Operational Training Needs Analysis
Counterterrorism

EDUCATE, INNOVATE, MOTIVATE

Operational Training Needs Analysis
Counterterrorism
2021

Contents

List of abbreviations

CKC – CEPOL Knowledge Centre

CNU – CEPOL National Unit

EASO – European Asylum Support Office

FRONTEX – European Border and Coast Guard Agency

EU – European Union

EU-STNA – European Union Strategic Training Needs Assessment

FRA – European Agency for Fundamental Rights

LE – Law Enforcement

MB – Management Board

MS – Member State

OTNA – Operational Training Need Analysis

SPD – Single Programming Document

Executive Summary

As defined by the Article 3 of the Regulation 2015/2219, CEPOL shall support, develop, implement and coordinate training for law enforcement officials. The **Operational Training Needs Analysis (OTNA) methodology** (as adopted by the Management Board (MB) decision 32/2017/MB (15/11/2017) and 09/2020/MB (29/05/2020)) establishes a structured training needs analysis procedure taking into account deliverables of the EU Strategic Training Needs Assessment (EU-STNA) process.[1] The methodology was piloted in 2018 with limited number of thematic priorities for CEPOL training portfolio planning 2019, namely CSDP Missions and Counterterrorism. In 2020, CEPOL conducted an analysis on Counterterrorism to grab new developments since 2018. The OTNA report 2022 is an incremental follow-up to the full OTNA 2020, hence limited in scope.

This report describes training priorities in the area of Counterterrorism for 2022, based on the analysis of the data received from law enforcement agencies and CEPOL National Units (CNUs). The analysis is based on the outcomes of the EU-STNA in the sense that main topics rated by relevance are strategic training priorities defined in the EU-STNA.Horizontal aspects of training are those cross-cutting issues that that were identified in the EU-STNA as such to be included in each EU-level training activity for law enforcement. The relevant chapter of the EU-STNA Report is available in Annex 1.

A short-term expert was contracted from the list of individual external experts, to assist CEPOL in the analysis of responses and drafting of the OTNA report.

In October 2020, CEPOL approached both 26 Member States (MSs)[2], and EU structures (hereinafter institutions), to provide direct contact points, dealing with the subject of the OTNA. A total number of 22[3] MSs and 6 EU structures[4] responded to this request, resulting in the nomination of 85 experts who would fill in the survey. Further on, the questionnaire was sent to these nominated contact points and distributed via the CEPOL Knowledge Centre (CKC) on Counterterrorism. This resulted in 75 individual completed answers from different law enforcement (LE) agencies and EU structures indicating an 85% response rate of MSs, which can be seen as a relatively high response rate.

All responses (75) indicated clear relevance for the scope of activity, and the **most relevant main topics** (out of the 15 individual topics) for law enforcement officials in this area were related to:

- **Foreign terrorist fighters** (75% of institutions found it relevant)
- **Radicalisation** (72% of institutions found it relevant)
- **Terrorism/Firearms trafficking** (63% of institutions found it relevant)
- **Financing terrorism** (56% of institutions found it relevant).

---

[1] European Union Strategic Training Needs Assessment aims at identifying those EU-level training priorities in the area of internal security and its external aspects to help build the capacity of law enforcement officials, while seeking to avoid duplication of efforts and achieve better coordination.

[2] The terminology 'Member States' (MSs) hereinafter refers to 26 Member States of the European Union participating in the CEPOL regulation, i.e. all EU MSs excluding Denmark.

[3] Responding countries: Austria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain and Sweden.

[4] Council of the EU, European Commission, European Union Agency for Law Enforcement Cooperation (Europol), European Border and Coast Guard Agency (Frontex), EU Agency for Fundamental Rights (FRA), and European Asylum Support Office (EASO).

