CEPOL
EUROPEAN UNION AGENCY FOR
LAW ENFORCEMENT TRAINING

Operational Training Needs Analysis

Cyber-attacks

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, December 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 978-92-9211-431-2 doi:10.2825/23601 QR-04-23-750-EN-N

Photograph: © cover: iStockPhoto.com/xijian

Contents

List of abbreviations ... 5

Executive summary ... 6

Introduction ... 8

Participants ... 10

Data processing ... 13

Analysis ... 15

Roles selected ... 15

Competency level ... 16

Level of training required ... 18

Urgency of training ... 20

Regional training needs ... 21

National or international training ... 23

Training activities proposed for certification or accreditation ... 24

Training needs per role ... 25

Heads of Cybercrime Units ... 25

Team Leaders ... 27

General Criminal Investigators ... 28

Cybercrime Analysts ... 30

Cybercrime Investigators ... 31

Cybercrime Experts ... 33

Digital Forensics Examiners ... 34

Incident Response Experts ... 37

First Responders ... 39

Trial and Appeal Judges ... 40

Investigative Judges ... 42

Conclusions ... 44

List of tables

Table 1. Summary of expected competencies ... 9

Table 2. Data recoding principles ... 14

Table 3. Summative competency ranking ... 17

Table 4. Summary of regional training needs ... 22

Table 5. Sample characteristics – Heads of Cybercrime Units ... 25

Table 6. Summary of competency development needs – Heads of Cybercrime Units 26
Table 7. Sample characteristics – Team Leaders 27
Table 8. Summary of competency development needs – Team Leaders 28
Table 9. Sample characteristics – General Criminal Investigators 28
Table 10. Summary of competency development needs – General Criminal Investigators................. 29
Table 11. Sample characteristics – Cybercrime Analysts 30
Table 12. Summary of competency development needs – Cybercrime Analysts 31
Table 13. Sample characteristics – Cybercrime Investigators 31
Table 14. Summary of competency development needs – Cybercrime Investigators 32
Table 15. Sample characteristics – Cybercrime Experts 33
Table 16. Summary of competency development needs – Cybercrime Experts 34
Table 17. Sample characteristics – Digital Forensics Examiners 34
Table 18. Summary of competency development needs – Digital Forensics Examiners 36
Table 19. Additional summary of competency development needs – Digital Forensics Examiners 37
Table 20. Sample characteristics – Incident Response Experts 37
Table 21. Summary of competency development needs – Incident Response Experts 38
Table 22. Sample characteristics – First Responders 39
Table 23. Summary of capacity development needs – First Responders 40
Table 24. Sample characteristics – Trial and Appeal Judges 40
Table 25. Summary of competency development needs – Trial and Appeal Judges 41
Table 26. Sample characteristics – Investigative Judges... 42
Table 27. Summary of capacity development needs – Investigative Judges 43

List of figures

Figure 1. Overview of responding countries 11
Figure 2. Share of responses per responding countries 12
Figure 3. Sectors represented by respondents 13
Figure 4. Roles selected by respondents 15
Figure 5. Current competency vs expected level – average per role (all roles) 17
Figure 6. Comparison of training and competency needs – average per role (all roles)...................... 19
Figure 7. Indicated level of training required – all roles and competencies... 20
Figure 8. Urgency of training – average per role (all roles) 21
Figure 9. Previous training attended – topics per competency level 23
Figure 10. Competency level – Heads of Cybercrime Units 26
Figure 11. Competency level – Team Leaders 27
Figure 12. Competency level – General Criminal Investigators 29
Figure 13. Competency level – Cybercrime Analysts 30
Figure 14. Competency level – Cybercrime Investigators... 32
Figure 15. Competency level – Cybercrime Experts 34
Figure 16. Competency level – Digital Forensics Examiners 35
Figure 17. Competency level – Incident Response Experts 38
Figure 18. Competency level – First Responders 39
Figure 19. Competency level – Trial and Appeal Judges 41
Figure 20. Competency level – Investigative Judges... 42

List of annexes

Annex 1. EU-STNA Chapter on Cyber-attacks 47
Annex 2. TCF Matrix 51
Annex 3. Description of cybercrime roles 52
Annex 4. Urgency levels 56
Annex 5. List of national or international training attended 57
Annex 6. Training proposed for accreditation or certification 60
Annex 7. Digital forensics – details on subtopics 63

List of abbreviations

CEPOL – European Union Agency for Law Enforcement Training
CSDP – Common Security and Defence Policy
CSE – Cybersecurity Essentials
EMPACT - European Multidisciplinary Platform Against Criminal Threats
EC – European Commission
EU – European Union
EUROJUST - European Union Agency for Criminal Justice Cooperation
EUROPOL – European Union Agency for Law Enforcement Cooperation
EU SOCTA – European Union Serious and Organised Crime Threat Assessment
EU-STNA – European Union Strategic Training Needs Assessment
FBI – Federal Bureau of Investigation (US)
GDPR - General Data Protection Regulation
IoT – Internet of Things
IT – Information Technology
JHA – Justice and Home Affairs
LE – Law Enforcement
LEA – Law Enforcement Agency
MB – Management Board
MoI – Ministry of Interior
MS – Member State
OSINT - Open-Source Intelligence
OTNA – Operational Training Need Analysis
SPD – Single Programming Document
SQL - Structured Query Language
TCF – Training Competency Framework
TNA – Training Needs Analysis

Executive summary

As defined under Article 3 of Regulation 2015/2219[1], the objectives of the European Union Agency for Law Enforcement Training (CEPOL) are to support, develop, implement and coordinate training for law enforcement (LE) officers, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of LE, in particular in the prevention of and fight against serious crime affecting two or more Members States (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.

Targeting the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online, is one of 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. Recognising the importance of improving cybersecurity capacity, within the context of the European Skills Agenda[2], in April 2023, the European Commission (EC) launched the Cybersecurity Skills Academy with the aim of filling the recognised cybersecurity knowledge and skills gap and developing the EU's cyber resilience[3]. In the EU Strategic Training Needs Assessment (EU-STNA) for 2022-2025, cyber-attacks were also placed as the top EU training priority. The EU-STNA also recognised digital skills and the use of new technologies as one of eight core capability gaps in which LE officials need capacity-building through training.

Following up on the strategic training priorities, CEPOL launched an **Operational Training Needs Analysis (OTNA) on Cyber-attacks** in December 2022, with a view to using the outcomes of the research to define its training portfolio for 2024-2026.

An online questionnaire resulted in **110 individual answers**[4] from LE Agencies in **23 EU Member States**[5], representing **88.46 %** of the countries participating in the CEPOL regulation[6], and one EU Justice and Home Affairs (JHA) agency, namely the European Union Agency for Criminal Justice Cooperation (EUROJUST). The best-represented sector was the **police**, constituting **75.45 %** (n=83) of responses. **Digital Forensic Examiners (Investigators)** were the most selected profile, as 30.38 % (n=50) of all respondents said they represented this group of professionals either in a personal or organisational capacity. Since some respondents represented more than one professional profile, the different profiles were selected **152 times** in total.

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

[2] Available on: https://ec.europa.eu/social/main.jsp?langId=en&catId=89&newsId=9723&furtherNews=yes#navItem-1

[3] Available on: https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy

[4] The figure represents the number of completed responses that were fit for analysis

[5] Responding countries: Austria, Bulgaria, Cyprus, Czechia, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

[6] All EU Member States except Denmark

The analysis was based on the draft Training Competency Framework (TCF)[7] on Cybercrime, drawn up by the Training Governance Model. This concept describes the expected level of different competencies professionals dealing with cybercrimes need in different roles to perform their job. Where the level of competencies indicated by survey respondents in different roles was lower than the expected level described in the TCF, a training need was identified. This approach is in line with CEPOL's New Strategy 2023-2027[8], Objective 3.1 *Establish a framework for the accreditation of law enforcement training programmes developed on the basis of the EU Law Enforcement Training Priorities*. Furthermore, the TCF is fully aligned with the training priorities for cyber-attacks established in the EU-STNA 2022-2025.

On average, the current competency level in cybercrime roles is between basic and intermediate. The largest competency gaps concern the roles of Digital Forensics Examiners, Cybercrime Experts and Incident Response Experts, which in the TCF are among the roles with the highest expected competency levels. Professionals in these roles would require further training on all competencies associated with the role. Investigative Judges whose competency level is below the expected level would require training on all topics, primarily on the most concrete gaps concerning cybercrime legislation and reporting and presenting cybercrime investigative data. The need for training that targets Cybercrime Investigators is also high and concerns all areas other than digital forensics. Cybercrime Analysts' core competency gaps are related to analysis and visualisation and general cybercrime knowledge; the expected competency level is advanced, whereas it currently seems to be closer to basic level. On average, First Responders and Team Leaders are relatively close to meeting the expected competency levels. Within the group of Team Leaders, the main competency gaps that would need to be addressed by training concern specific cybercrime knowledge and digital forensics. As for First Responders, they would benefit from receiving training on crime scene management and electronic evidence handling. Heads of Cybercrime Units and General Criminal Investigators are the only roles in which professionals are on average above the expected competency level, although there are still gaps in certain areas. General cybercrime knowledge, cybercrime legislation, and reporting and presenting cybercrime investigative data should be considered training priorities for the role of Heads of Cybercrime Units, and targeted training for General Criminal Investigators should cover crime scene management and electronic evidence handling.

The calculated average considering all roles suggests the need for training on all competencies at intermediate level. This principle applies to all roles with the most notable competency gaps, including Digital Forensics Experts, Cybercrime Experts, Incident Response Experts, Investigative Judges and Cybercrime Analysts. While the competency level of Cybercrime Investigators has not yet fully reached intermediate level, a request was made for advanced-level training on the topic of cybercrime investigation techniques, in line with the target set for the expected level of competency. Similarly, advanced-level crime scene management and electronic evidence handling for General Criminal Investigators should be covered.

