CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

Operational Training Needs Analysis

Digital Skills and the Use of New Technologies

EDUCATE, INNOVATE, MOTIVATE

Operational Training Needs Analysis

Digital Skills and the Use of New Technologies

2022

Contents

List of abbreviations

AI – Artificial Intelligence

CKC - CEPOL Knowledge Centre

CNU – CEPOL National Unit

CSDP – Common Security and Defence Policy

ECTC – European Counter Terrorism Centre

EMPACT – European Multidisciplinary Platform Against Criminal Threats

EQF – European Qualifications Framework

EU – European Union

EUROPOL - European Union Agency for Law Enforcement Cooperation

EU-STNA – European Union Strategic Training Needs Assessment

FRA – European Union Agency for Fundamental Rights

INTERPOL – The International Criminal Police Organisation

JHA – Justice and Home Affairs

LE – Law Enforcement

MB – Management Board

MS – Member State/s

OTNA – Operational Training Need Analysis

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 (LE) 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] Since piloting the methodology in 2018 by analysing training needs on the topics of Common Security and Defence Policy (CSDP) missions and Counterterrorism, CEPOL has produced a number of OTNAs on thematic security priority areas.

Digital skills and the use of new technologies was identified as the top core capability gap for law enforcement in the EU-STNA 2022-2025 report[3] covering– EMPACT 2022+. Following up on this strategic training priority, CEPOL launched the **OTNA on Digital skills and the use of new technologies** in 2021, with the aim to use the outcomes of the research for defining CEPOL's training portfolio addressing digitalisation of law enforcement for 2023-2025. A short-term expert was contracted from the list of individual external experts to assist CEPOL in the OTNA process, steps 3-6 (questionnaire, interviews and analysis of responses, overall analysis and drafting of the OTNA report).

In December 2021, CEPOL launched an online survey built around the strategic training priorities defined in the EU-STNA. In order to collect relevant data, the survey was addressed to direct contact points of 26 Member States[4] (MS) and EU structures (hereinafter institutions) dealing with the subject of the OTNA. Data was collected between 21 December 2021 and 2 February 2022, resulting in **45 individual answers** from different law enforcement (LE) agencies from **21 MS**[5] and EU structures, reportedly representing more than 15 252[6] LE officials. Considering the representativeness of the sample in terms of MS, the **81 % response rate** can be seen as a good level of responsiveness for a survey research, in this case, intended to represent the European LE community.

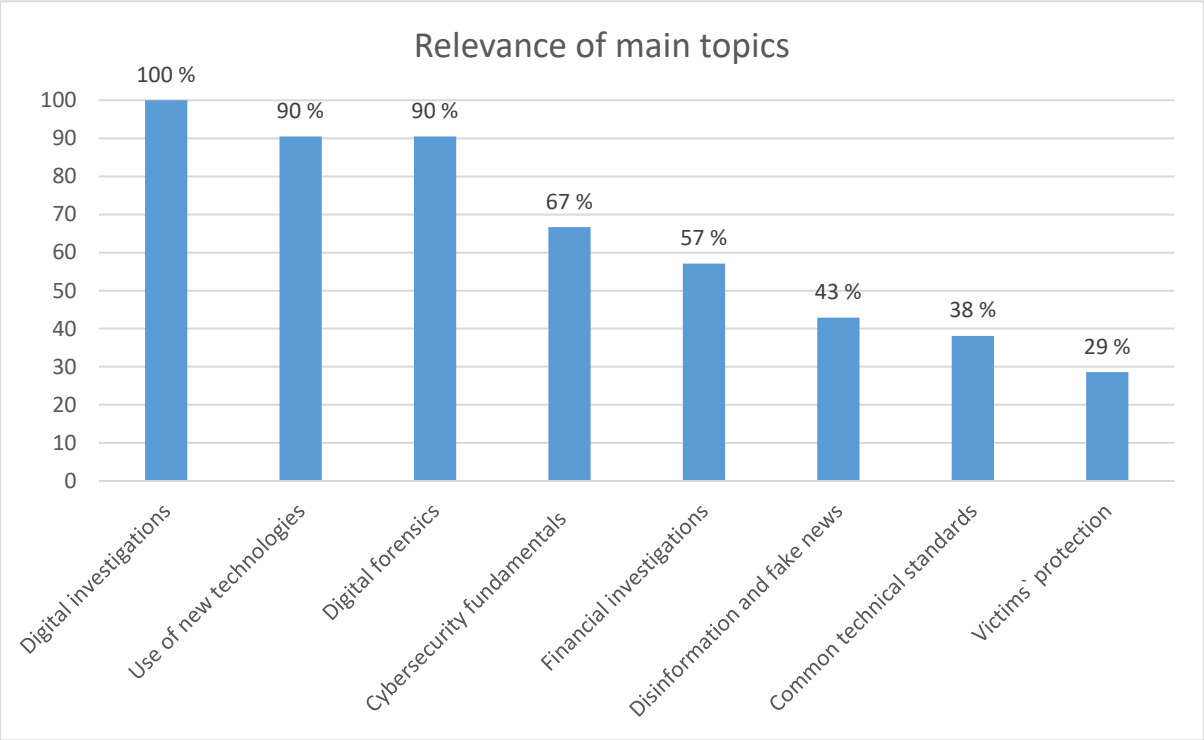
Based on the analysis of the collected data, this report describes training priorities in the area of digital skills and the use of new technologies for 2023-2025.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2219&from=EN
[2] The EU-STNA 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://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf
[4] The terminology 'Member States' (MS) hereinafter refers to 26 Member States of the European Union participating in the CEPOL regulation, i.e. all EU Member States excluding Denmark.
[5] Responding countries: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Malta, Poland, Portugal, Spain, Slovakia, Sweden, Slovenia and Romania.
[6] Number of officials performing their duties in the area related digital skills and use of new technologies, as indicated by the respondents. However, the total number is challenging to establish since instead of quantities, some respondents provided qualitative descriptions, e.g. stating that the use of new technologies is relevant in all LE professions.