The distribution of training needs depending on the indicated relevance rate is as follows:

Table 1. Relevance rate of main topics

Main topic	Relevance rate
Foreign terrorist fighters	75%
Radicalisation	72%
Terrorism/Firearms trafficking	63%
Financing terrorism	56%
Open source intelligence	51%
Encryption technologies used to facilitate terrorism	35%
Aftermath of attack	31%
E-evidence	31%
CBRN, CBRNE	31%
Critical infrastructure protection and cybersecurity	29%
De-radicalisation	27%
Covert Human Intelligence Sources	27%
Public-Private Partnerships in the fight against Terrorism	27%
Protection of soft targets	24%
Hostage-taking	21%

With the aim of better understanding training needs of LE organisations, various **horizontal aspects** were presented for the assessment of respondents under each topic. While their relevance varies depending on the topic, the overall assessment demonstrated that training should put emphasis on:

- **Cross-border exchange of information**
- **Information exchange**
- **Cooperation with non-EU countries**

The topic of *Prevention* had been a subject for de-prioritization in the previous survey among the horizontal aspects, but sliding up to the 4th place for 2022. Interestingly, *Cross-border exchange of evidence, Better use of EU instruments, and Cross-border exchange of criminal intelligence* seem to be equally relevant to all respondents, while also crossing the 50% relevance threshold. According to CEPOL's mandate "in its training activities, CEPOL should promote common respect for, and understanding of, fundamental rights in law enforcement"[5] therefore, in-spite of its low ranking, **fundamental rights should be given priority, at least in content, when designing the training portfolio on Counterterrorism**. This view could be reinforced with the fact that counterterrorism as a law enforcement activity is one of the most intrusive operational frameworks towards privacy and other fundamental rights.

---

[5] 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, Art. 4.

Table 2. Relevance rate of horizontal aspects

Horizontal aspects	Relevance rate
Cross-border exchange of information	85%
Information exchange	84%
Cooperation with non-EU countries	64%
Prevention	57%
Cross-border exchange of evidence	53%
Better use of EU instruments	53%
Cross-border exchange of criminal intelligence	53%
Undercover operations	32%
Common definitions	17%
Knowledge of cultural aspects and history	17%
Fundamental rights	15%
Protection of personal data	11%
Common sanctions	8%

Respondents indicated that **42 084 participants would need training in the area of Counterterrorism in 2022 in the 22 responding MSs and EU structures. By extrapolation it means 42 232 potential trainees from the European Union (26 MSs and EU structures)**[6]. Even though the number of participants indicated demonstrates a significant increase, more precisely in tenfold, compared to 2020 (4 144 participants were indicated by respondents), the overall number of participants extrapolated to the level of 26 MSs is characterised by few MSs (namely Finland, Germany and the Netherlands) indicating a wide distribution of Counterterrorism duties in the law enforcement services. This issue is discussed in more detail below.

Respondents were also asked for any additional topics that could be addressed by training in 2022. While their suggestions varied, the approximation and clustering of additional topics suggests that consideration could be given to:

- **Tactical training**
- **Behavioural threat assessment and management, including the interlink to radicalisation**
- **Evidence gathering from conflict zones**

Background

As defined by the Article 3 of the Regulation 2015/2219, CEPOL shall support, develop, implement and coordinate training for law enforcement officials, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of law enforcement, in particular in the areas of prevention of and fight against serious crime affecting two or more Member States and terrorism, maintenance of public order, international policing of major events, and planning and

---

[6] Median of number of indicated participants was calculated in order to be able to calculate the potential number of attendees should 26 MSs be interested in training. Calculation of extrapolation is based on the median, not the average of number of participants indicated to mitigate the distorting effects of extremely high and extremely low figures.

command of Union missions, which may also include training on law enforcement leadership and language skills.

The SPD 2020-2022 describes Operational Training Needs Analysis (OTNA) as a process to help the realisation of strategic goals through the implementation of operational training activities.

The OTNA identifies training interventions tailored for the MSs needs and constitutes the basis for the CEPOL training portfolio. All thematic areas shall be analysed based on the Operational Training Needs Analysis methodology.

