CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

Operational Training Needs Analysis
Online Fraud Schemes

EDUCATE, INNOVATE, MOTIVATE

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

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

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

PDF ISBN 978-92-9211-432-9 doi:10.2825/480073 QR-07-23-272-EN-N

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

Photograph: © cover: iStockPhoto.com/piranka

Contents

List of tables

List of charts

List of annexes

List of abbreviations

AI – Artificial Intelligence
AML - Anti-Money Laundering
ATM – Automatic Teller Machine
ATO - Account take over
BEC - Business Email Compromise
CEPOL – European Union Agency for Law Enforcement Training
CKC - CEPOL Knowledge Centre
CNU – CEPOL National Unit
CSDP – Common Security and Defence Policy
EU – European Union
EU-STNA – European Union Strategic Training Needs Assessment
HRCN – High-Risk Criminal Networks
JHA – Justice and Home Affairs
LE – Law enforcement
MB – Management Board
MS – EU Member State
NFT - Non-fungible token
OFCAN - European Anti-Fraud Office
OSINT – Open Source Intelligence
OTNA – Operational Training Need Analysis
PoS – Point-of-sale
PSD2 - Payment Services Directive
SEO - Search Engine Optimisation
SIM – Subscriber Identity Module
SPD – Single Programming Document
TTT – Train-the-trainer

Executive summary

Under the umbrella of fraud, economic and financial crimes, the topic of online fraud schemes is one the European Union's (EU) priorities in the fight against serious and organised crime as part of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) 2022-2025[1]. In the EU's Strategic Training Needs Assessment (EU-STNA) for 2022-2025, **online fraud schemes (fraud, economic and financial crimes)** were also placed among the prioritised thematic clusters where training for the European law enforcement (LE) audience should be delivered within a four-year cycle.

Following up on this strategic training priority, the European Union Agency for Law Enforcement Training (CEPOL) launched an **Operational Training Needs Analysis (OTNA) on online fraud schemes** in December 2022, with a view to using the outcomes of the research to define its training portfolio for 2024-2026. An online survey resulted in **39 individual answers** from LE agencies in **20 different MS[2]**, reportedly representing more than 3 288[3] officials in service.

In line with the training topics identified and prioritised in the EU-STNA, the OTNA survey included the seven main topics listed below.

- Card-not-present fraud
- Cyber scams
- Cybercrime facilitators
- Card-present fraud
- Cyber threat intelligence, dark web and Open Source Intelligence (OSINT)
- Intrusions into system networks of financial institutions
- Legal challenges in non-cash payment methods

Respondents were able to select the topics for which they wished to communicate the related training needs from their respective countries. Applying the established OTNA analysis approach whereby if more than 50 % of the responding MS select a topic, it is carried forward for further analysis, five out of seven topics passed this criterion, namely: **cyber scams**, **cyber threat intelligence**, **dark web and OSINT**, **card-not-present fraud**, **cybercrime facilitators** and

[1] Available on: https://www.europol.europa.eu/crime-areas-and-statistics/empact
[2] Responding countries: Austria, Belgium, Bulgaria, Cyprus, Czechia, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.
[3] The number of officials in service represented is approximate, as some respondents provided answers such as 'up to', 'more than' (rounded up to closest approximate) or 'not able to specify'.

legal challenges in non-cash payment methods. In terms of urgency[4], the main topics range from 85 % to 53 %, meaning that all of them are seen as either **crucial**, **urgent** or **moderately urgent**. In Chart 1, below, the topics are presented in descending order based on the combined average (orange bars), factoring in the popularity level and urgency rate.

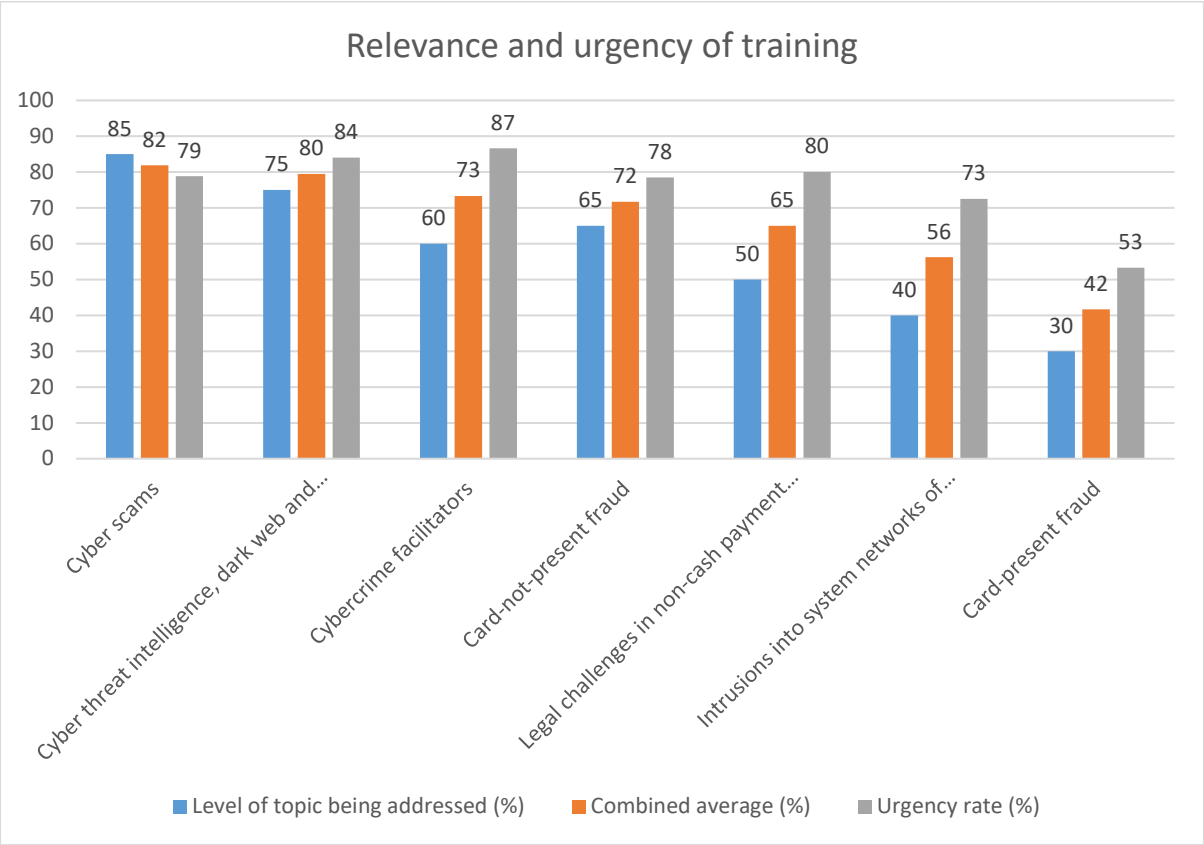


Chart 1. Popularity of main topics addressed

In addition to the main topics, the survey included eight horizontal aspects, namely **digital skills and the use of new technologies, high-risk criminal networks (HRCN)**, **financial investigations**, **crime prevention**, **cooperation, information exchange and interoperability**, **forensics**, **document fraud** and **fundamental rights and data protection.** All these aspects were considered relevant by more than half of the responding countries, with the final rates ranging from 78 % to 52 % as illustrated in Chart 2 below.

[4] See the explanation of urgency levels in Annex 3.