[7] See complete TCF Matrix in Annex 2.

[8] Adopted by the CEPOL Management Board on 22 November 2022 (15/2022/MB), https://www.cepol.europa.eu/documents/annex-management-board-decision-15-2022-mb

Despite the competency gaps uncovered, training in most areas is not considered very urgent. On average, the level of urgency ranges between secondary and moderate, suggesting that for most roles it would be useful to update skills and knowledge in 2-3 years' time.

The OTNA survey was primarily used to map competency development needs for each cybercrime profile rather than the number of officers needing training. Hence, a limitation of this study is that it does not provide an estimation of trainee volumes. It can also be assumed that some of the training needs that came up in the survey might actually indicate a shortage of staff dealing with cybercrime in European law enforcement agencies rather than the limited capacities of current officers. While no direct evidence is available, the imbalance between needs (high) and urgency (low) is one factor indicating that training provision alone cannot resolve all capacity challenges.

Data on previous training obtained through the survey indicates that basic and intermediate levels have been the most attended levels of training. Typically, previous basic training has concerned topics such as malware analysis, cyber forensics, digital forensics and incident response. Intermediate-level training has largely focused on different types of cyber forensics, including network, live data and mobile device forensics. Training on cyber intelligence and threat hunting has also been attended. There were fewer responses concerning advanced-level training, but those received indicated previous training related to cyber investigations and criminal cryptocurrencies in dark web markets. Professionals at all levels have also participated in cyber breach and attack simulations. Training has been delivered by EU training providers including CEPOL and the European Union Agency for Law Enforcement Cooperation (EUROPOL) and also by a variety of other international public and private sector organisations.

Most respondents were in favour of a certification or accreditation being offered for the completion of relevant cybercrime training activities. Certified or accredited training resulting in internationally recognised proof of the skills and knowledge achieved through training is considered to have added value in the labour market and cybercrime professions. Proposals were made for certification or accreditation of multiple standalone topics. For example, cybercrime fundamentals and role-based modules for Cybercrime Managers and First Responders were suggested, as well as training packages suitable for cyber forensics roles.

Introduction

As defined under Article 3 of Regulation 2015/2219[9], the objectives of the European Union Agency for Law Enforcement Training (CEPOL) are to support, develop, implement and coordinate training for law enforcement (LE) officers, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of LE, in particular in the prevention of and fight against serious crime affecting two or more Members States (MS) and terrorism, maintenance of public order, international policing of major events, and

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

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

CEPOL's Single Programming Document (SDP) for 2023-2026[10] describes the Operational Training Needs Analysis (OTNA) as a process to help the realisation of strategic goals through the implementation of operational training activities.

Building on the strategic training priorities defined by the EU-STNA, CEPOL launched the OTNA on cyber-attacks in 2022. This analysis concerning training needs relating to cyber-attacks has been performed in line with the Cybercrime TCF defining key competencies and establishing the expected level of skills and knowledge for key roles involved in combatting cybercrime at EU level. The TCF is aligned with the EU-STNA training priorities for cyber-attacks.

The TCF covers 11 roles, including Heads of Cybercrime Units, Team Leaders, General Criminal Investigators, Cybercrime Analysts, Cybercrime Investigators, Cybercrime Experts, Digital Forensics Examiners, Incident response Experts, First Responders, Trial and Appeal Judges and Investigative Judges and Prosecutors. It focuses on **10 core competency areas** and defines to which roles they are relevant and at what level. These include Digital Forensics, Network Management and Tracing, Programming, Scripting, Structured Query Language (SQL), Reporting and Presenting Cybercrime Investigative Data, Analysis and Visualisation, Cybercrime Legislation, General Cybercrime Knowledge, Specific Cybercrime Knowledge, Crime Scene Management and Electronic Evidence Handling, and Cybercrime Investigation Techniques. Table 1 below provides an overview of the competencies associated with and expected levels defined for each role. A **further description of the main functions of the roles and more detailed explanations of the related skillsets can be found in Annex 3.**

Table 1. Summary of expected competencies

	Digital Forensics	Network Management and Tracing	Programming, scripting, SQL	Reporting and Presenting Cybercrime Investigative Data	Analysis and Visualisation	Cybercrime Legislation	General Cybercrime Knowledge	Specific Cybercrime Knowledge	Crime Scene Management and Electronic Evidence Handling	Cybercrime Investigation Techniques
Heads of Cybercrime Units	🟩	🟩		🟧	🟩	🟦	🟦	🟦	🟩	🟩
Team Leaders	🟧	🟧	🟩	🟧	🟩	🟧	🟧	🟧	🟧	🟧
General Criminal Investigators						🟦	🟦		🟦	🟩
Cybercrime Analysts			🟧		🟦	🟩	🟦	🟩		🟩

[10] Available at: https://www.cepol.europa.eu/api/assets/media/downloads/2023/17-2022-mb-annex.pdf, Annex to Management Board decision, 17/2022/MB, CEPOL Single Programming Document for Years 2024-2026, (13 December 2022), p. 5.

Cybercrime Investigators	🟩	🟩	🟩	🟧	🟧	🟧	🟧	🟧	🟦	🟦
Cybercrime Experts	🟧	🟦	🟧	🟦	🟧	🟧	🟧	🟦	🟧	🟦
Digital Forensics Examiners	🟦	🟧	🟦	🟦	🟧	🟧	🟧		🟦	🟩
Incident response Experts	🟧	🟦	🟧	🟧	🟩	🟧	🟦	🟧	🟦	🟧
First Responders	🟩					🟩	🟩		🟧	
Trial and Appeal Judges	🟩	🟩		🟩		🟦	🟩	🟩	🟧	🟩
Investigative Judges and Prosecutors	🟩	🟩		🟧		🟦	🟧	🟩	🟧	🟩

🟩 **Basic**	🟧 **Intermediate**	🟦 **Advanced**

To develop a detailed overview of training needs in the field, an online survey was designed, programmed and delivered through a web-based survey tool, Qualtrics®. Through the survey, CEPOL invited 26 MS[11] and EU institutions to provide their views on training needs on the topic. Data collection took place between December 2022 and February 2023.

This report summarises the outcomes of the OTNA process, which are intended to be used for defining CEPOL's training portfolio on cyber-attacks. 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 study. The following chapters constitute the analytical core of the report: the 'Analysis' chapter sets out further details of the overall findings, and then the 'Training needs per role' chapter provides details on the competency assessment and the related needs of each cybercrime role individually. Finally, the conclusions summarise the key findings concerning each role and provide suggestions for further prioritisation of training needs.

Participants

Data collected through the survey consists of **110 answers** from different LEAs in **23 EU MS[12]** and EUROJUST. These responses represent **88.46 %** of EU MS participating in the CEPOL Regulation, and the level of contributions received can be considered to be a relatively good response rate to the survey. 50.91 % of the responses received were from people representing organisations and 47.27 % were from individuals[13].

The map below (Figure 1) gives an overview of the countries contributing to the process (responding countries are highlighted in blue).

[11] Those participating in the CEPOL Regulation, i.e. all EU MS apart from Denmark.

[12] Responding countries: Austria, Bulgaria, Cyprus, Czechia, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

[13] The origin of 2.00 % remains unknown since two respondents did not specify the coverage of their response.

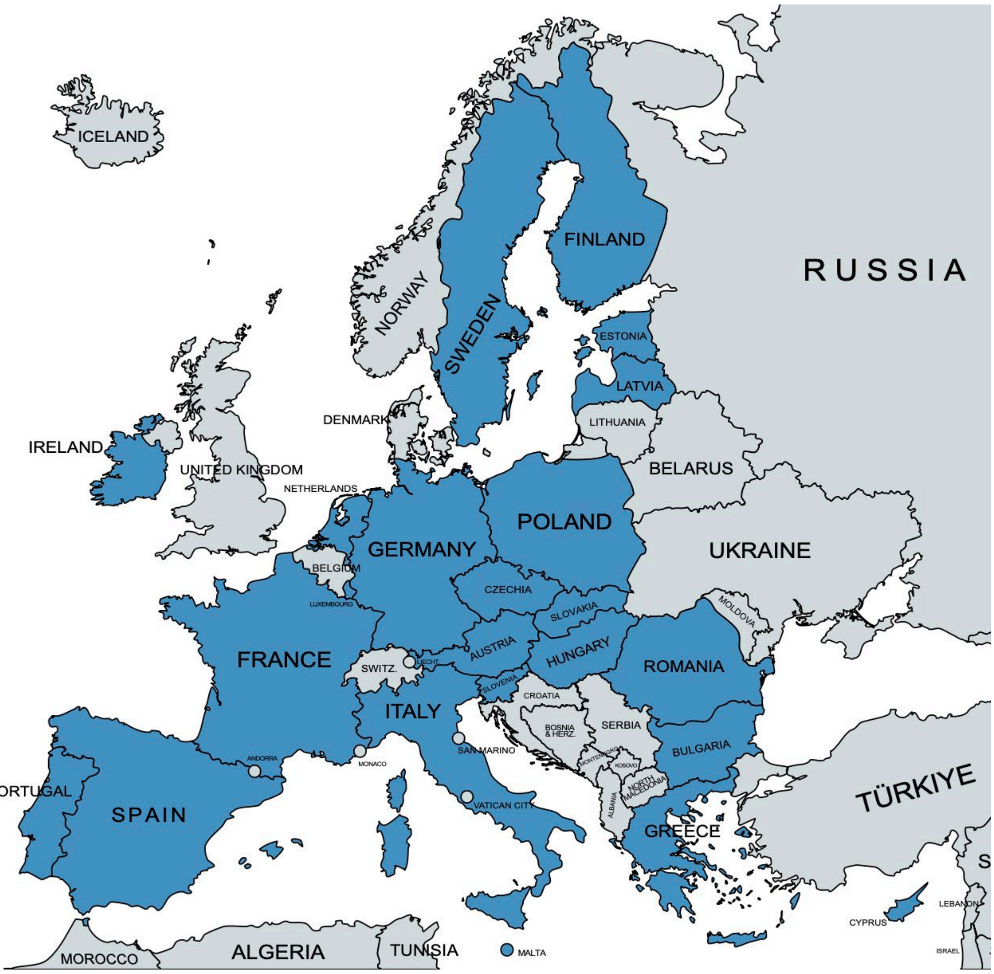

Figure 1. Overview of responding countries

While the response rate indicates generally a good representation of the different EU MS and their LE services, it must be noted that 40.90 % (n=50) of data was received from Polish respondents. Poland's high response rate has mostly impacted the analysis concerning the role of Digital Forensics Examiners, where 76.00 % (n=38) of responses represent Polish LE professionals. Portugal was the second largest contributor to the survey, constituting 10.26 % (n=12) of the sample. Also, Malta, Latvia and Sweden submitted more than five (>5) individual responses each. A compilation of all contributions received from the responding countries is presented below in Figure 2.

