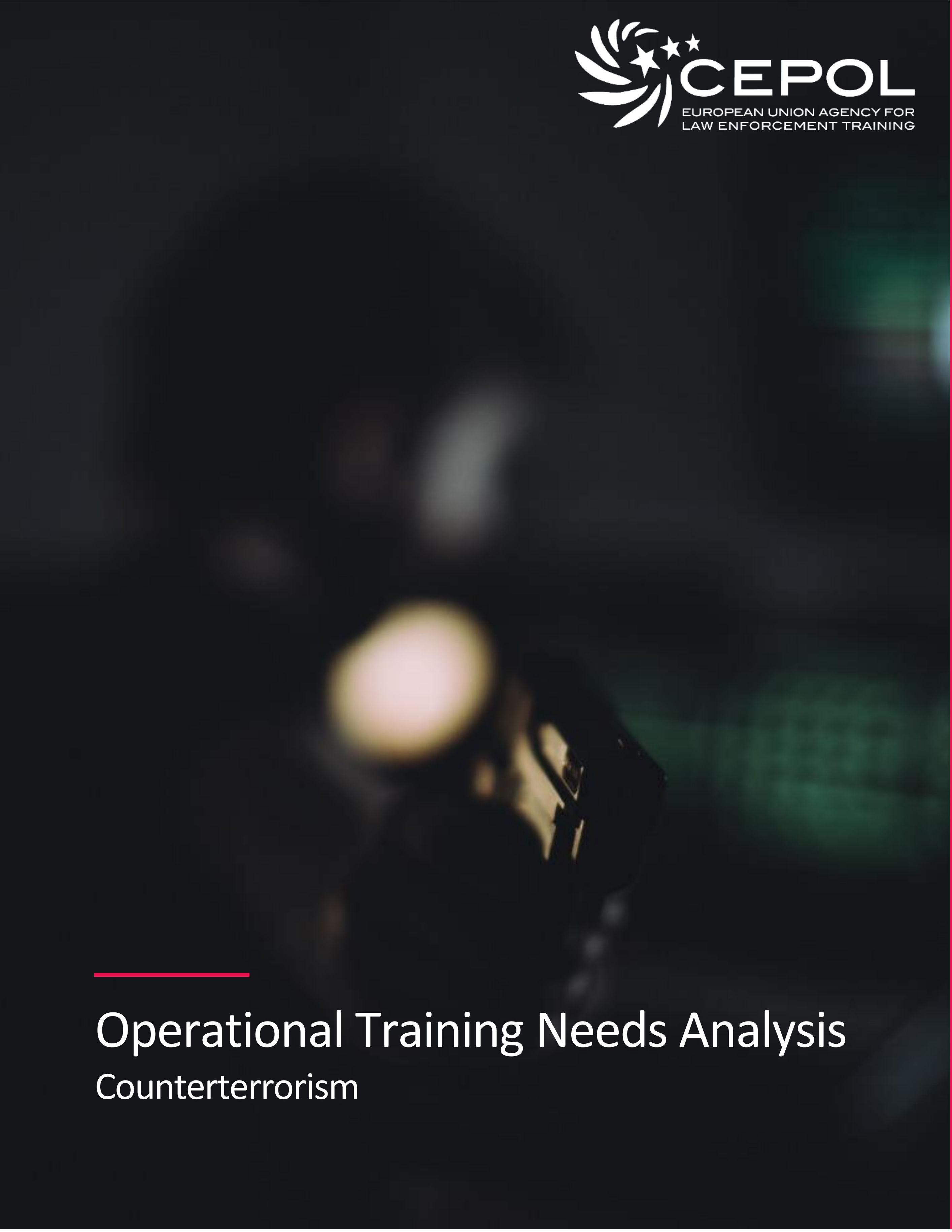
CEPOL
EUROPEAN UNION AGENCY FOR
LAW ENFORCEMENT TRAINING



Operational Training Needs Analysis

Counterterrorism

EDUCATE, INNOVATE, MOTIVATE

Operational Training Needs Analysis
Counterterrorism

2022

Contents

List of abbreviations

AI – Artificial Intelligence

CBRN-E - chemical, biological, radiological and nuclear substances and explosives

CKC - CEPOL Knowledge Centre

CSDP – Common Security and Defence Policy

EU – European Union

EUCP - European Union Crisis Protocol

eu-LISA – European Union Agency for the Operational Management of Large Scale IT Systems in the Area of Freedom, Security and Justice

EUROPOL – European Union Agency for Law Enforcement Cooperation

EUROPRIS - European Organisation of Prison and Correctional Services

EU-STNA – European Union Strategic Training Needs Assessment

ESDC – European Security and Defence College

FRONTEX – European Border and Coast Guard Agency

JHA – Justice and Home Affairs

JITS – Joint Investigation Teams

LE – Law enforcement

MB – Management Board

MS – Member State/s

OSINT – Open Source Intelligence

OTNA – Operational Training Need Analysis

PERCI - EU Platform on addressing illegal content online

PSYOPS - Physical fight against terrorism

PTD - Proactive Threat Detection

SIS – Schengen Information System

SIRENE - Supplementary Information Request at the National Entries

SPD – Single Programming Document

Executive Summary

As defined by Article 3 of Regulation 2015/2219[1], the European Union Agency for Law Enforcement Training (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.[2]

Protecting Europeans from terrorism and organised crime is one of the priority areas of the European Union's (EU) new Security Union Strategy for the period 2020-2025[3]. Alike the EU Counter-Terrorism Agenda adopted in 2020, the strategy underlines the importance of Member States' developing capabilities through training and sharing of best practices. In order to define the training portfolio responding to the needs of the European law enforcement (LE) officials and representatives from judicial authorities who are engaged in countering terrorism and radicalisation, CEPOL launched in 2021 the fourth[4] OTNA process on **Counterterrorism**.

A short-term expert was contracted from the list of individual external experts to assist CEPOL in the OTNA process, in particular steps 3-6 (questionnaire, interviews and analysis of responses, overall analysis and drafting of the OTNA report).

Building on the strategic training priorities defined by the EU-STNA report 2022-2025[5], covering EMPACT 2022+, an online survey was developed and addressed to direct contact points of 26 MS[6] and EU structures (hereinafter institutions) dealing with counterterrorism. Data was collected between 16 December 2021 and 3 February 2022, resulting in **53 individual answers** received from different LE agencies in **22 EU MS[7] and three EU institutions[8]**, reportedly representing up to **19 135 European LE officials**. In terms of MS, the responses indicate an **85 % response rate**, which can be considered as a relatively good level of responsiveness for a survey research intended to represent the European LE community.

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

[2] 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.
More: https://www.cepol.europa.eu/education-training/our-approach/eu-stna

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

[4] Previous exercises conducted in 2018 (pilot OTNA), 2020 and 2021

[5] https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf

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

[7] Responding countries: Bulgaria, Croatia, Cyprus, Czechia, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden

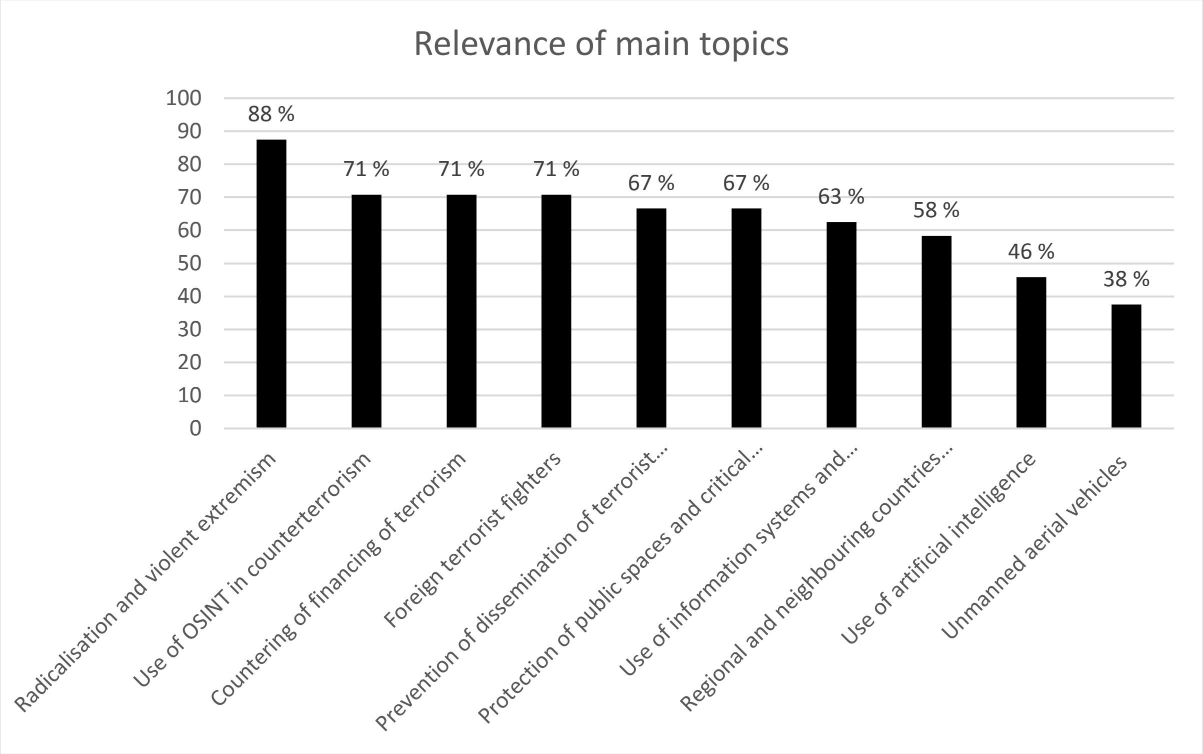
[8] Responding institutions: eu-LISA, Europol and Frontex

Based on the analysis of the collected data, this report describes **training priorities in the area of counterterrorism for 2023-2025**.