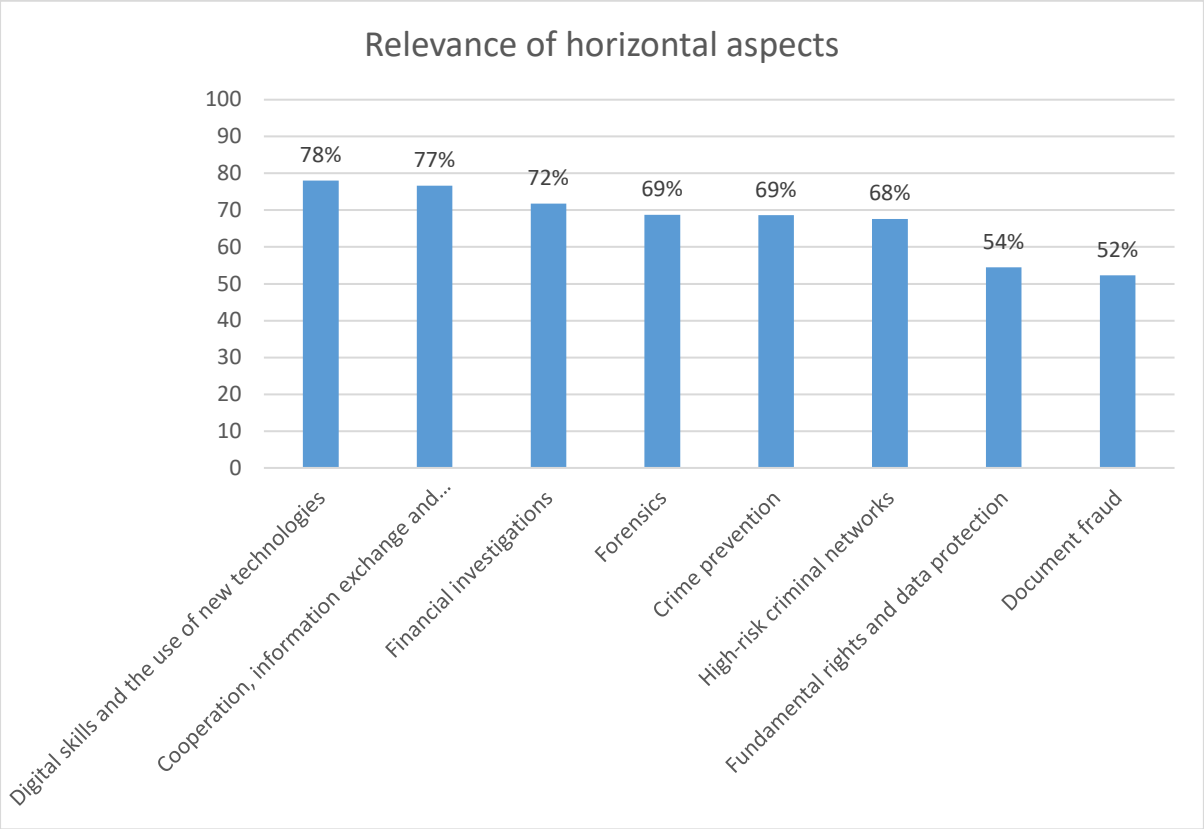


Chart 2. Relevance of horizontal aspects included in the survey

In total, **up to 27 404 participants would need training on these seven main topics.** For the prioritised five main topics, **22 932 potential participants** are foreseen.

The OTNA questionnaire gave respondents the opportunity to specify the profiles and indicate the number of LE officers who would need training in different topics. Based on the statistical analysis, the volume of trainees breaks down relatively equally between the different proficiency levels, with awareness-level training nevertheless being established as the largest category of potential trainees. However, as demonstrated in Table 1 below, the non-processed numbers communicated by the respondents suggest that **practitioners** are the priority group, followed by **advanced practitioners** and **experts** with almost equal shares.

Table 1. Proficiency levels and number of participants - all main topics

Proficiency level	Number of participants (median)	Number of participants (actual)
Awareness	7163	678
Practitioner	4927	3999
Advanced practitioner	6045	2577
Expert	5135	2516
Train-the-trainer	4134	270
Total	**27404**	**10040**

In terms of the profiles of participants, **prosecutors, investigative judges, magistrates**, **first responders and investigators** and **intelligence officers,** in that order, made up the top three trainee categories. Furthermore, as Table 2 illustrates, the actual number of **investigators and intelligence officers** was even higher than shown in the results of the calculations completed based on the OTNA methodology.

Table 2. Profiles of trainees – all main topics

Category	Number of participants (median)	Number of participants (actual)	Share % of all trainees
First responders	6539	806	23
Investigators and intelligence officers	4680	**7184**	16
Analysts	3536	721	12
Managers	2821	335	10
Prosecutors, investigative judges, magistrates	6994	531	25
Experts (Forensics, IT etc.)	2340	407	8
Other	1456	56	5
Total	**27404**	**10040**	**100**

Overall, 64 % of all responses received through the survey refer to organisation-level figures in terms of training needs, which indicates that the number of trainees across the MS can be at least, if not even more, what the median-based calculations extrapolated to EU level suggest.

Most subtopics included under the main topics also reached the 50 % relevancy threshold, with the exception of mimic and voice fraud under the main topic of cyber scams. Table 3, below, provides a summary of all the subtopics and their relevancy score, including those under the main topics selected by more than 50 % of the responding MS.

Table 3. Relevance of subtopics – all main topics presented in the survey

Main topic	Subtopic	Relevance (%)
Cyber scams	Online investment fraud selling novel investments and cryptocurrencies	81
	Account take over (ATO)	63
	Business and email compromise fraud	68
	Social engineering	64
	Helpdesk fraud	54
	Mimic and voice fraud	*36*

Cyber threat intelligence, dark web and OSINT	Dark web and OSINT	78
Card-not-present fraud	Phishing and vishing	83
	Compromised credentials used for online payments	80
	Mobile banking fraud	78
	Smishing	76
	Online payment scams	73
	E-commerce fraud	71
	Carding platforms	60
	Darknet marketplaces	58
	Subscriber Identity Module (SIM) swapping	54
Cybercrime facilitators	Cryptocurrencies	89
	New online tools and digital techniques	81
	Anonymisation	71
	Money muling	69
	Online forgery	60
	Encryption	53
	Use of deepfakes created with artificial intelligence (AI)	54
Legal challenges in non-cash payment methods	*No subtopics presented*	
Intrusions into system networks of financial institutions	Use of malware to intercept login details for online banking services	61
	Banking malware/point-of-sale (PoS) malware	48
	Logical attacks against Automatic Teller Machines (ATM)	38
Card-present fraud	Mobile payment fraud	52
	Contactless card fraud	50
	Skimming and shimming	40

Designed for prioritising tasks by first categorising items according to their urgency and importance, the Eisenhower Method was used for showing the distribution of the main topics by their urgency and relevance rate, and visualising the data in the form of a matrix. The Eisenhower Matrix (Chart 3) below displays the relationships between three numeric variables, namely relevancy, urgency and the number of trainees for each main topic. Each dot in the bubble chart corresponds to a single data point (main topic). The horizontal axis represents the popularity of the topic, the vertical axis represents the urgency rate, and the size of the bubbles corresponds to the number of trainees.