All responses indicated a clear relevance for the scope of this activity, the **most relevant main topics** (out of the 12 individual topics) for law enforcement officials in this area were related to:

- **Digital investigations** (100 % of respondents found it relevant)
- **Use of new technologies** (90 % of respondents found it relevant)
- **Digital forensics** (90 % of respondents found it relevant)
- **Cybersecurity fundamentals** (67 % of respondents found it relevant), and
- **Financial investigations** (57 % of respondents found it relevant)

Chart 1. The 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 above-mentioned topics of **digital investigations**, **use of new technologies**, **digital forensics**, **cybersecurity fundamentals** and **financial investigations** were selected for closer review and the results are therefore presented in this report. As a consequence of the recent COVID-19 pandemic that led Europe to an unprecedented 'infodemic', countering the spread of false or misleading information became a joint effort involving all European institutions. Since the ongoing Ukraine crisis has necessitated the further intensification of EU efforts in tackling information manipulation, **disinformation and fake news** was included in the analysis as an additional topic. Furthermore, since the data for this study was collected before the outbreak of the war in Ukraine, it must be noted that the topic of **victims' protection** has seemingly increased in

importance, and regardless of its relatively low ranking in this report, the topic should be addressed as part of the fundamental rights and data protection training portfolio.

In terms of urgency, the six most relevant main topics are ranging from 69 % to 47 %, meaning that all of them must be considered either **urgent** or **moderately urgent**[7] needs where training should be delivered within a year's period. On those that exceed the urgency threshold of 60 %, namely **digital investigations** and **digital forensics**, 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 **cybersecurity fundamentals**, **use of new technologies** and **financial investigations** during the next three years. The distribution of training needs on main topics based on relevance, urgency and indicated number of trainees[8] is illustrated in Table 1.

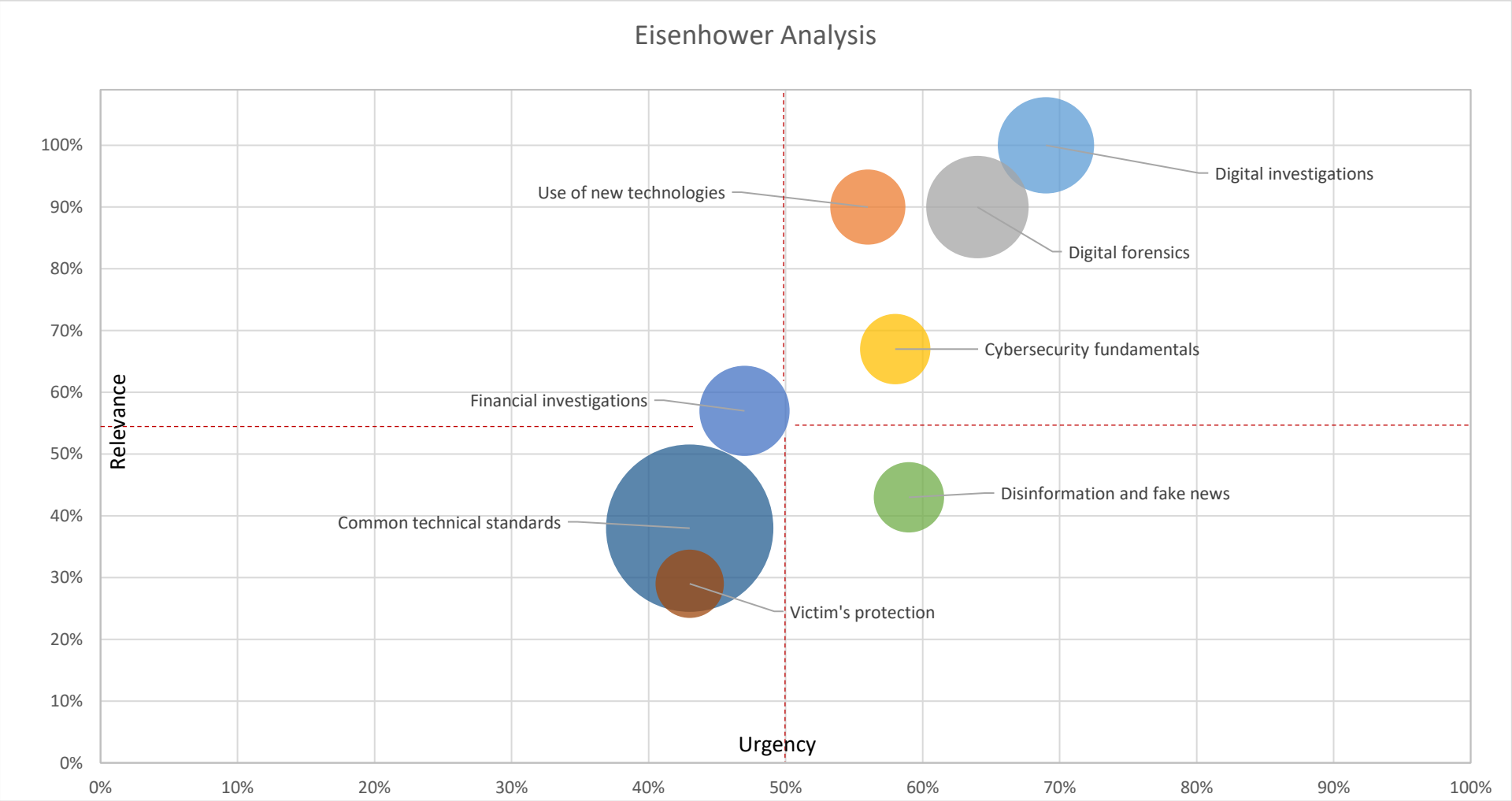
Table 1. Relevance, urgency and trainees of all main training topics

Main Topic	Relevance rate	Urgency rate	Trainees (median)	Trainees (actual)[9]
Digital investigations	100 %	69 %	1 833	62 719
Use of new technologies	90 %	56 %	1 430	59 290
Digital forensics	90 %	64 %	1 950	53 051
Cybersecurity fundamentals for EU law enforcement officials' everyday use and awareness raising	67 %	58 %	1 339	2 864
Financial investigations	57 %	47 %	1 716	61 407
Disinformation and fake news	43 %	59 %	1 339	1 119
Common technical standards	38 %	43 %	3 185	5 075
Victims' protection (how to protect victims' rights during investigations)	29 %	43 %	1 300	610
Average/total	**64 %**	**55 %**	**14 092**	**246 135**

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 below (Chart 2.) displays the relationships between three numeric variables, namely relevance, urgency and the number of 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. The 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.