Based on the data received from the MS and responding EU institutions, out of ten individual topics, the **most relevant main topics** for LE officials in this area were related to:

- **Radicalisation and violent extremism** (88 % of respondents found it relevant)
- **Use of OSINT in counterterrorism** (71 % of respondents found it relevant)
- **Countering of financing of terrorism** (71 % of respondents found it relevant)
- **Foreign terrorist fighters** (71 % of respondents found it relevant)
- **Prevention of dissemination of terrorist content online** (67 % of respondents found it relevant)
- **Protection of public spaces and critical entities resilience** (67 % of respondents found it relevant)
- **Use of information systems and cooperation mechanisms** (63 % of respondents found it relevant) and
- **Regional and neighbouring countries cooperation on specific terrorism cases** (58 % of respondents found it relevant).

Chart 1. Distribution of training needs depending on the indicated relevance rate



As per the OTNA methodology, training topics that more than 50 % of MS indicate as relevant training needs are to be considered for further analysis in terms of their content, urgency, proficiency level and number of participants. Based on this criterion, the topics of **radicalisation and violent extremism**, **use of OSINT in counterterrorism**, **countering of financing of terrorism, foreign terrorist fighters**, **prevention of dissemination of terrorist content online**, **protection of public spaces and**

critical entities resilience, **use of information systems and cooperation mechanisms** and **regional and neighbouring countries cooperation on specific terrorism cases** were selected for closer review. The other two remaining topics (< 50 %) were excluded from the further analysis process and hence are not elaborated in this report other than concerning their relevance, urgency and estimated volume of trainees (Table 1).

An interesting observation is that while the topic of digital skills and the use of new technologies as a horizontal aspect reached a notably high relevance rate (75 %) across all areas, the use of artificial intelligence (AI) as a main topic scored just below the 50 % threshold. Being a strategic training priority as per the EU-STNA and considering the acceleration of technology innovation in the LE context with a completely new set of challenges, the use of AI must be seen as an integral part of the training portfolio.

In terms of urgency, those eight most relevant main topics are ranging from 61 % to 49 %, meaning that all of them must be considered either **urgent** or **moderately urgent**[9] training needs where training should be delivered within a year's period. On those that scored higher than 60 %, namely **use of OSINT in counterterrorism**, training can be seen as an essential and necessary response to ensure quality performance. With less significance in terms of performance improvement, it would be advantageous for the audience to receive training on **all other prioritised main topics** during the next three years training cycle. The detailed distribution of training needs on main topics based on relevance, urgency and indicated number of trainees is presented below in Table 1.:

Table 1. Relevance and urgency rate of the main topics

Main Topic	Relevance rate	Urgency rate	Trainees (median extrapolated to the EU)[10]	Trainees (actual)[11]
Radicalisation and violent extremism	88 %	55 %	806	3 576
Use of OSINT in counterterrorism	71 %	61 %	533	24 192
Countering of financing of terrorism	71 %	52 %	663	2 303
Foreign terrorist fighters	71 %	48 %	858	16 128
Prevention of dissemination of terrorist content online	67 %	52 %	377	3 450
Protection of public spaces and critical entities resilience	67 %	54 %	1 053	4 806
Use of information systems and cooperation mechanisms	63 %	52 %	663	4 041
Regional and neighbouring countries cooperation on specific terrorism cases	58 %	49 %	780	3 774

[9] See explanation of urgency levels in Annex 3.

[10] Based on the statistical median extrapolated to the EU level

[11] While the OTNA methodology relies on the calculated statistical median when estimating the potential number of trainees, actual values as communicated by the survey respondents are added for comparison purposes.

Use of artificial intelligence by law enforcement	46 %	61 %	390	1 877
Unmanned aerial vehicles - threats and opportunities for law enforcement	38 %	57 %	1 365	17 678
Average/total	**64 %**	**54 %**	**7 488**	**81 826**

Designed for prioritising tasks by first categorising items according to their urgency and importance, the Eisenhower Method was used to visualise the data in the form of a matrix for further demonstrating the distribution of main topics by their urgency and relevance rate. The Eisenhower Matrix, also known as urgent-important matrix, below (Chart 2.) displays the relationships between three numeric variables, namely relevance, urgency and the number of potential trainees on each main topic. Each dot in the centre of a bubble corresponds to a single data point (main topic urgency and relevance rate). The size of the bubbles corresponds to the median number of trainees. Its vertical axis represents the relevance, and the horizontal axis the urgency rate. The order of implementation of tasks should be 1. Important/Urgent, 2. Important/Not Urgent, 3. Unimportant/Urgent, 4. Unimportant/Not Urgent.

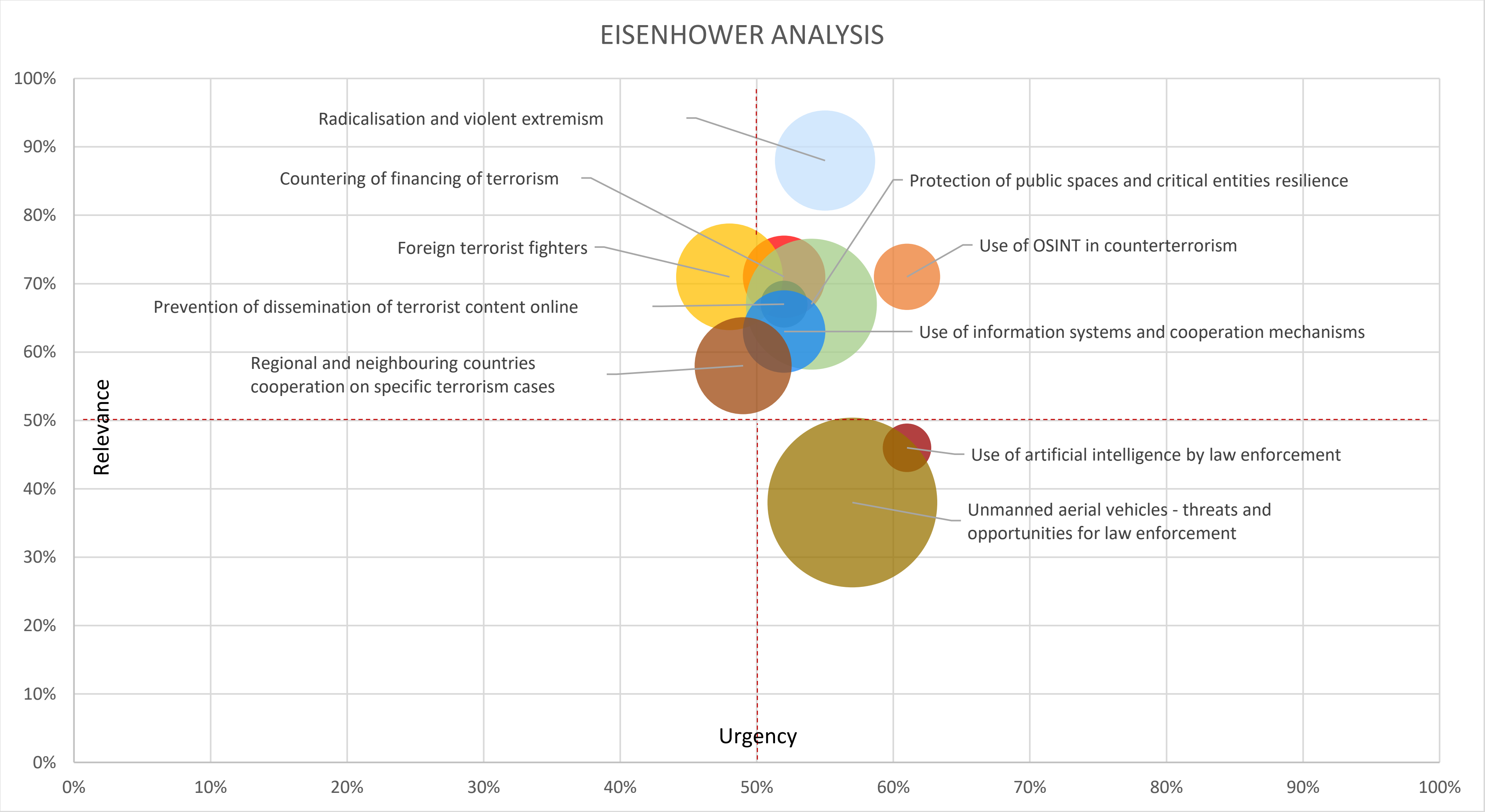


Chart 2. Urgent-important matrix

In reference to the findings, it can be concluded that the training need on most subtopics, presented under each main topic, is considerably high, as in most cases, their subtopics reached the 50 % threshold. The summary below presents up to five highest scoring subtopics of each prioritised main topic . Complete details of relevance rate of subtopics under prioritised main topics are presented in Table 5. on page 16.