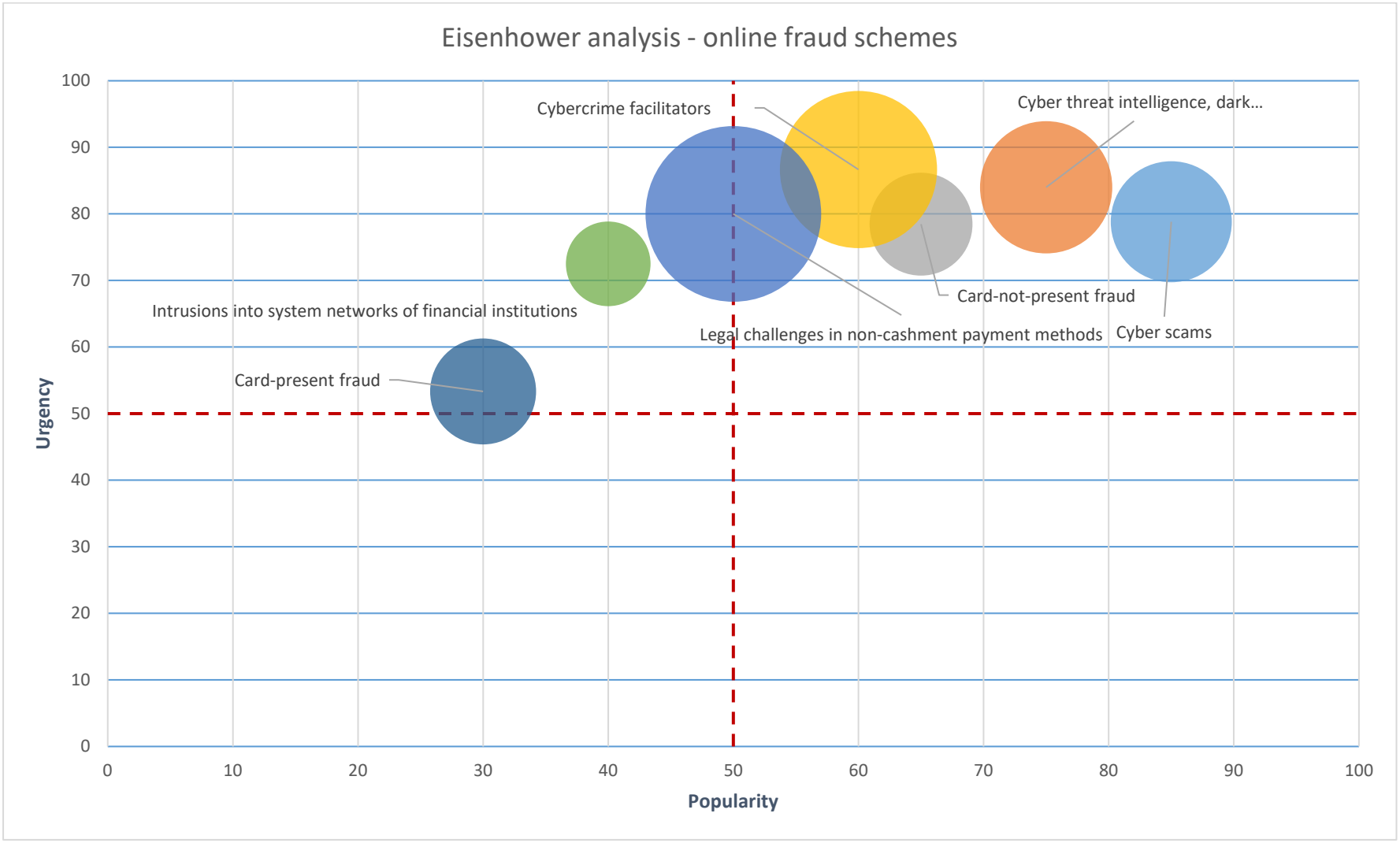


Chart 3. Eisenhower analysis – relevancy and urgency of training on main topics

Introduction

As defined under Article 3 of Regulation 2015/2219, the objectives of the European Union Agency for Law Enforcement Training (CEPOL) are to support, develop, implement and coordinate training for law enforcement officers, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of law enforcement (LE), in particular in the 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 EU missions, which may also include training on law enforcement leadership and language skills.

The Single Programming Document (SDP) for the years 2024-2026[5] describes OTNA as seeking to assist the realisation of strategic goals through the implementation of operational training activities. The OTNA methodology as adopted by CEPOL Management Board (MB) Decision 32/2017/MB (15/11/2017) was piloted in 2018. There were a limited number of thematic priorities for the 2019 CEPOL training portfolio, namely CSDP missions and Counterterrorism. The OTNA methodology was updated in 2020 (9/2020/MB) based on CEPOL's experience and the feedback of the MS. Since then, CEPOL has conducted multiple OTNAs each year on different topics defined in the EU-STNA, which have been complemented by extraordinary needs assessments as necessary, conducted by applying the OTNA methodology.

The methodology consists of a series of seven steps encompassing close and dynamic cooperation with the MS, in particular the CEPOL National Units and LE agencies, and involving CEPOL Knowledge Centres (CKC) in the design of the training portfolio. 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 LE officers, as defined in Article 2 of Regulation 2015/2219[6].

Building on the strategic training priorities defined by the EU-STNA and the experience gained from previous OTNA studies, CEPOL launched the OTNA on online fraud schemes in 2022. In order to develop a detailed overview of training needs in the field, an online survey was designed, programmed and delivered through the Qualtrics® web-based survey tool. Through

[5] https://www.cepol.europa.eu/about/key-documents?pg=1, Annex to Management Board Decision 17/2022/MB, CEPOL Single Programming Document for Years 2024-2026, (13 December 2022), p. 5.
[6] https://publications.europa.eu/en/publication-detail/-/publication/c71d1eb2-9a55-11e5-b3b7-01aa75ed71a1/language-en

the survey, CEPOL invited 26 MS[7] and EU institutions to provide their views on training needs relating to the topic. Data collection took place between 19 December 2022 and 3 February 2023.

The material collected consists mostly of quantitative data, complemented by a portion of text data. In order to analyse the results, data was first transferred from the online survey platform, Qualtrics®, to Microsoft Excel, and then processed by applying the OTNA methodology-based analysis approach, introduced in detail in the methodology and further explained in the 'Analysis' chapter of this report. Written responses were approached manually[8] and analysed by applying basic text analysis procedures.

This report summarises the outcomes of the OTNA process, which are intended to be used for defining CEPOL's training portfolio on online fraud schemes, aimed at strengthening European LE professionals' capacity to tackle this type of cyber-enabled crime. The report is structured into five main chapters. The executive summary provides an overview and summarises the overall findings of the process. The introductory part lays out the methodological and procedural dimensions of the study and provides an overview of the pool of respondents contributing to this OTNA. The following chapter is the analytical core of the report as it sets out in detail the training needs on the five main topics that were selected by at least 50 % of the responding MS. The penultimate chapter then presents each main topic in detail. Lastly, the conclusions summarise the findings of the OTNA process and communicate the key messages for further consideration by the users of this report.

Participants

In total, representatives from **20 MS**[9] responded to the survey, resulting in **39 individual completed answers** received from different LE agencies. In terms of Member States, the responses indicate a **77 % response rate**, which can be considered a relatively good level of responsiveness. The map below (Chart 4) shows an overview of the countries contributing to the process (responding countries are highlighted in blue).

[7] Hereinafter, 'MS' refers to the 26 EU Member States participating in the CEPOL regulation, i.e. all EU MS apart from Denmark.
[8] Meaning without using any qualitative analysis software.
[9] Austria, Belgium, Bulgaria, Cyprus, Czechia, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

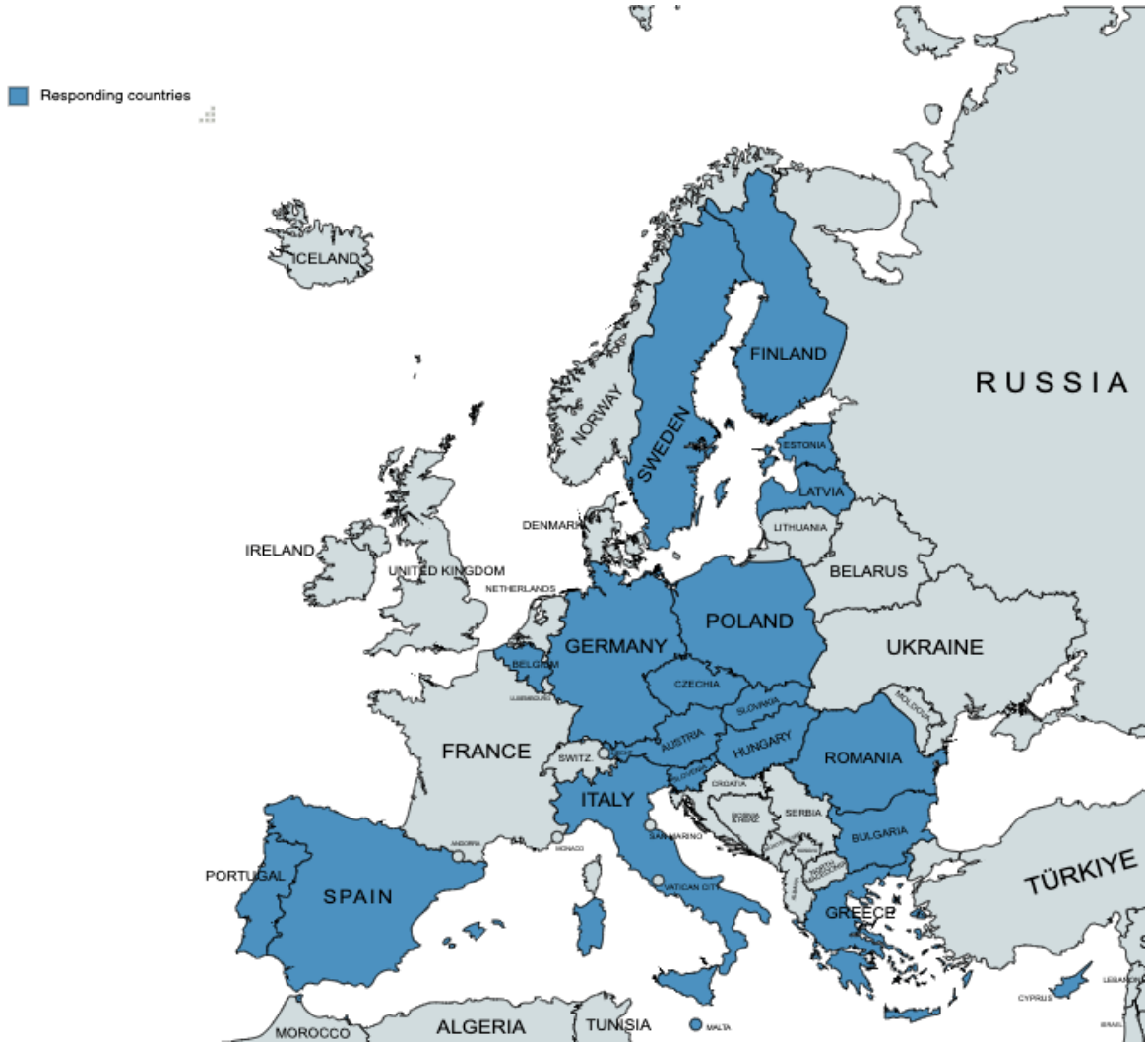


Chart 4. Overview of responding countries

The majority of the responses came from the **police or military police** (85 %), followed by the category of **other relevant bodies** (13 %) and **customs** (3 %). Responding organisations that fall into the 'other' category typically represent, for example, prosecutor's offices, tax authorities, intelligence services and the European Anti-Fraud Office's (OLAF) member organisations (national transparency authorities).