[7] See explanation of urgency levels in Annex 3.
[8] Based on median values, see further information on the methodology in the 'Analysis' section.
[9] While the OTNA methodology relies on calculated statistical medians for estimating the potential number of trainees, based on the Expert Group feedback, actual values, as communicated by the survey respondents, were added for comparison purposes.

Chart 2. Relevance and urgency rate of the main training topics



In reference to the findings, it can be concluded that the training need on most subtopics, presented under each main topic, is considerably high. In most cases, all subtopics reached the 50 % threshold with insignificant differences between the highest and lowest scores. Hence, 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 4 on page 14.

On **digital investigations**, all subtopics reached the 50 % threshold with relatively small differences, therefore, training should emphasise all suggested thematic areas in the following priority order (based on the relevance rate):

- Open-Source Intelligence (OSINT)
- Mobile devices for investigation
- Cyberattacks (Ransomware, DDOS, Botnets)
- Encryption, Anonymisation techniques (VPN, Spoof calls, Sim boxes)
- Software/tools developed to identify dark web crimes

Under the topic **use of new technologies,** the following thematic areas should take first priority:

- Critical impact of algorithms, e.g. in social media
- Use of various camera systems
- Internet of Things
- Illegal use of drones

All subtopics under the topic **digital forensics** were considered relatively high, therefore they should all be considered as training topics, in the following priority order:

- Identification, collection, extraction, analysis, interpretation and presentation of data, securing evidence
- Communication platforms forensics, identification of services, applications, etc.
- Operating systems forensics (macOS, Windows, Linux, Mobile OSS, etc.)
- Big data analysis
- Internet of Things

While all topics related to **cybersecurity fundamentals for EU law enforcement officials' everyday use and awareness raising** passed the relevance rate, the following thematic areas were given the highest score:

- Phishing attacks, Malware attacks, Ransomware removable media
- Cybersecurity fundamentals for construction of secure systems for EU agencies, law enforcement agencies (tools used, identifying cybersecurity, ways of understanding: specific threats, new ways of operations)
- Online safety and advice, social media crime prevention campaigning, new social media (TikTok, online video games, e.g. Roblox)
- In-depth understanding of the cybersecurity threats for artificial intelligence, 5G and other new technologies

- Cyber hygiene, passwords and authentication, mobile device security, working remotely, public Wi-Fi, cloud security, physical security

Under the topic **financial investigations,** the following thematic areas should be emphasised:

- Cryptocurrencies (their operation, tracing cryptocurrencies in illegal activity, securing cryptocurrencies)
- Tracking of assets
- Other virtual assets (token, assets in online casinos, Ready Player Me platform or similar, and securing different virtual assets)
- Alternative banking platforms

On **disinformation and fake news**, all five subtopics reached relatively high relevance rates. In a descending order, the subtopics were prioritised as follows:

- Social media investigation
- Domain, websites and forums investigation
- Manipulated pictures as evidence
- Automatic tools, crowdsourcing, and cybercrime services
- Education of law enforcement officials and the general population, explaining how to source information. Analyse the source of information for the users, disinformation through social media

Respondents indicated that **9 607 participants**[10] **would need training on the prioritised main topics in 2023.** Based on the volume of trainees communicated by the respondents, notably the highest need for training is at **awareness** level. The second highest ranking of potential participants is shared almost equally between **practitioner** and **advanced practitioner**, and as demonstrated in the table below (Table 2.) trainee volumes for the other two levels of training are considerably lower. Overall, the average **urgency for training** in the area of digital skills and the use of new technologies **is moderate (59 %),** meaning that it would be advantageous to receive training within a year's period. At **expert level**, while with a lower volume of trainees, indicated needs exceeded the threshold of urgent, where training within one year is essential in ensuring quality performance. For complete details of training dimensions, please consult the 'Analysis' section of this report.

Table 2. Proficiency levels and number of participants of all institutions

Proficiency level	Number of participants (median)	Number of participants (actual)
Awareness	3 081	131 780
Practitioner	2 054	67 104
Advanced practitioner	2 080	28 275
Expert	1 469	10 985
Train-the-trainer	923	2 306

[10] Presented numbers are based on calculated median values (reported total actual number of participants: 240 450). For further details on the calculation methodology, please see 'Analysis' section of this report.

Total	**9 607**	**240 450**

The OTNA questionnaire gave an opportunity to specify the profiles and indicate the number of LE officials who would need training in different topics. In terms of digital skills and the use of new technologies, most references were given to **investigators** (almost 40 % of all) and **experts** on forensics, IT, etc. (over 20 %), suggesting that these two profiles should be provided with the opportunity to be trained first. Analysts, intelligence officers, managers and cybersecurity officials were nearly equal to each other, ranging from 8 to 10 %. The lowest percentages of training needs were reported among prosecutors, investigative judges, magistrates, however, with only some two-percentage point differences compared to cybersecurity officials. As a new finding, the results of the OTNA research suggest that professionals working in technical support roles in the context of LE could be a potential target group, while designing the training portfolio on different topics related to digital skills and the use of new technologies.

In total, 26 respondents from 15 different countries, representing 58% of the responding MS, provided data on previous training attended at national or international level. In terms of content, most references were given to training on **open source intelligence (OSINT)** and using the publicly available data and electronic evidence for **investigative** purposes. Another main group of previous training responses focused on **cybercrime**, including a wide range of topics on prevention, intelligence and investigation of crime in the cyber environment. In lesser quantities, but frequently, mentioned was previous training related to both **cryptocurrencies** and **darknet**. Furthermore, the respondents reported a heterogenic group of other training topics relevant to digital skills and the use of new technologies. Notably, the highest quantities of previous training were attended by **expert** level officials, followed by **advanced practitioners** and **practitioners**. Most training (68 %) was reported to have been done in an **online format** (online module/course, webinar or other virtual implementation), 37 % onsite and the rest 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 years 2022-2024[11] 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[12].

