programme includes training on Excise fraud and excise fraud analysis. Frontex provides training on EUROSUR and on intelligence collection and analysis whilst Europol organises Joint Analytical Teams (JATs) and operational task forces, which is also very useful for intelligence sharing and analysis. The Customs Eastern Land Border Expert Team (CELBET) provides some training in the context of the movement of raw materials, precursors, skilled workers, uncontrolled trade of manufacturing machinery: this involves cross-border surveillance mechanisms as well as techniques and tactics, legal aspects, new technologies and quick solutions for information exchange. Existing training is considered to be rather fragmented and insufficient.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Excise Fraud related training.

1	*Excise fraud, general aspects and links to other serious and organised crime, (modus operandi of OCGs; constant changes in particular in alcohol fraud; links between OCGs; database about illicit sites and data linked to terrorism; excise fraud debriefing about intelligence sharing; money flows; profits of OCGs; interlinks and poly-criminality; interlinks between border police, police and customs; include prosecutors and judiciary staff)*
2	*Criminal investigation; evidence; innovative investigative techniques (e.g. tracking and tracing; training on EU tools and info exchange mechanisms; new technologies; evidence collection; digitalisation of evidence; JIT (Naples II) is necessary for customs officials; training on new threats, modi operandi, OCG structures; special techniques: how to use controlled deliveries as practical tool of international cooperation; legal differences between the Member States; crime enablers: use of legal business structures, manufacturing, shipping, warehousing, marketing, distribution; involve private sector; administrative investigative practices: good practice, exchange programmes)*
3	*Financial investigation in excise fraud cases (anti-money laundering measures; financial crime enablers: money laundering syndicates; underground banking/informal value transfer systems, money mules; criminal finances: bitcoins, block chain, virtual currencies, transfer of cash; the potential role of the FIUs; financial systems; online instruments; modi operandi; following the money; EU tools for financial investigations; asset recovery: importance and timing; good practices; EU tools; cooperation with the private sector; include prosecutors and judiciary staff)*
4	*Control of external borders vis-à-vis excise fraud, cross-border smuggling (cross-border surveillance mechanisms, techniques and tactics; detection of document fraud; risk profiling; use of equipment and tools; exchange of good practice; legislations of the Member States and how this impacts their action; include non-EU countries; identification of crucial intelligence during seizures; preservation of evidence; searches, document locations and recognition of*

	existing evidence; exchange of expertise and experience in addressing crime detection and prevention; for border guards concerning trade in cigarettes; high level awareness raising for managers; cooperation structures in the Member States; enhancement of the inter-service collaboration including police, border police and customs)
5	*Intelligence collection and analysis in relation to excise fraud (on operational, tactical and strategic level; for analysts on new techniques, analytical tools, artificial intelligence, big data analysis; JATs; available instruments at EU JHA agencies)*
6	*Illicit manufacturing and trade of cigarettes (cheap whites from Eastern Europe; counterfeit products; intra-EU smuggling; dismantling and investigating illegal production sites (for specialists): processes, competencies, role distribution between police and customs, money flows behind the crime and sharing information; EU instruments; sharing information; JITs; external border control, mainly with Turkey, EU Eastern and South East land external border and Mediterranean Sea borders [both west and east and to lesser extent central]; include border guard, police and customs; aligned controls)*
7	*Monitoring the production of tobacco, supply chain control in terms of raw tobacco, movement of raw materials, precursors, skilled workers, uncontrolled trade of manufacturing machinery (exchange of good practice; information about legislation; tackling illegal trade; legal aspects; multi-agency aspect to be considered; distinction between legal and illegal business; monitoring field workers)*
8	*Mineral oil fraud schemes and tax evasion (mineral oil trade and VAT fraud; fake declarations; misuse of oil products; exchange of good practices; methods, tools, equipment; legislation and procedures; designer fuels: info sheets, wikis with information; electronic devices for detection; training on EUROSUR related services especially in relation to smuggling by sea)*
9	*OSINT, e-Commerce (cryptocurrencies; possible future developments; electronic evidence; chain of evidence; storing evidence; OSINT; international agreements; cooperation; exchange of information and intelligence; include law enforcement, prosecution and judiciary; use of the internet for organising illicit distribution; sales of products; advertisement of the illicit products; future potential threats; analysis of data)*
10	*Prevention (for prevention specialists: exchange of good practices; cooperation with the private sector; tobacco manufacturing; software; artificial intelligence; sharing common and good practice on prevention; public awareness: health campaign; cooperation with shipping warehousing, internet providers; technological innovation to strengthen prevention of crime)*
11	*T1 Fraud – fraudulent use of Excise Movement Control System (EMCS) (use of EMCS by OCGs to facilitate their fraudulent activities; criminal analysis)*

2.20 Fundamental Rights

2.20.1 Environmental Challenges

The challenge with fundamental rights can be twofold, on the one hand affecting the police culture and approach, on the other creating personal value conflicts. Certain interventions may not be easy to bring in line with the fundamental rights principles, and police are often confronted with situations where they have to make quick decisions and cannot always reflect on the compatibility of their actions with fundamental rights. To have at minimum some basic knowledge and the guidance by their superiors is essential, and this implies a strong responsibility for management and leadership. Pressure exerted by the media and by politicians reinforces these challenges, but also represents an important monitoring process.

2.20.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Police officers and other law enforcement officials must recognise themselves as the guardians of the fundamental ethos of the rule of law, with an unwavering commitment and obligation to protect justice and rights. Naturally there is also the duty of care from the side of the state. As fundamental rights are closely connected with collective but also individual values (e.g. hate crime and xenophobia), a fundamental rights-based approach may at times go against the individual official's views, whilst professional requirements oblige them to respect those principles and not allow themselves to be driven by prejudice and stereotypes. This makes training on this topic essential with its potential of changing attitudes and enhancing self-awareness. Showing law enforcement officials how to deal with such dilemmas must aim at helping them to remain professional in dealing with perpetrators, including terrorists and returnees, and minorities.

One of the challenges for which training could be an essential solution, consists in the fact that the understanding of the fundamental rights principles is not the same everywhere. A particular point concerns CSDP missions involving the confrontation with non-European cultures and their way of dealing with fundamental rights. Extreme situations can be found in regions where crimes against humanity, genocide, as well as war crimes are committed in the context of their political and historical background.

b) Training needs

Summary

It speaks for itself that fundamental rights are a horizontal issue to be addressed in training on all types of law enforcement training. The main elements that are immanent in all kinds of topics are the use of force, deprivation of liberty, interviews and interrogations, working with victims and avoidance of re-victimisation, stop and search, prohibition of torture and ill treatment and finally the policing of assemblies, public order, and crowd control. Training on these issues should, where possible, involve private parties (NGOs, minority groups and social networks, and others) as experts, and apart from representatives from law enforcement also such from the judiciary sector should be invited to participate.

Further details

The training needs in this area focus on the general implementation of fundamental rights in the context of law enforcement work, like stop and search actions, public order interventions etc. In addition, they focus on specific contexts like asylum, visa, migration and integration policies, terrorism and serious and organised crime. Genocide and war crimes – specifically important in the context of CSDP missions – are topics that require a specific focus. In addition, duty of care needs to be addressed. This type of training involves a personal element as the values of individual trainees may be addressed, where these are conflicting with the principles of fundamental rights. How to "marry" the respect of fundamental rights with the occasional need for the use of violence and other police interventions is an important issue to address as is communication with the press for the sake of the image of law enforcement and the trust of the public.

Children's rights are a subject by itself, when dealing with young victims, and training is required in order to have specialised law enforcement officials who know how to work with

children and adolescents. Here, a strong preventive aspect can be detected and should be focused on.

Hate crime is a further topic that requires specialised training making officials aware of the need to step in by means of proper interventions and which other agencies to involve. They must understand the risk for re-victimisation, which could contribute to increasing an atmosphere of mistrust regarding the police as an institution of support and protection.

Other domains to be addressed where fundamental rights can play a role are JITs, the rapid technological changes and developments, and financial investigations in particular with regard to data protection issues. Training on intercultural competencies and awareness raising on interreligious issues is highly relevant in this context.

Subject of training should also be the role of and effective communication with the media (awareness, manipulation, terminology); this is essential as a trust building measure with regard to the public view on police work and the image of law enforcement.

The fact that not all Member States have the same understanding of the implementation of fundamental rights makes the sharing of good practices at EU level highly relevant. In general training on fundamental and human rights is provided, also at EU level, but the experts agreed that a more strongly coordinated approach would be beneficial. An effective means of training could consist in taking trainees out of their comfort zone by confronting them with certain minorities or other cultural groups, visit religious ambiances, etc., and create space for discussions.

Train-the-trainers as well as mentor programmes for already existing training were suggested for cascading and sharing good training practices in the context of this subject.

EIGE suggested to specifically integrate the gender-perspective, the issue of traumatised witnesses and victims as well as sexual and gender-based violence in all training activities. They recommended extending the thematic focus of fundamental rights by changing the title to "*Fundamental Rights and Gender Equality*". The gender perspective should feature in particular in relation to community policing and to crimes where victims and perpetrators are women. This could concern crime prevention and the identification and treatment of victims. The issue of gender-based violence should be addressed in training on all types crime, and under this category it should be a stand-alone topic, separate from minorities. Prevention of secondary victimisation is a further topic to be included.

CEPOL, with the support of the Fundamental Rights Agency (FRA), provides a 2-step activity on fundamental rights including police ethics and management of diversity; also hate crime is a subject in the CEPOL annual programme. As a horizontal topic, fundamental rights are integrated in other training activities where relevant. Close cooperation with FRA and EIGE is regular practice. In the future, however, these training activities must be stepped up.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by Member States, of subtopics in the area of Fundamental Rights, Hate Crime and Genocide related training.

1	*Fundamental rights in serious and organised crime and terrorism (stop radicalisation; dealing with victims of terrorist attacks and with crises; fundamental rights of terrorists and returnees; de-radicalisation by means of respectful treatment and respecting fundamental rights; interviewing techniques, how to communicate; stereotypes, racial profiling, prejudice and the*

	immanent risks; exchange of good practice; respecting the rule of law and fundamental rights; include judiciary staff and prosecutors.
2	*Human rights in asylum, visa, migration and integration policy (management and leadership responsibility; sharing good practices; strategies; role of the media and effective communication (awareness, manipulation, terminology); use of force; deprivation of liberty; interview and interrogations; victim-centred approach; stop and search; prohibition of torture and ill treatment; policing of assemblies, public order, crowd control; xenophobia; include judiciary staff and prosecutors)*
3	*Hate crime (exchange of good practice; tools and technologies for investigations; Train-the-Trainers' type of activity; mentor program for already existing trainers to share good practises and developing skills in delivering courses)*
4	*Gender-based violence, minorities, other vulnerable groups (victim-catered approach; visiting other cultural groups, e.g. religious places; avoidance of double victimisation (interviewing techniques); different legal systems; coordination with victim support organisations; community policing and interaction with minorities)*
5	*Rights of children (Convention of the Rights of the Child, national legislation, international standards and treaties; cooperation with victim support agencies; child abuse and exploitation; unaccompanied minors; trafficked children; interviewing children; cyber-bullying)*
6	*Crimes against humanity, genocide, war crimes (determination of the crime of genocide, crimes against humanity, war crimes; information exchange between immigration and law enforcement and prosecution services; investigation specifics: magnitude of evidence, traumatised witnesses and victims; sexual and gender-based violence; use of interpreters; cultural differences; use of open source information; cooperation with authorities of state where crimes were committed)*
7	*Privacy and data protection in cyber-investigations (obtaining the IP address; legal tools and mechanisms for cooperation, EU instruments, agencies role; online hate speech; awareness of data protection issues; border between the right to freedom of expression and relevant legislation; OSINT; exchange of good practice)*
8	*Duty of care (rights and obligations of law enforcement officials and their institutions; ethics and integrity; privacy; rest; chain of command; leadership responsibilities; consequences; management of expectations; dignity; right to be trained and to have continued training; EU values)*

2.21 CSDP Missions

2.21.1 Environmental Challenges

One of the first challenges identified in relation to CSDP missions is recruitment of personnel. It would appear that at times law enforcement officials chosen to be sent abroad might not necessarily possess the relevant specialisations or qualifications to perform functions in a CSDP mission, assignment which requires a very specific set of skills. In addition, most CSDP missions are populated by multinational police, military and civilian staff with different professional cultures and ways of thinking, and therefore flexible personalities are required to be able to adapt quickly to the new work environment in general and the specificities of the mission itself.

Often, missions are too short to instigate long-term change in the host countries. Staff deployed is frequently confronted with a complex national environment and sometimes

sceptical attitudes towards EU projects. Lack of support and engagement by the host country is not uncommon.

A further drawback is the high mission staff turnover in combination with the lack of thorough handovers. New officials therefore not always have the necessary set of information and institutional memory at their disposal; this impacts on the quality of their work. Also, the multiple thematic areas officials may be required to cover, in combination with a lack of resources, hampers the achievement of the expected results.

2.21.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

Pre-deployment training is indispensable. It has been noted that law enforcement officials in many cases are not entirely aware of the mission goals and are not ready for specific CSDP experience. Here, training could support the change in the working habits, helping the transition from an executive to a mentor-monitor-adviser mind-set.

Considering that the mandates of military and civilian missions are different, a closer cooperation between the two was highlighted as important element where training can facilitate achieving better cooperation, coordination and understanding of each other's procedures.

A lack of knowledge concerning conflict prevention and crisis management can frequently be found amongst the deployed law enforcement officials. Training and a lessons-learnt platform would be beneficial.

b) Training needs

Summary

Training needs in the domain of CSDP Missions are related to organisation of CSDP missions and security threats. Pre-deployment training covering soft skills, training in mission planning, strategic coordination and communication is necessary. There is also a need for closer synergies between civilian and military forces and a stronger link between them.

Law enforcement officials need to know the peculiarities of the country they are deployed to, therefore, cultural issues and perspective of host countries on human rights should be part of training. Furthermore, they should understand the basic principles of democratisation and good governance for the prosperity of the host country including protection of civilians, as well as prevention of and fight against corruption and its prevention.

In the domain of security threats knowledge on serious and organised crime, in particular EMPACT priorities and mechanisms, EU cooperation tools and mechanisms to fight security threats, including the role and support from the agencies and other EU entities feature among training needs. Conflict prevention and crisis management are high on the CSDP agenda and therefore training should be considered.

Further details

A mixed training on strategic planning would be beneficial in order to improve cooperation and enhance synergies between the civilian and the military component. CSDP management, command and planning would be beneficial for the mid-management level, including topics on risk analysis, decision-making and duty of care. Training should be more operation-oriented than it has been so far and should promote European identity and values. It has been also

mentioned that specific mission planning training could be of benefit for the EEAS staff in Brussels to design CSDP missions and operations.

Mentoring-monitoring-advising training could facilitate the mind-set change of deployed officials with regard to their role and to further develop their soft skills in the spirit of the mission. All pre-deployment training activities should include aspects of fundamental rights and gender issues, as well as awareness of security requirements (general and mission specific). The rights and obligations of mission personnel combined with anti-corruption awareness and the use of force and weapons must also find a place in training. In order to support the officials in their role as mentors/advisers, psycho-pedagogical content is recommended to be included in the training allowing them to cascade their knowledge in a more efficient way.

Crime prevention and fighting serious and organised crime sometimes is not given sufficient resources in the post-conflict zones, therefore additional attention is required from the mission perspective. Deployed officials should be aware of general trends and modi operandi in such topics like cyber-threats and -defence, terrorist threats, financial investigations and illegal immigration, as well they should possess knowledge in relation to the use of available law enforcement cooperation mechanisms and tools (including judicial components, e.g. JITs), and finally the role of the EU agencies and their capabilities.

Training on the use of databases could capacitate the deployed officials to support the host country in developing and using such. The use of information exchange channels, data protection, private security as well as the handling of sensitive information require special attention.

The main provider for pre-deployment and other mission-related training is the ESDC, whilst also CEPOL has provided training on this topic. This, however, is not considered to be sufficient and is recommended to be reinforced.

List of identified and prioritised training needs

The following list evidences the prioritisation, as done by the Member States, of subtopics in the area of CSDP Missions related training.

