EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies

Iulian Coman
Noemi Alexa
European Union Agency for Law Enforcement Training[1]

Abstract

Digitalisation, one of the key elements addressed by CEPOL in law enforcement training, is carried out based on the continuing and emerging technological innovations that needs to be given the highest priority across the European law enforcement community.

The new European Union Strategic Needs Assessment (EU-STNA), defines the strategic EU-level training priorities of law enforcement officials for the next 4-year cycle, 2022-2025, in line with the EMPACT priorities, emphasizing the importance of digital skills and use of new technologies, as one of the main horizontal aspects that should be addressed in all training activities.

Cyber-attacks, had the highest priority rank, as EU training need, within the Member States, indicating more than 7600 officials that would need to be trained. Law enforcement and judiciary authorities would need further awareness raising regarding cyber security, cyber-enabled and cyber-dependent crime, but also further improvement in dealing with e-evidence and international cooperation mechanisms.

Taking into consideration the deliverables of the EU-STNA process, CEPOL has further launched a structured training needs analysis in 2021, the OTNA on Digital skills and the use of new technologies, in order to define the training portfolio addressing digitalisation of law enforcement for 2023-2025. Amongst most relevant training topics of the responding countries, we can highlight the Digital investigations, use of new technologies and digital forensics, which would need to be included in law enforcement training activities.

Keywords: digitalisation, digital skills, new technologies, law enforcement training, EU priorities

Introduction

Technological innovations continue to change the law enforcement landscape and despite the investment already made in improving digital skills and the use of new technologies for law enforcement officials, further efforts in building professionals' capacity to use advanced technology and of deepening their understanding of how technology is utilized for criminal purposes, are still needed, as concluded by CEPOL's European Union Strategic Needs Assessment (EU-STNA) 2022-2025.

[1] Authors' emails: iulian.coman@cepol.europa.eu; noemi.alexa@cepol.europa.eu

Recent studies demonstrate that the increased cyber-crime activities, reflects also on the preparedness of the law enforcement officials on responding and tackling such offenses (e.g. Harkin, and Whelan 2021, Bieber 2019). The use of technology remains an important feature for serious and organized crime, in a rapid evolving digitalised society (ENISA 2021; EUROPOL 2021) and the specialised training on digital skills is important for all police officers. Online criminality is so common, that all the law enforcement officials should be equipped with the knowledge and skills to understand and proactively fight cybercrime (HMIC, 2015).

Assessment and Analyses of Training Needs

Training needs assessments (TNAs) is a strategic and organizational process that collects and analyses data to support decision makers to improve individuals' performance through training and are considered powerful tools to support organizational change and development, while supporting adjustments for the external stakeholders (Reed & Vakola 2006). The strategic role of the TNAs provide clear gaps in professional skills, institutional needs and insufficient knowledge and involve different parties to participate, that are directly or indirectly interested or involved in the training process (Ferreira & Abbad, 2013).

At European level, the need for continuous training of law enforcement and identifying threats and risks, has led different EU Agencies and Institutions to develop and apply TNAs in line with their business needs, through complex processes with stakeholders.

EU-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, develops annually a Training Needs Assessment exercise that is part of the development and update of their training courses, methodologies, materials and tools.

Europol identifies the priorities in the fight against serious and organised crime through an annual Serious and Organized Crime Threat Assessment (SOCTA) that uses mixed method involving qualitative and quantitative analysis techniques. The methodology consists of two key steps, identification of all threats related to serious and organized crimes and secondly the identification of the key threats. The advantage of Europol in this process is that the preliminary analysis that identifies intelligence gaps, is conducted based on the data already available within the agency, combined with strategic reports from EU partners, EU Member States (MS) and other stakeholders. Further questionnaires for identifying descriptive data, are sent to the MS and other stakeholders. All data is evaluated by using the 4x4 system.

European Security and Defense College (ESDC) presented the methodology for its Training Requirements Analysis (TRA) in 2020, in line with the EU Global Strategy 2016, Civilian Compact 2018 and EU Policy on Training, that consisted of five phases: identifying requirements, research including EU policies/guidelines/frameworks, questionnaires and interviews, mapping of existing security sector reform (SSR) training, analysis and preparation of high-level training outcomes. The TRA concluded in a final report – ESDC Executive Academic Board (EAB) Security Sector Reform (SSR) Report on Training Requirements Analysis for Civilian Common Security and Defense Policy (CSDP) Missions that identified existing CSDP civilian training requirements and gaps.