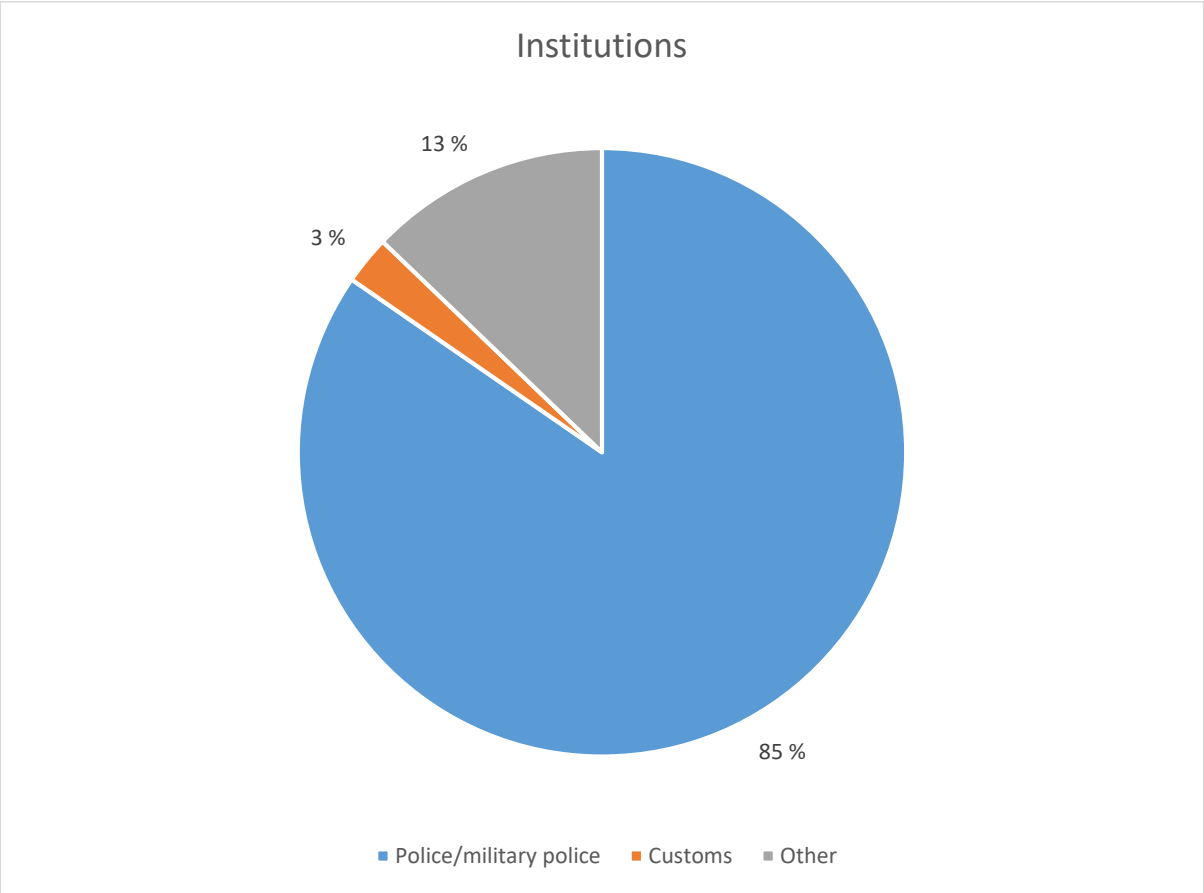


Chart 5. Sectors represented by respondents

The largest group of respondents specified that they represented an organisation with a mandate related to criminal intelligence and/or investigations. The following two groups of respondents represented organisations, departments or units dealing with cybercrime. With almost equal shares, responses were divided between organisations that stated they had a 'general' law enforcement mandate, or those that specifically handle cases related to tax crimes and offences, e.g. investigation and prevention of tax evasion and tax fraud. A few responding organisations reported that they dealt with economic and financial crimes or combatting fraud relating to the EU budget.

Analysis

This chapter presents the core analysis conducted on the topics included in the OTNA survey. The first two parts introduce the process and the outcomes of analysing the relevance of the main topics and related subtopics in the survey, including a list of additional subtopics suggested by the responding MS. The following part concerns the urgency of training needs, as well as the estimated volume and profiles of potential participants, and the last parts of the chapter discuss potential additional training needs and regional, subregional and/or nationwide training needs.

Relevance of topics and subtopics

In order to identify which main topics are the most important for the European LE community requiring CEPOL training in 2024-2026, the OTNA questionnaire included a multiple choice question where respondents could select one or more choices from a list of seven main topics. When analysing the results, the popularity score of each main topic was calculated by adding up how many MS found the topic relevant. The final rate was then calculated by dividing the sum of MS that found the topic relevant by the number of responding MS. Where several LE agencies submitted answers from the same MS, the responses were consolidated. If more than 50 % of MS found a certain topic relevant, it was considered relevant and was processed for further analysis as per the OTNA methodology. Based on this procedure, five out of the seven main topics passed the 50 % threshold, meaning that they were included in the analysis process for which the results are presented in the main body of this report.

Table 4. Ranking of prioritised main topics based on their popularity level

Main Topic	Rate of topic being addressed (%)
Cyber scams	85
Cyber threat intelligence, dark web and OSINT	75
Card-not-present fraud	65
Cybercrime facilitators	60
Legal challenges in non-cash payment methods	50

In order to gain further insight into training needs, various **subtopics** were presented under each topic. The questionnaire gave the respondents an option to rate the relevancy of subtopics and horizontal aspects by using a five-point Likert scale: not relevant at all; somewhat relevant; relevant; very relevant; and extremely relevant. To analyse the responses, this scale was converted into a numerical scale of 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 adding up the responses, except in cases

where several authorities from the same MS gave answers, and then calculating an average that was used as the final relevancy level for that particular country. The final relevance rate (percentage) was calculated by dividing the score by the maximum score[10]. If the relevance score reached 50 % of the maximum score, the subtopic was considered relevant.

The analysis revealed that training needs for most subtopics included under each main topic are considerably high, and in most cases, with all subtopics reaching the 50 % threshold, in most cases with very little difference between the highest and lowest scores. In descending order, Table 6 shows the relevance rate of all the subtopics.

Table 5. Relevance rate of most relevant subtopics from prioritised main topics

Main topic	Subtopic	Relevance (%)
Cyber scams	Online investment fraud selling novel investments and cryptocurrencies	81
	ATO	63
	Business and email compromise fraud	68
	Social engineering	64
	Helpdesk fraud	54
	Mimic and voice fraud	*36*
Cyber threat intelligence, dark web and OSINT	Dark web and OSINT	78
Card-not-present fraud	Phishing and vishing	83
	Compromised credentials used for online payments	80
	Mobile banking fraud	78
	Smishing	76
	Online payment scams	73
	E-commerce fraud	71
	Carding platforms	60
	Darknet marketplaces	58
	SIM swapping	54
Cybercrime facilitators	Cryptocurrencies	89
	New online tools and digital techniques	81
	Anonymisation	71
	Money muing	69
	Online forgery	60
	Encryption	53
	Use of deepfakes created with AI	54

[10] Maximum score was identified by multiplying the number of responding MSs that found the subtopic relevant with the highest relevancy score (5)

Legal challenges in non-cash payment methods	*No subtopics presented*

Additional subtopics

Through the OTNA questionnaire, the respondents also communicated potential **additional subtopics** related to the main topics of **legal challenges**, **card-not-present fraud** and **intrusions into networks and institutions**. All additional requests primarily concerned the **police**, but also judicial authorities, as the target audiences. Chart 6 below gives more details on the suggested additional subtopics.