1	*CSDP management, command and planning, risk analysis, decisions, duty of care (CSDP command and planning; practical training; structures and systems related to CSDP missions; European identity, values, unity of the EU; culture of knowledge; duty of care; use of force; use of force at civilian missions; enhancing the judicial dimension in CSDP missions and operations' life cycle; main judicial cooperation tools (such as JITs) for presentation to local counterparts and proactive promotion of judicial cooperation; awareness raising for EEAS staff based in Brussels in charge of designing such missions and operations)*
2	*CSDP missions and security threats (security threats: general trends, modi operandi, use of cooperation mechanisms, tools, EU instruments, roles of the agencies; sharing information and databases with non-EU authorities: cultural aspects of migration source countries and their political approach; their position with regard to human rights; instruments for sharing such information; soft skills in advising and mentoring)*
3	*Conflict prevention and crisis management (CSDP planning and decision-making process; common procedures and standards for mission management; awareness raising concerning existing procedures and standards; available EU tools for conflict prevention; information exchange)*
4	*Security and defence environment and the civilian and military capability development processes; Links between civilian and military missions (understanding of EU missions' goals;*

	systematic approach to CSDP; soft skills; CSDP strategic planning; mixed participants: civilian and military; search synergies; delineation of tasks between civilian and military already in planning phase; common understanding of strategic planning of CSDP missions; involving non-police officer experts)
5	*Security Sector Reform (strategic coordination and communication during the entire mission; anti-corruption expertise; reluctance in the host country)*
6	*Serious and organised crime and the Policy Cycle (migrant smuggling; firearms trafficking: information exchange channels; link between migration and security)*
7	*Crime prevention and corruption in the host country (how to operate in a corrupt environment; governance and oversights within rule of law institutions in post conflict countries; CPCC guidance on corruption prevention; recruitment of local staff; procurement of products and services from local of international markets)*
8	*Privacy, data protection, fundamental rights, democratic control, protection of civilians (all training should include the dimension of human rights and gender; rights and obligations of the mission personnel; use of social media; sensitive information handling; protection of information; war crimes, genocide; dealing with children; data protection, data retention; communication channels)*

2.22 Other Needs

This chapter mainly reflects the opinion as gathered from other professional groups and networks in the domain of law enforcement cooperation, which (which representatives) had previously not been consulted during the EU-STNA workshops. The thematic areas listed below are of very specific or a horizontal nature therefore could not be allocated to a particular thematic category. Training needs expressed to a great extent (but not limited to) originate from the strategic objectives of different LEWP networks and expert groups. An overview of the approached professional groups and networks can be found in Annex 4.*2.22.1 Environmental Challenges*

Challenges that can be solved only by other means than training were brought forward by the **European Medical and Psychological Experts Network for Law Enforcement (EMPEN**). They consist in the decrease of resources combined with an increasing work demand and risks, which enhances the psychological strain on law enforcement officials. Unpredictable conditions and schedules, low remuneration, a lack of appreciation combined with high expectations from their hierarchy as well as society add to the stress. In addition, a lack of communication and sharing of information doubles their work and leads to conflicts. Solutions would lie in amending policies and structures, and in financial management

The Association of Police Tactical Units (**ATLAS**) indicates that attacks on mass transportation means (high speed trains, metros, coaches) call for a lot of personnel due to the conditions in these environments. Therefore, this can only be tackled by bringing together several intervention teams.

The **European Network for the Protection of Public Figures** (ENPPF) identified the main challenge in the lack of harmonised European legislation, in particular in the area of threat assessment and the work of protection officers. Due to local laws it is difficult to do background checks on the public in different Member States.

2.22.2 Challenges related to knowledge, skills and competences and related training needs

a) Challenges

The **European Network of Law Enforcement Technology Services** (**ENLETS)** reports about a lack of standardised training for intelligence analysts at all levels. In particular training for senior analysts to manage the analysis process is expected to improve interoperability concerning exchange of intelligence and standardisation of the applied methodologies. Furthermore, there is limited training available on telematic data in modern vehicles, which presents significant opportunities to provide intelligence regarding the vehicle and its movements. in this area.

The **Police Network for Law Enforcement Dog Professionals (Kynopol)** point out the increased use of service dogs for a variety of searches, e.g. the determination of the cause of fires, searches for blood, sperm and human tissues as well as for cartridges and gunpowder. This requires additional training, and exchange of good practice between dog trainers.

For **the Schengen and the Visa Information Systems (SIS VIS)**, the increased exchange of the supplementary information due to the extensive use of the system often brings the SIRENE Bureaux on the edge of their efficiency. Moreover, the new systems and the new processes. as well two interoperability proposals for EU information systems for security, border and migration management will create new challenges for the SIRENE Bureaux. Operators need training in order to deal with this information effectively.

The **Informal Network of law enforcement authorities and expertise competent in the field of cultural goods (EU CULTNE**T) considers the huge variety of all European export-restricted cultural objects as a challenge with a view to the need to train customs officers so thoroughly that they would become experts on the identification of cultural objects.

b) Training needs

EMPEN suggests that some training can help law enforcement staff, even if only at a symptomatic level, to cope with the strain and pressure they experience. Courses on stress management, conflict management and communication might help to take some of that away and make space for improvements, at least in the working together with colleagues.

The training needs indicated by the **Association of the Police Tactical Units (ATLAS**) focus on cross-border coordination and communication in order to improve operations, also with other intervention units, both in urban areas or in a maritime environment. The emphasis lies on cooperation between different types of intervention teams and techniques.

Training needs listed by **ENLETS** include **i**ntelligence analysis, digital forensics for intelligence gathering, Automotive, OSINT (basic and advanced techniques), the examination of drones to recover GSP data and its subsequent interpretation.

For **SIS-VIS**, the evolution of the SIS legal instruments make regular and updated training by means of webinars as well as basic and advanced courses necessary. SIS AFIS training on facial recognition is further mentioned. Existing training initiatives for the SIRENE Bureaux should continue to ensure that the operators have adequate knowledge and skills to deal with the information exchange and in order to alleviate some of the workload. CEPOL and eu-LISA have been providing training on topics like SIS II and Schengen Evaluation as well Train-the-Trainers courses on SIS, VIS and Eurodac.

EU CULTNET indicates that training should always aim at police and customs officials as well as judiciary staff and in cooperation with experts like archaeologists, cultural heritage experts and scientists but also from Europol, INTERPOL, UNESCO, UNOCD, WCO, UNIDROIT, etc. It should promote international cooperation competencies, the harmonisation of knowledge, and the recognition of restricted cultural objects and potential risk objects. Further topics to include are international tools to combat illicit trade of cultural goods, data collection and analysis, new trends, interdisciplinary and cross-border cooperation, cyber-investigation tools, online sale platforms etc.

Training needs listed by the **European Union Intellectual Property Office (EUIPO)** focus on international cooperation issues, common tools (databases, information exchange platforms, EUIPO tools) and cooperative mechanism, criminal IP cases, preservation of evidence, and interagency cooperation for information sharing.

Training and the exchange of good practices on the level of **service dog training (Kynopol**) should contribute to the harmonisation dogs' usage and procedures. Member States could adapt and improve their dog training methods by learning from each other. Specific training topics mentioned are dog training on tracking, cadavers, banknote detection, and patrolling.

ENPPF indicates that joint EU-level training for security officials from various services concerning Joint Task Force cooperation, in particular in case of terror attacks affecting two bordering states and the protection of their leaders, could help achieve better coordination and cooperation. Knowledge on geo-politics and cultural mediation as well as threat assessment in case of foreign visits and CBRN protection could be a vital tool for CP officers. At EU level, CEPOL has provided training on violent attacks against the public (amok shootings) and on security during major events.

The **Operational Network to Counter Mafia-style Serious and Organised Crime (@ON)** generally confirms that the dissemination of knowledge on existing cooperation tools in the fight against organised crime, and in particular with a view to illicit assets abroad is considered imperative. As for other priorities, also here are mentioned a multidisciplinary approach and international/interdepartmental cooperation based on a deep knowledge of the cooperation instruments. A strong focus is put on asset recovery involving knowledge on the use of an administrative approach for seizure and confiscation, and for the prevention of criminal infiltration of the legal economy. Cooperation with Eurojust for JITs and Europol (AP Asset Recovery and AP Sustrans) as well as the use of EU information channels like SIENA and the FIU and the AMON channels are mentioned. And finally, training for end-users in the Member States of the systems is recommended, and Member States need support for this. Both CEPOL and Europol provide a high number of training and learning opportunities at EU level on organised crime-related topics.

Europol pointed out that Mafia style organised crime should be moved to the top of the priority list because the non-recognition of the problem and the lack of capacity building have led to the current situation of national law enforcement structures being significantly weakened and having insufficient resources and capabilities against organised crime and Mafia structures, with a particular focus on drug production and trafficking.

Where it concerns **Football Safety and Security,** training should focus on international cooperation, the development of partnerships and EU-networks as well as the exchange of good practices for the contact with fans. Furthermore, it should aim at harmonisation of approaches for public order, countering the use of pyro-techniques, safety and security measures, and especially such to prevent and counter terrorism in the context of football

events. CEPOL has cooperated with the Pan-European Think Tank of Football Safety and Security Experts to organise an EU-level training activity on this topic. Also its training activities on public order can be helpful here.

As for leadership and (English) language training, these have been regular activities in CEPOL's annual programme, involving an annual two-step activity on EU law enforcement leadership development and the same on professional English terminology.

List of identified and prioritised training needs

The following list shows the prioritisation, as done by Member States, of subtopics concerning other training needs.

1	*English language (specific professional terminology)*
2	*Leadership (leadership strategies; role of the EU; EU values; cooperation mechanisms and information exchange channels; duty of care; fundamental rights; crime prevention; data protection especially in cyber-investigations)*
3	*Schengen Information System (evolution of the SIS legal instruments and subsequent changes to the SIRENE Manual; implementation of the return decisions to the SIS; evolution of the SIS AFIS; training on biometrics; training for SIRENE Bureaux and operators; new systems: ETIAS and EES; interoperability of information systems; training on the SIS for the SIS end-users)*
4	*Football safety and security (exchange of information; cross-border cooperation; international co-operation (UEFA, CoE, INTERPOL, Europol, and other football-related EU networks); information management; established and emerging trends in football- related violence and misbehaviour; sharing good practices of policing football matches; media policy and communication strategy; football security, stadium safety; good practices of fan dialogue; preventing and countering terrorist threat to football and other sports events; preventing and countering use of pyrotechnics in stadia; no safe use of pyrotechnics in spectator areas)*
5	*Intellectual property rights (knowledge gaining [substantive, procedural law and practice] and understanding the mechanisms that facilitate international cooperation; common tools [databases; information exchange platforms; EUIPO tools]; cooperative mechanism; criminal IP case; preservation of evidence; cooperation with other agencies: obtaining information necessary for the investigation and confiscation of proceeds of crime)*
6	*Training on EU project and EU funds management (information and assistance in EU funds' management)*
7	*Stress management, conflict management, communication (burn-out, Chronic Fatigue Syndrome; confrontation with violence, being hurt, aggression (physical and verbal); responsibility for colleagues and victims; EU values)*
8	*Mafia style organised crime (multidisciplinary approach; instruments of police cooperation within European Union and internationally; judicial cooperation; information exchange; detect assets to undergo rotatory procedures; seize and confiscate the illicitly acquired assets by OCG; Analyst Project; FIUs; AMON; JITs; prevention: multidisciplinary approach; administrative approach; criminal infiltration into legal economy)*
9	*Protection of public figures (standards, quick and secure information exchange; good practices; coordination with the military and intelligence units; cooperation with foreign security officers about security modalities; Joint Task Force like cooperation; latest intelligence trends to prevent intelligence actions from non-EU states; close protection planning and performing, tactics in different environment; unconventional/hybrid/ asymmetrical threats; CBRN; Unmanned Aerial*

	Vehicles; threat analysis and prevention; surveillance and counter-surveillance techniques; basics of geopolitics; cultural mediation; emergency response: good practices, case studies)
10	*Training of service dog handlers (exchange of good practices and experiences; determination of causes of fires; blood, sperm and human tissues search; cartridge and gunpowder gasses searches; tracking, cadaver, patrol, banknote detection dogs)*

3. CONSULTATION WITH POTENTIAL EU TRAINING PROVIDERS

CEPOL invited European agencies and other entities, active in the field of internal security and supporting training initiatives, to share their opinion on the prioritisation of training needs in general and to indicate their availability to address by training particular thematic areas.

The following organisations took part in the consultation and expressed their availability to support training:

- 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 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 Security and Defence College (ESDC),
- European Union Intellectual Property Office (EUIPO),
- European Union's Judicial Cooperation Unit (Eurojust),
- European Union Agency for Law Enforcement Cooperation (Europol) and
- European Union Agency for Fundamental Rights (FRA).

3.1 General remarks

EMCDDA, Eurojust and Frontex agreed to the list of training priorities in general whilst, as explained at the beginning of this report, Europol is of the view that the list does not necessarily reflect the operational needs of law enforcement.

In the case of some thematic categories given lower priority by Member States, potential training providers recommended upgrading them.

Europol proposed giving higher priority to MTIC Fraud and Environmental Crime as they are EMPACT priorities,

while EASO and FRA claimed for higher relevance for the issue of Fundamental Rights since it is of a paramount importance to ensure that law enforcement officials are well aware and observe fundamental rights of an individual while exercising their duties.

Europol also pointed out that Mafia Style Organised Crime should be moved to the top of the priority list because the non-recognition of the problem and the lack of capacity building has led to the current situation of national law enforcement structures significantly weakened and having insufficient resources and capabilities against organised crime and Mafia structures, and drugs production and trafficking in particular.

Eurojust emphasised the importance of early involvement of the judiciary when it comes to the exchange of information in particular in complex cross-border cases.

EJTN suggested focusing on common fields based upon common needs rather than common priorities since priorities of judges and prosecutors differ from those of law enforcement officials.

Comments by Europol reflected the fact that some horizontal aspects, such as PNR, JITs as well as organised crime structures (how they operate as a holistic issue and the commodities as well as the crime area related activities they perform) should be reflected in all training categories, which is also one of the conclusions of the EU-STNA.

FRA indicated the Fundamental rights should also be considered as a horizontal, cross-cutting issue to be reflected in all training activities.

EIGE suggested to integrate gender perspective, the issue of traumatic witnesses/victims as well as sexual and gender-based violence in all trainings. Gender perspective should feature in particular in relation to community policing and to crimes where victims/perpetrators are also women – in the modules on prevention of crimes, identification and treatment of victims. Prevention of secondary victimisation should be also addressed. The issue of gender-based violence should be addressed in the context of all crimes.

All consulted stakeholders agreed to support training within their mandates and provided feedback on thematic categories. These comments can be found under the description of each category.

3.2 Thematic remarks

EIGE recommended that the thematic focus ***Fundamental Right****s* should be extended to include gender equality by changing the title to '*Fundamental Rights and Gender Equality'*. Under this category, gender-based violence should be a stand-alone topic, separated from minorities.

Eurojust suggested that, in relation to training in the field of ***Organised Property Crime****,* training should disseminate best practice on how to ensure that linked OPC incidents are identified as such and are consolidated in one investigation and prosecution (not separately as isolated property crime incidents). In addition to that, training on the international dimension should cover instruments for obtaining information on foreign criminal records (ECRIS), on DNA and biometric data, on the application of supervision measures in the country of residence of the perpetrators (as alternative to provisional detention), as well as on transfer of proceedings and of sentenced persons. Furthermore, training should include an introduction to the national legislation of the MOCGs source countries, particularly in relation to concrete investigative measures as well as competent authorities to request those measures, e.g. controlled delivery, undercover investigation, cross-border surveillance, house search, wiretapping, obtaining bank data, obtaining information on revenues and properties, obtaining DNA and biometric data, criminal records, summoning and hearing witnesses/experts, temporary transfer of detainees. In relation to financial investigations and asset recovery in the context of OPC investigations and prosecutions, training should include alternative approaches to money laundering investigations in OPC cases, such as asset seizure and confiscation by equivalent value, multidisciplinary approach and use of civil liability[21]. Frontex called attention to the fact that links between EU external border detections and on-going investigations against OCGs involved in car theft in EU Member States as well as cooperation

[21] For further information on best practices and recommendations for trainings/awareness raising activities, please *see* Reports produced within EMPACT OPC: OAP 2015 OA 8.1 and OAP 2016 OA 7.1.

between border control authorities with police and customs should feature under motor-vehicle crime.

Concerning ***Environmental Crime***, Eurojust suggested training on cooperation possibilities offered by Europol and Eurojust and other bodies supporting the fight against this type of crime.

Eurojust recommended a dedicated training programme to enhance the judicial dimension in the ***CSDP missions*** and operations' life cycle, when and where appropriate. Furthermore, they suggested training for EEAS staff based in Brussels to raise awareness of staff members in charge of designing such missions and operations.

In relation to ***Trafficking in Human Beings*** Europol pointed out that sexual exploitation should be explicitly mentioned as training priority area as still there are characteristics of the crime (for example the Voodoo method for Nigerians or the intra EU trafficking) that demand to continue the efforts on training and awareness. Furthermore, human smuggling should feature among links to other types of crime as migrants are a potential source for various forms of exploitation. EIGE proposed to include the topic of victim protection among training priorities.