On the topic **radicalisation and violent extremism**, the following four subtopics were considered as the most relevant:

- Prevention and countering of radicalisation leading to violent extremism and terrorism
- New forms of radicalisation
- Insider threats
- Radicalisation in prisons

Both subtopics presented under the main topic **use of OSINT in counterterrorism** scored notably high and should be emphasised in training:

- Value of digital evidence
- Methods of lawful interception

Under the topic **countering of financing of terrorism,** all subtopics were assessed as relevant and training should address them in the following priority order:

- Emerging threats (cryptocurrencies), and financial links to other types of crime (e.g. tax fraud, money laundering, trafficking of cultural goods)
- Understanding and investigation of crowdfunding online
- Public - Private sector partnerships
- Role of Financial Intelligence Units

All four subtopics presented under the main topic **foreign terrorist fighters** gained a high relevance rate, namely:

- Foreign terrorist fighters
- Travelling terrorists and returnees
- Law enforcement approach to family members of foreign terrorist fighters
- Battlefield information exchange

The following five subtopics were the highest scoring ones under the main topic **prevention of dissemination of terrorist content online**:

- Detection and investigation
- Manipulation of social media
- Digital trends
- Cooperation with Internet Referral Unit of Europol to take down terrorist content online
- Implementation of the Regulation on the Prevention of Dissemination of Terrorist Content Online

Related to **protection of public spaces and critical entities resilience**, the most relevant thematic areas are as follows:

- Sharing best practices on handling of attacks
- Cooperation between public and private sectors
- Risk assessment management
- Protection by security design
- Insider threats
- Cyberattacks on critical infrastructures

Only one subtopic presented under the main topic **use of information systems and cooperation mechanisms,** reached a high relevance rate:

- Interoperability of EU information systems and possibilities for CT Investigations

All subtopics related to **regional and neighbouring countries cooperation on specific terrorism cases** should be addressed by training in the following order:

- Joint investigations cases and best practices
- Cooperation with MENA countries

Cooperation as an advantage to face terrorism threatsAs presented below (Table 2.), horizontal aspects ranged from 75 % to 46 % in terms of their relevance. Reflecting the centrality of emerging technologies (such as AI, among others) in today's LE environment, the topic of **digital skills and the use of new technologies** gained the highest relevance rate. The lowest priority was given to **fundamental rights and data protection**, which regardless of its ranking should always be given high priority when designing CEPOL's training portfolio.

Table 2. Average relevance of horizontal aspects among prioritised main topics

Horizontal aspect	**Relevance**
Digital skills and the use of new technologies	75 %
Law enforcement/judicial cooperation, information exchange and interoperability	70 %
Cybercrime investigations	66 %
Criminal intelligence picture, high-risk criminal networks	64 %
Financial investigations	62 %
Crime prevention	56 %
Firearms trafficking	53 %
Document fraud	51 %
Forensics/Evidence	49 %
Fundamental rights and data protection	46 %

Responses indicated that approximately **5 733 participants**[12] would need training on the **prioritised main topics** in 2023. Overall, the highest training need is indicated by respondents in the proficiency

[12] Presented numbers are based on calculated median values (reported total number of actual trainees: 62 270). For further details on the calculation methodology, please see 'Analysis' section of this report.

levels of **awareness** and **practitioner**, followed by **advanced practitioner**. Regardless of the biggest volume of trainees, training at awareness level gained the lowest urgency score. Out of these three main groups, training of practitioners gained the highest urgency rate. While the volume of trainees is considerably lower at expert and train-the-trainer level, it must be noted that training of experts scored the highest in terms of urgency. Overall, the average **urgency for training** in the area of counterterrorism is **moderate (53 %)** meaning that it would be advantageous to receive training within a year's period.

Table 3. Proficiency levels and number of potential participants

Proficiency level	**Trainees (median extrapolated to the EU)**	**Trainees (actual)**
Awareness	1 950	44 808
Practitioner	1 508	8 832
Advanced practitioner	1 001	4 722
Expert	741	2 533
Train-the-trainer	533	1 375
Total	**5 733**	**62 270**

The **CEPOL Knowledge Center (CKC) on Counterterrorism** called the attention to the fact that as the proficiency level increases, the number of available staff decreases (e.g. less experts are available than first responders). Therefore, when designing the training portfolio, **the proportion of higher proficiency level training should not be lower to others**.

The OTNA questionnaire gave an opportunity to specify the profiles and indicate the number of LE officials who would need training in different topics. Most references were given to **first responders** (52 %), followed by **investigators** (26 %). These two profiles should be provided with the opportunity to be trained first. On the topic of protection of public spaces and critical entities resilience, the responding MS indicated additional training needs targeted to **counterterrorism operators** and **technicians** dealing with chemical, biological, radiological and nuclear substances and explosives (CBRN-E) matters. Regarding the topics of radicalisation and violent extremism and the topic of foreign terrorist fighters, the respondents indicated needs to include **multi-agency partners** (e.g. municipality representatives) and **negotiators** in the related training. Training for **experts** and **trainers,** particularly on detection topics, was also indicated as an additional need relevant to many of the main topics.

Data on previous training attended at national or international level was provided by 18 MS (78 %) indicating that most of the previous/recent training was related to radicalisation and violent extremism, foreign terrorist fighters, OSINT and counterterrorism, and countering of terrorism financing. Most of the previous training had been attended by **practitioner** (34 %) and **advanced practitioner** (33 %) level trainees. In terms of training delivery format, the division between online and onsite training was close to equal, indicating that just above half (51 %) of training had been attended onsite, 48 % online (online module/course, webinar or other virtual implementation) and the remaining 1 % in an undefined mode.

Background

As defined by Article 3 of 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 MS, and terrorism, maintenance of public order, international policing of major events, and planning and command of Union missions, which may also include training on law enforcement leadership and language skills.

The Single Programming Document (SDP) for 2022-2024[13] describes OTNA as a process to help towards the realisation of strategic goals through the implementation of operational training activities. The OTNA methodology, as adopted by the CEPOL Management Board (MB) decision 32/2017/MB (15/11/2017) was piloted in 2018 with a limited number of thematic priorities for the 2019 CEPOL training portfolio planning, namely CSDP missions and Counterterrorism. The OTNA methodology was updated in 2020 (9/2020/MB) based on CEPOL's experience and feedback from the MS.

The methodology consists of a series of seven steps encompassing close and dynamic cooperation with the MS, in particular CEPOL National Units, and LE agencies, and involving CEPOL Knowledge Centres (CKC) in the training portfolio design. 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 the CEPOL Regulation 2015/2219[14].

Building on the strategic training priorities defined by the EU-STNA and the experience gained from previous OTNA studies, CEPOL launched the OTNA on **Counterterrorism** in 2021. Outcomes of the research are presented in this report and will be used to define CEPOL's 2023 training portfolio on a diverse list of topics related to countering terrorism and radicalisation.

[13] https://www.cepol.europa.eu/sites/default/files/31-2021-MB%20Annex.pdf, p. 5.