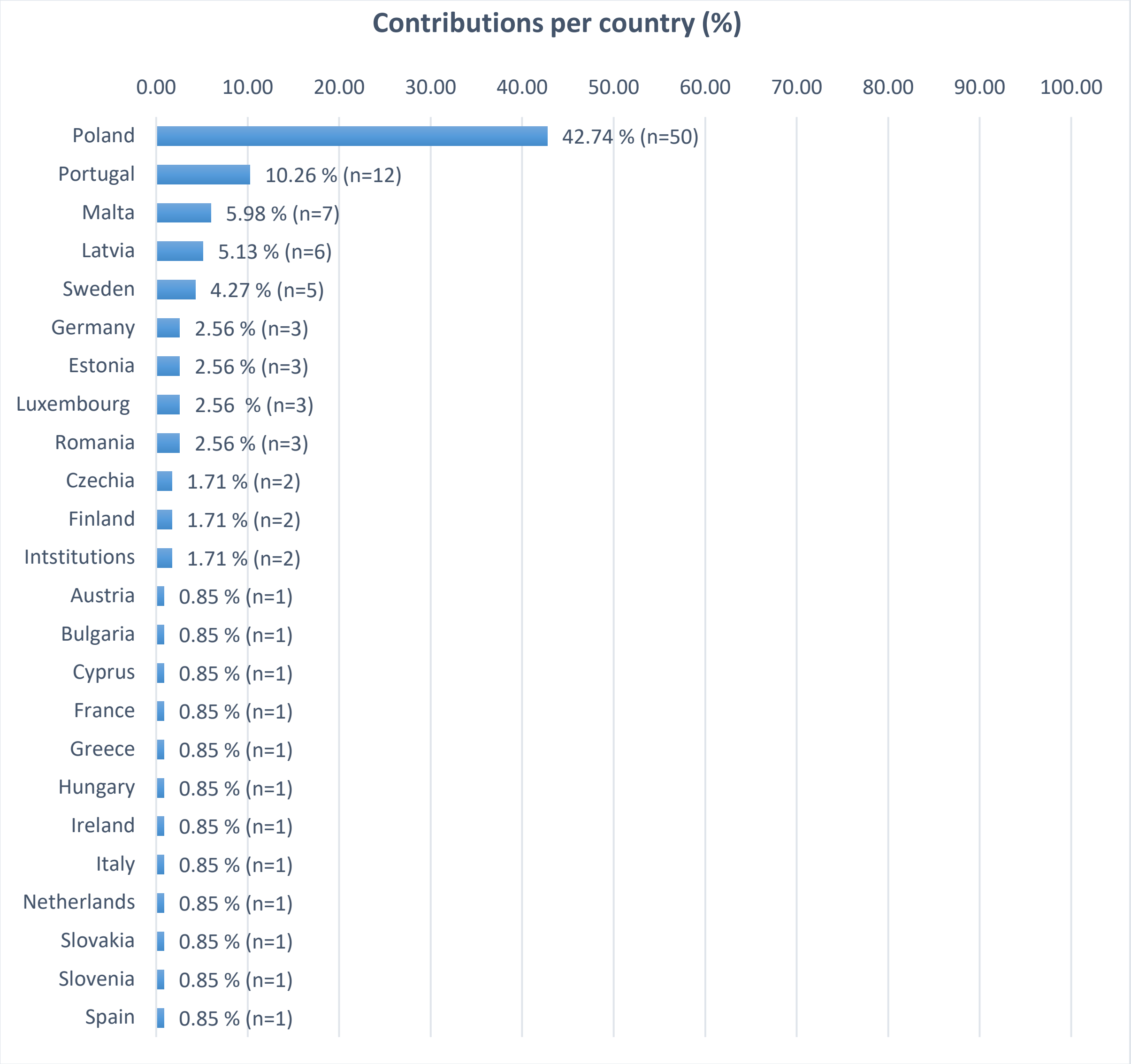

Figure 2. Share of responses per responding countries

For many roles, the level of MS's representativeness did not reach more than 30.00-40.00 % of the sample; however, the total number of responses received is higher than in most OTNA processes. The 'Training needs per role' chapter of this report, which presents the results for each cybercrime role, provides the demographics of each sample. It also provides role-specific details on the ratio of organisational and individual responses for each role. While a generalisation of results must always be reviewed critically, neither geographical nor other factors related to the representation[14] of responses have had an impact on the overall findings and conclusions of this TNA[15].

75.45 % of responses (n=83) were received from respondents representing the **police**, establishing this as the largest sector represented in the survey. With 11.82 % of responses

[14] Responses representing organisational vs individual professional capacity

[15] This conclusion is supported by additional analysis conducted where relevant for testing if e.g. national overrepresentation distorts the data

(n=13), **other** organisations created the second biggest segment of respondents[16]. These other organisations represent, among others, the Portuguese Tax and Customs Authority, the Information Technology (IT) and Development Centre at the Estonian Ministry of the Interior (MoI), the Polish Police Headquarters, the Romanian Intelligence Service and the Latvian Prosecutor's Office.

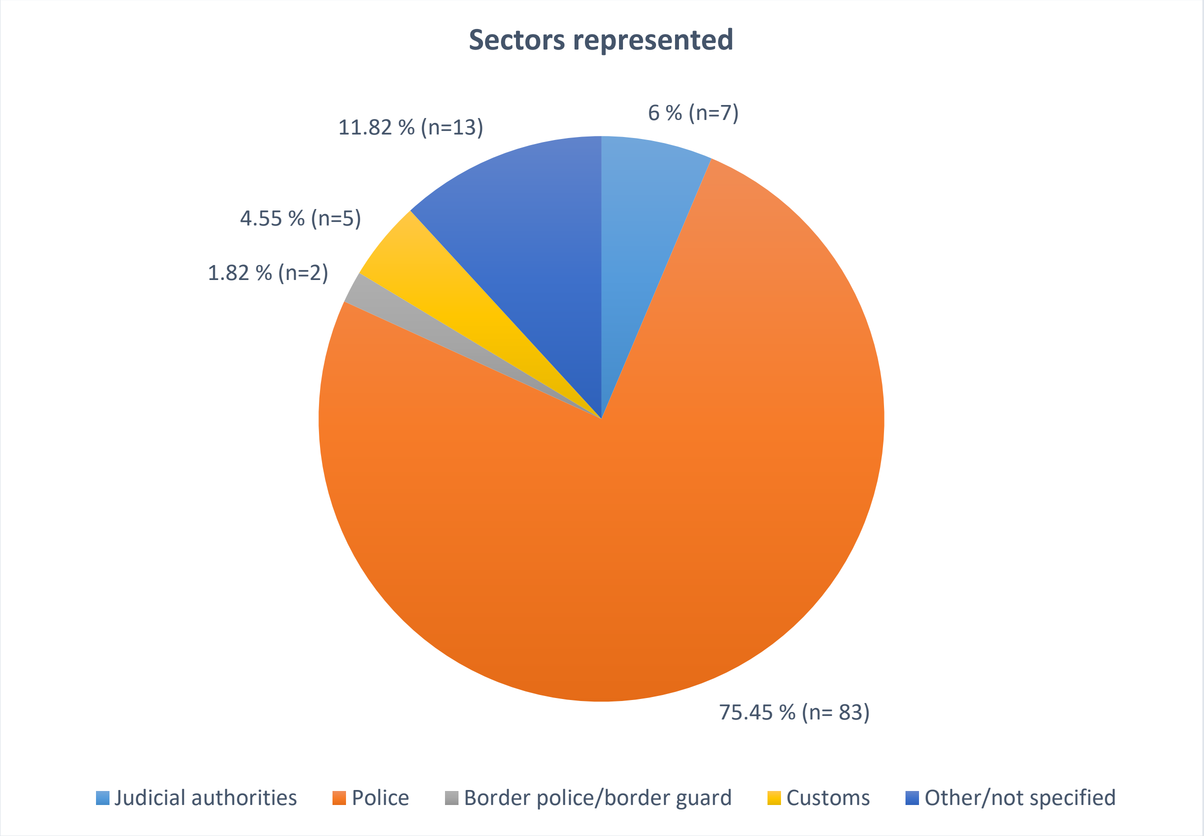

Figure 3. Sectors represented by respondents

Data processing

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 combining statistical analysis and simple manual content analysis procedures.

First, incomplete responses were eliminated from the dataset, although some responses that lacked minor details, without this having a fundamental impact on the analysis – were included. Next, the different roles were separated from the main dataset, enabling an analysis to be conducted within each individual role and also comparisons to be established later between the different data segments.

[16] Two responses with no type of organisation specified have been included in this category.

Responses concerning the current level of skills, level of training required and urgency of training were recoded to numeric values by using the conversion shown below.