Europol`s ECTC came up with an alternative order of priorities in relation to ***Counter-terrorism***: 1.OSINT and social network analysis; 2. Investigations, encryption and e-evidence; 3. Foreign Terrorist Fighters and Returnees; 4. Terrorism Prevention, De-radicalisation and Disengagement; 5. Radicalisation; 6. Terrorism Financing; 7. Critical Infrastructure Protection and Protection of Soft Targets; 8. CBRN, CBRNE; and 9. Fundamental Rights. Furthermore, Europol indicated that the grouping of OSINT and the interoperability of systems is potentially a bit wide, and that the needs mentioned under terrorism financing basically duplicate with what is done in the context of other priorities (drug trafficking, cigarette smuggling, etc.). ECTC's justification for favouring an alternative order of priorities is grounded in the fact to almost all terrorist attacks in the EU there is a strong internet dimension, and it is a real challenge for law enforcement agencies to address the technical hurdles of a highly volatile environment whilst striving to collect information in a constant changing landscape. The amount of digital data investigators are confronted with are huge, and the size, complexity, quality and diversity of these data sets require specialised investigation techniques and data processing applications. Handling digital evidence (e-evidence) needs special training and a certain level of understanding by both the investigators and the prosecutors/ judges.

In relation to ***Criminal Finances and Money Laundering***, Europol also proposes to have one point of cooperation with financial institutions. There should, for example, only be one training activity including both cryptocurrencies and new payment methods in order to avoid duplication.

Frontex asked for giving more focus to the item of situational monitoring and risk analysis under ***Border Management and Maritime Security*** by removing PNR. This latter topic would be better suited/more relevant than ETIAS and EES as systems, according to Europol. Furthermore, Frontex suggested that there should be a reference to EUROSUR related capabilities and services especially in terms of surveillance and situational awareness.

In relation to ***Illicit Trafficking, Distribution and Use of Firearms,*** Frontex recommended to remove "trafficking" from the title as firearms as a topic should be a more general area embracing issues like prevention, legislation, forensic examination. Europol recommended to exclude explosives from this area, as they are not firearms. Some further aspects such as tracing mechanisms, recognition of weapons, particularly firearms, as well as their parts and

the ammunition, if eligible, forbidden, under control measures, duly deactivated, etc. should be included among training needs, according to Frontex. Collaboration between border or coast guard, customs, police and forensics should be highlighted and enhanced and cooperation with INTERPOL should be included.

As for the ***Production, Trafficking and Distribution of Cannabis, Cocaine, Heroin***, Frontex suggested that it should be an aspect of cooperation with customs and border or coast guard. Profiling of shipments, routes and means of transportation, including vessels, as well as the use of modern technologies and services or tools, including analytics, should be added to the training needs.

Both Frontex and Europol emphasised to use the wording “new psychoactive substances (NPS)” so that there is a clear indication on the inclusion of precursors within the area of synthetic drugs.

Frontex called the attention to the fact that fraud related to alcohol products should feature among training needs related to ***Excise Fraud***.

Frontex recommended to widen the training needs portfolio under ***Risk Analysis*** by including items such as the establishment and management of risk analysis systems, including the creation and improvement of specialised risk analysis units at national, regional and local level; Common Integrated Risk Analysis Model (CIRAM); and the development of operational and tactical risk analysis products for border surveillance and check activities.

4. CONCLUSIONS

The outcomes of the EU-STNA provide a picture of an extraordinarily complex environment for law enforcement to grapple with. Crimes and modi operandi are often linked and there is no clear indication where one crime area ends and another one begins. These challenges are multiplied when we consider the new developments in science and technologies as well as the rapid digitalisation of everyday life. Changes of environment and the freedom, which people now have, to move themselves, goods and services across borders, create another area of new challenges for law enforcement. Whilst fortunately fundamental rights are given increasing importance and attention, this growing focus in the context of law enforcement also places new demands on the officials in their everyday work.

Considering the fact that these and other factors are determining people's lives at a personal and professional level, law enforcement training should pay tribute to that. Only thorough and suitable knowledge on specific issues and specialised skills enables law enforcement to confront and tackle these challenges in a professional and effective manner. Cross-border multidisciplinary and interdepartmental cooperation and training are a further key to a successful fight against serious and organised crime and terrorism.

Experts unanimously pointed out that training demand is high: as a rule it is never sufficient and should be continued and reinforced, even those that are provided at EU level by relevant agencies, like CEPOL, Europol, Frontex, eu-LISA, and by relevant entities like ESDC and others. The main goals to be achieved by means of training are not only to maintain current knowledge but also to improve it and to foster performance, to acquire new knowledge and to develop new skills and competencies.

The core capability gaps of law enforcement officials that can and shall be addressed by training include the following cross cutting thematic categories:

- Open Source Intelligence, data collection, analysis and application;
- Financial investigations, money flows, alternative banking, etc.;
- Elements of cyber-investigations, darknet and e-evidence;
- Document fraud;
- Fundamental and human rights;
- Crime prevention;
- Respective areas of forensics;
- Links between different crime areas.

As well as information exchange and cross-border cooperation related:

- Information exchange mechanisms, interoperability of the large scale IT systems, information exchange channels and procedures, including evidence handling, databases, Passenger Name Records (PNR), other, and with a special focus on the Schengen Information System, as well as other upcoming large scale IT systems (ETIAS and Entry-Exit System);
- EU cooperation tools and mechanisms, including Joint Investigation Teams (JITs), the European Arrest Warrant (EAW), freezing order, etc.; and the role and possibilities of the respective EU agencies and other entities.

Also, an increase of the importance of multidisciplinary cooperation and sharing of knowledge is conspicuous. EU-STNA sources overall recommended different law enforcement services

to be involved in training but also the private and academic sector. This is considered a key factor in the fostering of cooperation and of the exchange of information and intelligence between police, border guards, customs and other actors. Joint training with financial and tax authorities, prosecution and judiciary staff as participants or lecturers is frequently mentioned. Also for closer collaboration with the private sector it would be useful to invite them as to share their experiences and expertise; examples of this are the banking and financial sector, IT and communications, NGOs, postal and transport/logistics companies etc.

Better cooperation with non-EU Member States also is considered to require attention. Inviting officials from such countries, where relevant and admissible, to joint training with representatives from the Member States may potentially contribute to building up trust, a common understanding and networks, and hence to better collaboration.

An area which is considered advantageous for the work of law enforcement and judicial staff in the Member States are the support opportunities inherent in the work of EU agencies. Their role, and the support they offer as well as the EU cooperation tools and instruments, such as JITs, the European arrest warrant, the asset freezing order, mutual legal assistance etc. are all topics Member States officials can benefit from, and in particular in the context of EU-level training. Needless to say, that this must also comprise subjects like information exchange channels, like SIENA, SIS and others, as well as the interoperability of the large scale IT systems.

It goes without saying – and with reference to the initial paragraph about the rapid changes in modern day societies – that training always must feature the most recent criminal trends, techniques and modi operandi as well as policy, operational and technological developments.

5. WAY FORWARD

There is an urgent need for continuous coordinated EU-level training in the area of law enforcement. Very likely this will present quite a challenge as all actors involved must strive to address all the relevant and listed areas. In order to build an efficient and coordinated training portfolio addressing internal security threats of the EU, it is suggested to perform the following actions:

- **Coordination** of training activities offered by the agencies is highly relevant, on the basis of a systematic procedure and regular consultations. We, therefore, recommend that the agencies **align their work programmes**, **consult partner agencies, support others by providing trainers and material, and, where applicable, promote participation of the trainees**.
- To avoid overlapping and to improve coordination a mapping and **an analysis of available material on different topics as well as the related training provided** is necessary. This requires substantial additional resources at human and financial level, and a significant amount of time.
- Before training delivery, it is recommended that a **more detailed analysis is performed in each particular area in order to identify the level of proficiency, the urgency of training intervention in particular areas, and the required size and requirements for the target group**. This type of procedure is at present already applied by several JHA Agencies and by the ESDC, in line with their planning cycles and target groups.
- An aspect that can be extracted from the remarks given by the consulted experts is the fact that law enforcement officials often are not aware of the available training provided at EU level. This signals a strong need for **better promotion and visibility of training**.
- In the context of efficacy, it is highly recommended that after a certain period of time an assessment is performed in order to **measure the extent to which the outcomes of the EU-STNA have been addressed by training at EU level**.
- An **evaluation of the EU-STNA process** is planned for 2020. Afterwards, the **methodology will be adjusted** if necessary, **including an interim assessment** of the EU level training needs, and the next full cycle will run in line with the new EU Policy Cycle.
- In line with the latest trends and practices on the level of alignment of training and education throughout the European Union, some **common standards should be set for training on specific law enforcement work areas**. This will positively influence harmonisation of knowledge, and consequently cooperation, and facilitate the coherent implementation of the Rule of Law and the upholding of the EU values. Such a measure will furthermore pave the way for **certification of training** on selected topics, hence encouraging the mutual recognition of law enforcement training and education among the EU member states. This will further enhance trust among services and effectiveness of cross-border law enforcement cooperation.
- Finally this report has been presented to the European Commission (DG HOME), Standing Committee on Operational Cooperation on Internal Security of the Council of the European Union (COSI) and 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 2019-2021**.

ANNEX 1 LIST OF ACRONYMS

AFIS	Automated Fingerprint Identification System (SIS II)
AIRPOL	Law enforcement network of police and border guard units at European airports
AMIF	Asylum, Migration and Integration Fund
AMON	International Anti-Money Laundering Operational Network
API	Advanced Passenger Information
ARO	Asset Recovery Office
ATLAS	Association of the Police Tactical Units
ATM	Automated Teller Machine
CARIN	Camden Assets Recovery Inter-agency Network
CBRN defence	Chemical, biological, radiological and nuclear defence
CBRNE	Chemical, biological, radiological, nuclear and enhanced explosives defence
CCTV	Closed Circuit Television
CELBET	Customs Eastern Land Border Expert Team
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CIRAM	Common Integrated Risk Analysis Model
CoE	Council of Europe
COSEC	Combating Online Sexual Exploitation of Children
COSI	Standing Committee on Operational Cooperation on Internal Security
CSA/CSE	Child Sexual Abuse/Child Sexual Exploitation
CSDP	Common Security and Defence Policy (EU)
CSIRT	Computer Security Incident Response Teams
DDoS attack	Denial of Service attack
DG HOME	Directorate-General for Migration and Home Affairs
DPO	Data Protection Officer
DVI	Disaster Victim Identification
EASO	European Asylum Support Office
EC3	European Cyber-crime Centre
ECDS	European Global Ocean Observing System
ECRIS	European Criminal Records Information System

ECTC	European Counter-Terrorism Centre
EEAS	European Union External Exchange
EES	Entry-Exit System
EFCA	European Fisheries Control Agency
EFE	European Firearms Experts
ECTEG	European Cyber-crime Training and Education Group
EIGE	European Institute for Gender Equality
EIO	European Investigation Order
EJTN	European Judicial Training Network
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMCS	Excise Movement Control System
EMPACT	European Multi-disciplinary Platform Against Criminal Threats
EMPEN	European Medical and Psychological Experts Network for Law Enforcement
ESTP	European Statistical Training Programme
ENFSI	European Network of Forensic Science Institutes
ENISA	European Union Agency for Network and Information Security
ENLETS	European Network of Law Enforcement Technology Services
ENPPF	European Network for the Protection of Public Figures
EnviCrimeNet	European Network for Environmental Crime
ESDC	European Security and Defence College
ESP	Email Service Providers
ETIAS	European Travel Information and Authorisation System
EUCAP	European Union Capacity Building Mission
EU CULTNET	Informal Network of law enforcement authorities and expertise competent in the field of cultural goods
EUIPO	European Union Intellectual Property Office
eu-LISA	European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	EU Asylum Fingerprint Database
Eurojust	European Judicial Cooperation Unit
Europol	European Union Agency for Law Enforcement Cooperation
EUROSUR	European Border Surveillance System
EU-STNA	European Union Strategic Training Needs Assessment

FADO	False and Authentic Documents Online
FATF	Financial Action Task Force
FIU	Financial Investigation Unit
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HVT	High Value Target
IAEA	International Atomic Energy Agency (UN)
IBM	Integrated Border Management
ICMPD	International Centre for Migration Policy Development
ICOM	International Council on Museums
ILO	Immigration Liaison Officers
IMB	International Maritime Bureau
IMPEL	European Union Network for the Implementation and Enforcement of Environmental Law
INCB	International Narcotics Control Board
IOM	International Organisation for Migration
IP	Internet Protocol
ISO	International Standards Organisation
ISP	Internet Service Providers
ISPS	International Ship and Port Facility Security Code
IVTS	Informal Value Transfer Systems
JAT	Joint Analytical Team
J-CAT	Joint Cyber-crime Action Task Force
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
KYNOPOL	Police Network for Law Enforcement Dog Professionals
LEWP	Law Enforcement Working Party
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MLA	Mutual Legal Assistance
MMA	Monitoring, Mentoring and Advising
MOCG	Mobile Organised Crime Group

NFC	Near Field Communication
NGO	Non-Governmental Organisation
NPS	New Psychoactive Substances
OCG	Organised Crime Group
OLAF	European Anti-Fraud Office
@ON	Operational Network to Counter Mafia-style Serious and Organised Crime
OSCE	Organisation for Security and Cooperation in Europe
OSINT	Open Source Intelligence
P2P	Peer-to-Peer
PCCC	Police and Customs Cooperation Centre
PNR	Passenger Name Record
PSD2	Revised Payment Service Directive
RCEG	Radio Communication Expert Group
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SOC	Serious and Organised Crime
SOCTA	Serious and Organised Crime Threat Assessment
SSR	Security Sector Reform
SWAT	Special Weapons and Tactics (team)
THB	Trafficking in Human Beings
TISPOL	European Traffic Police Network
UEFA	Union of European Football Associations
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNODC	United Nations Office on Drugs and Crime
VAT	Value Added Tax
VIS	Visa Information System

ANNEX 2 LIST OF DOCUMENTS CONSULTED

AUTHOR	TITLE	DATE
Commission	Action Plan for strengthening the fight against terrorist financing (annex)	04/02/2016
Commission	Action plan on measures to support Italy, reduce pressure along the Central Mediterranean route and increase solidarity	04/07/2017
Commission	Action Plan on Unaccompanied Minors (2010 – 2014)	06/05/2010
Commission	Action Plan to improve the protection of public spaces	18/10/2017
Commission	Adopting the Practical handbook for implementing and managing the European Border Surveillance System (EUROSUR Handbook)	15/12/2015
Commission	Commission recommendation of 18.10.2017 on immediate steps to prevent misuse of explosives precursors	18/10/2017
Commission	Commission Staff Working Document: Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime	28/11/2016
Commission	Communication ANNEX on the EU Strategy and Action Plan for customs risk management: Tackling risks, strengthening supply chain security and facilitating trade	21/08/2014
Commission	Communication on a Digital Single Market Strategy for Europe	06/05/2015
Commission	Communication on a new EU approach to the detection and mitigation of CBRN-E risks	05/05/2014
Commission	Communication on Action Plan for an innovative and competitive Security Industry	26/07/2012
Commission	Communication on Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks	18/10/2017
Commission	Communication on Action plan to strengthen the European response to travel document fraud	08/12/2016
Commission	Communication on Action Plan to support the protection of public spaces	18/10/2017
Commission	Communication on an Action Plan for strengthening the fight against terrorist financing	04/02/2016
Commission	Communication on better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain	08/07/2014
Commission	Communication on 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
Commission	Communication on delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, ANNEX	21/04/2016
Commission	Communication on Eleventh progress report towards an effective and genuine Security Union	18/10/2017
Commission	Communication on establishing a new Partnership Framework with third countries under the European Agenda on Migration	07/06/2016

Commission	Communication on EU Action Plan against migrant smuggling (2015 – 2020)	27/05/2015
Commission	Communication on EU Action Plan against Wildlife Trafficking	26/02/2016
Commission	Communication on EU Action Plan on return	09/09/2015
Commission	Communication on EU strategy to step up the fight against cigarette smuggling and other forms of illicit trade in tobacco products	06/06/2013
Commission	Communication on European Agenda on Migration	13/05/2015
Commission	Communication on European Agenda on Security	28/04/2015
Commission	Communication on European Border and Coast Guard and effective management of Europe's external borders	15/12/2015
Commission	Communication on exchanging and Protecting Personal Data in a Globalised World	10/01/2017
Commission	Communication on Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking	21/10/2013
Commission	Communication on implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives	02/12/2015
Commission	Communication on Maximising the Development Impact of Migration The EU contribution for the UN High-level Dialogue and next steps towards broadening the development-migration nexus	21/05/2013
Commission	Communication on open and secure Europe: making it happen	11/03/2014
Commission	Communication on Overview of information management in the area of freedom, security and justice	20/07/2010
Commission	Communication on preserving and strengthening Schengen	27/09/2017
Commission	Communication on preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response	15/01/2014
Commission	Communication on safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century	25/01/2012
Commission	Communication on Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)	07/12/2012
Commission	Communication on Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)	07/12/2012
Commission	Communication on Stronger and Smarter Information Systems for Borders and Security	06/04/2016
Commission	Communication on supporting the prevention of radicalisation leading to violent extremism	14/06/2016
Commission	Communication on Tenth progress report towards an effective and genuine Security Union	07/09/2017
Commission	Communication on the Delivery of the European Agenda on Migration	27/09/2017
Commission	Communication on the EU Approach against Wildlife Trafficking	07/02/2014
Commission	Communication on the EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016	19/06/2012
Commission	Communication on the Global Approach to Migration and Mobility	18/11/2011
Commission	Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries	21/09/2010
Commission	Communication on the protection of children in migration	12/04/2017