The OTNA methodology (as adopted by the MB decision 32/2017/MB (15/11/2017)) was piloted in 2018 with a limited number of thematic priorities for CEPOL training portfolio planning 2019, namely CSDP Missions and Counterterrorism. OTNA methodology was updated in 2020 (9/2020/MB) based on CEPOL's experience and the feedback received from MSs.

The methodology consists of a series of seven steps, encompassing close and dynamic cooperation with MSs, in particular CEPOL National Units (CNUs) and involving CEPOL Knowledge Centres (CKCs) or where not available, expert groups, in the design of relevant questionnaires and training portfolios. The overall OTNA process entails data collection and analysis, conducted via and corroborated by introductory surveys, detailed questionnaires and expert interviews. The target group referred to in this methodology is law enforcement officials, as defined in Article 2 of Regulation 2015/2219[7].

In the course of November 2020, CNUs provided contact points to law enforcement agencies in their respective countries through filling out an introductory survey. The training needs survey was launched in December 2020 and was completed by 4 February 2021. Analysis, including three interviews[8] was carried out in February and March 2021. CKC on Counterterrorism validated the OTNA report in April 2021 and will design the training portfolio based on its outcomes.

Analysis

Consolidation of data

Data was processed from the online survey platform Qualtrics to Microsoft Excel. The data was synthetized and analysed by Excel functions. Additionally, three interviews were conducted with selected MSs to verify and consolidate the outcome of an increase in training needs.

CEPOL approached both 26 Member States[9], and EU structures, to provide direct contact points, dealing with the subject of the OTNA. A total number of 22[10] MSs and 6 EU structures[11] (hereinafter institutions) responded to this request, resulting in the nomination of 85 experts who would fill in the survey., As a next step, the questionnaire was sent to the nominated contact points and distributed via the CKC on Counterterrorism. This exercise resulted in 75 individual completed answers from

---

[7] https://publications.europa.eu/en/publication-detail/-/publication/c71d1eb2-9a55-11e5-b3b7-01aa75ed71a1/language-en.

[8] Germany (Police, Border Police) and Ireland (Police).

[9] The terminology 'Member States' (MSs) hereinafter refers to 26 Member States of the European Union participating in CEPOL regulation, i.e. all EU Member States excluding Denmark.

[10] Responding countries: Austria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain and Sweden.

[11] Council of the EU, European Commission, Europol, Frontex, FRA and EASO.

different law enforcement (LE) agencies and EU structures indicating an 85% response rate of MSs, which can be seen as a relatively high response rate. Regarding the institutions, 72% of the responses represented the Police, followed by the Judiciary (12%):