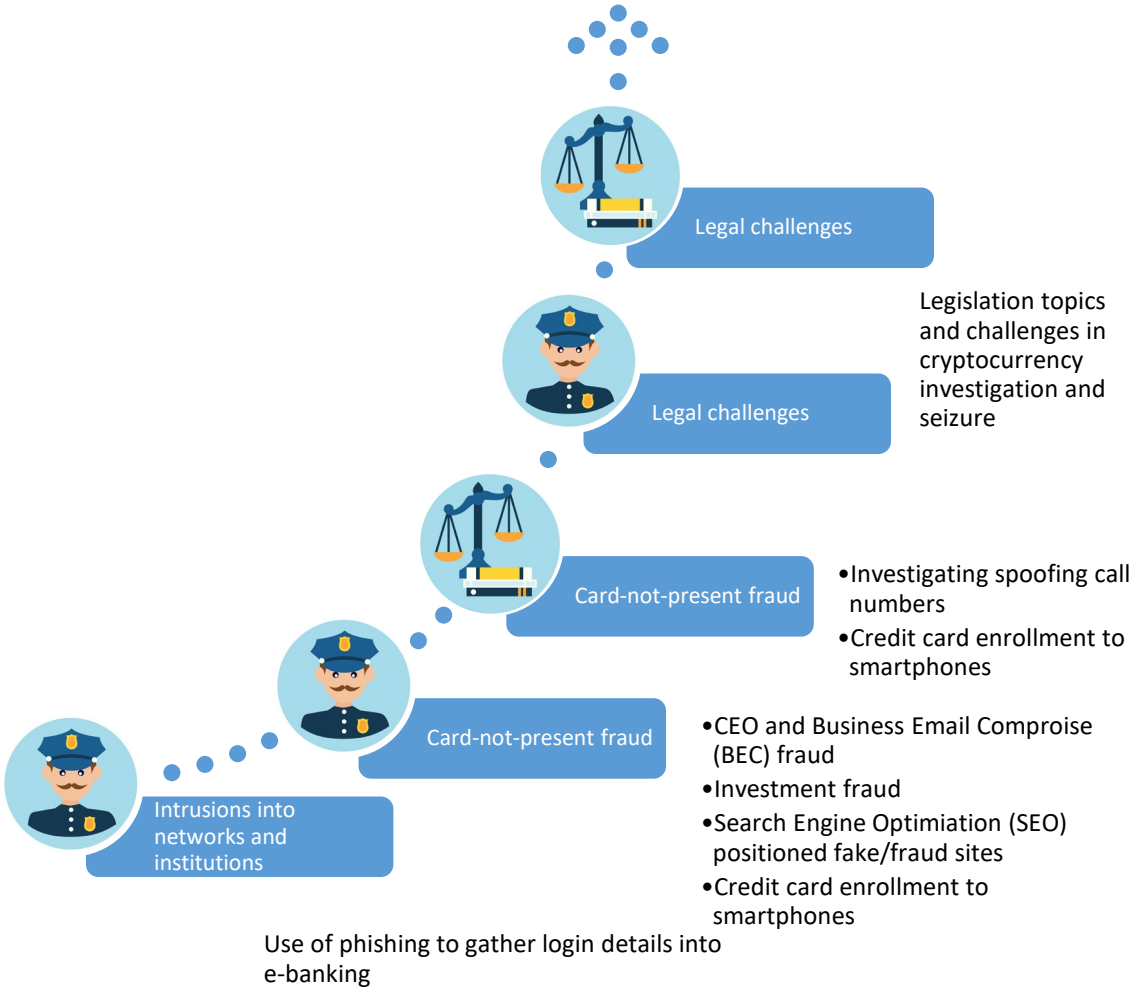


Chart 6. Additional subtopics[11]

[11] SmartArt design has been complemented with assets from Freepik.com. Law, justice & police icons by macrovector_official on Freepik, available on https://www.freepik.com/

Urgency and volume of training needs

To better understand the training needs under each main topic, the questionnaire gave the respondents an option of indicating the **urgency level of training** on the main topics and estimating the **number of participants** based on five different **professional levels**[12]. 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 of training was needed and how urgently LE officers would need training to improve their current performance. By choosing from a six-point urgency-level scale (most commonly known as a Likert scale)[13], respondents could state whether they thought the training need was: not urgent; somewhat urgent; moderate; urgent; very urgent; or alternatively, not applicable at all. Urgency in the context of OTNA methodology refers to the criticality of a timely training intervention and its impact on operational performance. In the analysis, responses were converted into a numerical scale from 0-5, where 1 refers to a low need with a minor expected impact on boosting performance and 5 refers to a crucial need as a critical response for ensuring the successful performance of duties. The minimum value is 0 because 'not applicable' means a zero training need. Where the same proficiency level was indicated by several LE agencies from the same MS, the highest rate indicated was taken into consideration.

Since CEPOL's training activities are aimed at law enforcement officials in the 26 EU MS, the number of participants indicated in the responses to the survey is considered to be the number of participants who would need training from the responding MS. In order to estimate the total number of LE officers who would need training in a certain topic at a certain proficiency level, OTNA methodology relies on calculations 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 by 26 (the number of MS[14]). In statistics, the median is the value separating the higher half from the lower half of a data set, so it can be considered the middle value. Based on this method of calculation, approximately **22 932 individuals** across the MS would need training on the five most frequently chosen[15] main topics in 2024.

[12] Awareness, Practitioner, Advanced practitioner, Expert and Train-the-trainer; please find a detailed description of proficiency levels in Annex 2.
[13] 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.
[14] All EU MS apart from Denmark.
[15] More than 50 % of MS selected the topic.

Table 6. Ranking of main topics based on urgency and trainee breakdown

Main topic	Level of topic being addressed (%)	Urgency rate (%)	Combined average (%)	Trainees (median)	Trainees (actual)
Cyber scams	85	79	82	3562	1676
Cyber threat intelligence, dark web and OSINT	75	84	80	3289	647
Cybercrime facilitators	60	87	73	6006	4784
Card-not-present fraud	65	78	72	2574	1771
Legal challenges in non-cash payment methods	50	80	65	7501	564
Average/total	**67**	**82**	**74**	**22932**	**9442**

A 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. However, a general limitation of this method of calculation is that it might also happen that the ranking of participants (median-based numbers extrapolated to EU level) differs from the actual responses. Without statistically processing the data, the respondents communicated that there would be **up to 9 442 potential trainees** on these five prioritised main topics related to online fraud schemes.

Profiles and proficiency levels

In addition to calculating the overall urgency rate and number of trainees per each prioritised main topic, training needs and the volume of trainees were analysed for each proficiency level. In terms of trainees, **awareness** and **advanced practitioner** levels formed the two main groups of potential training participants, with very similar numbers, followed by trainees at **expert**, **practitioner** and **train-the-trainer** level. Based on the statistical median figures, Table 8 provides an overview of the volume of trainees for each proficiency level. As a comparison, it provides the actual numbers of trainees as given by survey respondents, which place notably less emphasis on awareness-level training and place **practitioners**, **advanced practitioners** and **experts** as the largest groups of potential participants.

Table 7. Proficiency levels and number of participants – prioritised main topics

Proficiency level	Number of participants (median)	Number of participants (total)
Awareness	5889	552
Practitioner	3452	**3907**
Advanced practitioner	4875	**2469**
Expert	4160	**2248**
Train-the-trainer	4056	266
Average/total	**22932**	**9442**

In order to establish a more comprehensive picture of the target groups to be trained, the questionnaire offered the possibility of indicating **professional profiles**[16] and the related volumes of LE officers who need training under each main category. Based on the identified statistical median[17], **prosecutors, investigative judges and magistrates** constitute the largest single group of professionals that would require training on online fraud scheme topics, followed by **first responders**, **investigators and intelligence officers**. However, it is worth noting that based on the actual number of potential participants submitted by the responding MS, **investigators and intelligence officers** form the largest segment of trainees, with an even higher number of potential participants than any median-based calculation extrapolated to EU level. The reason behind this is that some MS, in particular Spain, indicated considerable volumes of officials[18] in need of training falling into this category.

Table 8. Profiles of potential participants – prioritised main topics

Category	Number of participants (median)	Number of participants (actual)	Share % of all trainees
Prosecutors, investigative judges, magistrates	**6123**	510	28
First responders	5031	680	21
Investigators and intelligence officers	4004	**7010**	17
Analysts	2912	595	12
Managers	2275	276	10

[16] Profiles presented in the survey included: first responders, public order officers, investigators, intelligence officers, analysts, managers, prosecutors and magistrates, judicial investigators, experts (forensics, IT etc.) and other.

[17] For more detailed description on the methodology, please see Section 'Analysis' of this report

[18] E.g. on the topic of Cybercrime facilitators, close to 4000 professionals at different proficiency levels

Experts (Forensics, IT etc.)	1365	324	6
Other	1222	47	5
Total	**22932**	**9442**	**100**

Trainees per country

Complementing the identification of the total number of trainees per each main topic, actual totals reported by each responding MS were calculated and can be used for further assessments, such as on a regional emphasis on training. While further details are given under the presentation of training dimensions, the table below provides an overview of the overall breakdown of training needs on leadership and management topics, based on the total volume of reported participants.