Commission	Communication on the Review of export control policy: ensuring security and competitiveness in a changing world	24/04/2014
Commission	Communication on Transatlantic Data Flows: Restoring Trust through Strong Safeguards	29/02/2016
Commission	Communication on Twelfth progress report towards an effective and genuine Security Union	12/12/2017
Commission	Communication: Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders	14/09/2016
Commission	Comprehensive Assessment of EU Security Policy	26/07/2017
Commission	Comprehensive Assessment of EU Security Policy	26/07/2017
Commission	Establishing a common "Return Handbook" to be used by Member States' competent authorities when carrying out return related tasks	01/10/2015
Commission	EU anti-corruption report	03/02/2014
Commission	Evaluation of Council Directive 91/477/EC of 18 June 1991, as amended by Directive 2008/51/EC of 21 May 2008, on control of the acquisition and possession of weapons	18/11/2015
Commission	Fifth Progress Report on the Partnership Framework with third countries under the European Agenda on Migration	06/09/2017
Commission	Joint Communication on Cyber Resilience, Deterrence and Defence	13/09/2017
Commission	Migration on the Central Mediterranean route. Managing flows, saving lives	25/01/2017
Commission	Ninth progress report towards an effective and genuine Security Union, Comprehensive Assessment (2 annexes)	06/07/2017
Commission	Progress Report on the implementation of the EU Strategy and Action Plan for customs risk management	19/07/2016
Commission	Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Additional Protocol supplementing the Council of Europe Convention on the Prevention of Terrorism (CETS No. 217)	18/10/2017
Commission	Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196)	18/10/2017
Commission	Protection of the European Union's financial interests — Fight against fraud 2016 Annual Report	20/07/2017
Commission	Recommendation for a Council Decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime	18/10/2017
Commission	Recommendation on proportionate police checks and police cooperation in the Schengen area	12/05/2017
Commission	Report from the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC)	18/04/2011
Commission	Report from the Commission to the Council and the European Parliament. Progress report on the implementation of the Commission Communication "Stepping up the fight against cigarette smuggling and other forms of illicit trade in tobacco products - a comprehensive EU strategy (Com (2013) 324 final of 6.6.2013)"	12/05/2017

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
Commission	Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program	19/01/2017
Commission	Reporting on the follow-up to the EU Strategy towards the Eradication of trafficking in human beings and identifying further concrete actions	04/12/2017
Commission	Risk Assessment and Mapping Guidelines for Disaster Management	21/12/2010
Commission	Staff working document - Executive summary of the impact assessment, accompanying the document on the mutual recognition of freezing and confiscation orders	21/12/2016
Commission	Recommendation on making returns more effective when implementing the Directive 2008/115/EC of the European Parliament and of the Council	07/03/2017
Commission	Staff working document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints	27/05/2015
Commission and HR CFSP	Communication on Addressing the Refugee Crisis in Europe: The Role of EU External Action	09/09/2015
Commission and HR CFSP	Communication on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	07/02/2013
Commission and HR CFSP	Communication on elements for an EU-wide strategic framework to support security sector reform	05/07/2016
Commission and HR CFSP	Joint report on countering hybrid threats - a European Union response	19/07/2017
Council of the EU	Common challenges in combating cybercrime	13/03/2017
Council of the EU	Conclusions of the Council of the European Union and of the Member States meeting within the Council on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism	20/11/2015
Council of the EU	Conclusions of the Council of the European Union and the representatives of the governments of the Member States on the protection of children in migration	08/06/2017
Council of the EU	Conclusions of the Foreign Affairs Council	09/02/2015
Council of the EU	Conclusions on Action Plan on the way forward in view of the creation of an European Forensic Science Area	13/06/2016
Council of the EU	Conclusions on Action Plan on the way forward with regard to financial investigation	13/06/2016
Council of the EU	Conclusions on addressing Trafficking in Human Beings (THB) for Labour Exploitation	09/06/2016
Council of the EU	Conclusions on countering environmental crime	12/12/2016
Council of the EU	Conclusions On EU Return Policy adopted at the Justice and Home Affairs Council meeting of 5 and 6 June 2014.	06/06/2014
Council of the EU	Conclusions on migration in EU development cooperation, Foreign Affairs (Development)	12/12/2014

Council of the EU	Conclusions on organised domestic burglary	13/10/2016
Council of the EU	Conclusions on recommending security checks in case of irregular migration	08/06/2017
Council of the EU	Conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021	19/05/2017
Council of the EU	Conclusions on strengthening the EU internal security's external dimension in the Western Balkans including via the Integrative Internal Security Governance	09/12/2016
Council of the EU	Conclusions on the administrative approach to prevent and fight serious and organised crime	09/06/2016
Council of the EU	Conclusions on the Commission Action plan to strengthen the European response to travel document fraud	27/03/2017
Council of the EU	Conclusions on the continuation of the EU Policy Cycle for organised and serious international crime for the period 2018-2021	28/03/2017
Council of the EU	Conclusions on the creation of an informal network of experts competent in the field of Disaster Victim Identification	12/06/2017
Council of the EU	Conclusions on the EU's Comprehensive Approach	12/05/2014
Council of the EU	Conclusions on the Integrative and Complementary Approach to Counter-Terrorism and Violent Extremism in the Western Balkans	03/12/2015
Council of the EU	Conclusions on the prevention of radicalisation leading to violent extremism	21/11/2016
Council of the EU	Conclusions on the Promotion and Protection of the Rights of the Child	03/04/2017
Council of the EU	Conclusions on the protection of children in migration	08/06/2017
Council of the EU	Conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems	01/06/2017
Council of the EU	Council Conclusions on Developing media literacy and critical thinking through education and training	01/06/2016
Council of the EU	Council Conclusions on EU External Action on Counter-terrorism	09/06/2017
Council of the EU	Council conclusions on Security and Defence in the context of the EU Global Strategy	18/05/2017
Council of the EU	Council conclusions on the Global Strategy on the European Union's Foreign and Security Policy	17/10/2016
Council of the EU	Council conclusions on the role of the youth sector in an integrated and cross-sectoral approach to preventing and combating violent radicalisation of young people	20/11/2015
Council of the EU	Cybersecurity Strategy of the European Union: - An Open, Safe and Secure Cyberspace [JOIN(2013) 1 final attached]	08/02/2013
Council of the EU	Decision on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime	23/06/2008
Council of the EU	Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [Prüm Decision]	23/06/2008
Council of the EU	Draft Action Plan on illicit trafficking in firearms between the EU and the South East Europe region (2015-2019)	14/11/2014
Council of the EU	Draft Council Conclusions on the Joint Communication to the EP and the Council: Resilience, Deterrence and defence: Building strong cybersecurity for the EU - examination with a view to their finalisation	20/11/2017

Council of the EU	EU Action plan on drugs 2017-2020	05/07/2017
Council of the EU	EU Cyber Defence Policy Framework	11/11/2014
Council of the EU	EU Drugs Strategy (2013-2020)	11/12/2012
Council of the EU	EU Policy on Training for CSDP	03/04/2017
Council of the EU	EU Western Balkan counter-terrorism initiative: integrative plan of action	04/12/2015
Council of the EU	European Council (23 and 24 October 2014) Conclusions on climate and energy policy framework	24/10/2014
Council of the EU	European Council (26-27 June 2014) Conclusions on strategic agenda of key priorities (freedom, security and justice)	27/06/2014
Council of the EU	European Union Maritime Security Strategy	24/06/2014
Council of the EU	GENVAL evaluation reports on cybercrime - overall final report and country reports	09/06/2017
Council of the EU	Implementation paper on Renewed European Union Internal Security Strategy and Counter- Terrorism Implementation Paper: first half of 2017	07/03/2017
Council of the EU	Malta Declaration by the members of the European Council on the external aspects of migration: addressing the Central Mediterranean route	03/02/2017
Council of the EU	MASP for Organised property crime Priority	07/11/2017
Council of the EU	MASP for synthetic drugs and new psychoactive substances	08/11/2017
Council of the EU	MASP on attacks against information systems	13/10/2017
Council of the EU	MASP on cannabis, heroin, cocaine	06/11/2017
Council of the EU	MASP on child sexual abuse and child sexual exploitation	06/11/2017
Council of the EU	MASP on environmental crime	07/09/2017
Council of the EU	MASP on excise fraud	18/10/2017
Council of the EU	MASP on facilitation of illegal immigration	18/10/2017
Council of the EU	MASP on firearms	07/11/2017
Council of the EU	MASP on fraud and counterfeiting of non-cash means of payment	31/10/2017
Council of the EU	MASP on missing trader intra community fraud	06/11/2017
Council of the EU	MASP on money laundering	21/09/2017
Council of the EU	MASP on trafficking in human beings	17/11/2017
Council of the EU	Mid-term review of the 2014 JHA strategic guidelines - Exchange of views	22/09/2017
Council of the EU	Opinion on "Combating radicalisation and violent extremism prevention mechanisms at local and regional level"	15-16/06/2016
Council of the EU	Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism	19/05/2014
Council of the EU	Seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"	09/06/2017
Council of the EU	Special meeting of the European Council, 23 April 2015 – statement on migrant situation in the Mediterranean	23/04/2015
Council of the EU	The European Council's strategic guidelines for justice and home affairs	06/07/2014

Council of the EU	Update on the conclusions, recommendations and way forward on INTCEN and Europol threat assessments mechanism	09/06/2017
Council of the EU	Common challenges in combating cybercrime	30/11/2015
Council of the EU	Communication on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe	23/11/2010
Council of the EU & Foreign Affairs Council	Council conclusions on CSDP	18/05/2015
Council of the EU / COSI	Future role of COSI	16/04/2014
Customs Cooperation Working Party	8th Action Plan (2016-2017) of the Customs Cooperation Working Party (CCWP)	11/12/2015
Customs Cooperation Working Party	Directors General of Customs Administration Customs and Inter-Agency Cooperation Meeting report	23/10/2017
Customs Cooperation Working Party	Draft 9th Action Plan developments - discussion	23/10/2017
Customs Cooperation Working Party	Joint Customs Operation - Magnum II, Final report	28/09/2017
Customs Cooperation Working Party/Slovakia	Draft of Final Report on Action 8.6.2 " Regional occurrence for excise fraud (mineral oils)	11/11/2017
EASO	Annual Training Report 2014	01/07/2015
EASO	Annual Training Report 2015	01/05/2016
EASO	Annual Training Report 2016	01/07/2017
EEAS	Strengthening Ties between CSDP and FSJ - Draft Road Map	05/12/2011
EMCDDA	Drugs and the darknet	28/11/2017
EMCDDA	European Drug Report 2017: Trends and Developments	01/06/2017
EMCDDA/Europol	EU Drug Markets Report	2017
ESDC	Approved document on prioritisation European Security and Defence College Training activities	12/07/2017
ESDC	CPCC Training requirements for civilian CSDP missions 2016/2017	29/04/2017
ESDC	European Security and Defence College prioritisation exercise 2018	09/03/2017
ESDC	Priorities for European Security and Defence College training activities in 2018	03/04/2017
ESDC	Prioritisation European Security and Defence College Training activities	13/06/2017
ESDC	Training Programme 2017	24/10/2016
eu-LISA	Annual report on the 2016 activities of the Eurodac central system, including its technical functioning and security pursuant to Article 40(1) of Regulation (EU) No 603/2013	01/05/2017
eu-LISA	Eurodac – 2016 statistics	01/04/2017

eu-LISA	High-level expert group on information systems and interoperability, Final report	01/05/2017
eu-LISA	Protecting Large-scale IT systems developed and/or managed by eu-LISA from modern threats A review of recent developments in IT security and associated technologies	01/012016
eu-LISA	SIS II – 2016 Statistics	01/02/2017
Eurojust	Cybercrime Judicial Monitor (CJM)	01/11/2016
Eurojust	Eurojust meeting on illegal immigrant smuggling	15/06/2017
Eurojust	European Arrest Warrant Casework - Report (2014-2016)	16/05/2017
Eurojust	Implementation of the Eurojust Action Plan against Trafficking in Human beings 2012-2016	17/01/2017
Eurojust	New psychoactive substances in Europe Legislation and prosecution — current challenges and solutions	01/01/2016
Eurojust	Strategic Seminar "Keys to Cyberspace" Eurojust, The Hague, 2 June 2016 Outcome Report	04/11/2016
Eurojust	Tactical meeting on Judicial Cooperation in Tax Crime matters (The Hague, 28 October 2016) – Outcome report	28/10/2016
Eurojust	Terrorism Convictions Monitor (TCM)	01/01/2014
Eurojust	The EAW and Prison Conditions - Outcome Report of the College Thematic Discussion	16/05/2017
Eurojust/Council of the EU	Conclusions of the 12th Annual Meeting of National Experts on Joint Investigation Teams (15 - 16 June 2016, The Hague)	05/10/2016
European Parliament	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))	26/06/2017
European Parliament	European Council meeting on the latest tragedies in the Mediterranean and EU migration and asylum policies	29/04/2015
European Parliament	European Parliament resolution of 11 February 2015 on anti-terrorism measures	11/02/2015
European Parliament	European Parliament resolution of 11 March 2015 on child sexual abuse online	11/03/2015
European Parliament	European Parliament resolution of 17 July 2014 on the crime of aggression	17/07/2014
European Parliament	European Parliament resolution of 9 July 2015 on the European Agenda on Security	09/07/2015
European Parliament	Prevention of radicalisation and recruitment of European citizens by terrorist organisations European Parliament resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI))	25/11/2015
European Parliament	Renewing the EU Internal Security Strategy European Parliament resolution of 17 December 2014 on renewing the EU Internal Security Strategy 2014/2918(RSP))	17/12/2014
European Parliament	Report on the fight against corruption and follow-up of the CRIM resolution (2015/2110(INI))	07/10/2016

European Parliament	Report on the mid-term review of the Stockholm Programme (2013/2024(INI))	04/03/2014
European Parliament	The fight against cybercrime European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI))	25/07/2017
European Parliament and the Council	The EU's comprehensive approach to external conflict and crises	18/12/2013
Europol	Internet Organised Crime Threat Assessment (IOCTA) 2017	01/07/2017
Europol	Serious and Organised Crime Threat Assessment (SOCTA) 2017	09/03/2017
Europol	Activity Report European Migrant Smuggling Centre	2017
Europol	Air Couriers	
Europol	An Outlook on developments in Jihadist Terrorism	
Europol	Annual Report on Euro counterfeiting	
Europol	Asset recovery Survey	
Europol	ATM Malware Technical Report	
Europol	Automated Card Shops	
Europol	Basic guide on virtual currencies for financial investigators	
Europol	Benchmark Exercise Fuel Card	
Europol	Common Law Enforcement Response to Darkweb	
Europol	Early Warning Notifications	
Europol	Enlargement Assessment	
Europol	EU Terrorism Situation & Trend Report (TE-SAT)	09/07/2017
Europol	Europol input for the Post-Visa Liberalisation Monitoring Mechanism	
Europol	Foreign Fighters' Bosnian Contingent	
Europol	Geographical hotspots for crime in the EU	
Europol	Intelligence Notifications	
Europol	Intelligence packages	
Europol	Internet Organised Threat Assessment	
Europol	Migrant smuggling in the EU	
Europol	Migrant smuggling networks	
Europol	North Caucasus	
Europol	Online sexual coercion and extortion as a form of crime affecting children	
Europol	Operational Assessments	
Europol	Quarterly Quantitative Reports on Cybercrime	
Europol	Ransomware: What You Need to Know	
Europol	Schengen police cooperation evaluation	
Europol	Sexual Extortion Strategic Assessment	
Europol	Situation report on ATM attacks	
Europol	The Most Relevant Cryptocurrencies	
Europol	Threat assessment special tactics	