Table 2. Data recoding principles

Data area	Text response	Recoded value
Level of competency[17]	None	0.00
	Basic	1.00
	Intermediate	2.00
	Advanced	3.00
Level of training required	No training is needed	0.00
	Basic	1.00
	Intermediate	2.00
	Advanced	3.00
Urgency of training	Not urgent at all	0.00
	Somewhat urgent	1.00
	Urgent	2.00
	Very urgent	3.00
	Extremely urgent	4.00

The current level of competency, level of training required, and urgency of training are based on a statistical average of each role. The current level of competency was analysed against the established TCF on cybercrime. For each role and competency associated with it, the comparative analysis included calculating the difference between the levels of expected competencies and current competencies reached, based on the competency gap (or surplus) that could be identified. The current competency level, gap or surplus and training requests made were then analysed against the expected competency. The urgency of training was estimated by using the established OTNA method[18], meaning that a maximum total urgency score was identified by multiplying the highest urgency rate (4.00) by the number of responses in each analysis group (role). The sum of urgency values (0.00-4.00) attributed to the different topics was then divided by the maximum urgency score and multiplied by 100.00, thus establishing the urgency of training on each topic as a percentage.

Colour coding following the TCF matrix has been used in later parts of this report ('Training needs per role' chapter) to support the statistical analysis and illustrate in a simple way the alignment and differences in competencies, as well as the related training needs.

[17] Used for both converting the TCF competency levels and survey responses concerning the current competency.

[18] The OTNA methodology as adopted by 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, namely the EU Common Security and Defence Policy (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 annually on different topics defined in the EU-STNA, which have been complemented by extraordinary needs assessments when requested, conducted by applying the OTNA methodology.

Analysis

This chapter presents the overall analysis conducted on the topics included in the survey. While the training dimensions of each cybercrime role are detailed later in this report, this chapter provides an overview of the competency levels and training needs for the roles surveyed, and summarises the views gained on regional training needs, previous training attended and training areas recommended for accreditation or certification.

Roles selected

Survey respondents were asked to indicate the role(s) they hold. With a share of 30.68 % (n=50) of all responses, **Digital Forensics Examiners** gained the highest attention, followed by **Cybercrime Investigators** with 11.73 % (n=19) and **Cybercrime Analysts** with 11.11% (n=18) of the survey sample. Among the other roles, the level of responses was generally more balanced, except for Trial and Appeal Judges which was only selected by one responding individual, thus not providing enough data to draw conclusions concerning the wider population. Figure 4 below summarises the details related to the roles selected by the respondents.

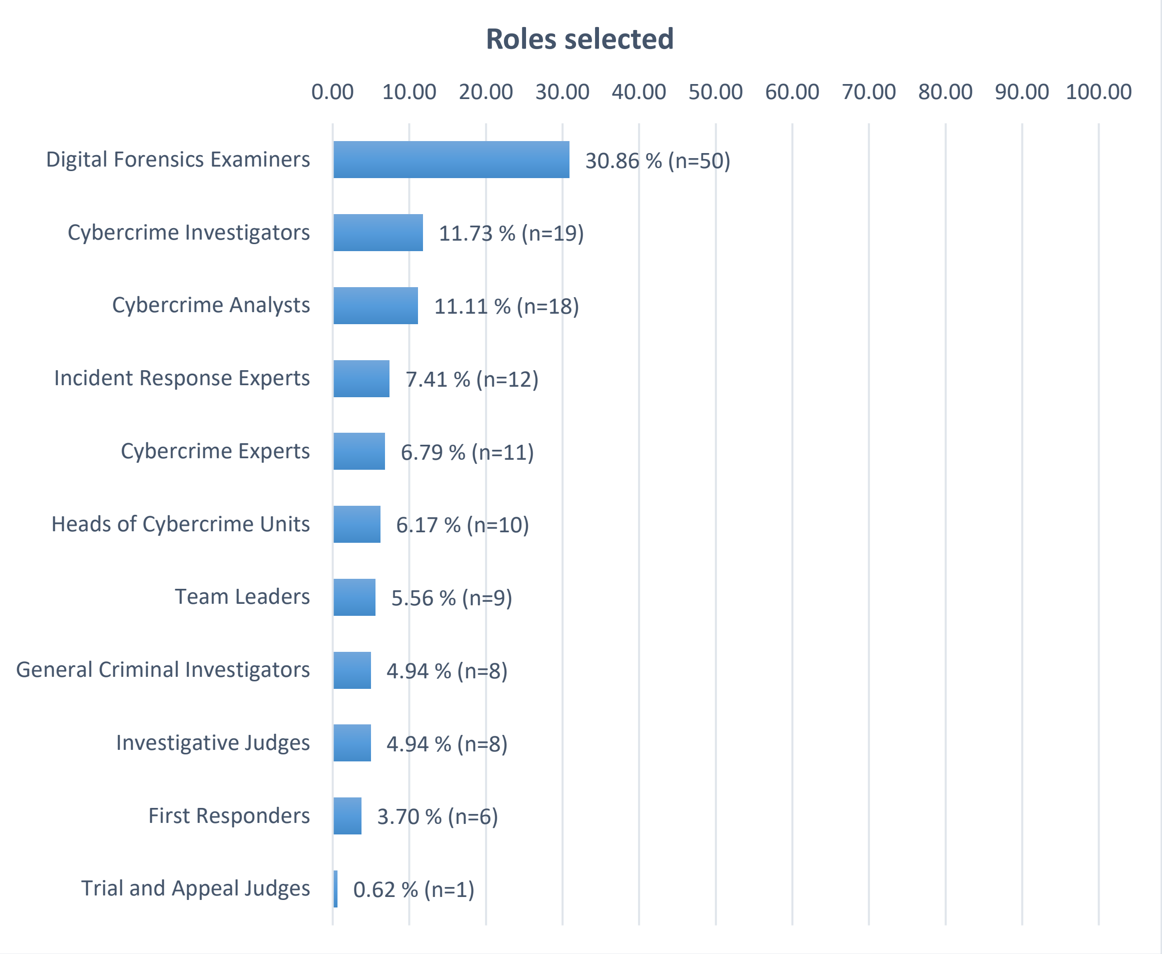

Figure 4. Roles selected by respondents

Competency level

Based on their selection of role(s), each respondent was requested to assess their current level of skills in relation to the competencies associated with each role. Specific details concerning the competencies related to the different roles are discussed in detail in chapter 'Training needs per roles' of this report. The analysis showed that **Heads of Cybercrime Units** and **General Criminal Investigators** are the only roles in which professionals' skills are above the expected competency levels. **First Responders** and **Team Leaders** are very close to meeting the expected competency levels, both with 0.23 units below the expected competency considering the average level. In terms of other roles, the gap varies between -0.56 units to -1.22. Perhaps the most striking observation is that the largest competency gaps concern the roles of **Digital Forensics Examiners**, **Cybercrime Experts** and **Incident Response Experts,** which in the TCF are among the roles with the highest expected competency levels.

Figure 5 below provides an overview of the current and expected competency levels for each role. It should be noted that while each role has multiple competency areas that are expected to be met at either basic (1.00), intermediate (2.00) or advanced (3.00) level, where in statistical analysis these are always whole numbers, in this comparison, the expected level is a calculated average of all competencies associated with the different roles.[19] For this reason, in order to ensure comparability with the current average competency displayed with two decimal places, the competency expectancy is also displayed as a decimal number, consisting of a whole number and a fractional part separated by a point.

[19] For example, the average competency level of Heads of Cybercrime Units (with nine competency areas) was reached by using the calculation formula (1+1+2+1+3+3+1+1+1) : 9 = 1.56.

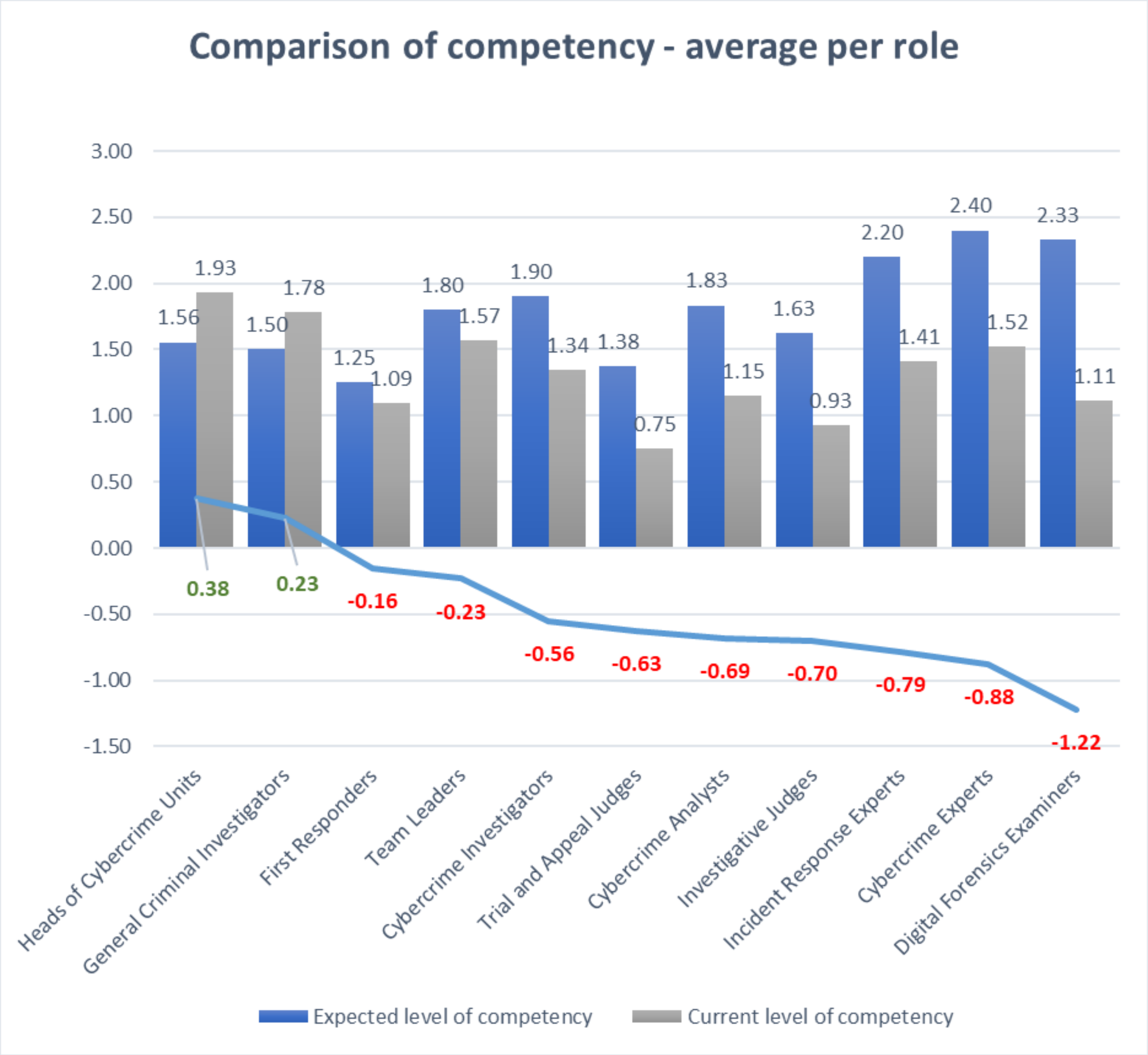

Figure 5. Current competency vs expected level – average per role (all roles)