In accordance with the Article 3 (2015 Regulation (EU) 2015/2219),CEPOL is mandated to support, develop, implement and coordinate training for law enforcement officials, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of law enforcement, in particular in the areas of prevention of and fight against serious crime affecting two or more Member States and terrorism, maintenance of public order, in particular international policing of major events, and planning and command of Union missions, which may also include training on law enforcement leadership and language skills.

Pursuant to the Article 4.1 of the Regulation 2015/2219, CEPOL is tasked to prepare multi-annual strategic training needs analyses and multi-annual learning programs.

Introduction of the European Union Strategic Needs Assessment (EU-STNA) and the Operational Training Needs Assessment (OTNA) is one of the performance indicators of CEPOL to ensure high quality, multidisciplinary, innovative and relevant training and learning options, accessible to its target group.

The EU-STNA aims at assessing strategic training needs and address EU priorities in the area of internal security and its external aspects, with a view to better coordinate training activities for law enforcement officials and avoid duplication of efforts.

As a follow up to this exercise, CEPOL regularly conducts training needs analyses on operational level, on the priority topics defined by the EU-STNA. The aim of these analyses is to get a detailed understanding of the number and profile of officials to be trained as well as on the proficiency and urgency level of training to be delivered.

EU-STNA Process and Methodology

EU level training activities refer to strands 3 and 4 of the Law Enforcement Training Scheme (LETS) as identified in Commission Communication COM (2013)172, and namely: strand 3 - thematic policing specialism; and strand 4 - European Union civilian missions and capacity building in third countries. EU-STNA only looks at EU level priorities, as national training (strand 1 of the above mentioned LETS) and bilateral/regional training cooperation (strand 2 of LETS) remains outside of the scope of the exercise. More specifically, the EU-STNA aims at identifying those EU level training priorities that can help close capability gaps for law enforcement officials.

It is a collective, EU-wide effort that requires participation from all stakeholders, so that training providers can deliver better, more targeted training to the European law enforcement community on the top priority topics.

The Council of the European Union, the European Parliament, together with the European Commission are the main addressee of the EU-STNA report, which provide background for the law enforcement training policy development for the upcoming years.

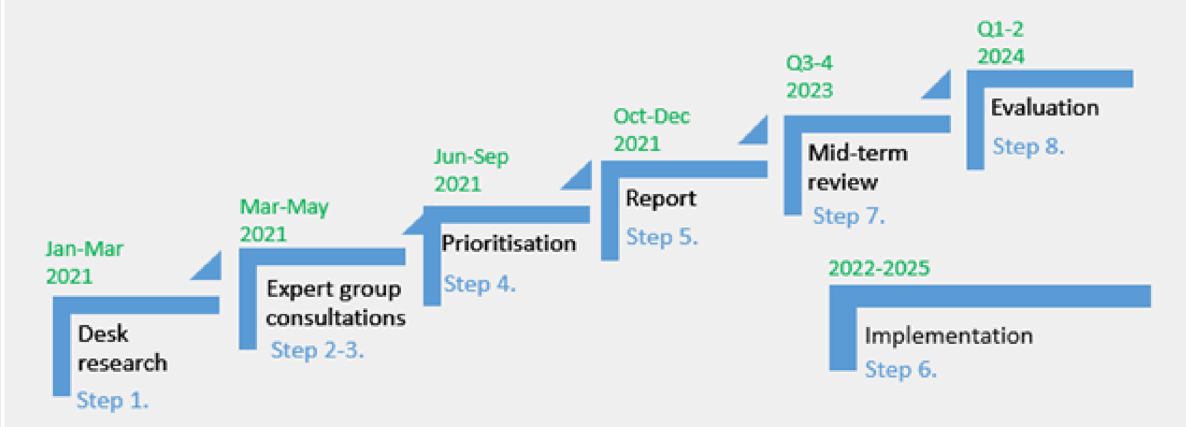
Member States are crucial in the EU-STNA process, as their experts assess capability challenges in law enforcement and corresponding training needs, and their policy makers prioritise those EU training needs. The successful implementation of the EU-STNA depends on the stakeholder (JHA agencies, EU networks) contributions, who are involved in the different steps of the EU-STNA process.