Europol	Trafficking in human beings for labour exploitation	
Europol	Trafficking of illegal firearms from Ukraine to the EU	
Europol	Update on counterfeiting and piracy in the EU	
Europol	Use of Virtual Currencies for Terrorism Financing purposes	
Europol	Visa liberalisation: Migratory and Security Impact Assessment	
Europol	Western Balkans	
Europol	Western Black Sea region Organised Crime Groups involved in organised property crime	
FRA	Apprehension of migrants in an irregular situation – fundamental rights considerations	
FRA	Child-friendly justice - Perspectives and experiences of children involved in judicial proceedings as victims, witnesses or parties in nine EU Member States	01/02/2017
FRA	Country reports for the comparative report on Severe labour exploitation: workers moving within or into the European Union	01/05/2015
FRA	Current migration situation in the EU: Oversight of reception facilities	01/09/2017
FRA	Current migration situation in the EU: Oversight of reception facilities	01/11/2017
FRA	EU Agency for Fundamental Rights work in the 'hotspots'	2018
FRA	European legal and policy framework on immigration detention of children	01/06/2017
FRA	Fundamental rights implications of the obligation to provide fingerprints for Eurodac	01/10/2015
FRA	Fundamental rights of migrants in an irregular situation in the European Union	01/11/2011
FRA	Fundamental Rights Report 2017	01/05/2017
FRA	Fundamental Rights Report 2017. FRA Opinions	01/05/2017
FRA	Fundamental rights-based police training – A manual for police trainers	01/12/2013
FRA	Guidance on how to reduce the risk of refoulement in external border management when working in or together with third countries	01/02/2016
FRA	Healthcare entitlements of migrants in an irregular situation in the EU-28	2018
FRA	Second European Union Minorities and Discrimination Survey (EU-MIDIS II) Muslims – Selected findings	01/09/2017
FRA	Second European Union Minorities and Discrimination Survey (EU-MIDIS II) Roma – Selected findings	01/11/2016
FRA	Severe labour exploitation: workers moving within or into the European Union	01/06/2015
FRA	Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data	13/03/2014
FRA	Violence against women: an EU-wide survey. Main results report	01/04/2014
Frontex	Africa-Frontex 2016 Intelligence Community Joint Report	01/04/2017
Frontex	Eastern Partnership Annual Risk Analysis 2017	2016
Frontex	Eastern Partnership Risk Analysis Network Quarterly: Quarter 1 January–March 2017	01/07/2017

Frontex	FRAN Quarterly: Quarter 1 January–March 2017	01/07/2017
Frontex	Risk Analysis for 2017	01/02/2017
Frontex	Training Needs Assessment 2016 report	01/12/2016
Frontex	Training Portfolio 2017	01/10/2016
Frontex	Turkey-Frontex Risk Analysis Network Annual Risk Analysis 2017	01/07/2017
Frontex	Western Balkans Annual Risk Analysis 2017	01/07/2017
Frontex	Western Balkans Quarterly: Quarter 1 January–March 2017	01/07/2017
Horizontal working party on cyber issues	Summary of discussions – Horizontal working party on cyber issues	26/09/2017
LEWP	Progress report - Conclusions on Action Plan on the way forward with regard to financial investigation	2017

ANNEX 3 LAW ENFORCEMENT GROUPS CONTRIBUTING TO EU-STNA

(In alphabetical order)

EU Policy Cycle EMPACT groups 2018-2021	
1	Cannabis, Cocaine and Heroin
2	Criminal Finances, Money Laundering and Facilitated Assets Recovery
3	Cyber-crime – Attacks against Information Systems
4	Cyber-crime – Child Sexual Abuse and Child Sexual Exploitation
5	Cyber-crime – 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 Expert Groups	
1	Border Management, Coast Guard and Maritime security
2	Corruption
3	Counter-terrorism
4	Crime Prevention
5	CSDP Missions
6	Forensics
7	Fundamental Rights, Hate Crime and Genocide

ANNEX 4 OTHER PROFESSIONAL GROUPS/NETWORKS CONSULTED

(In alphabetical order)

1 AIRPOL - Law enforcement network of police and border guard units at European airports

2 ATLAS Network - Association of the Police Tactical Units

3 EMPEN - European Medical and Psychological Experts Network for Law Enforcement

4 ENFAST - European Network of Fugitive Active Search Teams

5 ENLETS - European Network of Law Enforcement Technology Services

6 ENPPF - European Network for the Protection of Public Figures

7 EU CULTNET - informal enforcement authorities and expertise competent in the field of cultural goods

8 EUIPO - European Union Intellectual Property Office

9 KYNOPOL - Police Network for Law Enforcement Dog Professionals

10 Operational Network to Counter Mafia-style Serious and Organised Crime (@ON)

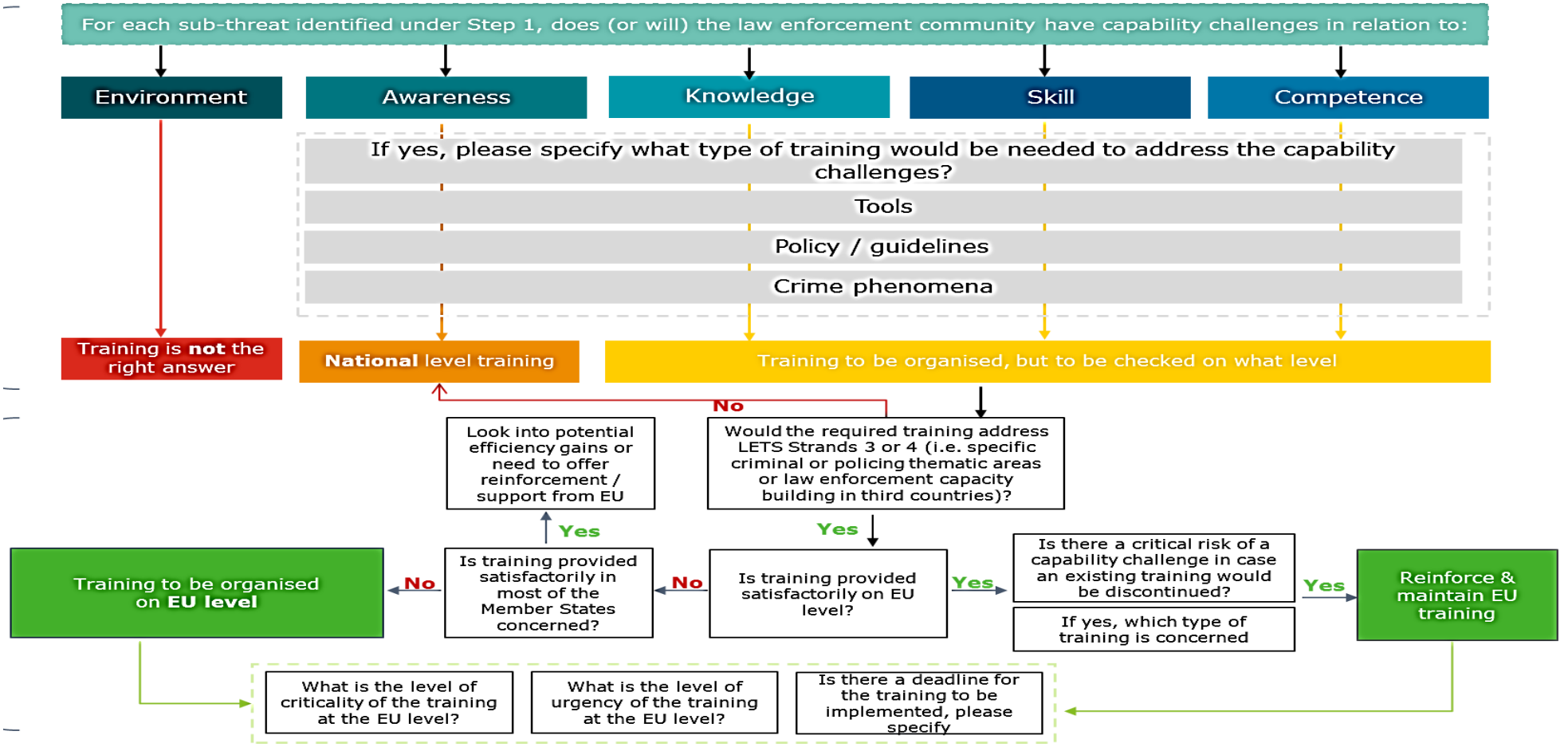
11 Pan-European Think Thank of football safety and security experts

12 RCEG - Radio Communication Expert Group

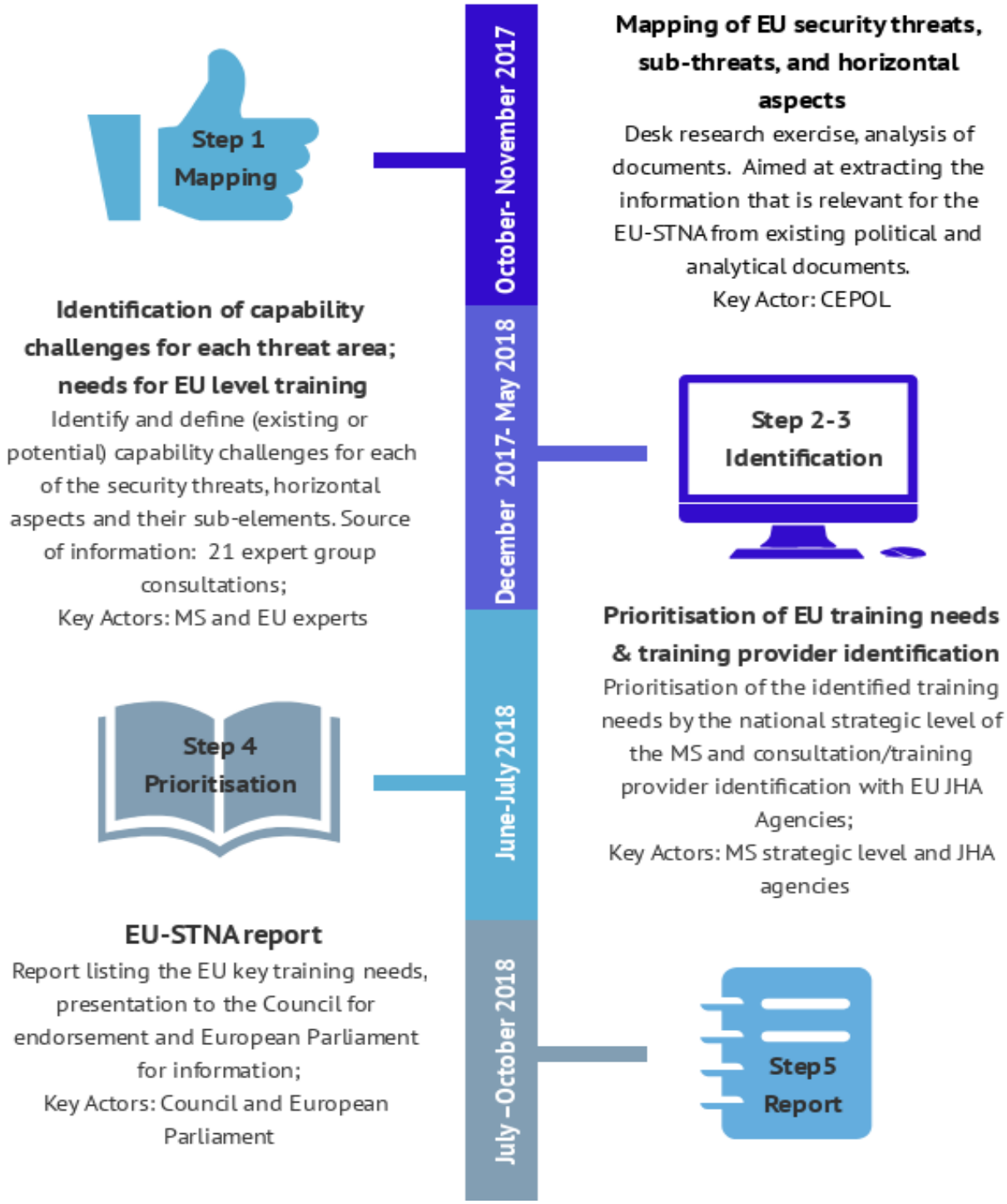
13 SIS-VIS Committee - Schengen Information System – Visa Information System

14 TISPOL - European Traffic Police Network

ANNEX 5 THE DECISION TREE



ANNEX 6 EU-STNA TIMELINE 2017/2018



ANNEX 7 IDENTIFIED EU-LEVEL TRAINING NEEDS

TRAINING NEEDS	POTENTIAL TRAINING PROVIDERS
Facilitation of Illegal Immigration	*Area for EJTN cooperation*
Investigation of illegal immigration cases (techniques; modi operandi; poly-criminality; case studies; exchange of good practices; cooperation with prosecution; THB aspects, including sham marriages)	CEPOL Frontex
Document fraud with focus on identity fraud (impostors; profiling; debriefing; common risk indicators; detection of false documents; new technologies for detection; identification of forged and inappropriately issued breeder documents; document profiling; debriefing; common risk indicators; new modi operandi)	CEPOL Frontex
Returns and PNR (EU instruments; legislation; relevant information systems; in particular the PNR [data assessment]; smart borders; Frontex role in return; human rights)	CEPOL eu-LISA Frontex
Risk analysis and OSINT (OSINT techniques; tools; best practices (CIRAM) involving private parties; Vulnerability assessment; common risk indicators; intelligence used for the investigations; analysis of data on secondary movements; human rights) Frontex recommends removing references of vulnerability assessment (VA) from here as VA has a specific methodology (CVAM) that is different to the one used in risk analysis (CIRAM). VA training under the umbrella of risk analysis might mislead the audience.	CEPOL Frontex
Financial investigations in relation to illegal immigration cases (alternative banking solutions; hawala money transfer system; asset recovery; cryptocurrencies and cryptography; existing EU tools; instruments and networks (CARIN/FIU's/AROs/JITs/ EIO/ PCCC), data protection; cooperation with the private sector)	CEPOL Eurojust Europol Frontex
Prevention of illegal immigration (how to design and implement prevention campaigns from the law enforcement perspective; cooperation between private-public sectors; interagency and international cooperation; including work with the neighbouring non-EU countries)	eu-LISA Frontex
Hotspots (evidence collection and THB identification; unaccompanied minors; human rights; identification of foreign terrorist fighters; profiling; common risk indicators; intercultural competencies; cultural mediation; interviewing techniques; use of interpreters)	CEPOL eu-LISA Europol Frontex
Counter-terrorism	*Area for EJTN cooperation*
Terrorism prevention, de-radicalisation and disengagement ("Lone wolves": understanding the nature of the phenomenon; exchange of good practices; cooperation with the government and the private sector; local and community approach; stronger cooperation with experts from the private sector; terrorism with Islamic roots; extreme right wing; strategies/methods; exchange of experiences; community policing; understanding all the aspects of terrorism)	CEPOL
Foreign Terrorist Fighters and Returnees (sources of recruitment of Foreign Terrorist Fighters; how to deal with returnees: identification and profiling, risk assessment; strategic issues [EU policy]; how to use returnees for disengagement of potential FTFs; exchange of information; best practices; how to deal with returnees and their families; minors [FTFs and returnees]: how to deal with minors, age issues and how to establish their age; fundamental rights)	CEPOL Frontex
Radicalisation (ability to read the signs and recognise terrorism: basic knowledge on indicators, cultural, regional aspects; community policing: links to mosques, shops, communities, evidence of radicalisation; at senior Level: background knowledge on radicalisation theories; OSINT as a tool for evaluation and analysis of trends in society with regard to radicalisation etc.)	CEPOL