Building on the strategic training priorities defined by the EU-STNA and the experience gained from previous OTNA studies, CEPOL launched the OTNA on **digital skills and the use of new technologies** in 2021. Outcomes of the research are presented in this report and will be used to define CEPOL's training portfolio responding to the need to continue equipping LE professionals with advanced digital skills to meet the requirements of digitalisation of our societies and the digital transformation of the LE environment.

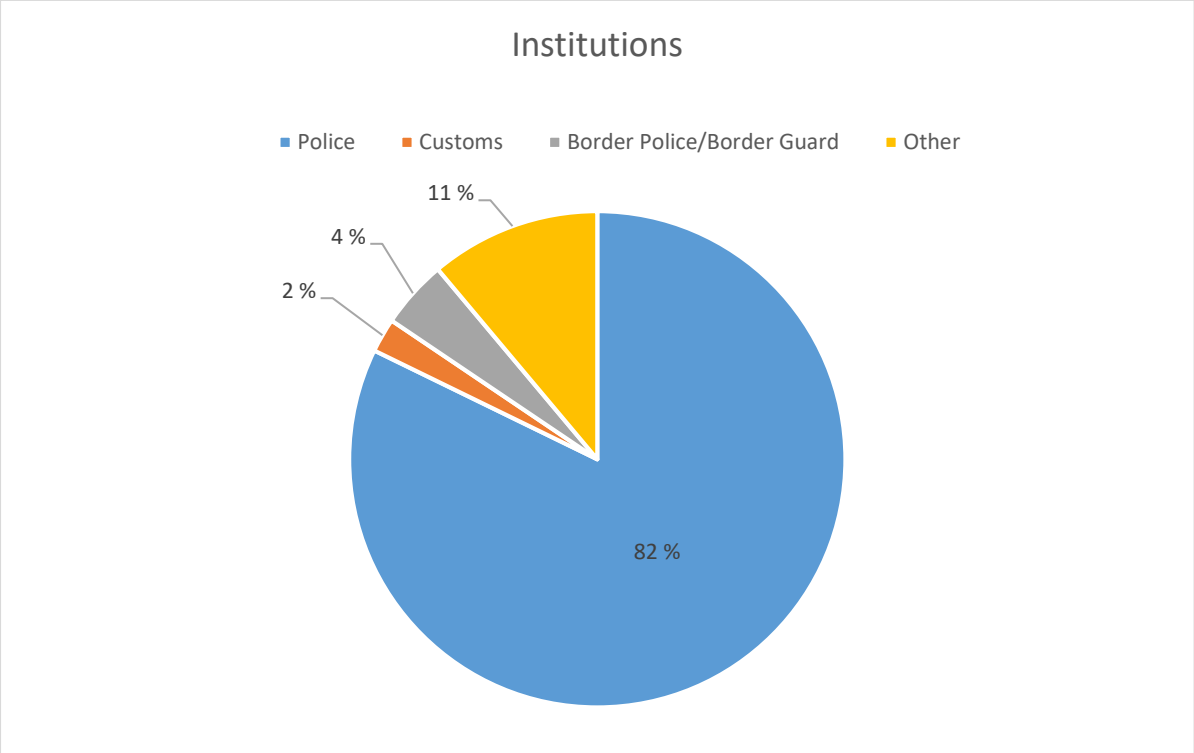
[11] https://www.cepol.europa.eu/sites/default/files/31-2021-MB%20Annex.pdf, p. 5.
[12] https://publications.europa.eu/en/publication-detail/-/publication/c71d1eb2-9a55-11e5-b3b7-01aa75ed71a1/language-en

Analysis

Consolidation of data and responses

In order to conduct the research on training needs in the field, CEPOL approached 26 MS[13] and EU structures (hereinafter institutions), to provide direct contact points dealing with the subject of the OTNA. In total, representatives from 21 MS and two EU structures[14] responded to the survey, resulting in 45 individual completed answers received from different LE agencies. In terms of MS, the responses indicate 81% response rate, which can be considered as a relatively good level of responsiveness. Most of the responses (82 %) were from **police representatives**, followed by the category of **other relevant bodies** (11 %).

Chart 3. Distribution of responding institutions



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

Relevance of topics

In line with the training priorities defined in the EU-STNA process, the main training topics in relation to digital skills and the use of new technologies by LE are:

- Digital investigations

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

- Financial investigations
- Use of new technologies
- Digital forensics
- Disinformation and fake news
- 'Victims' protection (how to protect victims' rights during investigations)
- Cybersecurity fundamentals for EU law enforcement officials' everyday use and awareness raising, and
- Common technical standards

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 nine main topics. While analysing the results, the relevance score of each main topic was calculated by summing up how many MS[15] found the topic 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. Where 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 to be processed for further analysis as per the OTNA methodology. Based on this method, five of all main topics passed the relevance threshold. As the recent times of crisis, namely the global COVID-19 pandemic followed by the war in Ukraine, have required that the EU take a proactive stance in countering the spread of false or misleading information, disinformation and fake news was included in the analysis as an additional topic. Also, considering the current Ukraine crisis, the future training portfolio design should address the topic of victims' protection, regardless of its relevance rate (43%).