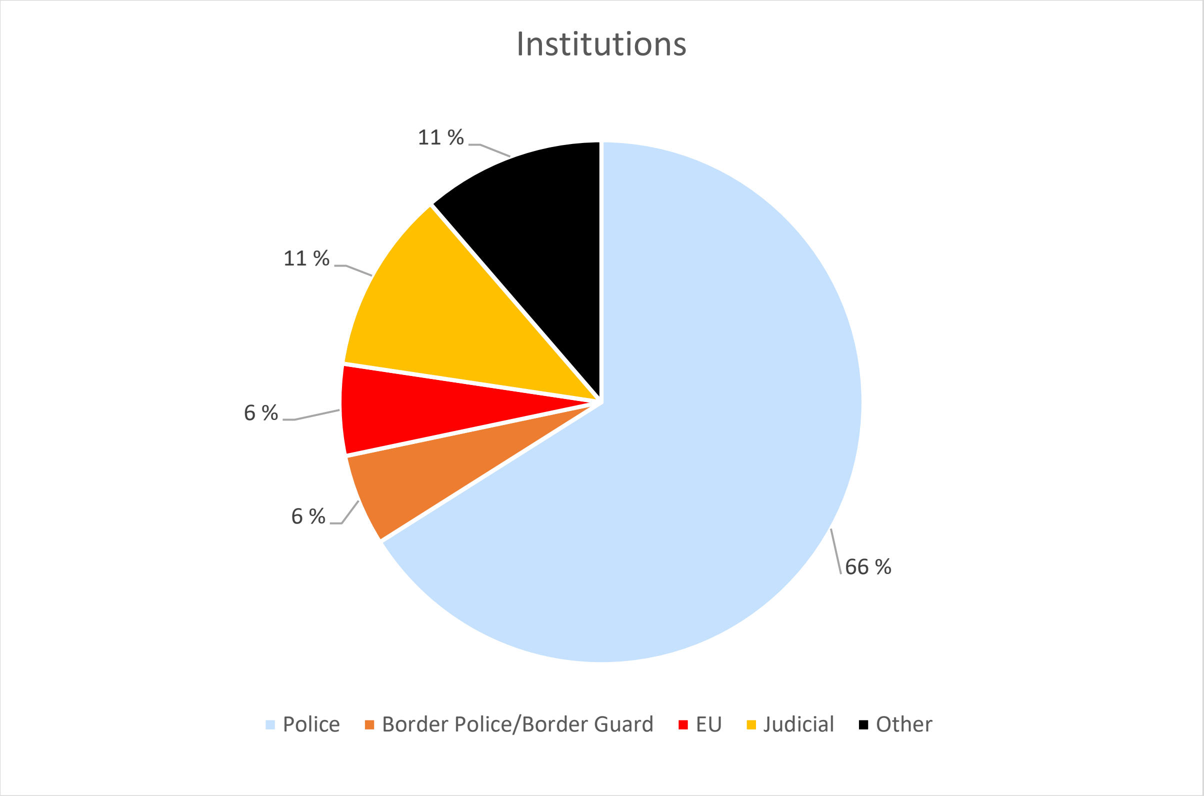
[14] https://publications.europa.eu/en/publication-detail/-/publication/c71d1eb2-9a55-11e5-b3b7-01aa75ed71a1/language-en.

Analysis

Consolidation of data and responses

In order to conduct the research, CEPOL approached 26 MS[15], and EU institutions to provide direct contact points dealing with the subject of this OTNA. In total, representatives of 22 MS and three institutions responded to the survey, resulting in 53 individual completed answers received from different LE agencies and EU institutions. In terms of MS, the responses indicate 85 % response rate, which can be considered as a relatively good level of responsiveness. Most of the responses (66 %) were from police representatives, followed by judicial authorities and other relevant bodies; however, both with a considerably lower share (11 %).

Chart 3. Distribution of responding institutions



The data collected was processed from the online survey platform Qualtrics to Microsoft Excel. The data was synthesised and analysed by Excel functions.

[15] The terminology Member States (MS) hereinafter refers to 26 MS of the EU participating in the CEPOL regulation, i.e. all EU MS excluding Denmark.

Relevance of topics

In line with the training priorities defined in the EU-STNA, the main training topics in relation to counterterrorism are:

- Radicalisation and violent extremism
- Use of OSINT in counterterrorism
- Countering of financing of terrorism
- Foreign terrorist fighters
- Prevention of dissemination of terrorist content online
- Protection of public spaces and critical entities resilience
- Use of information systems and cooperation mechanisms
- Regional and neighbouring countries cooperation, and
- Use of artificial intelligence

In order to identify which main topics are the most important for the European LE community requiring training to be provided by CEPOL in 2023-2025, the OTNA questionnaire presented multiple-select questions where the respondents could select one or more options in a list of ten main topics. While analysing the results, the relevance score of each main topic was calculated by summing up how many MS[16] found the topics relevant. The final relevance rate was then calculated by dividing the sum of MS that found the topic relevant by the number of responding MS. If several LE agencies submitted answers from the same MS, entries were consolidated. If more than 50% of MS found a certain topic relevant, it was considered relevant and selected for further analysis as per the OTNA methodology. Based on this method, six of all main topics passed the 50 % threshold of relevance rate.

Table 4. Relevance rate of main topics

Main Topic	Relevance
Radicalisation and violent extremism	88 %
Use of OSINT in counterterrorism	71 %
Countering of financing of terrorism	71 %
Foreign terrorist fighters	71 %
Prevention of dissemination of terrorist content online	67 %
Protection of public spaces and critical entities resilience	67 %
Use of information systems and cooperation mechanisms	63 %
Regional and neighbouring countries cooperation on specific terrorism cases	58 %
Use of artificial intelligence by law enforcement	46 %
Unmanned aerial vehicles - threats and opportunities for law enforcement	38 %

Training dimensions

[16] When calculating the relevance rate, EU institutions were considered as a separate category equivalent to MS

In order to gain further insights on necessary training themes and subjects, various **subtopics** and **horizontal aspects** were presented under each topic. The questionnaire gave the respondents an option to rate the relevance of subtopics and horizontal aspects by using a five-point Likert Scale with the following options: not relevant at all, somewhat relevant; relevant; very relevant and extremely relevant. For analysing the responses, this scale was converted into a numerical scale 0-1-2-3-4, where 0 represents the minimum value (not relevant at all) and 4 the maximum (extremely relevant). The relevance score of each subtopic was calculated by drawing the sum of the responses, while in those cases where several authorities from the same MS gave answers, an average was calculated and used as the final relevance level in the case of that particular country. The final relevance rate (percentage) was calculated by dividing the score by the maximum score[17]. If the relevance score reached 50 % of the maximum score, the subtopic or horizontal aspect was found relevant.

The analysis revealed that the training need on most subtopics, presented under each main topic, is considerably high, and in most cases, all subtopics reached the 50 % threshold. In a descending order, Table 5. below presents the subtopics and horizontal aspects under prioritised main topics based on their relevance rate.

Table 5. Relevance rate of subtopics and horizontal aspects (*in italics*) of prioritised main topics

Main topic	Subtopic / *Horizontal aspect*	Relevance
Radicalisation and violent extremism	Prevention and countering of radicalisation leading to violent extremism and terrorism	83 %
	New forms of radicalisation	77 %
	Insider threats	63 %
	Radicalisation in prisons	53 %
	Fundamental rights and data protection, including non-discrimination	43 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*75 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*67 %*
	Cybercrime investigations	*66 %*
	Crime prevention	*61 %*
	Criminal intelligence picture, high-risk criminal networks	*61 %*
	Financial investigations	*60 %*
	Forensics/Evidence	*55 %*
	Firearms trafficking	*44 %*
	Fundamental rights and data protection	*43 %*
	Document fraud	*40 %*
Use of OSINT in counterterrorism	Methods of lawful interception	88 %
	Value of digital evidence	86 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*89 %*
	Cybercrime investigations	*73 %*

[17] The maximum score is identified by multiplying the number of responding MS that found the subtopic or horizontal aspect relevant with the highest relevance score (5)

	Criminal intelligence picture, high-risk criminal networks	*65 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*64 %*
	Financial investigations	*62 %*
	Forensics/Evidence	*59 %*
	Firearms trafficking	*56 %*
	Crime prevention	*54 %*
	Document fraud	*46 %*
	Fundamental rights and data protection	*44 %*
Countering of financing of terrorism	Emerging threats (cryptocurrencies), and financial links to other types of crime (e.g. tax fraud, money laundering, trafficking of cultural goods)	78 %
	Understanding and investigation of crowdfunding online	65 %
	–Public- Private sector partnerships	61 %
	Role of Financial Intelligence Units	55 %
	Financial investigations	*75 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*74 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*71 %*
	Cybercrime investigations	*66 %*
	Criminal intelligence picture, high-risk criminal networks	*60 %*
	Forensics/Evidence	*53 %*
	Document fraud	*52 %*
	Firearms trafficking	*51 %*
	Crime prevention	*50 %*
	Fundamental rights and data protection	*37 %*
Foreign terrorist fighters	Travelling terrorists and returnees	87 %
	Foreign terrorist fighters	84 %
	Battlefield information exchange	81 %
	Law enforcement approach to family members of foreign terrorist fighters	73 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*75 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*73 %*
	Document fraud	*69 %*
	Forensics/Evidence	*65 %*
	Financial investigations	*64 %*
	Criminal intelligence picture, high-risk criminal networks	*62 %*
	Cybercrime investigations	*62 %*
	Fundamental rights and data protection	*58 %*
	Crime prevention	*55 %*
	Firearms trafficking	*56 %*
	Manipulation of social media	76 %
	Detection and investigation	74 %
	Digital trends	72 %