Investigations, encryption and e-evidence (raising awareness and promote the use of the existing tools and platforms to exchange information and encourage coordination at multilateral level; exchange best practices and modus operandi with governmental organisations, even broader than the EU; legal arrangements in the context of investigations; use of battlefield information as evidence; JITs and joint operations involving non-EU countries; alternatives to prosecution and conviction in terrorism cases)	CEPOL Eurojust Europol
Critical infrastructure protection and protection of soft targets (scenario training: distinction between hard targets and soft targets; threat assessment of most likely soft targets; data analysis; procedures – security measures; use of CCTV [what can be achieved with these – not the legal framework])	CEPOL
OSINT (use of modern resources [internet etc.] and social network analysis. Exchange of experiences; presentations by specialists [data mining, tools etc.]; importance and ways of sharing intelligence; databases (PNR), interoperability of systems [SIS, VIS, Eurodac, ETIAS, EES, ECRIS]; include experience gathering from private companies) Comment from Europol: the grouping of OSINT and interoperability of systems is potentially a bit wide.	CEPOL eu-LISA Eurojust
Terrorism financing (modi of money flows and alternative banking systems, incl. hawala, role of charities; crypto-currencies and new payment methods; money coming from other types of crime [THB, drug trafficking, cigarette smuggling] with the purpose of raising funds for terrorism [links to other serious crimes]; knowledge on each other's different frameworks at operational level; FATF 40 Recommendations, in particular 9 Special Recommendations on Terrorist Financing; include participants from the judiciary and prosecutors; involvement of the banking sector and other financial experts, customs and the tax office)	CEPOL
Chemical, biological, radiological and nuclear defence (CBRN or also CBRNE); (the reasons that could lie behind such an attack [psychological, legal, other issues]; the means used; does the means lead to an offender profile etc.)	CEPOL Europol
Fundamental Rights (respect for the Rule of Law and democracy; chain: investigation, accusation, trial, conviction; human values; identification of victimhood of a person used for/forced to terrorist actions; dilemma between security measures and human rights; policies and practises for providing support to victims of terrorist attacks and alternatives to prosecution and conviction in terrorism cases)	CEPOL Eurojust
Trafficking in Human Beings	*Area for EJTN cooperation*
Labour exploitation (training for frontline officers and border guards to identify potential labour exploitation victims; training on cultural differences; best practice for THB experts; involving labour inspectors.)	CEPOL EASO Frontex
Child trafficking (training on communication with children, also for judges and prosecutors; identification of trafficked children; better cooperation with social NGOs, labour inspectorates; social media monitoring)	CEPOL Eurojust Frontex
Victim identification (links and difference between THB and illegal immigration and human smuggling; evidence gathering, alternative evidence, victims' rights, also for prosecutors, judges and labour Inspectors; collecting evidence and interviewing techniques targeted at different forms of THB and different categories of victims; financial investigations/skills)	CEPOL Eurojust Frontex
Intelligence analysis (joint training for the national points of contact in EU and international agencies; available tools; databases; services by international agencies; victim identification; awareness for THB as part of OCG crimes; connection with other crimes to which victims are forced)	CEPOL Frontex
Financial investigations and operations, and asset recovery (training on available EU tools; European Investigation Order; financial flows; dismantling of OCGs; banking; business models; behaviour patterns of OCGs; financial investigations and AROs; cross-border dimension on asset recovery; use of intelligence-led investigations including financial investigations, as this can provide a diversity of evidence to be used in addition to victims' testimonies; preferably Train-the-Trainers' type of activity.)	CEPOL EJTN Frontex

Rights of victims (need for training to ensure interests/rights of victims in criminal proceedings: interviewing techniques of victims [traumatised persons, children], victim identification and referral for support; finding alternative ways to evidence gathering instead of victims' testimony; need for national and EU-level training for law enforcement officials, prosecutors as well as judges as they safeguard victims' rights and interest during the proceedings)	CEPOL EASO EJTN Eurojust Frontex
Online and social media (Train-the-Trainers on online investigations; cyber-crime experts can be trained for THB indicators; available tools for internet monitoring and OSINT; cooperation with private companies, judges, prosecutors; communication with cyber-specialists; use of social media; prevention, awareness campaigns, exchange of practices. Information collection and exchange with non-EU countries, basic online investigative skills for THB investigators)	CEPOL Frontex
Prevention (exchange of good practices; common EU campaign; need to adapt campaign as traffickers' modus operandi changes; need to measure effectiveness; multi-agency/multidisciplinary approach)	EUPCN Frontex
Forced and sham marriages (general training , including for judges and prosecutors; establishment of indicators and specific methods for investigation focused on the features of sham and forced marriages and on social media in this context; general knowledge and understanding of the phenomena; how to raise awareness campaigns; how to teach social sectors; Train-the-Trainers to further conduct training in the national language at EU level for frontline officers; interlinkage with the topic of migrant smuggling is strongly needed as the method is also used for facilitated illegal immigration)	CEPOL Eurojust Frontex
Document fraud (for frontline officers, prosecutors, investigators involved in THB)	CEPOL Frontex
Links to other crime types (drugs, firearms) for frontline officials (general training for frontline officers including indicators of other crime, in addition to victim identification, general/awareness training for investigators working in other crime areas)	CEPOL Frontex
Cyber-crime – Child Sexual Abuse and Sexual Exploitation	*Area for EJTN cooperation*
Combating online violence, distant child abuse and live streaming (undercover operations online; tools and mechanisms, including the potential of EU agencies, in particular Europol; experiences from other countries; data protection; human rights)	CEPOL Eurojust Europol
Darknet (undercover operations on darknet and deep web; securing, obtaining and handling of e-evidence; anonymization; new trends; removing material) Comment from Europol: training should be aimed at reaching a certified standard that must be maintained, renewed periodically and should be adaptable to fit within a strong framework governing and supporting undercover operations within each trainee's country. That framework includes working with informant handlers and supervisors or equivalent levels of oversight.	CEPOL EJTN Europol
CSA/CSE investigations (behaviour of offenders; interviewing techniques; data encryption; international cooperation and information exchange; involving IT, forensic and psychology experts; data retention; intelligence gathering and analysis; sharing of operational best practices; involving the judicial community and the private sector; data protection; human rights). Comment from Europol: Low need for an additional course as Europol is an organiser of the annual course on Combating Online Sexual Exploitation of Children	CEPOL Eurojust Europol
Prevention of CSA/CSE (countries with good prevention campaigns to share their experiences with others; EU prevention package; prevention campaigns for law enforcement agencies and judicial authorities; information exchange between law enforcement authorities and border control authorities)	EUCPN Europol
OSINT and social media analysis for victim identification (in-depth training on OSINT and social media analysis; technical skills; best practices; cooperation with non-EU countries and the private sector; data protection; human rights)	CEPOL Europol

Financial investigations in relation to CSA/CSE (money flows; cooperation with FIUs; financial intelligence) Comment from Europol: training is being developed under the EMPACT group on Cyber-crime – CSA/CSE this and next year.	CEPOL Europol
Criminal Finances and Money laundering	*Area for EJTN cooperation*
Tracing and recovery of proceeds from crime (freezing and confiscation of criminal assets; international cooperation)	CEPOL EJTN
Financial investigations (specialised training for investigators and prosecutors on financial investigations and cryptocurrencies; new technologies; darkweb; virtual currencies; anonymous payment methods; cooperation with private sector)	CEPOL EJTN Eurojust
Joint Investigation Teams addressing criminal finances (international legal assistance; role of EU agencies; cooperation with non-EU countries; funding possibilities)	CEPOL EJTN Eurojust
Money mules and crime enablers (modi operandi, mutual legal assistance; different typologies; cooperation with private entities; alternative banking, hawala; cooperation with non-EU countries)	CEPOL
Intelligence analysis (trends and new developments; collect, share and exploit relevant data and knowledge)	CEPOL
Document and identity fraud (mainly for first responders, how to detect and identify, best practices; forged non-ID documents [invoices etc.]; investment fraud; financial instruments; cooperation with private sector)	
Prevention of money laundering (awareness raising campaigns to law enforcement, the judiciary, the public and private sector; identification and sharing of good practices including case studies from investigations and prosecutions, trade-based money laundering; gold and precious metals as means of money laundering)	CEPOL Frontex
Undercover operations (recruiting and handling of, dealing with informants; intelligence collection and sharing abroad; good practices; observation; wiretapping)	CEPOL
Cyber-Crime – Attacks on Information Systems	
Cyber-investigations in general (Information exchange mechanisms, SIENA, role of EU agencies, data analysis, crime-as-a-service, investigation of criminal networks, modus operandi, crime-as-a-service, information collection and exchange with non-EU countries, multidisciplinary approach, cooperation with prosecution and judiciary, JITs, data protection)	CEPOL eu-LISA Eurojust Europol
Digital forensics and e-evidence (analysis in different operating systems, in cloud, data extraction, data protection, data retention, new technologies: cloud computing, cryptocurrencies, block chains, encryption, Big-data, Internet of things, autonomous systems, evidence securing, connections between machines, cooperation with private parties)	CEPOL Europol
Investigation of Network attacks, DDoS attacks (use of methods and not oriented to the use of tools (avoid dependence of tools), tactical - using cyber-simulators with the capacity to set different cyber-scenarios, technical, digital forensics, EU 'live-exercises' to promote closer cooperation and coordination process between public-private sector and "Computer Security Incident Response Team's.)	CEPOL Europol
Cyber-intelligence (analytical tools and intelligence packages, how to interpret data, best practices exchange, cooperation with J-CAT and European Cyber-crime Centre, crime-as-a-service, data protection)	Europol
Protection of critical infrastructure (first responders, intelligence gathering, analysis, cooperation channels and entities, sharing of best practices, common cyber-incident response protocol, data protection)	CEPOL Europol
Cyber-security and Hybrid threats (intelligence gathering ad analysis, international information exchange channels and tools, Cyber-espionage, new technologies, cooperation with private sector and different intelligence entities, cyber-security cases studies)	ESDC Europol

High level OSINT and social media analysis (techniques and tools, 'Free-tools' software, use of existing EU tools and information exchange mechanisms, cooperation with Europol and ECTEG, public communication of Cyber-Incidents)	CEPOL Europol
Undercover operations on darknet (techniques, cooperation with Europol and ECTEG, best practices) Comment from Europol: there are ongoing initiatives and Europol supports EMPACT initiatives and CEPOL's Online trade in Illicit Goods/Services - TOR, darknet	CEPOL
Prevention, cyber-awareness (community policing training in the area of cyber- and cyber-awareness, communication with private sector, media, showman capabilities, EU prevention campaigns, best practices)	CEPOL Europol
Malware investigations (first responders, different scenarios, malware detection and analysis, identification of organised criminal groups who are behind, 'Block chain' investigations, financial investigation elements, cryptocurrencies, data protection)	CEPOL
Illicit Trafficking, Distribution and Use of Firearms and Explosives	
General aspects and changes in the modus operandi (New developments; involvement of non-EU countries; information exchange channels and mechanisms; role and potential of the EU agencies [Europol, Eurojust, Frontex: EUROSUR Fusion Services, PNR, SIENA]; new legislative initiatives and their implications and application, *practical use of Europol`s tools*) Comment from Frontex: the cooperation with INTERPOL should be included as INTERPOL has iARMS system which is even promoted in EU documents.	CEPOL Eurojust Frontex
Firearms trafficking investigations, incl. financial investigations (investigation and information exchange; inclusion of financial investigations and asset recovery offices; seizures; role of CARIN and EFE; joint training with border/coast guard and customs authorities) Comment from Frontex: tracing mechanism should be added	CEPOL
Darknet and undercover operations (new payment methods, e.g. cryptocurrencies; alternative banking; potential links to terrorism financing; online trade)	CEPOL
OSINT (digital investigation techniques on open web; online trade, focus on sellers and buyers; intelligence picture on social platforms)	CEPOL
First responders training (detection; forensic techniques; crime scene investigation; securing of evidence; exchange of best practices and experiences)	CEPOL Frontex
JITs in relation to firearms trafficking (cooperation elements; role of Eurojust and Europol; cooperation with Western Balkans other non-EU countries)	CEPOL
Detection and investigation of document fraud in relation to firearms trafficking (new technologies for detection; identification of forged and inappropriately issued breeder documents)	CEPOL
Prevention (Enhancing existing projects; stronger cooperation with private sector; exchange of best practices in national campaigns related to safety and legal use of firearms)	CEPOL
Organised Property Crime	
OPC investigations and phenomena in general (new changing modus operandi; use of drones; fencing; mobile organised criminal groups and their structure; intelligence of the use of on-line platforms; statistics; administrative measures; poly-criminality; specialist training on cargo theft; pickpocketing and the links to THB; ATM attacks; domestic burglary; different investigative strategies; information exchange on perpetrators; HVTs; Prüm and other instruments; best practice to ensure that linked OPC incidents are identified as such and are consolidated in one investigation and prosecution; obtaining information on foreign criminal records [ECRIS]; application of supervision measures in the country of residence of the perpetrators; transfer of proceedings and of sentenced persons.; introduction to the national legislation of the MOCGs source countries; competent	CEPOL Eu-LISA

authorities to request measures [controlled delivery; undercover investigation; cross-border surveillance; house search; wiretapping; obtaining bank data; obtaining information on revenues and properties; obtaining DNA and biometric data; criminal records; summoning and hearing witnesses/experts; temporary transfer of detainees])	
Financial investigations and asset recovery in OPC cases (International cooperation; cooperation with prosecution and the judiciary; confiscating proceeds of crime; asset recovery; freezing orders; HVTs; involvement of non-EU countries; alternative approaches to money laundering investigations: asset seizure and confiscation by equivalent value; multidisciplinary approach and use of civil liability.)	CEPOL EJTN Eurojust
Motor vehicle crime (modi operandi; cooperation with the industry; technical and forensic possibilities; cooperation instruments and channels) Comment from Frontex: Links between EU external border detections and intra EU investigations and cooperation between border control authorities and police and even customs should be added.	
Crime against cultural goods (identification and recognition of the restricted cultural objects; recognise potential risk objects; involving customs officers; data collection and analysis; identification of and information exchange on looted material; counterfeiting; fake and forged cultural goods; alert and train judicial and cultural authorities to the importance and scale of the phenomenon of illicit trade in archaeological objects; lessons learnt; successful prosecutions; information about the EU directives; better understanding of relevant laws in other countries; EIO; MLAs; International Letters of Request; SIENA; international cooperation and tools: ICOM and UNESCO; good practices; cross-border cooperation; new trends; online trafficking; investigating with IT tools; how to harness technological progresses against traffickers; deep web; OSINT; social media analysis; online sale platforms; financing of organised crime through the illegal trafficking of cultural goods)	CEPOL Eurojust
OSINT (undercover investigations online; online markets; fencing; best practices; tools and techniques)	CEPOL
Administrative approach and prevention in OPC (administrative measures to support the fight against OPC; targeted prevention [potential victims]; including cooperation with private sector; new modus operandi; exchange of best practices)	CEPOL EUCPN
Minors and links to THB (Identification of THB cases; interviewing techniques; age assessment; human rights; involvement of psychologists; minor victims or offenders)	CEPOL
Document fraud in OPC (develop the knowledge and expertise on the link between document fraud and OPC as well as on OCGs producing and providing fraudulent and false documents)	CEPOL Frontex
Drugs – Production, Trafficking and Distribution of New Psychoactive Substances and Synthetic Drugs	
Intelligence, analysis and operations, incl. trafficking methods and routes (intelligence gathering and analysis; sharing cross-border; modus operandi; intelligence-led operational planning; cross-border surveillance; controlled delivery; multidisciplinary approach, i.e. links to other crime areas))	CEPOL EMCDDA Frontex
Profiling and identification of new psychoactive substances/precursors (detection; profiling of shipments; techniques and equipment; international cooperation and cooperation with judiciary and private partners (chemical industry, pharmaceutical companies, post); cooperation with non-EU countries; darknet sales; involve customs and border authorities; profiling regarding natural persons; financial transactions; ways of payment; recognition of and approaching of facilitators)	CEPOL EMCDDA
Detection and dismantling of illicit synthetic drugs labs (latest trends and developments; production methods, production of precursors, instruments and tools; role and potential of the EU agencies; personal safety measures; evidence collection; criminal facilitators; OCGs	CEPOL EMCDDA
OSINT and darknet (online investigations and investigations on the deepweb and darknet, tools and techniques, role of EU agencies and their potential, best practices, cryptocurrency investigations, identification of high value vendors)	CEPOL EMCDDA

Investigations, incl. financial investigations (modus operandi; financial flows; money mules; alternative banking systems; hawala; cryptocurrencies; offshore heavens; cooperation with FIUs and AROs; international cooperation and asset recovery)	CEPOL
Prevention of drug crime (train-the-trainer on social prevention methods; best practices; personal safety; guidelines and standards; involvement of private sector)	EUCPN
Document fraud, mislabelling practices and detection (mislabelling practices; cooperation with industry; risk created by mislabelling; exchange of experiences; cooperation with non-EU countries; detection equipment; container shipment controls)	CEPOL Frontex
Cyber-Crime – Non-Cash-Payment Fraud	*Area for EJTN cooperation*
Investigations (new modus operandi used by the OCGs; exchange of good practices; case studies; witness protection; European tracking systems; the EU most-wanted list; undercover operations; controlled deliveries)	CEPOL Europol
Online investigations, darknet, OSINT (advanced EU-level training; detection and investigation, gathering and securing evidence; live-exercises on darknet cases, e-evidence gathering, securing, handling, and validation; common concept of darknet; darknet and other crimes [Firearms, Drugs, CSA/CSE]); basic training on darknet; second step: platform for the tools; bring together tactical investigators and technical experts to share experiences and to better understand each other's work; exchange of good practices; detection, monitoring and investigations online; how to work on the deep web and the darknet; advanced training for specialists; basic for judicial staff)	CEPOL Eurojust Europol
Cyber-forensic, e-evidence (basic training on the use of tools and software and on encryption; available tools; software; data encryption; evidence; different devices; advanced training on digital forensics, tools and techniques for specialists, including new developments, use of artificial intelligence, big data analysis; analysis of the devices [e.g. amazon drones] and cryptography)	CEPOL Europol
Financial investigation, intelligence and operational aspects (financial investigations; new technologies and developments; tools; modi operandi; sharing good practices; trigger thinking; OSINT; available tools; case studies from different countries to be shared at EU level; capacities of different EU tools and instruments; agencies (e.g. Europol); cooperation mechanisms; undercover operations online; common concept; new intelligence sources; investigation of cryptocurrencies; how to follow the money; online investigations tools; data retention; fake companies)	CEPOL Europol
Social engineering/phishing (recognition and investigation of social engineering and phishing cases; disruption of the criminal industry and crime enablers; darknet for investigators; business email fraud; information exchange; social media analysis; general awareness campaigns for the civil society)	EUCPN Europol
Data protection (practical training on very specific topics; GDPR; training of DPO, [national and EU], information exchange, information protection; new legislation/regulations [e.g. e-Privacy, Police Directive, GDPR, PSD2], application of data protection [when, how and under which conditions] data protection will be applied; the consequences; possibilities of cooperation between law enforcement and the private sector; constraints, limitations, requirements, etc.; implementation of the legal framework in practice; cooperation; communication between experts; data exchange channels; the Budapest Convention; the Convention on Cyber-crime of the Council of Europe)	CEPOL Europol
Prevention (law enforcement officials should be trained on how to communicate with the society on preventive matters [locally and at EU level]; EU-level training to include information on recent modi operandi as a standard; research should be strengthened)	EUCPN Europol
Card present fraud (training for specialists for forensics and investigators; new trends and threats; new rapidly developing technologies (NFC); vulnerabilities; cooperation with private partners and non-EU countries; card fraud recognition; flight purchases)	CEPOL Europol