Table 3. Relevance rate of main topics

Main Topic	Relevance
Digital investigations	100 %
Use of new technologies	90 %
Digital forensics	90 %
Cybersecurity fundamentals for EU law enforcement officials' everyday use and awareness raising	67 %
Financial investigations	57 %
Disinformation and fake news	43 %
Common technical standards	38 %
Victims' protection (how to protect victims' rights during investigations)	29 %

Training dimensions

In order to gain further insights on necessary training themes and subjects, various **subtopics** were presented under each topic. The questionnaire gave the respondents an option to rate the relevance of subtopics and horizontal aspects, by using the five-point Likert Scale with the following options: not

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

relevant at all; somewhat relevant; relevant; very relevant; and extremely relevant. For analysing 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 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[16]. If the relevance score reached 50% of the maximum score, the subtopic 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 with very little differences between the highest and lowest scores. In a descending order, Table 4 below presents the subtopics prioritised on their relevance rate:

Table 4. Relevance rate of most relevant subtopics from prioritised main topics

Main topic	Subtopic	Relevance
Digital investigations	Open-Source Intelligence (OSINT)	80 %
	Mobile devices for investigation	78 %
	Cyberattacks (Ransomware, DDOS, Botnets)	78 %
	Encryption, Anonymisation techniques (VPN, Spoof calls, Sim boxes)	77 %
	Software/tools developed to identify dark web crimes	75 %
	Darknet, what is dark web, how to use dark web	74 %
	Digital fingerprints and metadata to identify persons and devices	74 %
	Raw data analysis	72 %
	Big data analysis, e.g. prediction of criminal behaviour with big data analysis	71 %
	Analysis techniques/tools for many types of data (normalisation, correlation, and fusion) including technical data from different domains	70 %
	Information technology as a knowledge management enabler	65 %
	Cloud platforms	64 %
	Use of Artificial Intelligence, including AI risks towards fundamental rights, especially on face recognition systems	63 %
	Internet of Things	63 %
	Lawful interception	62 %
Use of new technologies	Critical impact of algorithms, e.g. in social media	64 %
	Use of various camera systems	61 %
	Internet of Things	60 %
	Illegal use of drones	52 %

[16] The maximum score was identified by multiplying the number of responding MS that found the subtopic relevant with the highest relevance score (5).

	Use of drones by law enforcement	50 %
	Use of speech recognition technology	49 %
	Driverless cars	39 %
	Use of exoskeletons	26 %
Digital forensics	Identification, collection, extraction, analysis, interpretation and presentation of data; securing evidence	81 %
	Communication platforms' forensics, identification of services, applications, etc.	81 %
	Operating systems forensics (macOS, Windows, Linux, Mobile OSS, etc.)	76 %
	Big data analysis	70 %
	Internet of Things	64 %
Cybersecurity fundamentals	Phishing attacks, Malware attacks, Ransomware removable media	82 %
	Cybersecurity fundamentals for construction of secure systems for EU agencies, law enforcement agencies (tools used, identifying cybersecurity, ways of understanding: specific threats, new ways of operations)	77 %
	Online safety and advice, social media crime prevention campaigning, new social media (TikTok, online video games, e.g. Roblox)	76 %
	Cyber hygiene, passwords and authentication, mobile device security, working remotely, public Wi-Fi, cloud security, physical security	72 %
	Awareness-raising on cyberattacks for Justice and Home Affairs agencies, law enforcement agencies, as well as for the public	71 %
	Social media crime prevention campaigning	67 %
	Threats coming from owners and developers of platforms	59 %
Financial investigations	Cryptocurrencies (their operation, tracing cryptocurrencies in illegal activity, securing cryptocurrencies)	85 %
	Tracking of assets	69 %
	Other virtual assets (token, assets in online casinos, Ready Player Me platform or similar, and securing different virtual assets)	64 %
	Alternative banking platforms	63 %
Disinformation and fake news	Social media investigation	86 %
	Domain, websites and forums investigation	78 %
	Manipulated pictures as evidence	69 %
	Automatic tools, crowdsourcing, and cybercrime services	69 %
	Education of law enforcement officials and the general population, explaining how to source information Analyse the source of information for the users, disinformation through social media	67 %

Through the OTNA questionnaire, the respondents communicated a number of **further training needs and/or potential subtopics** related to the prioritised main topics, including the following topics and suggestions:

- Digital transformation in general
- Basics of digital investigations for investigators of traditional crimes
- Common level of digital skills and competences in EU countries
- Cyber threat intelligence basic course
- Malware analysis basic course
- Virtual cryptocurrencies
- Malware analysis and reverse engineering
- Tools and techniques for deepfake detection
- Digital forensics (cryptography, vehicle forensics, cloud forensics)
- Financial investigations (wallet interception and decrypting, follow the money process)
- Working on geolocation data, devices and platforms
- Wi-Fi sniffing
- OSINT intelligence and analysis, and
- (Email) phishing

To better understand the training needs in each main topic, the questionnaire gave the respondents an option to indicate the **urgency** level **of training** on topics related to digital skills and new technologies and estimate the **number of participants** at five different **professional levels**[17]. 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 LE officials would need the training to improve their current performance. By choosing from a six-point urgency level scale (most commonly known as Likert Scale)[18], 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 a timely training intervention and its impact to 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 two 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

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

[18] 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

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[19]). 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 **9 607 participants** across the MS would need training on digital skills and the use of new technologies[20] 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. Based on the number of potential trainees reported through the survey, the total was much higher due to some MS[21] reporting a considerable volume of LE officials in need of awareness, practitioner and advanced practitioner level training in digital investigations, use of new technologies, financial investigations and digital forensics. Without statistically processing the data, the respondents communicated up to 240 450 potential trainees on the prioritised main topics related to digital skills and the use of new technologies.

Table 5. Relevance and urgency rate of prioritised main topics

Main Topic	Relevance rate	Urgency rate	Trainees (median)	Trainees (actual)
Digital investigations	100 %	69 %	1 833	62 719
Use of new technologies	90 %	56 %	1 430	59 290
Digital forensics	90 %	64 %	1 950	53 051
Cybersecurity fundamentals for EU law enforcement official's everyday use and awareness raising	67 %	58 %	1 339	2 864
Financial investigations	57 %	47 %	1 716	61 407
Disinformation and fake news	43 %	59 %	1 339	1 119
Average/total	**75 %**	**59 %**	**9 607**	**240 450**

Besides calculating the overall urgency rate and number of trainees per each prioritised main topic, training needs and the volume of trainees were also analysed per each proficiency level. Very little differences on the indicated urgency rates could be identified between the different proficiency levels, resulting in the fact that the training need in all categories is moderately urgent, but there are considerable differences in terms of numbers of participants. In terms of volumes, the highest need is indicated by respondents in the proficiency levels of **awareness** and **advanced practitioner**, followed by **practitioner** and **expert**-level training which have a relatively small difference between them.