Prevention of dissemination of terrorist content online	Cooperation with Internet Referral Unit of Europol to take down terrorist content online	70 %
	Implementation of the Regulation on the Prevention of Dissemination of Terrorist Content Online	67 %
	European Union Crisis Protocol (EUCP) as a tool to prevent violent content from going viral on the web/networks in the immediate aftermath of a terrorist/extremist attack	66 %
	Use of PERCI	63 %
	Understanding and investigation of crowdfunding online	62 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*76 %*
	Cybercrime investigations	*75 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*69 %*
	Criminal intelligence picture, high-risk criminal networks	*65 %*
	Forensics/evidence	*57 %*
	Financial investigations	*55 %*
	Crime prevention	*56 %*
	Firearms trafficking	*45 %*
	Fundamental rights and data protection	*42 %*
	Document fraud	*47 %*
Protection of public spaces and critical entities resilience	Sharing best practices on handling of attacks	78 %
	Risk assessment management	72 %
	Cooperation between public and private sectors	71 %
	Protection by security design	70 %
	Cyberattacks on critical infrastructure	65 %
	Cybersecurity	65 %
	Insider threat	61 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*67 %*
	Criminal intelligence picture, high-risk criminal networks	*63 %*
	Crime prevention	*62 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*61 %*
	Cybercrime investigations	*55 %*
	Firearms trafficking	*54 %*
	Forensics/evidence	*50 %*
	Document fraud	*46 %*
	Financial investigations	*45 %*
	Fundamental rights and data protection	*40 %*
The use of information systems and cooperation mechanisms in fight against counterterrorism	Interoperability of EU information systems and possibilities for CT Investigations	73 %
	Law enforcement/judicial cooperation, information exchange and interoperability	*71 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*70 %*
	Cybercrime investigations	*68 %*

	Criminal intelligence picture, high-risk criminal networks	*64 %*
	Financial investigations	*62 %*
	Crime prevention	*58 %*
	Firearms trafficking	*56 %*
	Forensics/Evidence	*55 %*
	Document fraud	*54 %*
	Fundamental rights and data protection	*48 %*
Regional and neighbouring countries cooperation on specific terrorism cases	Joint investigations cases and best practices	74 %
	Cooperation with MENA countries	73 %
	Cooperation as an advantage to face counterterrorism threats	72 %
	Law enforcement/judicial cooperation, information exchange and interoperability	*75 %*
	Criminal intelligence picture, high-risk criminal networks	*71 %*
	Digital skills and the use of new (including darknet, OSINT)	*70 %*
	Financial investigations	*69 %*
	Forensics/Evidence	*63 %*
	Cybercrime investigations	*63 %*
	Firearms trafficking	*60 %*
	Crime prevention	*54 %*
	Document fraud	*56 %*
	Fundamental rights and data protection	*48 %*

While none of the horizontal aspects reached the same level in terms of relevance as the highest-scoring main topic (88 %), the majority of them reached a > 50 % relevance rate with relatively high scores. **Digital skills and the use of new technologies** was considered as the most relevant horizontal aspect, which directly reflects the increasing role of emerging technologies (such as AI) integration in the modern LE environment. Despite the fact that **fundamental rights and data protection** remained as the lowest scoring, promoting common respect for, and understanding of, fundamental rights in law enforcement, must remain a priority when designing the training portfolio on counterterrorism. Table 6. below presents the overview of the horizontal aspects' ranking.

Table 6. Average relevance of horizontal aspects among prioritised topics

Horizontal aspect	**Relevance**
Digital skills and the use of new technologies	75 %
Law enforcement/judicial cooperation, information exchange and interoperability	70 %
Cybercrime investigations	66 %
Criminal intelligence picture, high-risk criminal networks	64 %
Financial investigations	62 %
Crime prevention	56 %
Firearms trafficking	53 %
Document fraud	51 %
Forensics/Evidence	49 %
Fundamental rights and data protection	46 %

Through the OTNA questionnaire, the respondents were able to communicate other **potential subtopics** related to the prioritised main topics. Additional suggestions were provided on six main topics, namely radicalisation and violent extremism, use of OSINT in counterterrorism, foreign terrorist fighters, the use of information systems and cooperation mechanisms, protection of public spaces and critical entities resilience, as well as regional and neighbouring countries cooperation. In terms of radicalisation and violent extremism, training on **assessing human behaviour and spotting risks related to radicalisation**, as well as **treatment of survivors/victims of terrorism** were communicated as specific needs. On the topic of foreign terrorist fighters, training needs on specific topics such as **returnees, disengagement and reintegration**, as well as considering **border detection of individuals of interest linked to terrorism, extremism or battlefield background**, as an additional training topic, were communicated by the MS. On the use of OSINT in counterterrorism, training on **Virtual Undercover Agents** was requested. Related to the use of information systems and cooperation mechanisms, training on **the SIRIUS platform** facilitating online investigations would be needed. The role of **special intervention units in responding to attacks on critical infrastructures** was an additional topic requested within the main topic of protection of public spaces and critical entities resilience. Furthermore, regional and neighbouring countries cooperation, particularly with **Sahel countries,** was indicated as a desired area to be considered in training.

Not directly linked with any particular main topic, but communicated through a section dedicated to further training needs related to counterterrorism, was a number of other topics. These included e.g. a variety of **CBRN-E related** training needs (training for first responders, forensics, case management, detection of threats and special training for mobile sensor integration unit, particularly red and yellow zone). **Joint training and/or exercises** were requested in a few topics, namely practical training on counterterrorism risk assessment specifically for border control and migration management (potentially in cooperation with Frontex), EU Crisis Protocol (EUCP) exercises or tabletop exercises with partner states and the private sector, radicalisation in prisons topics in cooperation with the European Organisation of Prison and Correctional Services (EuroPris), and the Joint Investigations Teams (JIT) management and cross-border exercises in general. **Different areas of analysis** (strategic analysis, big data, geo-analysis methodologies, social network analysis) were highlighted as important. Further suggestions included the use of individual risk assessment tools, interviewing techniques, mobile forensics, cryptocurrencies, psychological operations (PSYOPS), physical fight against terrorism, Proactive Threat Detection (PTD) and detection of terrorist activities at the border.

To better understand the training needs in each main topic, the questionnaire gave the respondents an option to indicate the level of **urgency of training** on topics related to counterterrorism and estimate the **number of participants** at five different **professional levels**[18]. A multiple rating matrix with a fixed sum function (facilitating an option to indicate quantities of trainees) was used to collect information on what level training is needed and how urgently would LE officials need the training to improve their current performance. By choosing from a six-point urgency level scale (most commonly

[18] Awareness, Practitioner, Advanced practitioner, Expert and Train-the-trainer; please find detailed description of proficiency levels in Annex 2.

known as Likert Scale)[19], respondents could express their opinion if a training need is not urgent; somewhat urgent; moderate; urgent or very urgent, or alternatively, not applicable at all. Urgency in the context of the OTNA methodology refers to the criticality of timely training intervention and its impact on the operational performance. In the analysis, responses were converted into a numerical scale from 0-5, where 1 refers to a low need with an expected minor impact on the performance boost and 5 to a crucial need as a critical response for ensuring successful performance of duties. The minimum value is 0 because 'not applicable' corresponds to a zero training need. Where the same proficiency level was indicated by several LE agencies from the same MS to the attributes of the training, the highest rate indicated was taken into consideration.

Since CEPOL's training activities address law enforcement officials from 26 EU MS and EU institutions, the number of participants indicated in the responses to the survey are considered as the number of participants who would need training from responding MS or EU institutions. In order to estimate the total number of LE officials who would need training in a certain topic at a certain proficiency level, the OTNA methodology relies on a calculation based on the identified statistical median of the number of trainees. The estimate of the number of participants at EU-level is then calculated by multiplying the median with 26 (as per the number of MS[20]). In statistics, the median is the value separating the higher half from the lower half of a data set, hence, it can be considered as the middle value.

Based on this method of calculation, approximately **5 733 participants** would need training on counterterrorism in 2023. As the basic feature of the median in describing data is that it is not skewed by a small proportion of extremely large or small values, and therefore provides a better representation of a typical value, it might happen that the rank of proficiency levels in each topic is different at EU-level to the rank which is based on the responses given to the survey. Without statistically processing the data, the respondents communicated up to 62 270 potential trainees on the prioritised main topics. Hence, it must be noted that the extrapolated figure is <10 % compared to the total that can be reached by simply summing up the entries provided by the responding MS. The most considerable difference between the actual and consolidated numbers based on the statistical median concerns the topics of use of OSINT in counterterrorism and foreign terrorist fighters, where one responding MS[21] reported a considerable volume of LE officials in need of training, particularly at awareness level.