The process of the EU-STNA started with a desk research from key policy documents on EU internal security issues, followed by clustering on 17 thematic categories, one of the categories being Cyber-attacks. Further to the desk research, expert consultations were held on the available information and a gap analysis was conducted to define those areas where EU level intervention is required and to determine relevant training to address the capability challenges identified across Member States. EU Member States prioritized the final list of training needs, with the opinion of EU institutions and relevant agencies.

In October 2021, CEPOL initiated the drafting of the EU-STNA Report, which lists the key EU training needs and indicates potential training providers. The Report was finalised in November 2021, then shared with the Directorate-General for Migration and Home Affairs of the European Commission (DG HOME).

The mid-term review of possible new threats and training priorities will be conducted in 2023, more precisely during months 27–30 of the EU policy cycle. Finally, the evaluation focusing on assessing the impact of the second EU-STNA and identifying possible improvements for the next cycle, will be carried out by an external evaluator, contracted by CEPOL in 2023. Thus, the evaluation will be conducted during the first half of 2024 in order to allow sufficient time for possible methodology adjustments and for the alignment of the next EU-STNA with the future EMPACT cycle 2026–2029.

Figure 1: EU-STNA process structure



Findings

The EU-STNA process identified eight core capability gaps (Figure 2) constituting the main areas in which law enforcement officials need capacity building through training, with *digital skills and use of new technologies,* being the most identified in all expert group discussions for all thematic areas. Furthermore, 230 training needs were identified, clustered in 17 thematic areas as well as 9 other specific training needs included under a separate category. It has to be noted that the core capability gaps are relevant for all thematic areas of training.

Figure 2: Core capability gaps

Core capability gaps	Thematic training areas	
o **Digital skills and use of new technologies** o **High-risk criminal networks** o **Financial investigations** o **Cooperation, information exchange and interoperability** o **Crime prevention** o **Document fraud** o **Forensics** o **Fundamental rights and data protection**	1. Cyber-attacks 2. Criminal finances, money laundering and asset recovery 3. Counter-terrorism 4. Trafficking in human beings 5. Drug trafficking 6. Migrant smuggling 7. Child sexual exploitation 8. Online fraud schemes 9. Organised property crime	10. Border management and maritime security 11. Firearms trafficking 12. Missing trader intra-community fraud 13. Corruption 14. Excise fraud 15. Intellectual property crime, counterfeiting of goods and currencies 16. Environmental crime 17. External dimensions of European security 18. Other thematic areas

After a thorough desk research of EU policy documents and strategic reports and series of consultation with expert groups, networks and other stakeholders, the list of EU-level training needs of law enforcement officials was composed and it was sent to prioritisation to the MS authorities via a survey. Responders were asked to rank the EU level training needs by assigning a numerical value that corresponds to its priority (e.g. 1 means a training need of highest priority, 2 – second priority, etc.) by first ranking the main categories against each other and after that rank the training needs within each thematic category.

After submitting the priority order, in line with the EU-STNA methodology the ranking has been weighted (multiplied) by the coefficient equal to the proportion of the country's representation in the European Parliament. The final list of priorities is therefore reflecting the sum priority scores given by the Member States.

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.

Figure 3: List of training needs for digital skills core capability gap

Digital skills and 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 cyber-threats (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, dark net, 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

Member States have indicated that at present a total of 110 368 law enforcement officials would need EU-level training in the areas identified, with 7 659 officials in the area of cyber-attacks, for all training needs (Figure 4).

The key training priorities relate to the modi operandi and investigation techniques of cyber-attacks. Digital skills of law enforcement officials and the judiciary as well as their ability to deal with e-evidence need substantial improvement through training. Investigators should benefit from training on the operation of criminal networks and on national and international cooperation mechanisms. Besides investigators, cybercrime analysts should also be trained.