Table 9. Volume of potential trainees per responding country – actual values

Country	Number of trainees	Share of all participants (%)
Spain	6409	67.9
Italy	607	6.4
Greece	584	6.2
Sweden	500	5.3
Portugal	341	3.6
Estonia	311	3.3
Czechia	178	1.9
Hungary	157	1.7
Romania	94	1.0
Poland	73	0.8
Cyprus	48	0.5
Finland	39	0.4
Belgium	26	0.3
Austria	18	0.2
Germany	15	0.2
Bulgaria	12	0.1
Latvia	12	0.1
Malta	8	0.1
Slovenia	6	0.1
Slovakia	4	0.0
Total	**9442**	**100**

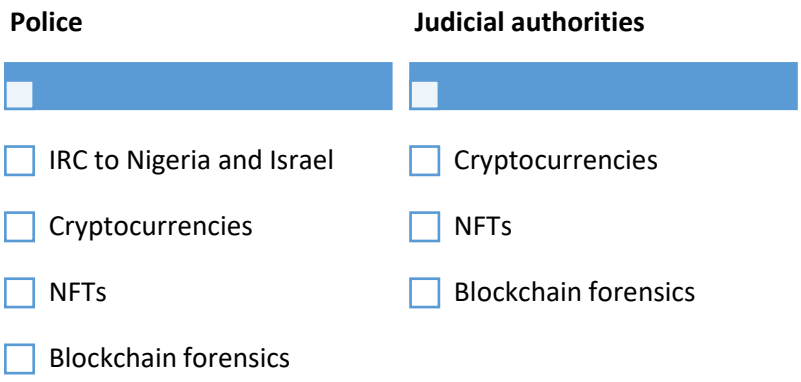
Due to a good number of responses received from Spain, the share of potential Spanish participants notably overpowers the total overview. It must be noted that all responses representing the same organisation might cause a multiplication in numbers, and it should

also be mentioned that one respondent communicated considerably high volumes of participants compared to other respondents. This respondent was invited for an interview, but in the end the interview was not able to be conducted[19].

Further training suggestions

Through an open text field, respondents were also able to specify other professionals in need of training and insert the related numbers. Only about 8 % (n=3) of respondents expressed further training needs, which included: **police** and **judicial authorities** as training audiences for common topics of **cryptocurrencies**, **non-fungible tokens** (**NFT)** and **blockchain forensics**, and specific **police** training on the topic of **IRC to Nigeria and Israel.** Chart 7 below compiles the core topics and the related target audiences of suggested further training needs[20]. Further suggestions on the first three topics were made mostly for **practitioner** level training, and also for advanced practitioner and expert training, but in notably fewer quantities. The need for training on these topics was assessed as being urgent. On the topic of IRC, training requests concerned (individual) expert-level training with less urgency.

Chart 7. Further training suggestions



While not submitted through the section(s) in the survey dedicated either to further training suggestions or additional subtopics, but provided as a general comment, topics related to **online tobacco sales** and **money laundering** were also brought up for consideration as potential training topics.

[19] Situation as of 12 March 2023. The report will be revised accordingly if the respondent can be reached and an interview conducted before closing the OTNA process.
[20] Other suggestions for further training included topics such as common economic activities, tactical casualty care, shooting training in real situations, police car innovation, deep fake, disinformation and OSINT.

Regional training needs

For the first time, the OTNA surveys launched in 2022 were also used for mapping initial views on regional training needs. This particular survey on online fraud schemes collected only a very moderate level of feedback on regional training needs, which either suggested a specific topic such as **cryptocurrencies** (training needed in Czechia), made an overall reference to all topics being regional training needs (Slovenia), or indicated regional needs but without providing specifying the topic or region. In order to clarify those potential regional training needs – for example, relatively high numbers of trainees with specific profiles coming from one responding MS, Portugal – one respondent was invited for an interview. While the further clarifications provided by this respondent did not uncover any particular training need that needed to be urgently addressed locally, it was confirmed that additional training on all topics would be relevant for Portuguese LE professionals. In this case, the training needs more specifically referred to specialised experts investigating smuggling crimes and tax fraud (approximately 350 individuals), who would benefit from receiving online training delivered at unit level.

National or international training

The OTNA questionnaire included a question referring to previous national or international training on online fraud schemes. In terms of topics, training data was provided in a free-form text, so the presentation differed between each topic. The text entries provided were approached by implementing a light text analysis, based on word spotting in an Excel spreadsheet, grouping similar entries and establishing categories of entries representing thematically similar topics. 28 % of respondents (n=11) provided such details, with around 30 entries concerning training attended on different topics. More than two thirds (67 %) of these were reported as being attended online, through different types of virtual implementation (webinar, online module or course), which indicates that online training delivery suits this target audience well. Most of the training received was at practitioner level (46 %), with expert training being the second most attended level (23 %).

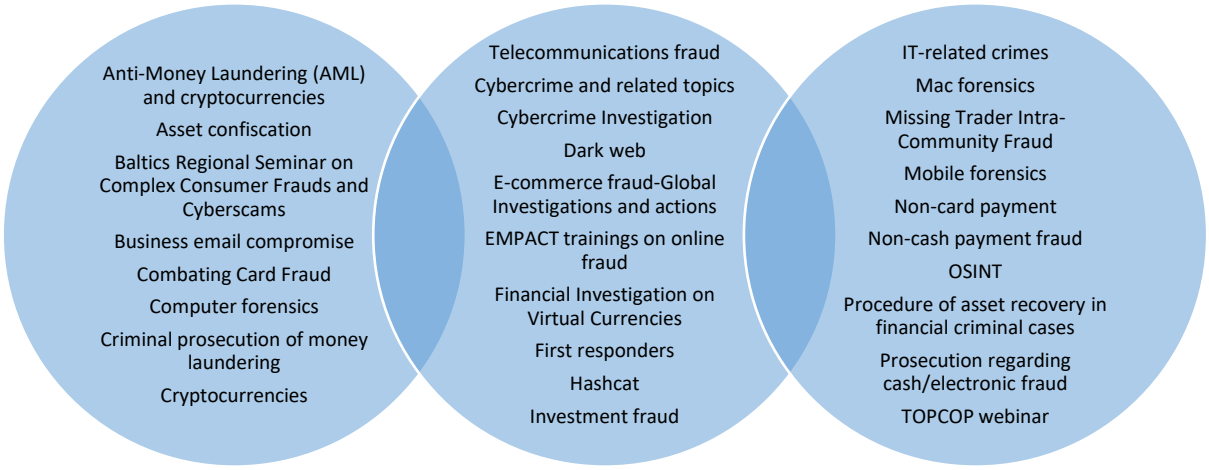


Chart 8. National or international training attended

Training dimensions for main topics

As per the methodology explained in the previous chapter, five of the most selected main topics were analysed in terms of relevancy of subtopics, level of proficiency, potential number of participants per profile, and urgency of training needs. This chapter presents the training needs related to each main topic in more detail. After a summary of training needs, the first table of each main topic shows the relevance rate of subtopics in descending order. The second table demonstrates the estimated number of participants per different proficiency level, both those calculated in line with the OTNA methodology[21] and, for comparison, the figures communicated by the responding MS, as well as the urgency rate of the training to be delivered.

Cyber scams

Cyber scams was the most frequently selected main topic, highlighted by 85 % of responding countries. The need for training on the topic is **urgent** (79 %) with **up to 3 562 trainees** requiring training within a one-year period.

[21] 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 are further explained in the 'Analysis' chapter of this report.

Table 10. Relevance rate of subtopics – cyber scams

Main topic	Subtopic	Relevance (%)
Cyber scams	Online investment fraud selling novel investments and cryptocurrencies	81
	Business and email compromise fraud	68
	Social engineering	64
	ATO	63
	Helpdesk fraud	54
	Mimic and voice fraud	36

Investigators and intelligence officers are suggested as the main target group for the training, primarily at awareness level. The estimated number of trainees in this category is the highest regardless of the method of calculation[22]. **First responders** and **analysts** form the next largest groups of potential trainees, with indications of training offered to participants at different levels.

Table 11. Profiles and number of potential trainees – cyber scams

Profile/ proficiency level	Awareness	Practi-tioner	Advanced practi-tioner	Expert	TTT	Median total	Actual total
First responders	52	299	130	208	0	**689**	158
Investigators and intelligence officers	520	221	78	182	52	**1053**	1085
Analysts	260	78	26	104	39	**507**	157
Managers	78	91	52	26	26	**273**	82
Prosecutors, investigative judges, magistrates	52	130	130	52	156	**520**	105
Experts (Forensics, IT etc.)	0	78	26	130	52	**286**	80
Other	52	0	182	0	0	**234**	9
Total	1014	897	624	702	325	**3562**	1676

[22] Statistical median vs actual numbers.