[19] A Likert scale is commonly used to measure attitudes, knowledge, perceptions, values, and behavioural changes. A Likert-type scale involves a series of statements that respondents may choose from in order to rate their responses to evaluative questions

[20] All EU MS except Denmark

[21] Portugal with 20 000 trainees on the topic use of OSINT in counterterrorism and 10 000 on the topic foreign terrorist fighters, both at entries indicating need of awareness level training

Table 7. Relevance, urgency rate and number of trainees on prioritised main topics

Main Topic	Relevance rate	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Radicalisation and violent extremism	88 %	55 %	806	3 576
Use of OSINT in counterterrorism	71 %	61 %	533	24 192
Countering of financing of terrorism	71 %	52 %	663	2 303
Foreign terrorist fighters	71 %	48 %	858	16 128
Prevention of dissemination of terrorist content online	67 %	52 %	377	3 450
Protection of public spaces and critical entities resilience	67 %	54 %	1 053	4 806
Use of information systems and cooperation mechanisms	63 %	52 %	663	4 041
Regional and neighbouring countries cooperation on specific terrorism cases	58 %	49 %	780	3 774
Average/total	**70 %**	**53 %**	**5 733**	**62 270**

In addition to calculating the overall urgency rate and number of trainees per each prioritised main topic, training needs and volume of trainees was analysed per each proficiency level. On average, the training need in the area of counterterrorism is **moderately urgent** (53 %), meaning that it would be advantageous to the audiences to receive training within a year's period in order to improve their performance. However, training alone would not play a significant role in the competence development. Perhaps the most emerging finding is that while the indicated numbers of trainees is lower in these categories, the highest urgency for training is indicated among **experts**, however, only slightly higher than **advanced practitioner**. Considering both values, the most emerging need could be pointed at being training of **practitioners**. An interesting finding is that while awareness level training reached the highest number of potential trainees, training of this segment was ranked as the least urgent.

Table 8. Proficiency levels and number of participants

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	44 %	1 950	44 808
Practitioner	55 %	1 508	8 832
Advanced practitioner	57 %	1 001	4 722
Expert	59 %	741	2 533
Train-the-trainer	50 %	533	1 375
Total	**53 %**	**5 733**	**62 270**

In order to establish a more comprehensive picture on target groups to be trained, the questionnaire offered the possibility of indicating **professional profiles**[22] and the related volumes of LE officials who need training under each main category. Most references were given to **first responders** (52 %), followed by **investigators** (26 %). These two profiles should be provided with the opportunity to be trained first. The rest of the profiles gained a much lower weighting; intelligence analysts, analysts and managers all equal in terms of trainee quantities (6 % each). On top of those seven pre-set categories, through an open text field, the respondents were able to specify other professionals in need for training and insert the related numbers.

Training of **intelligence officers** was communicated as a need across all prioritised main topics. Related to radicalisation and violent extremism, the respondents indicated needs to consider **multi-agency partners** (e.g. municipality) and negotiators as a training audience; the latter was also indicated as a potential segment for training on the topic of foreign terrorist fighters. Training for **experts and trainers on detection topics** -related to the use of information systems and cooperation mechanisms in the fight against counterterrorism, foreign terrorist fighters, protection of public spaces and critical entities resilience, and regional and neighbouring countries cooperation on specific terrorism cases, - were also indicated. On the topic of protection of public spaces and critical entities resilience, training designed for **counterterrorism operators** and for those working in **technician roles** related to CBRN-E were communicated as additional target groups that would need training to improve their performance for effective operations in different environments.

In terms of responding authorities, Germany and Portugal were the biggest contributors to the questionnaire. From both MS, eight individual responses were received, which in most cases represent different organisations. Also, multiple authorities from Spain, Romania, Italy, Poland, Estonia and Croatia submitted their individual responses. This might result in the data (e.g. the number of participants extrapolated to the EU level) being potentially impacted by the stronger presence of a few countries. While the number of potential trainees communicated by the respondents were quite moderate and the variance between the numeric entries of different MS was not extreme, notably the largest quantities of trainees were reported from Portugal, indicating considerable training needs on most of the prioritised main topics, and particularly high on the use of OSINT in counterterrorism and foreign terrorist fighters[23]. This responding organisation was invited for an interview with the goal to further discuss their training needs, however, their representative was not available for a meeting during the available timeframe.

National or international training

The OTNA questionnaire had a section with a question referring to previous national or international training attended on counterterrorism, where 18 responding MS (78 %) provided data on previous training. In terms of topics, training data was provided in a free text form, therefore the presentation

[22] First responders; investigators; intelligence analysts; analysts; managers; prosecutors, investigative judges and magistrates; experts (on forensics, IT etc.)

[23] 20 000 trainees on the topic 'Use of OSINT in counterterrorism' and 10 000 on the topic 'Foreign terrorist fighters'; up to 1 000-2 000 reported on most of the other prioritised main topics

and level of detail provided was not uniform. Provided text entries were approached by implementing light text analysis, i.e. based on word identification in an Excel spreadsheet, grouping similar entries and establishing categories of entries representing thematically similar topics.

In addition to reporting overarching topics such as fight against terrorism, terrorism and organised crime interlinkages, terrorism trends in Europe and beyond as the 21st century phenomenon, a few thematic categories could be clearly identified. Topics related to understanding terrorist threats posed by and countering the different forms of radicalisation and violent extremism (e.g. right-wing, Jihadism) established a clear category of training that the European LE audience has been attending. As a separate topic, foreign terrorist fighters (individuals traveling to conflict zones to engage in terrorist acts) was an area where training has been attended regularly. OSINT and counterterrorism (intelligence, analysis and techniques), events giving tools for preventing and combating terrorism financing and money laundering, were among the most mentioned topics, while a considerable number of past training on CBRN-E topics were also reported. Also, a number of individual topics were reported, but due to their scattered nature they were not further analysed.

The nature of previous training reported by the respondents varied from short courses to thematic study trips or exchange periods, and furthermore, to completed university degrees. Most of the previous training seemed to be attended by practitioner (34 %) and advanced practitioner (33 %) level professionals, followed by experts (19 %). Awareness level trainees represented 10 % of the overall volumes communicated, and train-the-trainer held the last position with a share of 4 %. In terms of training delivery format, the division between online and onsite training was close to equal, indicating that just above half (51 %) of training has been attended onsite, 48 % online (online module/course, webinar or other virtual implementation) and the remaining 1 % in an undefined mode. Not many details were provided in terms of training providers, however, in many cases the presentation of topics/titles of the attended training indicated that they were provided by CEPOL.

Training dimensions for main topics

As methodologically explained in the previous chapter, each of the six prioritised main topics was analysed in terms of relevance of subtopics and horizontal aspects, level of proficiency, potential number of participants per profile, as well as urgency of training needs. This chapter presents more detailed training needs related to each main topic. After a summary of training needs, the first table of each main topic shows the relevance rate of subtopics and the horizontal aspects in a descending order. The second table demonstrates the estimated number of participants per different proficiency level, both as calculated in line with the OTNA methodology[24] and for comparison purposes, the figures as communicated by the responding MS, as well as the urgency rate of training to be delivered.

Radicalisation and violent extremism

Radicalisation and violent extremism is the most relevant main topic, as indicated by the MS (relevance 88 %). The training need is **moderately urgent**, and the largest amounts of trainees are in need of **awareness** level training, followed by **practitioners**. Notably the biggest target group to be trained are **first responders** (with a share over 50 %), and **investigators**, holding the second place. Training should be delivered within one year to **approximately 806 trainees.** Within this main topic, training should focus on the most relevant subtopics and horizontal aspects, as indicated below.

Table 9. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Radicalisation and violent extremism	Prevention and countering of radicalisation leading to violent extremism and terrorism	83 %
	New forms of radicalisation	77 %
	Insider threats	63 %
	Radicalisation in prisons	53 %
	Fundamental rights and data protection, including non-discrimination	43 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*75 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*67 %*
	Cybercrime investigations	*66 %*
	Crime prevention	*61 %*
	Criminal intelligence picture, high-risk criminal networks	*61 %*
	Financial investigations	*60 %*
	Forensics/Evidence	*55 %*
	Firearms trafficking	*44 %*
	Fundamental rights and data protection	*43 %*
	Document fraud	*40 %*

[24] The number of trainees is presented as a figure extrapolated to the EU and calculated based on the statistical median; the related methodology and process is further explained in the 'Analysis' section of this report.

Table 10. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (extrapolated to the EU)	Trainees (actual)
Awareness	47 %	260	1 183
Practitioner	57 %	195	1 129
Advanced practitioner	58 %	130	721
Expert	58 %	130	348
Train-the-trainer	54 %	91	195
Average/Total	**55 %**	**806**	**3 576**

Use of OSINT in counterterrorism

Use of OSINT in counterterrorism is the second most relevant main topic, as indicated by the MS (relevance 71 %). On average, the training need is **urgent**, particularly at advanced practitioner, expert and practitioner levels. In terms of quantities, **investigators** and **first responders** would need the training most. Overall, training should be delivered within one year to approximately **741 trainees**. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects, as indicated below.

Table 11. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Use of OSINT in counterterrorism	Methods of lawful interception	88 %
	Value of digital evidence	86 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*89 %*
	Cybercrime investigations	*73 %*
	Criminal intelligence picture, high-risk criminal networks	*65 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*64 %*
	Financial investigations	*62 %*
	Forensics/Evidence	*59 %*
	Firearms trafficking	*56 %*
	Crime prevention	*54 %*
	Document fraud	*46 %*
	Fundamental rights and data protection	*44 %*

Table 12. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	53 %	130	20 842
Practitioner	64 %	117	1 692
Advanced practitioner	67 %	104	938
Expert	66 %	104	516
Train-the-trainer	55 %	78	204

Average/Total	**61 %**	**533**	**24 192**

Countering of financing of terrorism

Countering of financing of terrorism, scoring equally with the topic use of OSINT in counterterrorism, is the third most relevant main topic, as indicated by the MS (relevance 71 %). While the training need is **moderately urgent** at all proficiency levels, the foreseen number of trainees is the highest at **awareness** level. **Investigators** are the biggest training audience indicated by the respondents, other profiles have seemingly fewer potential participants. In total, it would be advantageous for **approximately 663 trainees** to receive training within a year's period. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects, as indicated below.