[19] All EU MS except Denmark
[20] This figure concerns the six prioritised main topics
[21] e.g. Italy with 30 000 trainees for awareness, 15 000 practitioner and 5 000 advanced practitioner -level training

Considering the urgency of training, the highest need is at **expert**-level, however, the differences in terms of urgency are marginal between the different proficiency levels.

Table 6. Proficiency level and number of participants

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (total)
Awareness	55 %	3 081	131 780
Practitioner	61 %	2 054	67 104
Advanced practitioner	56 %	2 080	28 275
Expert	64 %	1 469	10 985
Train-the-trainer	58 %	923	2 306
Average/total	**59 %**	**9 607**	**240 450**

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. Overall, **investigators** were clearly the biggest professional group (nearly 40 % of all) in need of training, followed by **experts** (approximately 20 %). These two profiles should be provided with the opportunity to be trained first. Differences between the following groups (analysts, intelligence officers and managers), as well as the segment of prosecutors, investigative judges and magistrates that came last in terms of priority, were minimal. Through an open text field, the respondents were also able to specify other professionals in need for training and insert the related numbers. While most respondents did not communicate further training needs, it was suggested that professionals working in technical support roles in the context of LE should be considered as a target group while designing the training portfolio on digital skills and the use of new technologies. Furthermore, some respondents had reflected the centrality of digital skills and the capability to master new technologies in all LE professions, particularly mentioning e.g. the importance of developing the knowledge of intelligence officers and analysts on handling data in an online environment, as well as the skills of investigators in collecting and using digital evidence.

In terms of MS, the biggest numbers for target groups were notably reported by Italy, from where one responding institute reported high volumes of trainees[23] in most main topics and at all professional levels, however, particularly high among awareness, practitioner and advanced practitioner level LE officials. Considering particular prioritised main topics, another Italian respondent (representing a different authority) reported a number of trainees being in need of expert level training on cybersecurity fundamentals. France expressed a high need[24] for awareness level training on the use of new technologies, followed by the Czech Republic that also communicated a training need at all professional levels, with the main emphasis on building awareness[25]. Furthermore, both the Czech

[22] Investigators; intelligence officers; cybersecurity officials; analysts; managers; prosecutors, investigative judges and magistrates; experts (forensics, IT etc.)
[23] Up to 30 000 trainees for awareness, 15 000 practitioner and 5 000 advanced practitioner-level training in all prioritised main topics, except cybersecurity fundamentals
[24] Potentially 5 000 participants
[25] Estimated 1 000 participants in need for awareness-level training

Republic and France reported a high volume of trainees[26] for the topic of digital investigations in all professional categories. In order to clarify some differences in the responses coming from Italy and France, their respondents were invited for an interview with the aim to clarify the root causes for the variability of data and consolidated training needs. The discussion held with the Italian representative confirmed that there is a high training need for equipping officials involved in operational activities with the basic awareness on most topics[27] related to digital skills and the use of new technologies. Furthermore, there are considerable numbers of other professionals that would need training on the same topics but at different proficiency levels[28]. For France, while the matter could not be unravelled thoroughly, as not all respondents agreed to be interviewed, it also became evident that the submitted numbers of trainees refer to different individuals who need to develop advanced knowledge in new technologies, with fewer numbers regarding those working in more specialised roles[29], and at national level, a higher volume of officials in need of introductory level training.

National or international training

The OTNA questionnaire had a section with a question referring to previous national or international training attended on digital skills and the use of new technologies. In terms of topics, training data was provided in a free-text form, therefore their presentation 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 total, 26 respondents from 15 different countries, representing 58% of the responding MS, provided data on previous training attended at national or international level. In terms of content, most references were given to training on **open source intelligence (OSINT)** and using the publicly available data and electronic evidence for **investigative** purposes. Another main group of previous training focused on **cybercrime**, including a wide range of topics on prevention, intelligence and investigation of crime in the cyber environment. Fewer times, but frequently mentioned, was training related to both **cryptocurrencies** and **darknet**. Furthermore, the respondents reported a heterogenic group of other training topics relevant to digital skills and the use of new technologies. Notably the highest numbers of previous training were attended by **expert**-level officials, followed by **advanced practitioners** and **practitioners**. Most training (68 %) was reported to have been done in an **online format** (online module/course, webinar or other virtual implementation), 37 % onsite and the rest in an undefined mode. Details on training providers were mentioned in a limited manner; at EU-level, mentioning CEPOL and also making reference to INTERPOL training activities. International professional associations focused on information technology, and globally recognised cyber security certification bodies were mentioned as training providers[30] on e.g. specialised expert training on digital forensics and cybersecurity-related topics. In most cases, it can be assumed that the respondents were referring to training activities implemented by the MS, and different national-level training providers were mentioned.

[26] In total, 4 000-5 000 participants reported from both countries
[27] Potentially 30 000 awareness-level participants for the topics of digital investigations, financial investigations, digital forensics and the use of new technologies
[28] Up to 15 000 practitioner and 5 000 advanced practitioner level trainees from e.g. specialised departments
[29] e.g. OSINT investigators, online pseudonymous investigators and mobile phone investigators
[30] e.g. EC-Council; ISACA

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, 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 in a descending order. The second table demonstrates the estimated number of participants per different proficiency level, both calculated in line with the OTNA methodology[31] and for comparison purposes, the figures as communicated by the responding MS, as well as the urgency rate of training to be delivered.