Each cybercrime role comes with a different number and/or level of competencies. Considering the ratio of competencies associated with the role, the level of gaps related to them and the overall competency gap, Table 3 below provides an indicative ranking of the roles and the related competency gaps.

Table 3. Summative competency ranking

Role	No of competencies associated with role	Share of cybercrime competencies associated with role (%)	No of competencies with gaps	Share of competencies with gap (%)	Gap (average)
Digital Forensics Examiners	9	90.00	9	100.00	-1.22

Cybercrime Experts	10	100.00	10	100.00	-0.88
Incident Response Experts	10	100.00	10	100.00	-0.79
Investigative Judges	8	80.00	8	100.00	-0.70
Cybercrime Analysts	6	60.00	4	66.67	-0.69
Cybercrime Investigators	10	100.00	9	90.00	-0.56
Team Leaders	10	100.00	7	70.00	-0.23
Trial and Appeal Judges[20]	8	80.00	5	62.50	-0.63
First Responders	4	40.00	2	50.00	-0.16
Heads of Cybercrime Units	9	90.00	3	33.33	0.38
General Criminal Investigators	4	40.00	1	25.00	0.23

Level of training required

On average, the highest demand concerns intermediate-level training. An exception to this finding, which is applicable to most roles and topics, are the training needs of First Responders, which are closer to basic level. This is explained by the fact that their average expected competency is at basic level in all competencies other than crime scene management and electronic evidence handling, where a well-aligned request is made for intermediate-level training.

Arranged by the level of training requested (in descending order from the highest to the lowest), Figure 6 below summarises the comparison of average training requests and competencies[21] concerning both current and expected levels. While the first bar (blue in colour) communicates the average level of training requests made, the grey bar in the middle provides a comparison of the level that the experts in each specific role are currently at. The third (yellow) bar shows the average expected competency level, which should be the baseline for experts serving in different cybercrime roles. Full details on each role and the related competencies are given in the 'Training needs per role' chapter of this report.

[20] Role not fully fit for prioritisation due to low number of responses (n=1) for that role.

[21] As above: the expected level is presented as a calculated average of all competencies associated with the different roles, so it is displayed as a decimal number.

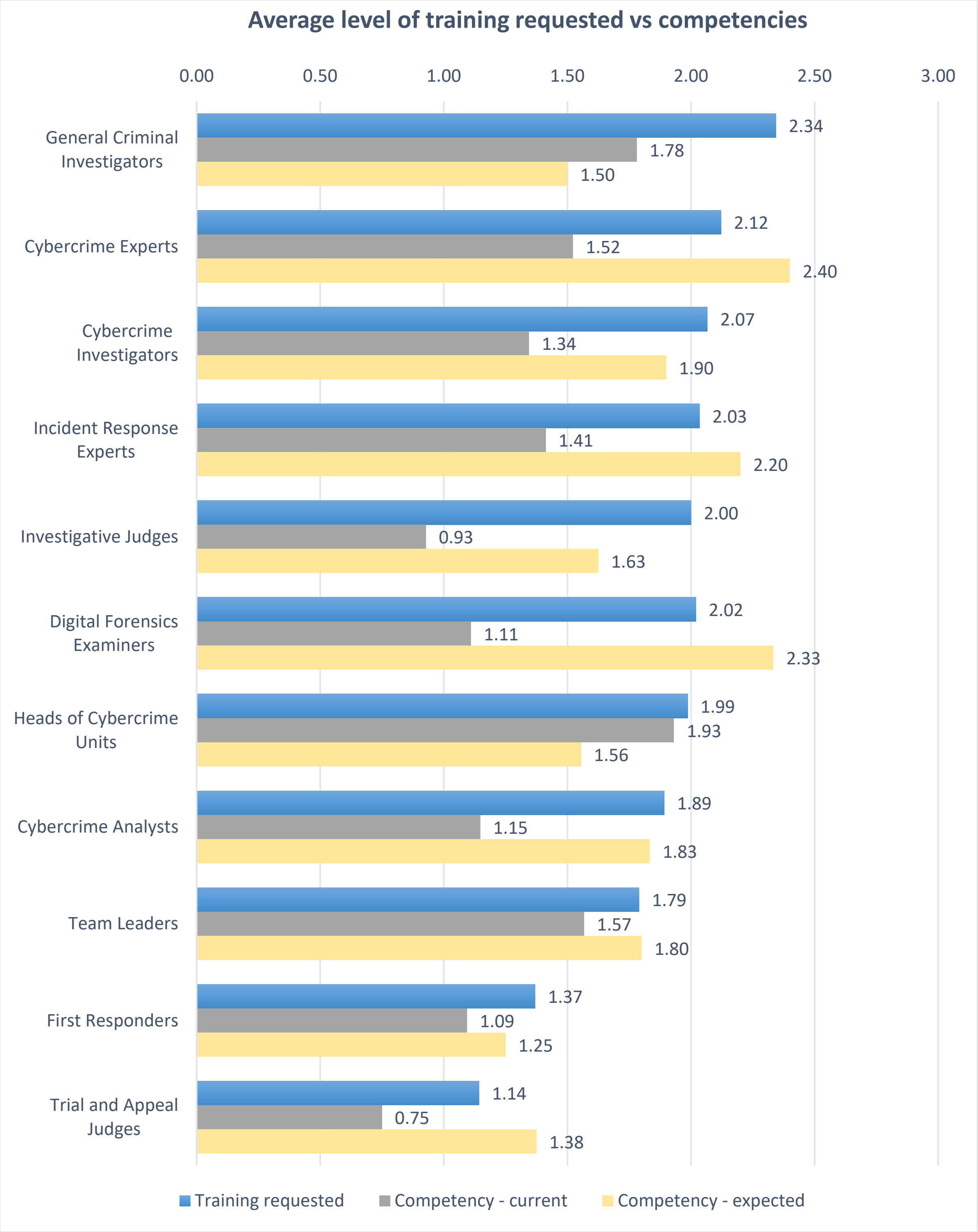

Figure 6. Comparison of training and competency needs – average per role (all roles)

Figure 7 below provides an overview of the level of training requested for different competencies.