Table 13. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Countering of financing of terrorism	Emerging threats (cryptocurrencies), and financial links to other types of crime (e.g. tax fraud, money laundering, trafficking of cultural goods)	78 %
	Understanding and investigation of crowdfunding online	65 %
	Public - Private sector partnerships	61 %
	Role of Financial Intelligence Units	55 %
	Financial investigations	*75 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*74 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*71 %*
	Cybercrime investigations	*66 %*
	Criminal intelligence picture, high-risk criminal networks	*60 %*
	Forensics/Evidence	*53 %*
	Document fraud	*52 %*
	Firearms trafficking	*51 %*
	Crime prevention	*50 %*
	Fundamental rights and data protection	*37 %*

Table 14. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	40 %	260	1 317
Practitioner	58 %	130	291
Advanced practitioner	60 %	104	276
Expert	56 %	91	268
Train-the-trainer	44 %	78	151
Average/Total	**52 %**	**663**	**1 317**

Foreign terrorist fighters

Foreign terrorist fighters, with an equal ranking compared to the previous two topics (use of OSINT in counterterrorism and foreign terrorist fighters), is the fourth most relevant main topic as indicated by the MS (relevance 71 %). The training need is **moderately urgent** at all proficiency levels. In terms of volume of trainees, **awareness** level participants are the largest training audience, while **practitioners** hold the highest urgency rate. Considering the profiles of potential trainees, **first responders** would need the training most, followed by **investigators.** Overall, **approximately 858 trainees** would benefit from receiving training within a period of one year. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects, as indicated below.

Table 15. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Foreign terrorist fighters	Foreign terrorist fighters	88 %
	Travelling terrorists and returnees	85 %
	Law enforcement approach to family members of foreign terrorist fighters	74 %
	Battlefield information exchange	78 %
	Financial investigations	*85 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*81 %*
	Forensics/Evidence	*75 %*
	Fundamental rights and data protection	*72 %*
	Criminal intelligence picture, high-risk criminal networks	*69 %*
	Crime prevention	*68 %*
	Cybercrime investigations	*65 %*
	Document fraud	*63 %*
	Firearms trafficking	*62 %*
	Law enforcement/judicial cooperation, information exchange and Iinteroperability	*60 %*

Table 16. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	51 %	520	11 262
Practitioner	58 %	260	2 675
Advanced practitioner	50 %	208	1 376
Expert	53 %	104	533
Train-the-trainer	53 %	52	282
Average/Total	**53 %**	**1 144**	**16 128**

Prevention of dissemination of terrorist content online

Prevention of dissemination of terrorist content online is the fifth most relevant main topic, as indicated by the MS (relevance 67 %). The training need is **moderately urgent** overall, however, it is **urgent** at practitioner level. **First responders** represent the largest group of trainees, followed by **investigators.** In total, it would be advantageous for **approximately 494 trainees** to receive training within a period of one year. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects, as indicated below.

Table 17. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Prevention of dissemination of terrorist content online	Detection and investigation	78 %
	Digital trends	77 %
	Use of PERCI	67 %
	European Union Crisis Protocol (EUCP) as a tool to prevent violent content from going viral on the web/networks in the immediate aftermath of a terrorist/extremist attack	72 %
	Understanding and investigation of crowdfunding online	*67 %*
	Cooperation with Internet Referral Unit of Europol to take down terrorist content online	*73 %*
	Manipulation of social media	*78 %*
	Implementation of the Regulation on the Prevention of Dissemination of Terrorist Content Online	*73 %*
	Firearms trafficking	*53 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*80 %*
	Cybercrime investigations	*78 %*
	Criminal intelligence picture, high-risk criminal networks	*72 %*
	Financial investigations	*63 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*75 %*
	Crime prevention	*63 %*
	Document fraud	*47 %*
	Forensics/Evidence	*64 %*
	Fundamental rights and data protection	*50 %*

Table 18. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	55 %	104	2 157
Practitioner	67 %	156	675
Advanced practitioner	48 %	104	291
Expert	51 %	78	204
Train-the-trainer	49 %	52	123

Average/Total	**54 %**	**494**	**3 450**

Protection of public spaces and critical entities resilience

Holding an equal relevance rate with the above topic, protection of public spaces and critical entities resilience is the sixth most relevant main topic, as indicated by the MS (relevance 67 %). The training need is **moderately urgent**, although interestingly distributed in a way that where the volume of trainees is the highest, namely at awareness level, the urgency of training delivery is the lowest. Then again, while the expert level represents a marginal group in terms of quantities, the urgency among that segment is the highest. Considering the profiles of trainees, **managers** would need training most, followed by an equal distribution between analysts, investigators and intelligence analysts. Overall, **approximately 780 trainees** would find it advantageous to receive training within a year's period. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects as indicated below.

Table 19. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Protection of public spaces and critical entities resilience	Sharing best practices on handling of attacks	78 %
	Risk assessment management	72 %
	Cooperation between public and private sectors	71 %
	Protection by security design	70 %
	Cyberattacks on critical infrastructures	65 %
	Cybersecurity	65 %
	Insider threats	61 %
	Digital skills and the use of new technologies (including darknet, OSINT)	*67 %*
	Criminal intelligence picture, high-risk criminal networks	*63 %*
	Crime prevention	*62 %*
	Law enforcement/judicial cooperation, information exchange and interoperability	*61 %*
	Cybercrime investigations	*55 %*
	Firearms trafficking	*54 %*
	Forensics/Evidence	*50 %*
	Document fraud	*46 %*
	Financial investigations	*45 %*
	Fundamental rights and data protection	*40 %*

Table 20. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	40 %	260	3 352
Practitioner	38 %	182	792
Advanced practitioner	42 %	104	352
Expert	55 %	78	188

Train-the-trainer	44 %	56	122
Average/Total	**44 %**	**780**	**4 806**

Use of information systems and cooperation mechanisms

Use of information systems and cooperation mechanisms is the seventh most relevant main topic, as indicated by the MS (relevance 63 %). The training need is **moderately urgent**, with most participants at **awareness** level. **Investigators** are the biggest group of trainees, with a considerable difference from the following profiles, namely analysts, managers and intelligence analysts that are nearly equal to each other. Overall, **approximately 780 trainees** would find it advantageous to receive training within a year's period. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects as indicated below.

Table 19. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
The use of information systems and cooperation mechanisms in fight against counterterrorism	Interoperability of EU information systems and possibilities for CT investigations	73 %
	Law enforcement/judicial cooperation, information exchange and interoperability	*71 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*70 %*
	Cybercrime investigations	*68 %*
	Criminal intelligence picture, high-risk criminal networks	*64 %*
	Financial investigations	*62 %*
	Crime prevention	*58 %*
	Firearms trafficking	*56 %*
	Forensics/Evidence	*55 %*
	Document fraud	*54 %*
	Fundamental rights and data protection	*48 %*

Table 20. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	40 %	260	2 321
Practitioner	38 %	182	791
Advanced practitioner	42 %	104	431
Expert	55 %	78	303
Train-the-trainer	44 %	56	195
Average/Total	**44 %**	**780**	**4 041**

Regional and neighbouring countries cooperation

Regional and neighbouring countries cooperation is the eighth most relevant main topic, as indicated by the MS (relevance 58 %). Overall, the training need is **moderately urgent**. The highest volume of trainees is for **awareness** level training, followed by practitioners, although the latter is taking a secondary position in terms of urgency rate. Looking at the urgency levels, expert training, while with less participants, holds the highest urgency score. In terms of professional profiles, the most communicated training needs are among **investigators**, and they are significantly higher than the following two, namely analysts and intelligence analysts. Overall, **approximately 780 trainees** would find it advantageous to receive training within a year's period. Within this main topic, training should focus on the most relevant subtopics and horizontal aspects, as indicated below.