Cyber threat intelligence, dark web and OSINT

Cyber threat intelligence, dark web and OSINT is the second most selected main topic by the MS (75 %), with an urgency rate of 84 % considered as **crucial,** with up to **3 289 professionals** in need of being trained within a one-year period.

Table 12. Relevance rate of subtopics – cyber threat intelligence, dark web and OSINT

Main topic	Subtopic	Relevance (%)
Cyber threat intelligence, dark web and OSINT	Dark web and OSINT	78

On the topic of cyber threat intelligence, dark web and OSINT, **investigators and intelligence officers** also represent the core segment of suggested trainees, although the focus of the training should potentially be primarily at **expert** level, followed by advanced practitioner and awareness levels. **Analysts** and **experts (Forensics, IT etc.)** form the second largest group of participants.

Table 13. Profiles and number of potential trainees – cyber threat intelligence, dark web and OSINT

Profile/ proficiency level	Awareness	Practi-tioner	Advanced practi-tioner	Expert	TTT	Median total	Actual total
First responders	104	104	182	208	0	**598**	75
Investigators and intelligence officers	130	78	78	260	0	**546**	225
Analysts	130	130	130	169	0	**559**	129
Managers	39	78	52	39	52	**260**	36
Prosecutors, investigative judges, magistrates	416	130	130	78	0	**754**	98
Experts (Forensics, IT etc.)	0	156	78	130	26	**390**	77
Other	0	0	182	0	0	**182**	7
Total	819	676	832	884	78	**3289**	647

Card-not-present fraud

Card-not-present fraud was the third most popular main topic, selected by 65 % of the responding MS. The training need is **urgent** (78 %) and **up to 2 574 individuals** would benefit from receiving training within the next year.

Table 14. Relevance rate of subtopics – card-not-present fraud

Main topic	Subtopic	Relevance (%)
Card-not-present fraud	Phishing and vishing	83
	Compromised credentials used for online payments	80
	Mobile banking fraud	78
	Smishing	76
	Online payment scams	73
	E-commerce fraud	71
	Carding platforms	60
	Darknet marketplaces	58
	SIM swapping	54

On this main topic, **first responders** are suggested as the primary training audience with trainees at all proficiency levels but with most emphasis on practitioner, advanced practitioner and Train-the-trainer (TTT) training. However, in terms of the volume of participants as actually communicated by the responding MS, the highest number of trainees is again among **investigators and intelligence officers**.

Table 15. Profiles and number of potential trainees – card-not-present fraud

Profile/ proficiency level	Awareness	Practi-tioner	Advanced practi-tioner	Expert	TTT	Median total	Actual total
First responders	104	221	182	78	130	**715**	146
Investigators and intelligence officers	52	78	104	104	65	**403**	**1374**
Analysts	260	91	78	78	26	**533**	92
Managers	78	26	52	26	52	**234**	53

Prosecutors, investigative judges, magistrates	0	130	52	52	0	**234**	25
Experts (Forensics, IT etc.)	0	78	52	52	39	**221**	72
Other	52	0	182	0	0	**234**	9
Total	**546**	**624**	**702**	**390**	**312**	**2574**	**1771**

Cybercrime facilitators

Selected by 60 % of responding MS, **cybercrime facilitators** was the fourth prioritised topic, with an urgency rate of 87 % and up to **6 006 participants** that would require training within the next year.

Table 16. Relevance rate of subtopics – cybercrime facilitators

Main topic	Subtopic	Relevance (%)
Cybercrime facilitators	Cryptocurrencies	89
	New online tools and digital techniques	81
	Anonymisation	71
	Money muling	69
	Online forgery	60
	Use of deepfakes created with AI	54
	Encryption	53

Prosecutors, investigative judges, magistrates take the top position of all trainees statistically, indicating the highest volumes of participants for **TTT** training, followed by **practitioner** and **awareness**-level participants. However, considering the ratio of median and actual totals, **investigators and intelligence officers** at **awareness** and **expert** levels again show up as the core group of trainees.

Table 17. Profiles and number of potential trainees – cybercrime facilitators

Profile/ proficiency level	Awareness	Practi-tioner	Advanced practi-tioner	Expert	TTT	Media n total	Actual total
First responders	910	130	130	26	26	**1222**	203

Investigators and intelligence officers	520	117	104	52	26	**819**	**4124**
Analysts	130	130	143	429	39	**871**	145
Managers	78	52	182	26	338	**676**	71
Prosecutors, investigative judges, magistrates	416	520	221	130	676	**1963**	163
Experts (Forensics, IT etc.)	0	52	117	78	26	**273**	71
Other	0	0	182	0	0	**182**	7
Total	**2054**	**1001**	**1079**	**741**	**1131**	**6006**	**4784**

Legal challenges in non-cash payment methods

Selected by just half of the responding MS (50 %), **legal challenges in non-cash payment methods** was included in the analysis as the last topic. On this area, **up to 7 051 participants** would potentially require training with a high level of urgency (80 %) within one year.

No subtopics in this category were put forward in the survey. However, participants suggested matters relating to the Payment Services Directive (PSD2) to be considered for a training subject, as well as topics related to cryptocurrency investigation and seizure.

Potentially, the largest groups of training participants would be formed by **prosecutors, investigative judges, magistrates**, especially at **TTT** level, but also **first responders**, **investigators and intelligence officers** and **managers,** which recorded high levels of potential training participants. However, the distance between the median-based and actual totals is relatively big, suggesting perhaps slightly lower volumes of trainees.

Table 18. Profiles and number of potential trainees – cybercrime facilitators

Profile/ proficiency level	Awareness	Practi-tioner	Advanced practi-tioner	Expert	TTT	Median total	Actual total
First responders	130	91	1300	156	130	**1807**	98

Investigators and intelligence officers	260	91	104	728	0	**1183**	**202**
Analysts	130	78	78	156	0	**442**	72
Managers	26	26	0	130	650	**832**	34
Prosecutors, investigative judges, magistrates	780	286	156	130	1300	**2652**	**119**
Experts (Forensics, IT etc.)	0	52	0	143	0	**195**	24
Other	130	130	0	0	130	**390**	15
Total	**1456**	**754**	**1638**	**1443**	**2210**	**7501**	**564**

Conclusions

The results of the OTNA on online fraud schemes suggest that most of the training topics and related subtopics put forward in the survey are important for the European LE audience. The main topics took the following order of popularity: **cyber scams**, **cyber threat intelligence, dark web and Open-Source Intelligence (OSINT)**, **card-not-present fraud**, **cybercrime facilitators** and **legal challenges in non-cash payment methods**. They were all considered urgent or even crucial, and all had relatively large pools of potential participants.

Factoring in multiple layers of data (such as the popularity of the main topics selected, the urgency of training indicated and the number of potential participants calculated in different ways, as well as other contributions provided through the survey), the application of a weighted scoring model and/or calculating the combined average would indicate cyber-related topics (cyber scams, cyber threat intelligence, dark web and OSINT, card-not-present fraud, cybercrime facilitators) to be further prioritised. Cybercrime facilitators came in as the topic with potentially the largest training audience, as the 12 MS alone that selected this topic indicated that around 4 784 professionals in their units were in need of training. Also in relation to cyber-related crime, another topic for which the training need is evident is card payment fraud, specifically the unauthorised use of credit or debit card data in non-face-to-face settings. A specific concern brought up by some respondents was the impression that the knowledge and skills related to investigating smishing remained limited among European LE professionals.

All horizontal aspects also gained relatively high relevance rates, with most emphasis placed on **digital skills and the use of new technologies** and **cooperation, information exchange and interoperability**. Altogether, combining the indications of the priorities for the main topics and horizontal aspects, the findings of this OTNA suggest a continued, comprehensive training emphasis on topics that relate to European law enforcement professionals' knowledge and skills in relation to maintaining cyber safety and dealing with e-crime. Considering the degree to which cybercrime is being recognised as an area where there is increasing criminality across Europe and is also being seen as an external threat, the findings of this study confirm that the needs in this field strongly reflect what has been recognised at policy and strategy levels. The EU's cybersecurity strategy (2020) and the related Council conclusions[23], for example, recognised improved information-sharing, including through education, training and exercises, as a central part of necessary capacity building.