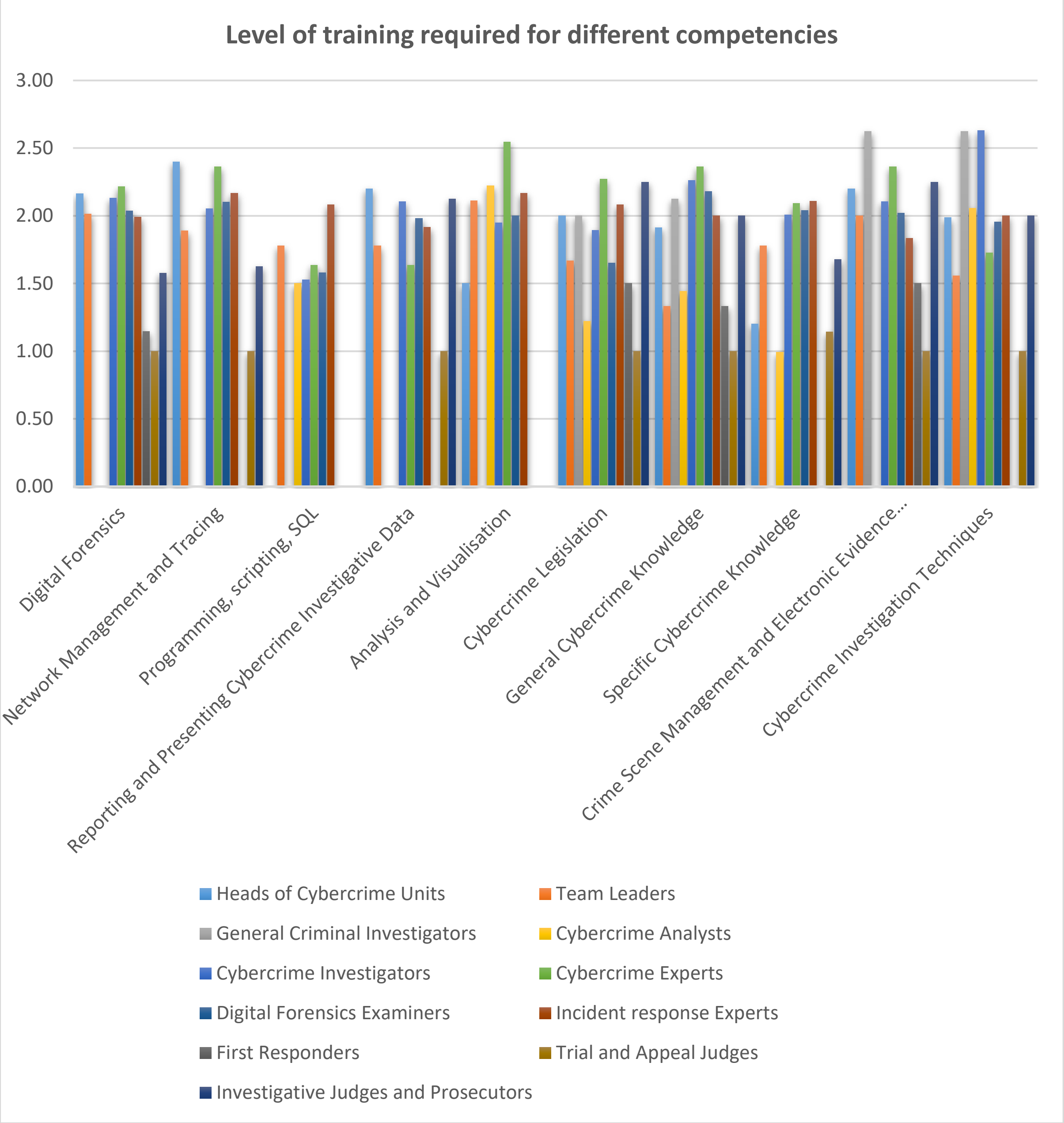

Figure 7. Indicated level of training required – all roles and competencies

Urgency of training

Survey respondents were requested to give their estimation of the urgency for training for different competencies relevant to their selected role(s). The analysis process suggests that while competency gaps remain and training needs are indicated, the urgency for training expressed is moderate among all roles. Heads of Cybercrime Units who are already above the expected level of competency – and have requested training at the same level (average) at which they are currently at – have also attributed the highest urgency. Indicating an average urgency of 44.46 % means that training is moderately urgent, and it would be advantageous to receive training within a year to improve performance, but not significantly advantageous. In all other roles, the average urgency ranges between 33.59 % and 22.01 %, indicating that the training need is secondarily urgent and it would be useful if the training was delivered but that it could be delivered within (upcoming) 2-3 years (see Annex 4 for full details of urgency levels). However, the urgency level varies between the different topics included under each role, and further details concerning each role and the related competency areas are presented in the following chapter (Training needs per role) of this report.

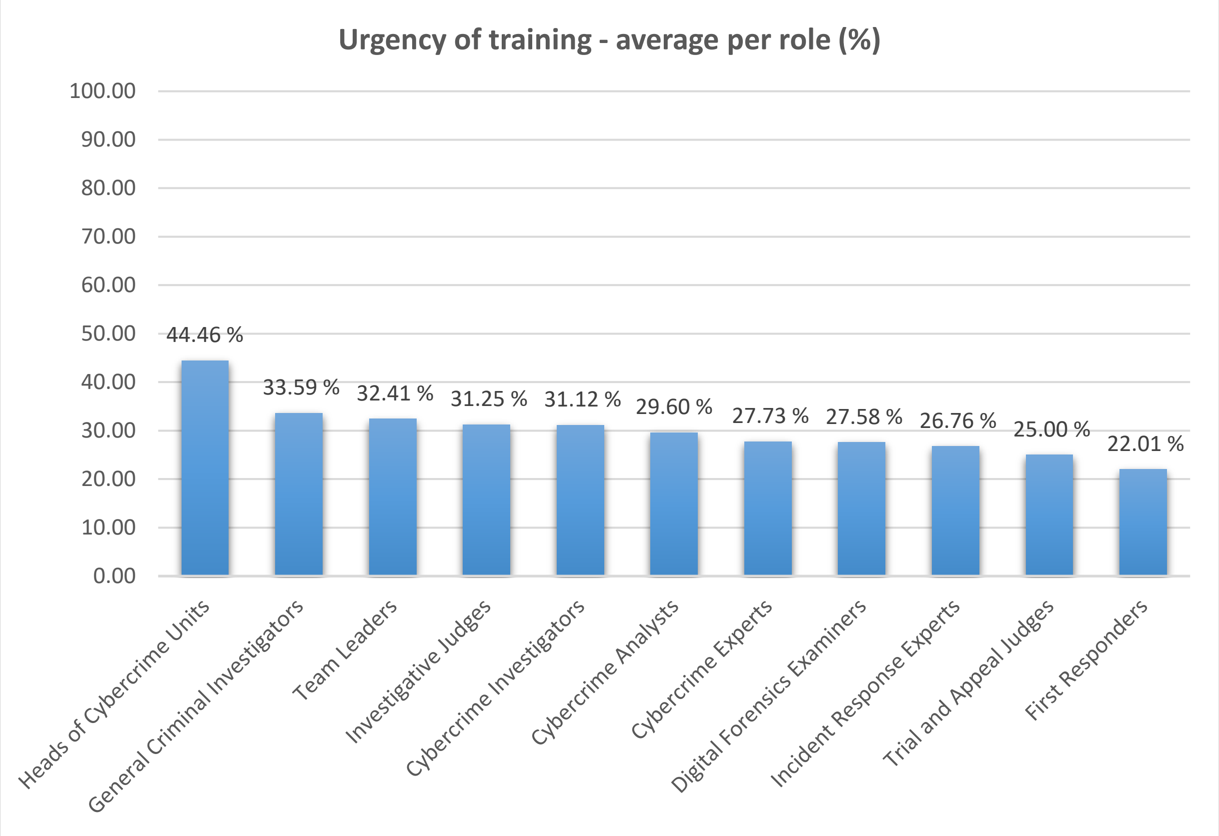

Figure 8. Urgency of training – average per role (all roles)

Regional training needs

Through the OTNA survey, respondents were able to communicate their views on training needs at regional level. This included an opportunity to provide suggestions for topics and specify the geographical area where the training would be required. Regional needs were expressed concerning 9 out of the 11 roles included in the survey. Most of the training needs expressed tend to address a country rather than a region, and some of the submissions overlapped with each other, thereby preventing the analysis process from differentiating to which role(s) they are primarily related. Table 4 below provides an overall summary of the topics and regions or countries suggested for regional training.

Table 4. Summary of regional training needs

Region concerned	Training topic	Target group
Czechia	Cryptocurrencies	Cybercrime Experts
Germany, Baden-Württemberg	Incident Response techniques	Incident Response Experts and Cybercrime Experts
	Fast Triage of Windows Systems	
	Blockchain-Analysis	
	Fast Triage with Firewall	
Luxembourg	Car forensics	Cybercrime Investigators
Malta	Cybersecurity Essentials (-)	Team Leaders, Cybercrime Investigators and First Responders
	Dark web	
	Mobile forensics	
Poland	Cryptocurrencies	Cybercrime Analysts
	Malware analysis	
	Data cloud	
	Advanced training in Adobe Photoshop or alternative software to to enhance the quality of photos regarding individuals or car registration numbers	Cybercrime Experts
	Data acquisition and data analysis - various types of mobile phones	
	Conducting investigations	
	Cryptocurrencies	
	Malware analysis and forensics	
	Data cloud	
	Mobile forensics	
	Cloud forensics	
	MacOS forensics	
	File System forensics	
	SQLite browsing and reporting	
	Mobile passcode cracking	
	Windows forensics	
	Identifying vulnerabilities	
	Network	
	Cloud	
All regions	Cryptocurrency	Team Leaders
	Forensics	
	Cloud forensics	
	Investigative techniques	Cybercrime experts
	Incident response	

	Open-Source Intelligence (OSINT)	Heads of Units, Team Leaders, General Criminal Investigators, Cybercrime Analysts, Cybercrime Investigators, Cybercrime Experts, Incident Response Experts and First Responders

National or international training

The OTNA questionnaire included a question about any previous training on cybercrime attended during the last three years. Training data was provided by respondents representing eight professional roles, but the level of details received was relatively scattered, including incomplete entries and submissions provided in national languages that could not be included in the analysis. A complete list of national or international training attended is available in Annex 5 of this report, and provides further details on topics, levels, target groups and organisers of past training. Figure 9 below summarises the training attended at each competency level; those listed under the green bar are basic-level training, the orange set concerns intermediate-level training topics, and under the blue bar training attended at advanced level is listed.

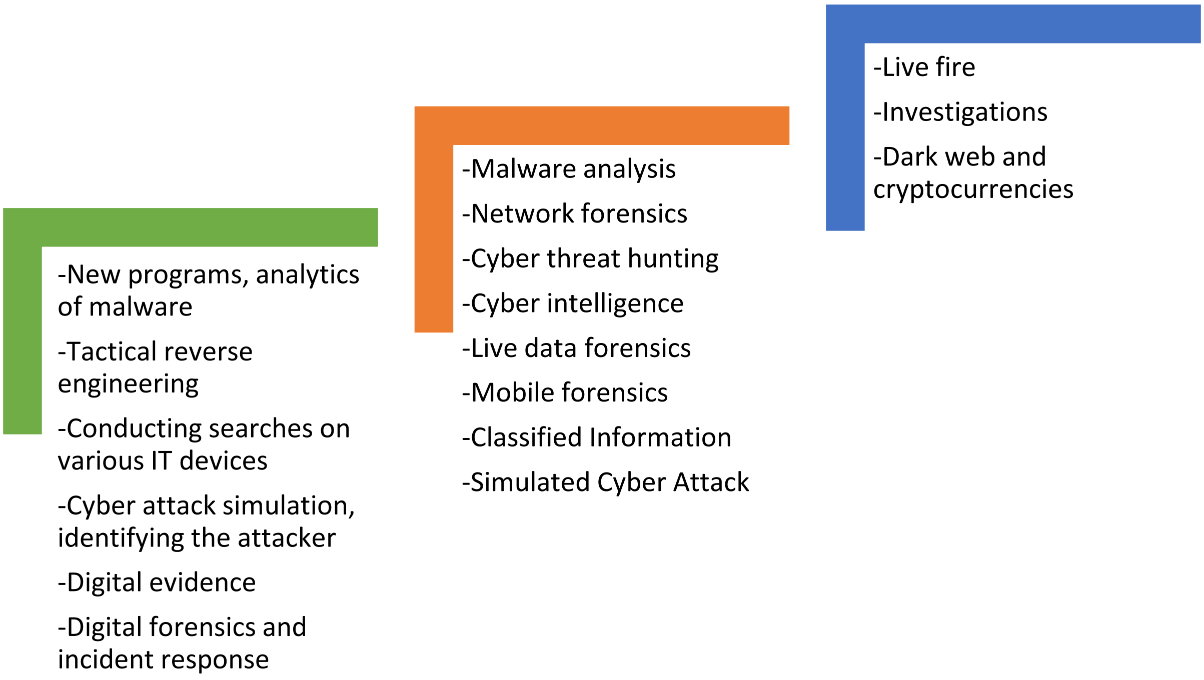
-New programs, analytics of malware
-Tactical reverse engineering
-Conducting searches on various IT devices
-Cyber attack simulation, identifying the attacker
-Digital evidence
-Digital forensics and incident response
-Malware analysis
-Network forensics
-Cyber threat hunting
-Cyber intelligence
-Live data forensics
-Mobile forensics
-Classified Information
-Simulated Cyber Attack
-Live fire
-Investigations
-Dark web and cryptocurrencies