Digital investigations

Digital investigations appear as the most relevant main topic, as indicated by the MS (relevance 100 %). The need for training on digital investigations is **urgent** or **moderately urgent** at all proficiency levels, however, while the biggest volumes in terms of numbers of potential trainees were reported for **practitioner** and **awareness** level training, the highest urgency rate was identified for **expert** and **train-the-trainer** level training. In terms of profiles, **investigators** and **experts (forensics, IT, etc.)** were notably the biggest target groups communicated by the respondents, followed by **analysts** and **intelligence officers,** but in lower numbers. In total, training should be delivered within one year to **approximately 1 833 trainees**. Within this main topic, training should focus on the most relevant subtopics, as indicated below.

Table 7. Relevance rate of subtopics of digital investigations in descending order

Main topic	Subtopic	Relevance
Digital investigations	Open-Source Intelligence (OSINT)	80 %
	Mobile devices for investigation	78 %
	Cyberattacks (Ransomware, DDOS, Botnets)	78 %
	Encryption, Anonymisation techniques (VPN, Spoof calls, Sim boxes)	77 %
	Software/tools developed to identify dark web crimes	75 %
	Darknet, what is dark web, how to use dark web	74 %
	Digital fingerprints and metadata to identify persons and devices	74 %
	Raw data analysis	72 %
	Big data analysis, e.g. prediction of criminal behaviour with big data analysis	71 %
	Analysis techniques/tools for many types of data (normalisation, correlation, and fusion) including technical data from different domains	70 %
	Information technology as a knowledge management enabler	65 %

[31] 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.

	Cloud platforms	64 %
	Use of Artificial Intelligence, including AI risks towards fundamental rights, especially on face recognition systems	63 %
	Internet of Things	63 %
	Lawful interception	62 %

Table 8. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (actual)
Awareness	58 %	520	33 766
Practitioner	70 %	468	19 338
Advanced practitioner	67 %	455	6 930
Expert	76 %	260	1 623
Train-the-trainer	74 %	130	1 062
Average/Total	**69 %**	**1 833**	**62 719**

Use of new technologies

Use of new technologies is the second most relevant main topic, as indicated by the MS (relevance 90 %). The training need is **moderately urgent,** with relatively small differences between different proficiency levels. In terms of urgency rate, the highest priority by the respondents was given to **train-the-trainer**, followed by **advanced practitioner**, practitioner and expert level training. Nevertheless, the volume of LE officials in need for **awareness level** training is notably the biggest of all. In total, training should be delivered within one year to **approximately 1 430 trainees**. As communicated by the MS, **investigators** represent over 60 % of professionals in need of training, followed by **experts (forensic, IT, etc.),** but with considerably less references given. Within this main topic, training should focus on the most relevant subtopics, as indicated below.

Table 9. Relevance rate of subtopics of new technologies in descending order

Main topic	Subtopic	Relevance
Use of new technologies	Critical impact of algorithm, e.g. in social media	64 %
	Use of various camera systems	61 %
	Internet of Things	60 %
	Illegal use of drones	52 %
	Use of drones by law enforcement	50 %
	Use of speech recognition technology	49 %
	Driverless cars	39 %
	Use of exoskeletons	26 %

Table 10. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (actual)
Awareness	48 %	520	36 582

Practitioner	57 %	260	16 312
Advanced practitioner	59 %	260	5 311
Expert	56 %	260	878
Train-the-trainer	60 %	130	207
Average/Total	**56 %**	**1 430**	**59 290**

Digital forensics

Digital forensics is the third[32] most relevant main topic as indicated by the MS (relevance 90 %). The highest volume of trainees was reported at **awareness** level, although expert, advanced practitioner and practitioner level training received a higher urgency rating among the respondents. Overall, the training need on the topic of digital forensics is **urgent**, but considered **crucial** at expert level. **Experts (Forensic, IT, etc.)** would need the training most, and **investigators** were the second priority. In total, **approximately 1 339 trainees** would need to receive training within a year's period. Within this main topic, training should focus on the most relevant subtopics, as indicated below.

Table 11. Relevance rate of subtopics of digital forensics in descending order

Main topic	Subtopic	Relevance
Digital forensics	Identification, collection, extraction, analysis, interpretation and presentation of data; securing evidence	81 %
	Communication platforms forensics, identification of services, applications, etc.	81 %
	Operating systems forensics (macOS, Win, Linux, Mobile OSS, etc.)	76 %
	Big data analysis	70 %
	Internet of Things	64 %

Table 12. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (actual)
Awareness	52 %	520	30 430
Practitioner	62 %	260	15 334
Advanced practitioner	74 %	260	5 566
Expert	84 %	169	1 467
Train-the-trainer	51 %	130	254
Average/Total	**64 %**	**1 339**	**53 051**

Cybersecurity fundamentals

Cybersecurity fundamentals for EU law enforcement officials' everyday use and awareness raising is the fourth most relevant main topic, as indicated by the MS (relevance 67 %). The training need is **moderately urgent**. However, the categories of awareness, practitioner and train-the-trainer either

[32] In terms of relevance score, it is equal with the use of new technologies

met or exceeded the threshold of urgent training need. In terms of both urgency and number of potential participants, **awareness level** training should be provided as a priority. Training for **experts (forensic, IT, etc.)** was the most communicated need, followed by **managers** and **investigators.** In general, training needs were distributed across all professional profiles, however, with less references given to managers. Overall, **approximately 1 716 trainees** would need training on cybersecurity fundamentals within a year's period. Within this main topic, training should focus on most relevant subtopics as indicated below.