Chart 1. Distribution of responding institutions
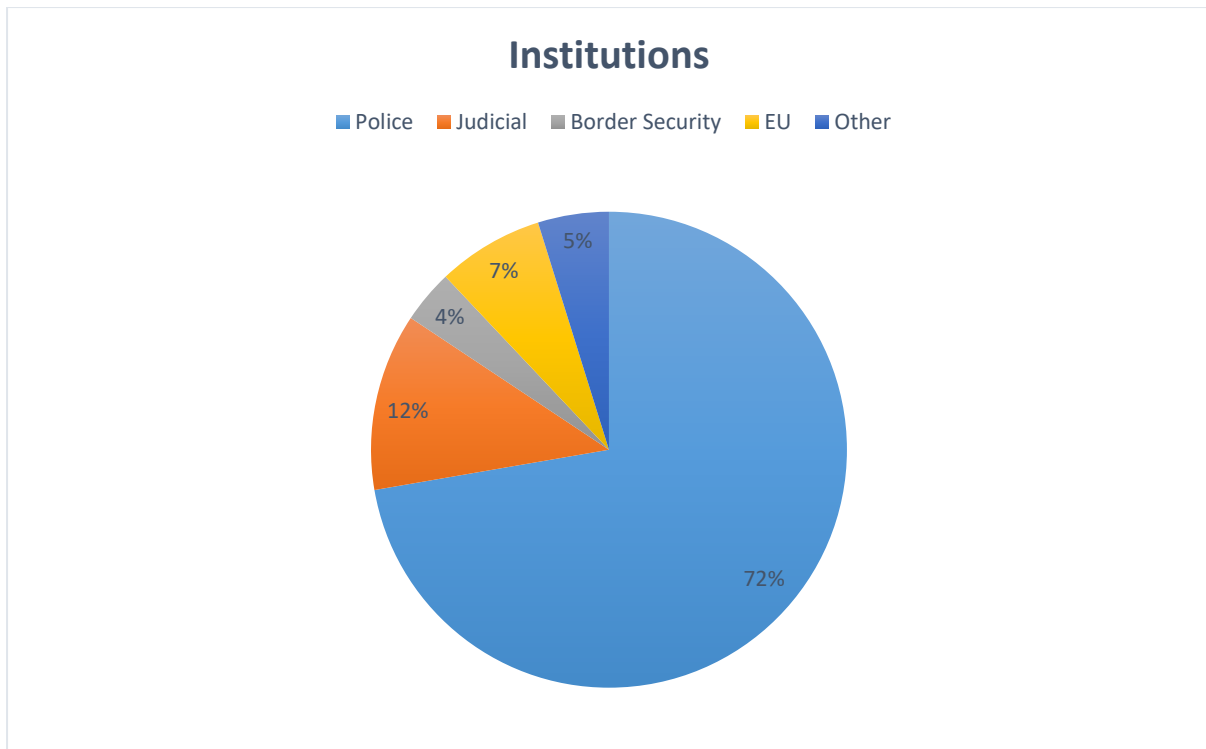
Relevance of topicsPotential training needs were presented based on the outcomes of the survey that took place two years ago, in line with the training priorities defined in the EU-STNA process. Main training topics in relation to Counterterrorism were identified, as follows:

- Terrorism/Firearms trafficking
- Foreign terrorist fighters
- Radicalisation
- De-radicalisation
- Financing terrorism
- Open-source intelligence
- E-evidence
- Encryption technologies used to facilitate terrorism
- Covert Human Intelligence Sources
- Critical infrastructure protection and cybersecurity
- CBRN, CBRNE
- Protection of soft targets
- Aftermath of attack
- Hostage-taking

- Public-Private Partnerships in the fight against Terrorism

All responses (75) indicated clear relevance for the scope of activity and the **most relevant main topics** (out of the 15 individual topics) for law enforcement officials in this area were related to:

- **Foreign terrorist fighters** (75% of MSs found it relevant)
- **Radicalisation** (72% of MSs found it relevant)
- **Terrorism/Firearms trafficking** (63% of MSs found it relevant)
- **Financing terrorism** (56% of MSs found it relevant)

The final relevance rate of a given main topic was calculated by summing up how many institutions found each topic relevant. Where several institutions submitted identical answers from the same MS, entries were consolidated. The ratio of relevance was calculated by dividing the sum of institutions that found the topic relevant, by the number of responding MSs. Training topics where more than 50% of MSs indicated a relevant training need could be considered as adding value for Union-level deployment.

The distribution of training needs depending on the indicated relevance rate is as follows:

Table 3. Relevance rate of main topics

Main topic	Relevance rate
Foreign terrorist fighters	75%
Radicalisation	72%
Terrorism/Firearms trafficking	63%
Financing terrorism	56%
Open source intelligence	51%
Encryption technologies used to facilitate terrorism	35%
Aftermath of attack	31%
E-evidence	31%
CBRN, CBRNE	31%
Critical infrastructure protection and cybersecurity	29%
De-radicalisation	27%
Covert Human Intelligence Sources	27%
Public-Private Partnerships in the fight against Terrorism	27%
Protection of soft targets	24%
Hostage-taking	21%

Identification of horizontal aspects

With the aim of better understanding training needs, various horizontal aspects were presented for assessment under each topic.