Table 19. Relevance rate of subtopics and horizontal aspects in descending order

Main topic	Subtopic / *Horizontal aspect*	Relevance
Regional and neighbouring countries cooperation on specific terrorism cases	Joint investigations cases and best practices	74 %
	Cooperation with MENA countries	73 %
	Cooperation as an advantage to face terrorism threats	72 %
	Law enforcement/judicial cooperation, information exchange and interoperability	*75 %*
	Criminal intelligence picture, high-risk criminal networks	*71 %*
	Digital skills and the use of new technologies (including darknet, OSINT)	*70 %*
	Financial investigations	*69 %*
	Forensics/evidence	*63 %*
	Cybercrime investigations	*63 %*
	Firearms trafficking	*60 %*
	Crime prevention	*54 %*
	Document fraud	*56 %*
	Fundamental rights and data protection	*48 %*

Table 20. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Trainees (median extrapolated to the EU)	Trainees (actual)
Awareness	40 %	260	2 374
Practitioner	38 %	182	787
Advanced practitioner	42 %	104	337
Expert	55 %	78	173
Train-the-trainer	44 %	56	103
Average/Total	**44 %**	**780**	**3 774**

Conclusions

Based on the outcomes of the OTNA on counterterrorism, the majority of the main training topics, as prioritised in the EU-STNA, are relevant for the responding European LE officials. Out of ten topics presented in the OTNA questionnaire, eight topics exceeded the 50 % relevance threshold, namely: **radicalisation and violent extremism**, **use of OSINT in counterterrorism**, **countering of financing of terrorism**, **foreign terrorist fighters**, **prevention of dissemination of terrorist content online, protection of public spaces and critical entities resilience**, **use of information systems and cooperation mechanisms** and **regional and neighbouring countries cooperation on specific terrorism cases.**

The relevance rate of the prioritised main topics vary between 88 % and 58 %, however, it is worth noting that many of the topics reached the same level of relevance, but with differences on other aspects measured. For example, while the topics of use of OSINT in counterterrorism, countering of financing of terrorism and foreign terrorist fighters all reached an equal score (71 %) in terms of relevance, the use of OSINT appears as the only topic that reached an average urgency > 60 %, meaning that training within one year is essential for quality performance. Overall, considering both factors of relevance and urgency, the topics related to counterterrorism establish an ensemble with a number of main topics and subtopics that should be covered by training. In addition to the main topics and subtopics given, the responding MS communicated quite a considerable amount of further training needs through the questionnaire. Considering terrorism being one of the main threats for Europe, it is t expected that the importance of continuously developing the abilities to anticipate, prevent and respond to terrorist threats is mentioned in a number of training needs.

Considering the topic as a whole, **first responders** are seemingly the biggest group of professionals that would need training on counterterrorism, followed by **investigators**. Additionally, on the topic of protection of public spaces and critical entities resilience, **counterterrorism operators** and CBRN-E related **technicians** were indicated as potential target groups that would need to improve their performance through training. In terms of quantities, the highest training need is expressed for **awareness** and **practitioner** level professionals, but when taking into account the ratio of urgency and the number of potential trainees, training of practitioners appears to have a slightly higher priority. Across the topics, an average training need is **moderately urgent**.

Based on the findings of this research, approximately **5 733 participants** would need training on counterterrorism protection in the coming years. It should be noted that this research indicates considerably fewer participants than the previous OTNA report (2021) on counterterrorism[25] that demonstrated a significant increase compared to the year before (2020). However, these reports are not directly comparable with each other due to the new EU-STNA cycle with renewed priorities and different main topics presented in the questionnaire. Considering the volume of LE professionals that the responding MS indicate through their contributions and the extrapolated number of potential trainees reached after processing the data by statistical means, the trainee volumes based on the

[25] Extrapolated figure 42 232 potential participants in OTNA conducted in 2021

findings of this research appear to be in between the two OTNAs from 2020 and 2018, which both identified < 10 000[26] potential participants. As explained in the 'Analysis' section of this report, it must be also noted that the quantity of potential participants, as communicated by responding MS, is considerably higher than the estimated volume of trainees calculated based on the established OTNA methodology; hence, the number of individuals in need of training can only secondarily direct the portfolio design.

This research confirmed the need for a versatile training portfolio on the topic of counterterrorism, covering a number of different topics that have only limited differences in terms of their considered relevance, urgency and estimated volume of trainees. Besides a considerable amount of additional training topics and/or subtopics, several respondents emphasised the need for joint training and exercises, also recognised by the EU's Counter-Terrorism Agenda (2020)[27] as important for developing channels and capabilities for cross-border communication and operations, and improving the pooling of resources that can be mobilised during incidents.

In order to meet the high demand of training on different topics, it will be mandatory to maintain an innovative approach to the design of training events and materials as a means of enabling the European LE professionals involved in this field to continuously develop their skills and knowledge.

[26] 2020/4 144 and 2018/9 256 potential participants at EU level

[27] https://ec.europa.eu/home-affairs/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf

Annex 1. EU-STNA Chapter on Counterterrorism

Environmental challenges

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

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

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

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

Challenges

Law enforcement capacities should be enhanced both in the field of prevention and in the fight against terrorism. Training should focus on more efficient detection and investigation of financing of terrorism and preventing the dissemination of terrorist content online, preventing and combatting the use of unmanned aerial vehicles (UAVs) and chemical, biological, radiological and nuclear (CBRN) weapons in terrorism, protection of public spaces, and the use of artificial intelligence for investigations.Officials should be aware of the motivation of terrorists, in particular the cultural and religious aspects and the psychology of perpetrators, including that of foreign terrorist fighters and returnees. Community policing, as well as cooperation with NGOs and religious communities are imperative.

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

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

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

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

Training needs

Summary

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

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

Member States indicated that 5 375 officials need training in this area in 2023.

Further details

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

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

Officials dealing with counterterrorism should be familiar with the techniques used in financial investigations (financial analysis and forensics), so that they can trace the financial flows related to terrorist activities. Officials should also have a good understanding of national data protection regulations. Training should be delivered in cooperation with financial institutions and cover emerging threats and the financial links to other types of crime, such as tax fraud, money laundering, illicit trafficking in cultural goods, drugs, small arms and misuse of non-profit organisations Preventing the dissemination of terrorist content online, in the context of emerging digital trends, and the implementation of the new regulation are ranked fourth in the list of training needs. Furthermore, training is necessary on the identification of foreign terrorist fighters and returnees and on how their family members should be dealt with by law enforcement. Again, consideration should be given to providing knowledge on fundamental rights and on cultural and religious aspects

.
As mentioned earlier, cooperation is essential both at local level with NGOs and religious communities and at international level with law enforcement agencies. Training, especially joint training activities, could enhance cooperation among stakeholders. Regional and cross-border cooperation in specific terrorism cases could be enhanced by sharing best practices and implementing cross-border exercises. Moreover, training is needed on the protection of public spaces and on the resilience of critical entities, with a focus on sharing views and best practices for handling attacks and testing different prevention and response measures.

Hybrid threats are a combination of different actions against protected state and non-state domains, frequently involving elements of cybercrime; therefore, training should cover countering hybrid threats and include aspects related to cybersecurity. In fact, there is a need for raising awareness of hybrid threats and the role which law enforcement plays in responding to them at EU level. In addition, officials need training on the use of UAVs, with an emphasis on both the related threats posed by terrorists and the opportunities for law enforcement. This should be complemented with training on the use of AI to combat terrorism.

List of identified and prioritised training needs

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

	Counterterrorism
1	Radicalisation: preventing and countering radicalisation that leads to violent extremism and terrorism; new forms of radicalisation; fundamental rights and data protection, including non-discrimination
2	Use of OSINT in counterterrorism; value of digital evidence; methods of lawful interception
3	Countering the financing of terrorism: emerging threats, financial links to other types of crime and criminal organisations (e.g. tax fraud, money laundering, illicit trafficking in cultural goods, drugs, small arms and abuse of non-profit organisations); setting up and managing public-private partnerships, modus operandi and new modes of terrorist financing (e.g. crowdfunding platforms, use of crypto assets and bitcoin trading (including use of non-fungible tokens (NFT)); collection and use of financial intelligence
4	Prevention of dissemination, detection and investigation of terrorist content online; digital trends; use of the EU platform to combat illegal content online (PERCI) and implementation of regulation on addressing dissemination of terrorist content online
5	Foreign terrorist fighters, travelling terrorists and returnees; law enforcement approach to family members of foreign terrorist fighters
6	Use of information systems and cooperation mechanisms in the fight against terrorism
7	Protection of public spaces and resilience of critical entities; sharing best practices on handling attacks
8	Regional and cross-border cooperation on specific terrorism cases
9	Unmanned aerial vehicles: threats and opportunities for law enforcement
10	Use of AI by law enforcement
11	Tackling document fraud

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 to 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, and 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 skeptical colleague, countering sophisticated denialism 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 as a 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 the 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

Annex 3. Urgency levels

Urgency in the context of this questionnaire refers to the criticality of timely training intervention and its impact to the operational performance.

Urgency scale level	1	2	3	4	5
Training need is	Low	Secondary	Moderate	Urgent	Crucial
Training impact	Training has a minor role in the performance boost, it would refresh the knowledge, officials could benefit from training, and however, it is not essential.	It would be useful if the training would be delivered, however, the need is not urgent. Training can be delivered in (predictable) 2-3 years' time, it is needed to stay updated.	It would be advantageous to receive training within a year's period, it would improve the performance, however, not significantly.	Training is essential, it is necessary to be delivered within a year's period, it is important to perform qualitatively.	Training is critical, it is necessary as soon as possible, it is crucial for the successful performance of duties.