Figure 4: List of identified and prioritized training needs for cyber-attacks

	Cyber-attacks
1	Investigating cyber-attacks on information systems and modus operandi: analysing latest cyber-attacks and EU emergency response; developing alternative investigation techniques and EU tools, including their use
2	Latest challenges for dealing with encryption, anonymisation and bulletproof hosting services
3	Identifying, handling, securing, preserving, analysing and exchanging e-evidence
4	Combatting crime-as-a-service used by criminals and criminal groups in illegal activities
5	Effective international cooperation
6	Protocols to tackle large-scale cyber-attacks
7	Raising awareness of cyber-attacks for EU agencies, law enforcement agencies and the public, including a coordinated approach for prevention; cyber-enabled and cyber-dependent crime awareness, cyber threats and cybercrime investigation
8	Big data analysis
9	Blockchain analysis
10	Using artificial intelligence, machine learning and deep learning in cybercrime investigation
11	Cybercriminal profiling and motivation analysis
12	Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection

OTNA Process and Methodology

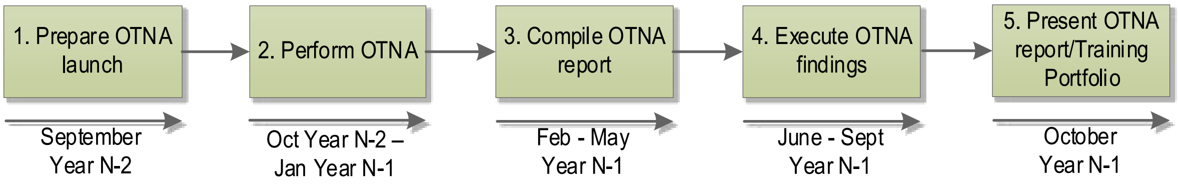
The CEPOL Regulation mandates the Agency to incorporate training needs assessments and analyses in its planning. CEPOL completed the second EU Strategic Training Needs Assessment (EU-STNA) in 2021, identifying strategic level training priorities for law enforcement officials across Europe for the next 4-year cycle 2022-2025 of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). In order to analyse the particular training needs in more details, CEPOL is conducting the OTNAs.

The OTNA methodology is a complex approach to operational level analysis aiming at getting a detailed picture of training needs of a given thematic priority from relevant experts in Member States. The OTNA methodology is applied to core capability gaps and thematic training priorities as defined in the EU-STNA. It collects data on:

- subtopics to be addressed by training;
- proficiency level of training needed;
- urgency level of training needed;
- number of participants who would need the training;
- profile of participants who would need training.

Outcomes of the OTNAs are valid for 3 years; a mid-term OTNA review as well as certain ad-hoc TNAs may be performed to address the emerging training needs and new developments.

Figure 5: OTNA process structure



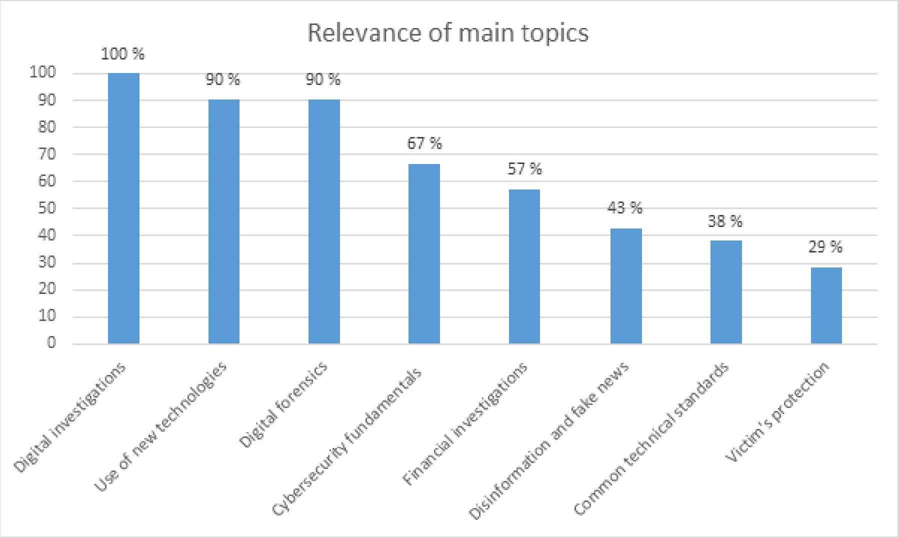
Findings

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 and EU structures 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 agencies and EU structures of 21 different MS, reportedly representing more than 15252 law enforcement officials. Considering the representativeness of the sample in terms of MS, 81 % response rate can be seen as a good level of responsiveness for a survey research, in this case, intended to represent the European law enforcement community (CEPOL 2022, *OTNA Report on digital skills and the use of new technologies*).