Respondents could validate the relevance of each horizontal aspect. The relevance score of each horizontal aspect was calculated by drawing the sum of the responses. Where several LE services gave answers from the same country, the average given by LE services for each horizontal aspect was calculated and used as the relevance level indicated by that particular country.

While their relevance varies depending on the topic, the overall assessment demonstrated that training should put emphasis on:

- **Cross-border exchange of information**
- **Information exchange**
- **Cooperation with non-EU countries**

The topic of *Prevention* had been a subject for de-prioritization last year among the horizontal aspects but sliding up to the 4th place for 2022. Interestingly, *Cross-border exchange of evidence, Better use of EU instruments, and Cross-border exchange of criminal intelligence* seem to be equally relevant to all respondents, and also crossing the 50% relevance threshold. According to CEPOL's mandate "in its training activities, CEPOL should promote common respect for, and understanding of, fundamental rights in law enforcement"[12] therefore, in-spite of its low ranking, **fundamental rights should be given priority, at least in content, when designing the training portfolio on Counterterrorism**. This view could be reinforced with the fact that Counterterrorism, as a law enforcement activity, is one of the most intrusive operational frameworks towards privacy and other fundamental rights.

Furthermore, it could be estimated, with some degree of support from the data, that horizontal aspects with more theoretical and strategic character (such as *Common definitions,* and *Knowledge of cultural aspects and history*) are de-prioritized over more technical/operational-level aspects. Finally, *Common sanctions* has stirred only very low interest, leaving it virtually insignificant.

Table 4. Relevance rate of horizontal aspects

Horizontal aspects	Relevance rate
Cross-border exchange of information	85%
Information exchange	84%
Cooperation with non-EU countries	64%
Prevention	57%
Cross-border exchange of evidence	53%
Better use of EU instruments	53%
Cross-border exchange of criminal intelligence	53%
Undercover operations	32%
Common definitions	17%
Knowledge of cultural aspects and history	17%
Fundamental rights	15%
Protection of personal data	11%
Common sanctions	8%

Respondents indicated that **42 084 participants would need training in 2022 in the 22 responding MSs and EU structures. By extrapolation it means 42 232 potential trainees from the European Union (26 MSs and EU structures)**[13]. Even though the number of participants indicated demonstrates

---

[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, Art. 4.

[13] Median of number of indicated participants was calculated in order to be able to calculate the potential number of attendees, should 26 MSs be interested in training. Calculation of extrapolation is based on the

a significant increase, more precisely in tenfold, from 2020 (4 144 participants were indicated by respondents), the overall number of participants extrapolated to the level of 26 MSs is characterised by few MSs (namely Finland, Germany and the Netherlands) indicating a wide distribution of Counterterrorism duties in the law enforcement services.

As the biggest numbers of participants were reported by Germany and Finland, an interview was conducted to clarify the increase in training needs. As per the interviews with German representatives, the number of potential participants refers to all of the officials dealing with any or all of the main topics in Germany. Similarly, for Finland the number of participants approximates the number of police officers in the police service, thus concurring to the status with Germany. Hence, it can be projected that these MSs have indicated that possibly an awareness-level training could be available e.g. via online modules. This notion is further reaffirmed by the fact that the first responsibility of awareness-level training lies with the MSs, and that the interviewed respondents had not presumed that the responsibility of training would be reassessed.

Table 5. Indicative target group per MS and EU structures

MS / EU	LE officials
Staff of Union bodies	165
Austria	800
Croatia	4
Cyprus	5
Czech Republic	30
Estonia	15
Finland	7 346
France	50
Germany	22 070
Greece	220
Hungary	1 400
Ireland	250
Latvia	32
Lithuania	9
Luxembourg	N/A
Malta	24
Netherlands	6 579
Poland	140
Portugal	316
Romania	68
Slovakia	120
Spain	1 640
Sweden	486
Total	**42 084**

Respondents were also asked to provide any additional topics that could be addressed by training in 2022. While their suggestions varied, the approximation and clustering of topics suggests that consideration could be given to:

---

median, not the average number of indicated participants, to mitigate the distorting effects of extremely high and extremely low figures.