Figure 9. Previous training attended – topics per competency level

Responses concerning previous training were divided almost equally between intermediary and basic level training, with few occasions being indicated where training had been attended at advanced level. Training providers most commonly mentioned included CEPOL, Europol, the FBI, national and local LE authorities and centres with dedicated mandates to deal with cybersecurity matters established in different MS. Reference was also made to foreign academic institutes, particularly the Norwegian Police University College. A few private sector operators were mentioned as well, such as Cyberbit, MediaRecovery, ForSec, eLearn Security and Global Network Systems.

Training activities proposed for certification or accreditation

As part of the survey, respondents were asked which groups of training activities or knowledge would be proposed for certification or accreditation and to provide justification on why this would be required. Views on 8 out of the 11 roles were expressed, with largely overlapping inputs. Certification and/or accreditation (including by other international bodies and legal regulations) was generally supported and seen as a requirement for being able to credibly confirm and prove the acquisition of knowledge in the labour market and for certain professions. However, some respondents would rather opt for academically accredited cybercrime programmes, which, unlike certifications with a fixed validity period, never expire. Some respondents noted, however, that accrediting particular training on specific topics is not necessarily simple, because knowledge needs to be continuously updated. Proposals made included, for example, role-based certified modules or programmes such as the Cybercrime Managers' certification, certified First Responders' training, the Computer Forensics Expert Certificate and Certified Forensic Analyst training, as well as general cybercrime knowledge. Several standalone topics were also proposed, for example in a number of knowledge areas related to forensics (mobile forensics, computer forensics, digital forensics, filesystem analysis and forensics, network forensics, cloud forensics, live data forensics) for certification. OSINT, incident response, Internet of Things (IoT), blockchain technology, cryptocurrencies, cloud data analysis, basic coding languages, dark web, data recovery, analysis and visualisation, digital evidence, identifying security breaches and threat prevention, malware analysis, the EU’s General Data Protection Regulation (GDPR) and network security and analysis. A complete list of proposals can be found in Annex 6.

Training needs per role

This chapter presents a summary of competency status and the related training needs for each specific profile. Under each role, the first table shows the basic features of the sample (respondents representing the population). Then, a figure entitled 'comparison of competency' draws a comparison between the current average level of competency – reached through the sample for each role – and the expected level as set in the TCF. It also shows the competency gap or surplus in each competency area related to each role. Lastly, a summary of competency details and related development needs, including the level and urgency of training required, is provided in the form of a table. For data illustration, the table utilises the colour coding of the TCF, with green referring to basic, orange to intermediate and blue to advanced level. Although each topic contains subtopics, for the presentation of the data, the overall topic of digital forensics has been considered. For details at subtopic level for each role where the competency of digital forensics is applicable, a 'zoom in' table is available in Annex 7.

Heads of Cybercrime Units

Table 5. Sample characteristics – Heads of Cybercrime Units

Number of responses:	10
Number of countries represented:	9
Share of responding countries:	39.13 %
Names of countries represented:	Cyprus, Finland, France, Greece, Luxembourg, Romania, Slovakia, Slovenia, Sweden
Sectors represented:	90.00 % Police, 10.00 % Other
Responses referring to:	70.00 % Organisation, 30.00 % Individual

With a few thematic exceptions, the survey results indicate that the level of current skills related to **cybercrime investigation techniques, crime scene management and electronic evidence handling, specific cybercrime knowledge, analysis and visualisation, network management and tracing, and digital forensics** are above the target level.

A skills gap concerns three areas, namely **reporting and presenting cybercrime investigative data, cybercrime legislation and general cybercrime knowledge.** The most striking observation is that while the expected competency in **cybercrime legislation** is set for advanced level, the current competency is above intermediate level and the average request is still made for basic-level training. In terms of Heads of Cybercrime Units' training, these results suggest that competencies in **cybercrime legislation, general cybercrime knowledge**, and **reporting and presenting cybercrime investigative data** should be addressed.

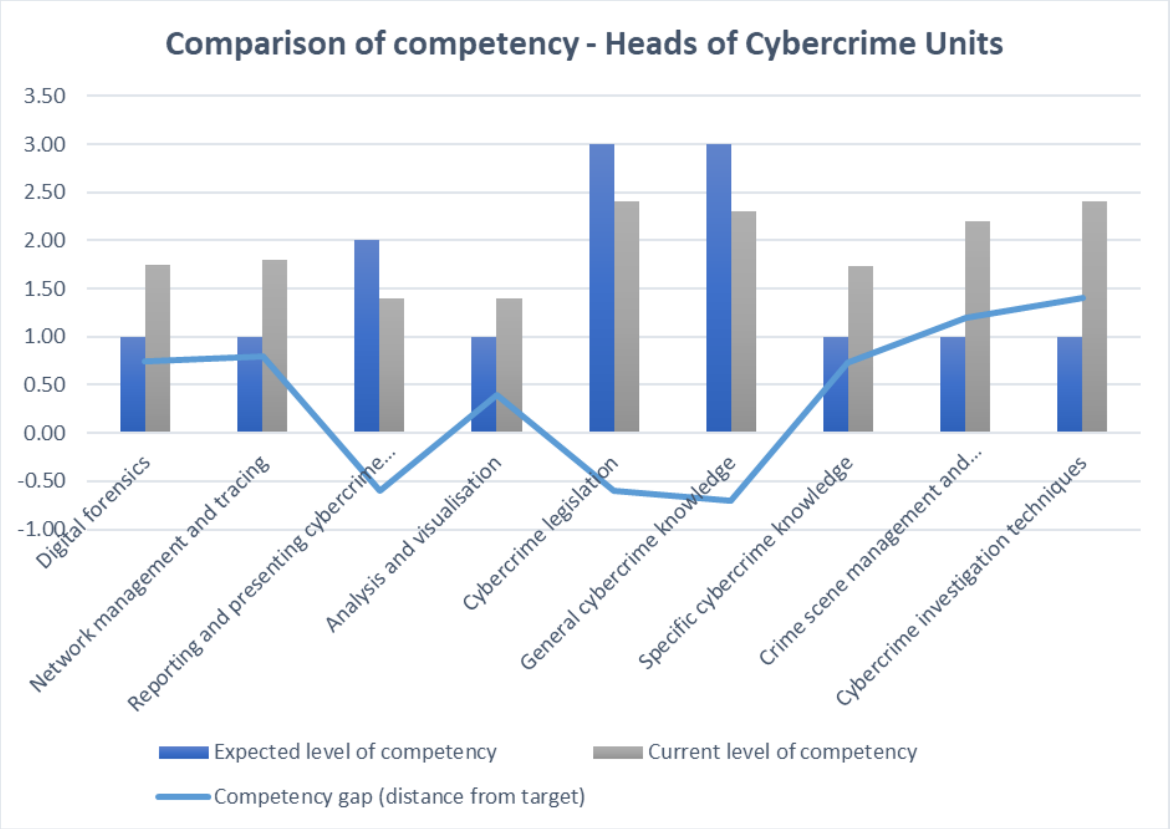

Figure 10. Competency level – Heads of Cybercrime Units

The average demand is for intermediate-level training, with a moderate urgency level of 46.66 %. The urgency associated with training needs does, however, vary considerably between the different topics.

Table 6. Summary of competency development needs – Heads of Cybercrime Units

	Digital forensics	**Network management and tracing**	**Reporting and presenting cybercrime investigative data**	**Cybercrime legislation**	**General cybercrime knowledge**	**Specific cybercrime knowledge**	**Crime scene management and electronic evidence handling**	**Cybercrime investigation techniques**	**Average**
Expected level of competency	1.00	1.00	2.00	3.00	3.00	1.00	1.00	1.00	**1.56**
Current level of competency	1.75	1.80	1.40	2.40	2.30	1.73	2.20	2.40	**1.93**
Competency gap	0.75	0.80	-0.60	-0.70	-0.73	0.73	1.20	1.40	**0.38**
Level of training required	2.16	2.40	2.30	1.50	2.00	1.91	1.20	2.20	**1.99**
Urgency of training required (%)	16.88	80.00	53.33	50.00	66.67	17.50	40.00	73.33	**44.66**

Team Leaders

Table 7. Sample characteristics – Team Leaders

Number of responses:	9
Number of countries represented:	8
Share of responding countries:	34.78 %
Names of countries represented:	Estonia, Finland, Greece, Ireland, Malta, Netherlands, Portugal, Slovakia
Sectors represented:	77.78 % Police, 11.11 % Customs, 11.11 % Other
Responses referring to:	77.78 % Organisation, 22.22 % Individual

Team Leaders' competencies meet or slightly exceed targets in the areas of **programming, scripting, SQL, cybercrime legislation** and **general cybercrime knowledge.** The gap in competency concerning other areas ranges between -0.22 and 0.73 units, specific cybercrime knowledge and digital forensics being the topics with the highest difference in expected and current levels.