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

All responses indicated clear relevance for the scope of activity, the most relevant main topics (out of the 12 individual topics) for law enforcement officials in this area were related to digital investigations, use of new technologies and digital forensics.

Figure 6: Relevance of main topics



Respondents indicated that 9607 officials would need training on the prioritized main topics in 2023. Based on the volume of trainees communicated by the respondents, notably highest need for training is at awareness level. Second highest number of potential participants divides almost equally between practitioner and advanced practitioner.

Figure 7: Proficiency levels and number of participants of all institutions

Proficiency level	Number of participants (median)	Number of participants (actual)
Awareness	3081	131780
Practitioner	2054	67104
Advanced practitioner	2080	28275
Expert	1469	10985
Train-the-trainer	923	2306
Total	**9607**	**240450**

Conclusions

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

Future trainings should target practitioners and advanced practitioners (online modules or online courses) in the area of use of new technologies (artificial intelligence and big data analysis) and disinformation and fake news (deep fakes). For the awareness level, webinar and e-lessons should be developed, in the area of use of new technologies (illegal use of drones, use of cameras, 5G, automotive) and disinformation and fake news (detecting tampered evidence).

All the results indicate that the demand for training in terms of topics and volume of potential trainees is high and flexible learning solutions are needed for further preparing the law enforcement officials for the digital era.

References

- Anderson, J. E. (2000) Training needs assessment, evaluation, success, and organizational strategy and effectiveness (Doctoral dissertation). Utah State University, Logan, Utah.
- Ap, Z., (2019) Impulsivity and Risky Cybersecurity Behaviors: A Replication, 1-4.
  Available from: https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a European Law Enforcement Training Scheme, Brussels, 27.3.2013, COM (2013) 172 final.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Agenda on Security (28.04.2015 COM(2015) 185 final).
- Decision 32/2017/MB (15/11/2017) of the Management Board of the European Union Agency for Law Enforcement Training On CEPOL Operational Training Needs Analysis Methodology.
- ESDC Executive Academic Board (EAB) Security Sector Reform (SSR) Report on Training Requirements Analysis for Civilian Common Security and Defense Policy (CSDP) Missions.
  Available from: https://issat.dcaf.ch/Learn/Resource-Library/Other-Documents/Civilian-Coordinator-for-training-in-Security-Sector-Reform-CCT-SSR-ESDC-EAB-SSR-Report-on-Training-Requirements-Analysis-for-Civilian-CSDP-Missions
- Ferreira, R. & Abbad, G. (2013) Training Needs Assessment: Where We Are and Where We Should Go, 1-6.
- Harkin, D. & Whelan, C. (2021) Perceptions of police training needs in cyber-crime. International Journal of Police Science & Management. Online First (forthcoming), 1-2.
  Available from: https://journals.sagepub.com/doi/10.1177/14613557211036565 https://www.researchgate.net/publication/334726198_Impulsivity_and_Risky_Cybersecurity_Behaviors_A_Replication

- Operational Training Needs Analysis on Digital Skills and the Use of New Technologies.
  Available from: https://www.cepol.europa.eu/sites/default/files/OTNA_Report_Digital_Skills.pdf
- Reed, J., & Vakola, M. (2006) What role can a training needs analysis play in organisational change? *Journal of Organizational Change Management*, 19, 393 – 400.
- Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL)
- Regulation (EU) 2015/2219 on the European Union Agency for Law Enforcement Training
- Serious and Organized Crime Threat Assessment (SOCTA) 2021.
  Available from: https://www.europol.europa.eu/publications-events/main-reports/socta-report
- The European Union Strategic Training Needs Assessment (EU-STNA) 2022 – 2025.
  Available from: https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf
  Website: https://www.cepol.europa.eu