- **Tactical training**
- **Behavioural threat assessment and management, including the interlink to radicalisation**
- **Investigation techniques on terrorism and terrorism financing**
- **Cybercrime, including collecting and managing of e-evidence**
- **Evidence gathering from conflict zones**

As part of processing and approximating the additional topics, an interview was conducted with Ireland to confirm the data submitted in the interview. Ireland indicated that one topic of interest for the police would be Covert Human Intelligence Sources. The topic can be included both under Investigation techniques on terrorism and terrorism financing, but also to a certain extent under Behavioral threat assessment and management.

There are some further considerations when it comes to e.g. tactical training, as it is evident that most tactical training activities may require physical presence, special conditions and equipment, as well as a somewhat limited number of participants at each event, the cost-effectiveness may hence be lower compared to e.g. classroom-type activities.

 Regarding behavioural threat assessment and management, the interviews with German contact points confirmed that there is awareness of CEPOL' previous activities in this field, even though not necessarily under the Counterterrorism portfolio and there is a recognised need to approximate targeted and serious violent crime prevention activities with Counterterrorism activities to manage persons with high risk of violent attacks, such as mass killings.

In terms of terrorism financing, it should be noted that the topic is not only covered in main topics, but it was also considered as one of the most relevant. Furthermore, it should also be noted that when it comes to e-evidence relating specifically to cybercrime, e-evidence has in general been regarded with 31% relevance under main topics; and evidence-gathering from conflict zones could be seen as including also OSINT methodologies with 51% relevance, hence indicating that these topics may likely be addressed by EU-level training instruments at least to some extent The suggested scope of target groups varied as well, however being mostly low or moderate in the number of participants from each MS. The median was 20 participants. Finally, it should be noted that e.g. the suggestion of Ireland on an additional topic of Covert Human Intelligence Sources could be taken into consideration to be included under the main topic of Undercover Operations.

Conclusion

This OTNA report describes training priorities in the area of Counterterrorism for 2022. The relatively high number of respondents and MSs indicates an interest for both the topics under assessment, and the services provided by CEPOL. The OTNA report 2022 is an incremental follow-up to the full OTNA 2020, hence limited in scope. Consequently, direct comparison to the full OTNA may not be possible, nor recommended.

The most **relevant main topics** identified in the OTNA for law enforcement officials (Foreign terrorist fighters; Radicalisation; Terrorism/Firearms trafficking; and Financing terrorism) seem to reflect the crime threats projected in public discussions, and thus confirm the importance of these topics In terms of **horizontal aspects,** the focus should be maintained on the traditional challenges of information

exchange and increasingly on cooperation with non-EU countries. Also, **"new" topics** such as Tactical training; Behavioural threat assessment and management (including the interlink to radicalisation); Investigation techniques on terrorism and terrorism financing; Cybercrime (including collecting and managing e-evidence); and Evidence-gathering from conflict zones were indicated as topics of interest for the MSs.

Finally, as the European Union is founded on the strong commitment towards human rights, it should be noted that inspire of its low ranking, **fundamental rights** should be given priority in content when designing the training portfolio on Counterterrorism. This view could be reinforced with the fact that counterterrorism, as a law enforcement activity, is one of the most intrusive operational frameworks towards privacy and other fundamental rights.

Annex 1. EU-STNA Chapter on Counterterrorism

2.2.1 Environmental Challenges

Counterterrorism measures are to be seen not only as part of law enforcement intervention, but also as part of prevention. Both require cooperation between police and other actors. Investigators need both the public and private sector to support their work, whilst community policing plays a very important role in the prevention of radicalisation, e.g. links to certain communities, religious institutions, etc. Cross-border cooperation is of the utmost importance for counterterrorist experts, though prevention work has a more local focus and demands cooperation with the municipalities, NGOs, the health sector, and social workers.