Table 13. Relevance rate of subtopics of cybersecurity fundamentals in descending order

Main topic	Subtopic	Relevance
Cybersecurity fundamentals	Phishing attacks, Malware attacks, Ransomware removable media	82 %
	Cybersecurity fundamentals for construction of secure systems for EU agencies, law enforcement agencies (tools used, identifying cybersecurity, ways of understanding: specific threats, new ways of operations)	77 %
	Online safety and advice, social media crime prevention campaigning, new social media (TikTok, online video games, e.g. Roblox)	76 %
	Cyber hygiene, passwords and authentication, mobile device security, working remotely, public Wi-Fi, cloud security, physical security	72 %
	Awareness-raising on cyberattacks for Justice and Home Affairs agencies, law enforcement agencies, as well as for the public	71 %
	Social media crime prevention campaigning	67 %
	Threats coming from owners and developers of platforms	59 %

Table 14. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (actual)
Awareness	63 %	520	485
Practitioner	60 %	416	299
Advanced practitioner	50 %	390	202
Expert	56 %	260	1 756
Train-the-trainer	61 %	130	122
Average/Total	**58 %**	**1 716**	**2 864**

Financial investigations

Financial investigations is the fifth most relevant main topic, as indicated by the MS (relevance 57 %). The training need is **moderately urgent**, meaning that it would be advantageous for **approximately 1 950 trainees** to receive training within a year's period. While in general the training needs and volume of trainees is distributed almost equally across different professional groups, the biggest training

audience seems to be i**nvestigators**. Within this main topic, training should focus on the most relevant subtopics, as indicated below.

Table 15. Relevance rate of subtopics of financial investigations in descending order

Main topic	Subtopic	Relevance
Financial investigations	Cryptocurrencies (their operation, tracing cryptocurrencies in illegal activity, securing cryptocurrencies)	85 %
	Tracking of assets	69 %
	Other virtual assets (token, assets in online casinos, Ready Player Me platform or similar, and securing different virtual assets)	64 %
	Alternative banking platforms	63 %

Table 16. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (actual)
Awareness	50 %	585	30 230
Practitioner	45 %	130	15 235
Advanced practitioner	40 %	520	10 154
Expert	53 %	390	5 180
Train-the-trainer	48 %	325	608
Average/Total	**47 %**	**1 950**	**61 407**

Disinformation and fake news

Disinformation and fake news reached the relevance rate of 43 % and did not exceed the threshold, as set in the OTNA methodology, however, due to the emerging importance of the topic, it was included in the analysis. The training need is **moderately urgent** or **urgent** at all proficiency levels, however, **practitioner** level training with 73 % urgency rate is where training would be most desired. In terms of profiles of trainees, **experts (on forensic, IT, etc.)** established the largest target group (over 40 % of potential participants communicated by the respondents), followed by **investigators** and **intelligence officers**; these groups together sharing another 40 % of the total volume of trainees. In total, **approximately 1 339 trainees** would require training within a period of one year. Within this main topic, training should focus on most relevant subtopics, as indicated below.

Table 17. Relevance rate of subtopics of disinformation and fake news in descending order

Main topic	Subtopic	Relevance
Disinformation and fake news	Social media investigation	86 %
	Domain, websites and forums investigation	78 %
	Manipulated pictures as evidence	69 %
	Automatic tools, crowdsourcing, and cybercrime services	69 %
	Education of law enforcement officials and the general population, explaining how to source information.	67 %

	Analysing the source of information for the users, disinformation through social media	

Table 18. Urgency and number of participants per proficiency level

Proficiency level	Urgency rate	Number of participants (median)	Number of participants (actual)
Awareness	60 %	416	287
Practitioner	73 %	520	586
Advanced practitioner	49 %	195	112
Expert	60 %	130	81
Train-the-trainer	53 %	78	53
Average/Total	**59 %**	**1 339**	**1 119**

Conclusions

The outcomes of the OTNA on digital skills and the use of new technologies indicate that half of the main topics are relevant and relatively urgent for law enforcement officials. Based on the 50 % relevance threshold, **digital investigations, use of new technologies, digital forensics, cybersecurity fundamentals and financial investigations** should be given the highest priority when designing training activities. Analysis of data showed that the training need in the area of digital skills and the use of new technologies overall is high. Under most prioritised main topics, all or almost all subtopics gained high relevance scores, meaning that the training portfolio in this area should address a variety of different topics. Based on the results, seemingly the most crucial training topic is digital investigations that reached the relevance rate of 100 %[33] with all of its subtopics exceeding the relevance threshold as well, and an average urgency rate of 69 %, indicating that training at all professional levels is essential and necessary to be delivered within a period of one year. The following two, namely **digital investigations** and the **use of new technologies** both reached the rate of 90 % relevance with nearly equal estimated amounts of trainees, with the topic of digital investigations indicating a higher urgency in terms of training delivery.

Overall, approximately **9 607 participants in the EU MS would need training on digital skills and new technologies in 2023**. The use of new technologies is a continuously growing component of LE work, and as the results of this research indicated, the need for advanced digital skills is spread across the different professions in the field. In terms of the most emerging training needs, most references were given to **investigators** and **experts** (on forensics, IT, etc.), suggesting that these two profiles should be provided with the opportunity to be trained first. As a general conclusion, it could be seen that awareness level training on **digital forensics** and **cybersecurity fundamentals** is relevant for everyone in the field of LE, regardless of the professional group or proficiency level, while the demand for training on the topics of **digital investigations** and **the use of new technologies** generally appears among higher level trainees, who in most cases consist of **investigators**. Interestingly, this research also brought up another potential segment for training, namely professionals who are working in different kinds of **technical support roles** in the context of LE. Therefore, on top of focusing on the development of skills and knowledge of those representing the core professions and the traditional training audiences, this could be an area to be further explored. While the training needs amongst the technical support staff were not further elaborated by the respondents of the OTNA survey, it is well known that apart from those providing specialist capabilities[34], a variety of roles in today's LE context require at least awareness level training on digital skills and new technologies, and should be counted in for EU-level training.

All in all, the results indicate that **the demand for training in terms of topics and volume of potential trainees is high**, hence, CEPOL must continue investing in flexible learning solutions that can respond to the need of further equipping the European LE community for the digital era. Since the analysis on previous or recent training revealed that more than two thirds of the activities were taken in different

[33] Meaning that at least one responding institute from each MS rated the topic relevant
[34] For example, IT project managers, systems administrators, database managers and similar

virtual formats, this indicates that the training audiences in question could benefit from the development of new online resources and particularly by expanding CEPOL's training offer via the agency's online learning platform, LEEd [35].

[35] https://leed.cepol.europa.eu/

Annex 1. EU-STNA chapter on digital skills and the use of new technologies

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

Detailed list of training needs:

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

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

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, 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 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.