Card-not-present fraud (specialised training on detection and investigation of CNP fraud; cooperation with private companies and non-EU countries; EU cooperation mechanism, information exchange tools; new technologies; new payment methods; how to work with private companies [DHL, UPC})	CEPOL Europol
Logical attacks on ATMs (for first responders: technical challenges and available services and tools; exchange of good practices; detection; common definition; common understanding; malware analysis; psychical check of the ATMs offenders; including the private sector experts, e.g. the security industry, especially on incident handling)	CEPOL Europol
Document fraud (recognition of fake documents using different technologies; cooperation between different investigation departments; digitalisation; facial recognition; block chains; smart documents; emerging documents; cooperation with investigators and with document fraud departments; modi operandi of the OCGs)	CEPOL Europol
Airline fraud; e-commerce (new payment methods; cryptocurrencies; investigation of those; cooperation with different entities, customs etc.; sharing good practices and case studies; modi operandi; detection and confirmation of the incident for first responders: stakeholders; payments methods applied by providers; new payment methods; basic on national level and more advanced training at EU level) Comment from Frontex: links to various cross border crime such as migrants smuggling, THB, drugs trafficking, etc. should be addressed.	CEPOL Europol
Document Fraud	
Identity fraud (Impostors; modus operandi; identity registration process in different countries; documents requested online; facial recognition)	CEPOL Frontex
Fraudulent ID and travel documents (detection of document fraud; modus operandi; e-documents; trends, developments; training for border guards; new areas of document fraud; new techniques in document verification; security features; involvement of private sector (airlines, hotels, banks); exchange of best practices on biometrics enrolment; document granting and issuing procedures)	CEPOL Frontex
Document fraud investigations (modus operandi; exchange of best practices; tools, databases and information channels including SIENA; Counterfeiting Monitoring System (CMS); database interoperability; links to other crimes; cooperation with prosecution)	CEPOL Eurojust Europol Frontex
Online markets and darknet for document fraud investigators (modus operandi; specific characteristics of the internet; how to monitor the network; future developments; criminal activities on darknet; international cooperation; digital manipulation; security management; involving private sector; risk analysis)	CEPOL Frontex
Drugs – Production, Trafficking and Distribution of Cannabis, Cocaine, Heroin	
Online markets and darknet (cooperation and communication between drug investigation units and specialised cyber-crime units; cyber-crime, darknet, cryptocurrency, open net and social networks, OSINT; new methods, tools and techniques; manual on darknet; good practices; information exchange and cooperation with non-EU countries; multidisciplinary approach)	CEPOL EMCDDA
Illicit manufacturing of drugs, detection (specialised training for first responders and new officers on risk assessment; indicators; chemical substances; production of chemicals; risk assessment of the infrastructure: travel, user facilities, surveillance; interpretation of data; identification of modi operandi; precursors: new modi operandi methods, current trends and concealment methods; intelligence through INCB and international cooperation)	CEPOL EMCDDA Frontex
Criminal profiling regarding legal and national entities (drugs; container shipments; profiling; company profiling [wittingly and unwittingly exploited] and cargo shipments; profiling regarding natural persons; financial transactions; ways of payment; recognition of facilitators and how to approach them)	CEPOL

Comment from Frontex: add or specify profiling of shipments, routes and means of transportation, including vessels, as well as using modern technologies and services or tools for this reason, including analytics.	
Prevention (training for prevention officials on communication methods and how to reach people on social media; good practices exchange with other countries; joint prevention campaigns; Train-the-Trainers: basic prevention elements of the drug use; cooperation with NGOs; profiling of parcels by DHL other postal services; prevention of cannabis cultivation)	
Investigations, incl. financial investigations (exposure techniques; concealment methods; new tools and methods for investigations; overview of legislation in different countries concerning financial investigations; cryptocurrencies and alternative banking; trends, modi operandi)	CEPOL
Detection and dismantling of illicit laboratories (personal protection; suspicious indicators [smell, products], also for prosecutors; data entry: information on modi operandi and new trends should be entered in a database with most recent examples of daily operations; exchange of good practices)	CEPOL EMCDDA Eurojust
Links to other types of crimes (firearms; THB; migrant smuggling; OPC; exchange of good practices at EU level about OCGs and their way of working; links to other crimes; organised motorcycle gangs, etc.)	CEPOL EMCDDA
Document fraud (specialised training for investigators and prosecutors; identification and sharing of knowledge and good practices)	CEPOL Eurojust Frontex
Border Management and Maritime Security	
Prevention and detection of document fraud and identity fraud (fraud recognition; procedures, protocol; tools and equipment; risk analysis; cooperation with border/police operators, customs, forensic experts, consulate/embassies, document issuing authorities, also private sector/airlines; transport document control; specific falsified documents; English course on specific terminology; sharing good practices; identification of the nationality of the person; exchange of information [also with non-EU authorities]; EUCAPS, military and police cooperation)	CEPOL Frontex
Prevention of serious and organised crime and terrorism from the border/coast management perspective (EU Maritime Security Strategy 2014 and implementation reports; risk analysis at an early stage [before the vessel arrives in the port]; common procedures and definition for ferries, cruises, postal vessels, pleasures vessels, cargos; harmonised approach to check persons and cars; maritime customs activities; PNR in maritime security; joint training of border guards and police and other services to foster mutual trust and information and intelligence exchange and improving communication; cooperation with the private sector)	Frontex
Maritime surveillance and operational preparedness (interagency cooperation; exchange of practice; practical training; operation of different assets in different situations in dangerous, out-of-the-ordinary meteorological conditions; operational preparedness 24/7: need for unified guidelines and training on the common procedures; refresher training courses at EU level as well as proficiency training within the maritime aspect; link to the external dimension (ECDS); Standard operational procedures concerning fundamental rights) *Comment from Frontex: There should be a reference to EUROSUR related capabilities and services (as it results from the EU Regulation), especially in terms of surveillance and situational awareness.*	Frontex
Border management and organised criminal groups (European Integrated Border Management strategy for different targets groups at all levels; study visits for mutual learning [technical possibilities]; OCGs: new trends, phenomena, modi operandi; cyber-crime: good practice exchange; basic knowledge to use cyber-investigation tools; cooperation with cyber-specialists; for first responders: awareness raising on exchange systems and tools, (Schengen information system) and their functioning; emphasis on data quality; screening the mixed	Eu-LISA Frontex

flows; unregistered migrants; fingerprinting, evolution of the SIS AFIS; standard operational procedures concerning fundamental rights)	
Situational monitoring and risk analysis (risk analysis; interoperability with the involvement of Frontex; identification of high-risk travellers; PNR; security control of ships; Common Control Centres; involving private partners and shipping companies) *Comment from Europol: PNR is out of context here; interoperability with EU systems or national risk assessment instead of interoperability with Frontex*	Frontex
Hotspots (THB, vulnerable groups, asylum seekers; managing (securing) of Hotspots; harmonising approaches; dealing with falsified documents; Fast Intervention Teams; specific English language for de-briefers; psychological profiling (e.g. Foreign Terrorist Fighters); cooperation with NGOs; prevention)	CEPOL Frontex
Internal borders, secondary movements (biometric data for the detection of multiple identities; protection on unaccompanied minors and separated children; behaviour analysis; interoperability of systems, SIS, VIS, ETIAS and EES, and others) *Comment from Europol: PNR would suit here better than ETIAS and EES*	CEPOL Eu-LISA Frontex
Ensuring freedom of movement, fundamental rights (ensuring rights of travellers; data protection and privacy issues; interoperability of systems; SIS, VIS, Eurodac, ETIAS, EES, ECRIS)	CEPOL Eu-LISA Frontex
Search and Rescue Operations (cooperation between Member States and non-EU countries in order to enhance efficiency and efficacy; procedures under adverse conditions; specialised medical treatment and first aid included in training on SROs; exchange of good and established practice)	Frontex
Identification of victims and vulnerable groups (Behaviour analysis techniques supporting identification, body language, facial expression, micro-mimics, level of vulnerability; interviewing techniques; cultural, religious aspects; indicators)	Frontex
Migrant smuggling cases and THB (other crimes: firearms trafficking, drugs trafficking, etc.; EU Policy Cycle in general; latest trends in smuggling of migrants, THB, including modi operandi, trends; exchange of good practice; connection with OCGs subject; information on the available and upcoming legislative initiatives, modifications at EU level; new technologies and interoperability of systems; risk analysis methods and profiling of vessel behaviour; behaviour analysis; cultural awareness, mediation and interview techniques; implementation of the return decisions to the SIS; EU Maritime Security Strategy 2014 and implementation reports; maritime cross-border criminality; Maritime Threat Analysis including all types of documents concerning persons and goods; Aquapol cooperation)	CEPOL Frontex
Environmental crime from the border management perspective (detection; technologies; protected species; illegal trafficking)	CEPOL Frontex
Maritime security threats (piracy, armed robbery; training for relevant law enforcement officials on maritime security threats; ship security; joint operations)	Frontex
Crime Prevention	
Prevention of terrorism (recognition of early warning indicators; multidisciplinary cooperation; sharing information between Member States; good practices; common understanding of the crime prevention; risk assessment; knowledge on the different types of terrorism and related crime prevention steps; private sector; awareness on radicalisation, including aspects of potential infiltration in the military training; identification, profiling)	CEPOL

Cross-border information exchange for administrative purposes (between field officers and case officers; between law enforcement and administrative bodies; administrative approach; EU information exchange channels, mechanisms, tools, like SIENA, SIS, VIS, EURODAC, ETIAS, EES, etc.; role of different agencies)	CEPOL EUCPN Eu-LISA Frontex
Prevention of SOC (including cyber-crime; administrative tools to prevent, counter, disrupt and suppress SOC; backgrounds, modus operandi, root; for management level: change the view / perception of prevention (particularly at senior level); show that crime prevention is effective; different elements and steps in crime prevention; creation of a good and effective crime prevention policy; offender prevention: socio-economic factors; recruitment; reasons for involving in criminal activities; special focus on minors, victims, offenders, how to work with them; cooperation with the civil sector, social partners, and industries; cyber-: new tools, developments; role of EU agencies)	CEPOL EUCPN
Multidisciplinary preventive approach and cooperation (awareness of investigators and middle management of the opportunities and importance of crime prevention; administrative approach; cooperation with private sector; building trust; mutual understanding; working in network; prevention and external dimensions: intercultural competencies, different cultures, standards and legislation, cooperation mechanisms with international organisations, private sector etc.)	CEPOL EUCPN
Prevention of the misuse of legal frameworks, corruption (misconduct and trust to police; for top managers: corruption and crime prevention; definition; policy documents; indicators; building culture of and respect the legality; threats against employees as well as decision-makers; rights of law enforcement)	CEPOL EUCPN Frontex
Forensics	*Area for EJTN cooperation*
Securing and processing evidence (crime scene recovery: what to recover and how; assurance that the evidence complies with the chain of custody; ISO Standard 21043; evidence management system [high level of variation between Member States])	CEPOL Frontex
Collection, handling, processing, use and reporting of forensic data (formulating reports and understanding submitted data and reports [for forensic experts and professionals outside of the forensic area]; P2P network, data sharing in a centralised way; validation and update of the databases; Present data evidence to court: understanding of the technology; combination of different types of data [physical and digital]; training at judiciary level in terms of acceptance of new forensic developments in the use within the legal system; use of forensic science developments in legal proceedings and pre-trial investigations, digital forensic science; chain of custody and evidence strength and resistance; evolution of the SIS AFIS)	CEPOL Frontex
Gathering evidence from a crime scene, CSI (police, forensic practitioners, judiciary staff and first attending officers and Investigators should be involved at different levels in this activity: good practice and cooperation; specific data and substances collected; knowledge required; quality assurance by the technical staff; training for middle management: ISO Standard and to what extent it facilitates standardisation and uniformity; documentation techniques from good enough until excellent; good practices on Crime Scene Examination, the technical/scientific interpretation of the facts (Volume Crimes versus Major Crimes); cross-border crime scene and united evidence management)	CEPOL Frontex

Digital forensics and e-evidence, cyber-enabled crimes (constant updating of hardware; continuous training on digital market and digital media; how to interpret what you have and how to present it; fake news; new challenges: electricity vehicles forensic, drones forensic [the examination of drones to recover GSP data and its subsequent interpretation]; internet of things' forensics; social media and instant messaging forensics; digital evidence on digital traces; way to gather information and to treat it; e-discovery methodology and utilising this for intelligence gathering)	CEPOL
Interpretation of results, (transparent) formulation of conclusions and case assessment and interpretation (opinion-based vs. factual results; DNA interpretation. Potential or limitation of Likelihood Ratio (LR) calculations; [common understanding of] fingerprints; factual evidence plus indirect evidence interpretation in conjunction; strands of evidence such as likelihood ratio and interpretation methods, investigation, intelligence to approach accuracy; awareness raising; target group: forensic professionals; common methodology in the EU Member States)	CEPOL
Standardisation of case work methods (legal framework on EU and national level; use of compatible databases; exchange of good practice manuals and sharing ideas through expert meetings; forensic case management process harmonisation at EU; unified EU forensic report layout)	
Document examinations (document examination techniques, high tech crime experts, document fraud)	CEPOL Frontex
Financial forensics (training of forensic auditors; analysis and financial investigations)	CEPOL
Technology Watch and forensics in relation to firearms (new tools, approaches, solutions; involving researchers and academia)	CEPOL
Training for ballistic experts (best practices; new developments; experiences of other countries; different automated ballistic systems; data protection)	
Specific crime areas and related forensic disciplines (e.g. drugs, other; knowledge on NPS and precursors; explosives; trafficking; nanoparticles and nanomaterial; involving expertise from academic; training of technical assessors with SOC knowledge (accreditation); identification of incoming refugees; cross-border fraud in money flows, alternative banking systems, cryptocurrencies; CBRN; Smuggling of goods and persons; online violence)	CEPOL EMCDDA (can cover drug aspects of certain forensic courses)
Fundamental rights in forensics (data protection, the right to be forgotten [GDPR, CCTV, imagery in general terms; collection of evidence; interviewing children; retention and destruction of items, physical and electronic; secure access solutions on biometrics)	CEPOL
Corruption	*Potential area for EJTN cooperation*
Financing and facilitating organised crime, anonymous payments and corruption, cross-border cooperation (criminal and procedural codes; modi operandi; sharing of good practice; legal frameworks: use of agents provocateurs; the use of full transcriptions in court; training on cryptocurrencies: modi operandi; tracking financial transactions; tactics; cooperation with banks; anonymous bank accounts; long money flow to enhance the understanding of criminal transactions; financial	CEPOL EJTN Eurojust