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

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 require 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 broad perspective, not forgetting that terrorism is a phenomenon involving not only 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 in many cases also prisons.

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

Law enforcement officials 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 actions.

b) Training needs

Summary

For counterterrorist 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, counterterrorism 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 counterstrategies and methods, the exchange of good practices between EU MSs and beyond – as terrorism is a global threat – is imperative, involving representatives of countries with a lot of counterterrorism experience and proven ,tested policies. Scenario training has been highly recommended, and it should include basic knowledge elements, in order to ensure a common understanding (e.g. a common definition of terrorism).

Training should follow a multidisciplinary approach, bringing together investigators from 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 training content.

Training on counterterrorism constitutes a regular element in CEPOL's Annual Programme, and it was underlined that this fact should be maintained or even reinforced.

EU-level training is offered by CEPOL concerning subjects like fighting and preventing terrorism, identification and de-radicalisation of foreign fighters, links between terrorism and organised crime, as well financial crime, while 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 of subtopics in the area of Counterterrorism related training, as done by MSs:

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 promoting 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 that in 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, while striving to collect information in a constantly changing landscape. The amount of digital data investigators are confronted with is 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.

Annex 2. Proficiency levels

	Level 1 – Awareness	Level 2- Practitioner	Level 3 – Advanced Practitioner	Level 4 - Expert	Level 5 – Train-the-trainer
Definition	Refers to those who only need an insight into the particular topic, they do not need specific skills, competences and knowledge to perform the particular tasks, however require general information in order to be able efficiently support the practitioners working in that particular field.	Refers to those who independently perform their everyday standard duties in the area of the particular topic.	Has increased knowledge, skills and competences in the particular topic because of the extended experience, or specific function, i.e. team/unit leader.	Has additional competences, highly specialised knowledge and skills. Is at the forefront of knowledge in the particular topic.	Officials who are to be used as trainers for staff
Description	Has a general factual and theoretical understanding of what the topic is about, understands basic concepts, principles, facts and processes, and is familiar with the terminology and standard predictable situations. Taking responsibility for his/her contribution to the performance of practitioners in the particular field.	Has a good working knowledge of the topic, is able to apply the knowledge in the daily work, and does not require any specific guidance in standard situations. Has knowledge about possible situation deviations and can practically apply necessary skills. Can assist in the solution development for abstract problems. Is aware of the boundaries of his/her knowledge and skills, is motivated to develop self-performance.	Has broad and in-depth knowledge, skills and competences involving a critical understanding of theories and principles. Is able to operate in conditions of uncertainty, manage extraordinary situations and special cases independently, solve complex and unpredictable problems, direct work of others. Is able to share his/her knowledge with and provide guidance to less experienced colleagues. Is able to debate the issue with a sceptical colleague, countering sophisticated denialist talking points and arguments for inaction.	Has extensive knowledge, skills and competences, is able to link the processes to other competency areas and assess the interface in whole. Is able to provide tailored advice with valid argumentation. Is able to innovate, develop new procedures and integrate knowledge from different fields. Is (fully or partially) responsible for policy development and strategic performance in the particular area.	Has knowledge and skills to organise training and appropriate learning environment using modern adult training methods and blended learning techniques. Is familiar with and can apply different theories, factors and processes of learning in challenging situations. Experienced with different methods and techniques of learning. Can prepare and conduct at least one theoretical and one practical training session for law enforcement officials.
EQF equivalent	EQF Level 3-4	EQF Level 5	EQF Level 6	EQF Level 7	n/a
EQF levels – Descriptors defining levels in the European Qualifications Framework, more information is available at https://ec.europa.eu/ploteus/en/content/descriptors-page				Images from https://askfortheworld.wordpress.com/levels/	