In total, approximately **9 442 participants** in the EU Member States would need training on online fraud scheme topics in 2024. The demand for training straddles the different proficiency levels and concerns multiple categories of professionals, with **investigators and intelligence officers**, **prosecutors, investigative judges and magistrates** and **first responders** coming out as the primary target groups.

The previous training attended by those who contributed to this study suggests that different modes of online training suit the audience of online fraud scheme training particularly well. Hence, while maintaining a certain level of on-site training activities will always remain beneficial, continuing and developing virtual activities on different themes and topics would seems to be a feasible way to respond to training needs in this area. CEPOL mainstreams cybercrime across its overall learning and training strategy, with an existing training catalogue that already covers a variety of cyber-related crime topics. Considering the evolving nature of online criminality, a continuing high-quality online training portfolio could offer a flexible avenue for reacting and responding to emerging new themes and topics with, for example, ad-hoc webinars. The maintenance and development of other innovative, transferable learning resources, such as online learning modules, could also reach a wide audience and support development needs further.

[23] Available on: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf

Annex 1. EU-STNA chapter on online fraud schemes

Online fraud schemes

Environmental challenges

Online fraud covers different types of fraud schemes that are constantly evolving in line with technological developments. Due to its multifaceted nature, investigators dealing with this area of crime should have the competences to tackle the varied forms of this fraud. The pandemic has given an impetus to online fraudsters, while law enforcement is lagging behind in terms of investigative resources. Furthermore, investigations are lengthy and require additional support from well-trained law enforcement officers. However, individuals possessing the knowledge needed for these types of investigations are better paid in the private sector, which again raises capacity issues within law enforcement.
Differences in Member States' approaches to and legislation on data protection, data retention and cybercrime hinder cross-border cooperation. The same is true for judicial cooperation: there is no proper legal framework in place to follow when it comes to the exchange of information and intelligence.
Cooperation with the private sector is essential; however, companies are reluctant to share data and information with law enforcement. As companies seek to protect their brand name and reputation, and insurance companies might not compensate for fraud-related losses, fraud cases remain underreported.
The adequate management of digital evidence is imperative for ensuring the effectiveness of investigations. Member States should invest more resources in high-tech software and hardware that can be used efficiently for detecting and managing digital evidence. The admissibility of digital evidence in different countries is another legislative issue that obstructs the cross-border prosecution of cases.

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

Challenges

Online fraud schemes are perpetrated in many forms and law enforcement should be aware of the crime patterns in each type of fraud and their combinations. Officials investigating other crime areas should also improve their knowledge on fraud schemes, as these may be linked to many other crimes. It is nevertheless important to maintain the balance between training and operations so that the time dedicated by law enforcement officers to training at EU or national level does not result in even more prolonged investigations and pending cases.
New fraud typologies are related to emerging online tools and digital techniques for committing crimes; therefore, investigators should be acquainted with digital investigation tools and tackle the criminal use of encryption, anonymisation, bulletproof hosting services

and the darknet. In practice, law enforcement has a lack of trained investigators and a lack of digital and technical skills. Even though part of this capacity building requires EU-level support, it is also a national responsibility. The expert group suggested that each police force should be responsible for developing digital skills within their units.
While criminals use virtual currencies, virtual tokens and online payment methods for online fraud, investigators lack the capacity to apply financial investigation and disruption techniques. Furthermore, the use of deepfakes created with artificial intelligence makes fraud detection challenging.

Criminal networks engaged in online fraud are highly collaborative, providing criminal services to one another in a chain, distancing themselves in this way from the crime and rendering the identification of suspects by law enforcement more difficult. There is a need for providers with expertise in taxation, banking, law, finance, IT and combatting money laundering, but also for low-skilled collaborators such as money mules, call centre operators and cash carriers. Inter-agency cooperation is not strong enough at international level, and the same can be said for the cross-border exchange of e-evidence. According to the respondents, it is difficult to obtain data from foreign countries and apply data protection regulations throughout investigations. Law enforcement lacks information from the private sector, even though well-functioning public-private partnerships are needed in order to disrupt criminality. Cumbersome cooperation with banks and with international partners leads to offences often being investigated as stand-alone smaller cases without revealing the international fraud schemes behind them.

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

Training needs

Summary
Training is needed on the different aspects of fraud schemes, on their modus operandi, and on effective investigation methods. This should cover the broad range of fraud types, including investment fraud, CEO fraud, business email compromise fraud, non-delivery fraud, bank fraud, social benefit fraud, subsidy fraud, romance fraud and fake invoice fraud, and other fraud methods such as helpdesk fraud and online system fraud.
Furthermore, officers need training on digital investigation techniques, digital forensics, and cooperation tools and mechanisms at national and international level.
Member States indicated that 6 285 officers need training in this area.

Further details
The most relevant training topic is related to online payment fraud, including carding platforms, internet and mobile banking fraud, online payment requests, fraudulent near-field communication (NFC) transactions, SIM swapping, smishing, phishing, vishing, and e-commerce fraud.
Ranked as the second priority, training is required on the modus operandi of cyber scams such as online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud and helpdesk fraud.

Training on crime patterns related to card-present fraud, such as skimming, contactless card fraud, and mobile payment and mobile-app payment fraud, is slightly lower on the priority list, but still considered necessary. The same is true of training on tackling intrusions into transaction networks, such as banking malware/POS malware, logical attacks against ATMs, and the use of malware to intercept login details for online banking services.
In addition, training should focus on improving law enforcement officers' knowledge of tools and techniques that facilitate cybercrime, and should cover cryptocurrencies, encryption, anonymisation, online forgery, the use of deepfakes created with artificial intelligence and money muling. In order to enhance the digital skills of law enforcement officers, training should also cover cyber-threat intelligence and the use of the darknet and open source intelligence.
As there is a shortfall in human capacity for investigations and for attending training sessions, it is suggested that with regard to technological developments and investigation tools, train-the-trainers activities be organised at EU level, with the aim of cascading the new knowledge to a broad range of officers at national level.
In addition, training should also focus on mechanisms for national and international cooperation between law enforcement agencies and on cooperation with the private sector. Joint training activities with the involvement of private-sector actors could enhance relations between law enforcement and the public sector.

List of identified and prioritised training needs

The following list shows Member States' order of prioritisation of topics requiring training to combat online fraud schemes.

	Online fraud schemes (Fraud, economic and financial crimes)
1	Card-not-present fraud: compromised online payments, e-skimming, mobile banking fraud, online payment requests, SIM swapping, smishing, phishing and vishing, e-commerce fraud, carding platforms and darknet marketplaces
2	Cyber scams: online investment fraud selling novel investments and cryptocurrencies, business email compromise fraud, mimic and voice fraud, helpdesk fraud, social engineering
3	Cybercrime facilitators: cryptocurrencies, encryption, anonymisation, online forgery, new online tools and digital techniques, use of deepfakes created with AI, money muling
4	Card-present fraud: skimming, contactless card fraud, mobile payment fraud
5	Cyber threat intelligence, dark web and OSINT
6	Intrusions into system networks of financial institutions: banking malware/POS malware, logical attacks against ATMs, use of malware to intercept login details for online banking services
7	International law enforcement cooperation, public–private partnership, inter-agency cooperation (cooperation with financial institutions, internet service providers and online platforms)
8	Information exchange and cross-border exchange of evidence
9	Legal challenges in non-cash payment methods
10	High-risk criminal networks
11	Crime prevention
12	Fundamental rights and data protection

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 officers.
EQF equivalent	EQF Level 3-4	EQF Level 5	EQF Level 6	EQF Level 7	
EQF levels – Descriptors defining levels in the European Qualifications Framework, more information is available at https://europa.eu/europass/en/description-eight-eqf-levels					

Annex 3. Urgency levels

Urgency in the context of this questionnaire refers to the criticality of training being delivered in a certain timeframe and its impact on operational performance.

Urgency scale level	1	2	3	4	5
Training need is	Low	Secondary	Moderate	Urgent	Crucial
Training impact	Training plays a minor role in boosting performance; it would refresh knowledge; officers could benefit from training; however, it is not essential.	It would be useful if the training were delivered; however, the need is not urgent. Training can be delivered in (predictable) 2-3 years' time; it is needed to stay up-to-date.	It would be advantageous to receive training within a year; it would improve performance, but not significantly.	Training is essential; it is necessary that it be delivered within a year; it is important for qualitative performance.	Training is critical; it is necessary as soon as possible; it is crucial for the successful performance of duties.

Operational Training Needs Analysis

Online Fraud Schemes

European Union Agency for Law Enforcement Training
Offices: 1066 Budapest, Ó utca 27, Hungary
Telephone: +36 1 803 8030/8031 • Fax: +36 1 803 8032 •
Email: info@cepol.europa.eu
www.cepol.europa.eu