criminal analysis for analysts; strategies to disrupt criminal structures; cooperation with the private sector; detection of informal and secret ways of financing political parties; tracking financial transactions in relation to public procurement; seizures of tax declarations, financial transactions, process of tax declaration, use of hawala; interagency and cross-border cooperation with a specific focus on anti-corruption: use of SIENA, and other information sharing channels at EU level; collaboration between Member States in the gathering of evidence; knowledge on collaboration possibilities; involve judiciary, prosecution, and private sector)	
Ethics and integrity in public administration (assessment of risks and vulnerabilities related to corruption; horizontal issue in the context of corruption: sensitisation by means of training, prevention; conflict of interests; state capture; risk assessment in the context of large public projects; corruption in the public procurement process; how to recognise the possibility of corruption; obligation to report about suspicious transactions; best practices on verification of persons; anti-corruption assessments of legislation. Involve judiciary, prosecution, and private sector)	ESDC Eurojust Frontex
Evidence collection and reporting techniques (uniform way of gathering and presenting data; use of data in court [law enforcement officials and prosecutors]; assessment of evidence for judges; training for judiciary and prosecution)	CEPOL Eurojust
Informants and witnesses (witness protection; how to attract informants; interviewing techniques in relation to informants; protection of whistle-blowers; involve judiciary and prosecution)	CEPOL Eurojust
Corruption in sports, suspicious money transfers (use of analytical tools to detect corruption; joint training with the private sector; social network analysis; use of IT tools in the context of investigations; geographic special information analysis; techniques to retrieve information from different websites in connection with sports [e-sports]; use of e-sport games to pay bribery and gathering evidence in this context; darkweb, also in the context of online sport games; involve judiciary, prosecution and private sector)	CEPOL
Missing Trader Intra-Community Fraud	
Criminal investigations, innovative techniques (training on JITs, general and advanced level is required; access official databases [customs have no access to police databases and vice versa]; tax authorities/administrations to be invited for training)	CEPOL Eurojust Europol
Carousel fraud crime patterns (General training on the fraud patterns; general overview of the phenomena; custom procedures; information exchange; cooperation mechanism re import and customs data bases.; training also for judges and prosecutors to understand the phenomena; tax authorities/administrations to be invited as well; info on investigation, incl. administrative investigation practices)	CEPOL Eurojust
MTIC fraud in economic sectors (clothing, products from China, Turkey etc.; introduction to MTIC for customs officers; food: acquisition fraud; electricity and gas plus different legislations on gas and electricity; e-Commerce; tax authorities/ administrations to be invited for training)	CEPOL
Financial investigations, anti-money laundering, financial crime enablers (specialised training on financial investigations for investigators and prosecutors in MTIC; exchange of intervention strategies against facilitators in criminal finances; sharing knowledge, trends and modi operandi; modern techniques enabling	CEPOL Eurojust

investigators to follow the criminals and their developments; hawala; cryptocurrencies; alternative banking platforms; money laundering syndicates; underground banking/Informal Value Transfer Systems (IVTS); money mules; asset recovery: asset tracing, identification, valuation, management; non-conviction-based confiscation; cooperation with non-EU countries; collecting evidence for first responders; what to do on the crime scene; how to keep digital evidence admissible later; include prosecutors and judges, and tax authorities/administrations)	
Online investigations, OSINT, darknet (Informant handling; OSINT; identification of OCGs on deep web and darkweb; social media; digital evidence and computer forensics; OCG systems and methods; including tax authorities/administrations)	CEPOL
Intelligence collection and analysis (operational, tactical strategic level; information channels and tools; how to gain access to data; exchange of good practices among authorities from the same country and among Member States; big data analysis, control of movement of goods and related money moves; data protection, banking secrecy; information exchange; analytical tools and software; big data analysis; exchange of data and practice to understand each other's systems and products better; including tax authorities/administrations)	CEPOL
Prevention (awareness raising campaigns for law enforcement, the judiciary and the public; training of relevant actors; identify and share good practice from investigations and prosecutions; including tax authorities/administrations)	CEPOL
Environmental Crime	
Illicit waste trafficking (tools; methods for data collection and analysis; good practices; document border controls; cooperation with non-EU countries and environmental authorities; waste dumping; role and potential of the EU agencies; vessel trafficking; damage evaluation and provide proof to the court) *Comment from Frontex: vessels of interest profiling, monitoring and tracking*	CEPOL Frontex
Investigations, including financial investigations (modus operandi; latest trends; new developments, illegal profits; cryptocurrencies; money flows; evidence collection; JITs; good practices; cooperation with judges and prosecutors; FIUs and AROs; international cooperation; cooperation possibilities provided by Eurojust, Europol and the existing international networks of practitioners dealing with environmental crime)	CEPOL Eurojust Europol
Environmental crime in general aspects (modus operandi, new trends; exchange of best practices; role, support and potential of EU agencies [Europol, Frontex: EUROSUR, EFCA] and other relevant authorities; criminal actors and legal businesses; origin, transit and destination countries)	CEPOL Frontex
Prevention of environmental crime (use of new technologies; cooperation elements with Eurojust, Europol, Frontex, others; cooperation with media, communication techniques; stronger cooperation with academics, NGOs; exchange of good practices)	CEPOL EUCPN Eurojust Frontex
OSINT and darknet, focus on environmental crime (online trade; identification of endangered species; information collection tools and methods; analysis of data; sellers and buyers)	CEPOL
Wildlife trafficking (identification of protected species; better collaboration between customs and border control authorities; role and potential of the EU agencies; intelligence on trafficking routs; good practices)	CEPOL EUCPN

Document fraud, focus on environmental crime (organised criminal groups involved in document fraud; import/export certificates or fraudulent declarations; misclassification of documents; cooperation with relevant authorities; exchange of good practices; cooperation with prosecutors and other relevant stakeholders)	CEPOL Eurojust
Excise Fraud	
Excise fraud, general aspects and links to other serious and organised crime, (modus operandi of OCGs; constant changes in particular in alcohol fraud; links between OCGs; database about illicit sites and data linked to terrorism; excise fraud debriefing about intelligence sharing; money flows; profits of OCGs; interlinks and poly-criminality; interlinks between border police, police and customs; include prosecutors and judiciary staff)	CEPOL Eurojust
Criminal investigation; evidence; innovative investigative techniques (e.g. tracking and tracing; training on EU tools and info exchange mechanisms; new technologies; evidence collection; digitalisation of evidence; JIT (Naples II) is necessary for customs officials; training on new threats, modi operandi, OCG structures; special techniques: how to use controlled deliveries as practical tool of international cooperation; legal differences between the Member States; crime enablers: use of legal business structures, manufacturing, shipping, warehousing, marketing, distribution; involve private sector; administrative investigative practices: good practice, exchange programmes)	CEPOL Europol
Financial investigation in excise fraud cases (anti-money laundering measures; financial crime enablers: money laundering syndicates; underground banking/informal value transfer systems, money mules; criminal finances: bitcoins, block chain, virtual currencies, transfer of cash; the potential role of the FIUs; financial systems; online instruments; modi operandi; following the money; EU tools for financial investigations; asset recovery: importance and timing; good practices; EU tools; cooperation with the private sector; include prosecutors and judiciary staff)	CEPOL Eurojust
Control of external borders vis-à-vis excise fraud, cross-border smuggling (cross-border surveillance mechanisms, techniques and tactics; detection of document fraud; risk profiling; use of equipment and tools; exchange of good practice; legislations of the Member States and how this impacts their action; include non-EU countries; identification of crucial intelligence during seizures; preservation of evidence; searches, document locations and recognition of existing evidence; exchange of expertise and experience in addressing crime detection and prevention; for border guards concerning trade in cigarettes; high level awareness raising for managers; cooperation structures in the Member States; enhancement of the inter-service collaboration including police, border police and customs)	CEPOL Frontex
Intelligence collection and analysis in relation to excise fraud (on operational, tactical and strategic level; for analysts on new techniques, analytical tools, artificial intelligence, big data analysis; JATs; available instruments at EU JHA agencies)	CEPOL
Illicit manufacturing and trade of cigarettes (cheap whites from Eastern Europe; counterfeit products; intra-EU smuggling; dismantling and investigating illegal production sites (for specialists): processes, competencies, role distribution between police and customs, money flows behind the crime and sharing information; EU instruments; sharing information; JITs; external border control, mainly with Turkey, EU Eastern and South East land external border and	CEPOL Eurojust Europol Frontex

Mediterranean Sea borders [both west and east and to lesser extent central]; include border guard, police and customs; aligned controls)	
Monitoring the production of tobacco, supply chain control in terms of raw tobacco, movement of raw materials, precursors, skilled workers, uncontrolled trade of manufacturing machinery (exchange of good practice; information about legislation; tackling illegal trade; legal aspects; multi-agency aspect to be considered; distinction between legal and illegal business; monitoring field workers)	CEPOL Frontex
Mineral oil fraud schemes and tax evasion (mineral oil trade and VAT fraud; fake declarations; misuse of oil products; exchange of good practices; methods, tools, equipment; legislation and procedures; designer fuels: info sheets, wikis with information; electronic devices for detection; training on EUROSUR related services especially in relation to smuggling by sea)	CEPOL
OSINT, e-Commerce (cryptocurrencies; possible future developments; electronic evidence; chain of evidence; storing evidence; OSINT; international agreements; cooperation; exchange of information and intelligence; include law enforcement, prosecution and judiciary; use of the internet for organising illicit distribution; sales of products; advertisement of the illicit products; future potential threats; analysis of data)	CEPOL Eurojust
Prevention (for prevention specialists: exchange of good practices; cooperation with the private sector; tobacco manufacturing; software; artificial intelligence; sharing common and good practice on prevention; public awareness: health campaign; cooperation with shipping warehousing, internet providers; technological innovation to strengthen prevention of crime)	CEPOL
T1 Fraud – fraudulent use of Excise Movement Control System (EMCS) (use of EMCS by OCGs to facilitate their fraudulent activities; criminal analysis)	CEPOL
Fundamental Rights	
Fundamental rights in serious and organised crime and terrorism (stop radicalisation; dealing with victims of terrorist attacks and with crises; fundamental rights of terrorists and returnees; de-radicalisation by means of respectful treatment and respecting fundamental rights; interviewing techniques, how to communicate; stereotypes, racial profiling, prejudice and the immanent risks; exchange of good practice; respecting the rule of law and fundamental rights; include judiciary staff and prosecutors.	CEPOL Eurojust Frontex FRA
Human rights in asylum, visa, migration and integration policy (management and leadership responsibility; sharing good practices; strategies; role of the media and effective communication (awareness, manipulation, terminology); use of force; deprivation of liberty; interview and interrogations; victim-centred approach; stop and search; prohibition of torture and ill treatment; policing of assemblies, public order, crowd control; xenophobia; include judiciary staff and prosecutors)	CEPOL EASO Eurojust Frontex FRA
Hate crime (exchange of good practice; tools and technologies for investigations; Train-the-Trainers' type of activity; mentor program for already existing trainers to share good practises and developing skills in delivering courses)	CEPOL FRA
Gender-based violence, minorities, other vulnerable groups (victim-catered approach; visiting other cultural groups, e.g. religious places; avoidance of double victimisation (interviewing techniques); different legal systems; coordination with victim support organisations; community policing and interaction with minorities)	CEPOL EASO ESDC FRA

Rights of children (Convention of the Rights of the Child, national legislation, international standards and treaties; cooperation with victim support agencies; child abuse and exploitation; unaccompanied minors; trafficked children; interviewing children; cyber-bullying)	CEPOL ESDC Frontex FRA
Crimes against humanity, genocide, war crimes (determination of the crime of genocide, crimes against humanity, war crimes; information exchange between immigration and law enforcement and prosecution services; investigation specifics: magnitude of evidence, traumatised witnesses and victims; sexual and gender-based violence; use of interpreters; cultural differences; use of open source information; cooperation with authorities of state where crimes were committed)	CEPOL
Privacy and data protection in cyber-investigations (obtaining the IP address; legal tools and mechanisms for cooperation, EU instruments, agencies role; online hate speech; awareness of data protection issues; border between the right to freedom of expression and relevant legislation; OSINT; exchange of good practice)	CEPOL FRA
Duty of care (rights and obligations of law enforcement officials and their institutions; ethics and integrity; privacy; rest; chain of command; leadership responsibilities; consequences; management of expectations; dignity; right to be trained and to have continued training; EU values)	ESDC Frontex
CSDP Missions	
CSDP management, command and planning, risk analysis, decisions, duty of care (CSDP command and planning; practical training; structures and systems related to CSDP missions; European identity, values, unity of the EU; culture of knowledge; duty of care; use of force; use of force at civilian missions; enhancing the judicial dimension in CSDP missions and operations' life cycle; main judicial cooperation tools (such as JITs) for presentation to local counterparts and proactive promotion of judicial cooperation; awareness raising for EEAS staff based in Brussels in charge of designing such missions and operations)	CEPOL ESDC Eurojust Europol
CSDP missions and security threats (security threats: general trends, modi operandi, use of cooperation mechanisms, tools, EU instruments, roles of the agencies; sharing information and databases with non-EU authorities: cultural aspects of migration source countries and their political approach; their position with regard to human rights; instruments for sharing such information; soft skills in advising and mentoring)	CEPOL ESDC
Conflict prevention and crisis management (CSDP planning and decision-making process; common procedures and standards for mission management; awareness raising concerning existing procedures and standards; available EU tools for conflict prevention; information exchange)	CEPOL ESDC
Security and defence environment and the civilian and military capability development processes; Links between civilian and military missions (understanding of EU missions' goals; systematic approach to CSDP; soft skills; CSDP strategic planning; mixed participants: civilian and military; search synergies; delineation of tasks between civilian and military already in planning phase; common understanding of strategic planning of CSDP missions; involving non-police officer experts)	CEPOL ESDC

Security Sector Reform (strategic coordination and communication during the entire mission; anti-corruption expertise; reluctance in the host country)	CEPOL ESDC
Serious and organised crime and the Policy Cycle (migrant smuggling; firearms trafficking: information exchange channels; link between migration and security)	CEPOL ESDC Frontex
Crime prevention and corruption in the host country (how to operate in a corrupt environment; governance and oversights within rule of law institutions in post conflict countries; CPCC guidance on corruption prevention; recruitment of local staff; procurement of products and services from local of international markets)	CEPOL ESDC
Privacy, data protection, fundamental rights, democratic control, protection of civilians (all training should include the dimension of human rights and gender; rights and obligations of the mission personnel; use of social media; sensitive information handling; protection of information; war crimes, genocide; dealing with children; data protection, data retention; communication channels)	CEPOL ESDC
Other Needs	
English language (specific professional terminology)	CEPOL Frontex
Leadership (leadership strategies; role of the EU; EU values; cooperation mechanisms and information exchange channels; duty of care; fundamental rights; crime prevention; data protection especially in cyber-investigations)	CEPOL Frontex
Schengen Information System (evolution of the SIS legal instruments and subsequent changes to the SIRENE Manual; implementation of the return decisions to the SIS; evolution of the SIS AFIS; training on biometrics; training for SIRENE Bureaux and operators; new systems: ETIAS and EES; interoperability of information systems; training on the SIS for the SIS end-users)	CEPOL eu-LISA Frontex
Football safety and security (exchange of information; cross-border cooperation; international co-operation (UEFA, CoE, INTERPOL, Europol, and other football-related EU networks); information management; established and emerging trends in football- related violence and misbehaviour; sharing good practices of policing football matches; media policy and communication strategy; football security, stadium safety; good practices of fan dialogue; preventing and countering terrorist threat to football and other sports events; preventing and countering use of pyrotechnics in stadia; no safe use of pyrotechnics in spectator areas)	CEPOL
Intellectual property rights (knowledge gaining [substantive, procedural law and practice] and understanding the mechanisms that facilitate international cooperation; common tools [databases; information exchange platforms; EUIPO tools]; cooperative mechanism; criminal IP case; preservation of evidence; cooperation with other agencies: obtaining information necessary for the investigation and confiscation of proceeds of crime)	CEPOL EUIPO
Training on EU project and EU funds management (information and assistance in EU funds' management)	
Stress management, conflict management, communication (burn-out, Chronic Fatigue Syndrome; confrontation with violence, being hurt, aggression (physical and verbal); responsibility for colleagues and victims; EU values)	Frontex
Mafia style organised crime (multidisciplinary approach; instruments of police cooperation within European Union and internationally; judicial cooperation;	CEPOL Eurojust Europol

information exchange; detect assets to undergo rotatory procedures; seize and confiscate the illicitly acquired assets by OCG; Analyst Project; FIUs; AMON; JITs; prevention: multidisciplinary approach; administrative approach; criminal infiltration into legal economy)	
Protection of public figures (standards, quick and secure information exchange; good practices; coordination with the military and intelligence units; cooperation with foreign security officers about security modalities; Joint Task Force like cooperation; latest intelligence trends to prevent intelligence actions from non-EU states; close protection planning and performing, tactics in different environment; unconventional/hybrid/ asymmetrical threats; CBRN; Unmanned Aerial Vehicles; threat analysis and prevention; surveillance and counter-surveillance techniques; basics of geopolitics; cultural mediation; emergency response: good practices, case studies)	
Training of service dog handlers (exchange of good practices and experiences; determination of causes of fires; blood, sperm and human tissues search; cartridge and gunpowder gasses searches; tracking, cadaver, patrol, banknote detection dogs)	Frontex

CEPOL European Union Agency for Law Enforcement Training
O utca 27, 1066 Budapest, Hungary

T +36 1 8038030
F +36 1 8038032

www.cepol.europa.eu

Budapest, October 2018