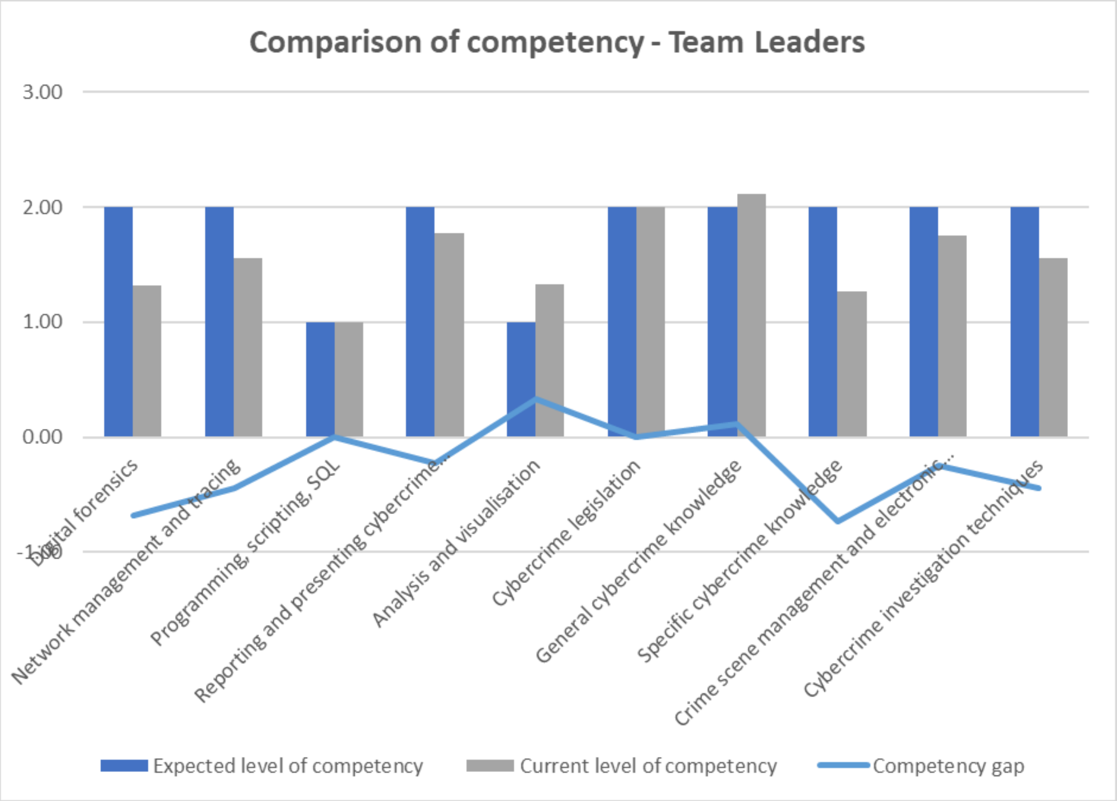

Figure 11. Competency level – Team Leaders

The average demand is for intermediate-level training, but with relatively low average urgency (32.41 %). Overall, training needs are well in line with the current level of competency; in all areas except general cybercrime knowledge, the need is for training to reach the next competency level. In terms of general cybercrime knowledge, while the respondents indicated a current competency above intermediate level, a request for basic-level training was made. This might be partially explained by the fact that 77.78 % of respondents were representing their organisations in a wider sense and not themselves as individual professionals.

Table 8. Summary of competency development needs – Team Leaders

	Digital forensics	Network management and tracing	Programming, scripting, SQL	Reporting and presenting cybercrime investigative data	Analysis and visualisation	Cybercrime legislation	General cybercrime knowledge	Specific cybercrime knowledge	Crime scene management and electronic evidence	Cybercrime investigation techniques	Average
Expected level of competency	2.00	2.00	1.00	2.00	1.00	2.00	2.00	2.00	2.00	2.00	**1.80**
Current level of competency	1.32	1.56	1.00	1.78	1.33	2.00	2.11	1.27	1.75	1.56	**1.57**
Competency gap	-0.68	-0.44	0.00	-0.22	0.33	0.00	0.11	-0.73	-0.25	-0.44	**-0.23**
Level of training required	2.01	1.89	1.78	1.78	2.11	1.67	1.33	1.78	2.00	1.56	**1.79**
Urgency of training required	22.22	22.22	59.26	59.26	19.44	22.22	25.00	55.56	13.89	25.00	**32.41**

General Criminal Investigators

Table 9. Sample characteristics – General Criminal Investigators

Number of responses:	8
Number of countries represented:	8
Share of responding countries:	30.43 %
Names of countries represented:	Estonia, Greece, Hungary, Latvia, Luxembourg, Poland, Slovakia
Sectors represented:	75.00 % Police, 12.50 % Border police/border guard, 12.50 % Other[22]
Responses referring to:	75.00 % Organisation, 25.00 % Individual

General Criminal Investigators responding to the survey possesses a good level of current competency in areas other than **crime scene management and electronic evidence handling**. Within that area, a considerable gap of -1.38 units remains. However, while the average of current competencies is not yet intermediate, the demand for training is still for advanced-level training.

[22] Sector represented was not specified by one respondent.

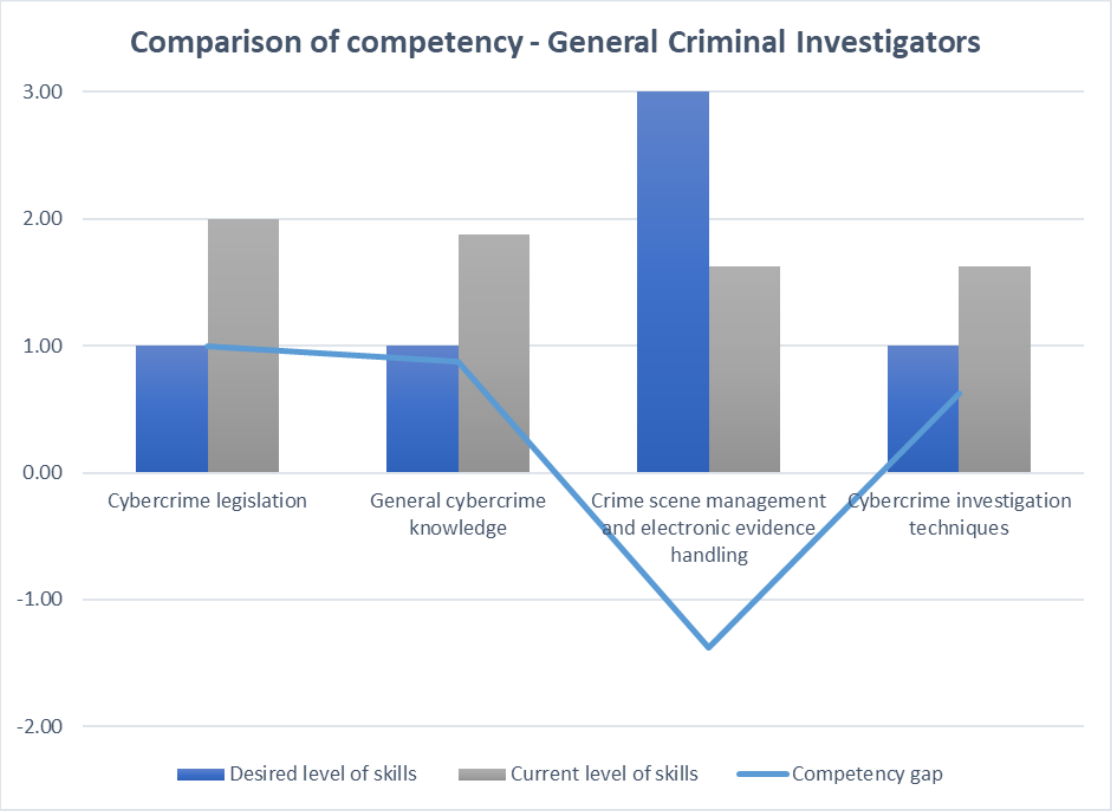

Figure 12. Competency level – General Criminal Investigators

Another observation is that while the expected competency in cybercrime investigation techniques is at basic level, requests are for advanced-level training. The average training urgency is 33.59 %, which suggests a secondary urgency for delivery of the training (within 2-3 years' time). Results of the survey suggest that training of General Criminal Investigators should focus on upskilling the experts on the topic of **crime scene management and electronic evidence handling**.

Table 10. Summary of competency development needs – General Criminal Investigators

	Cybercrime legislation	General cybercrime knowledge	Crime scene management and electronic evidence handling	Cybercrime investigation techniques	Average
Expected level of competency	1.00	1.00	3.00	1.00	**1.50**
Current level of competency	2.00	1.88	1.63	1.63	**1.78**
Competency gap	1.00	0.88	-1.38	0.63	**0.23**
Level of training required	2.00	2.13	2.63	2.63	**2.34**
Urgency of training required	25.00	37.50	31.25	40.63	**33.59**

Cybercrime Analysts

Table 11. Sample characteristics – Cybercrime Analysts

Number of responses:	18[23]
Number of countries represented:	6
Share of responding countries:	26.09 %
Names of countries represented:	Greece, Luxembourg, Poland, Portugal, Slovakia, Sweden
Sectors represented:	72.22 % Police, 11.11 % Customs, 16.67 % Other
Responses referring to:	72.22 % Organisation, 27.78 % Individual

Among the responding Cybercrime Analysts, the current level of skills is below the expected level in all areas except cybercrime legislation and cybercrime investigation techniques. In terms of specific cybercrime knowledge, the expected level is basically met since the difference is only 0.01 units, but gaps concerning the remaining topics range between -1.06-1.88 units.

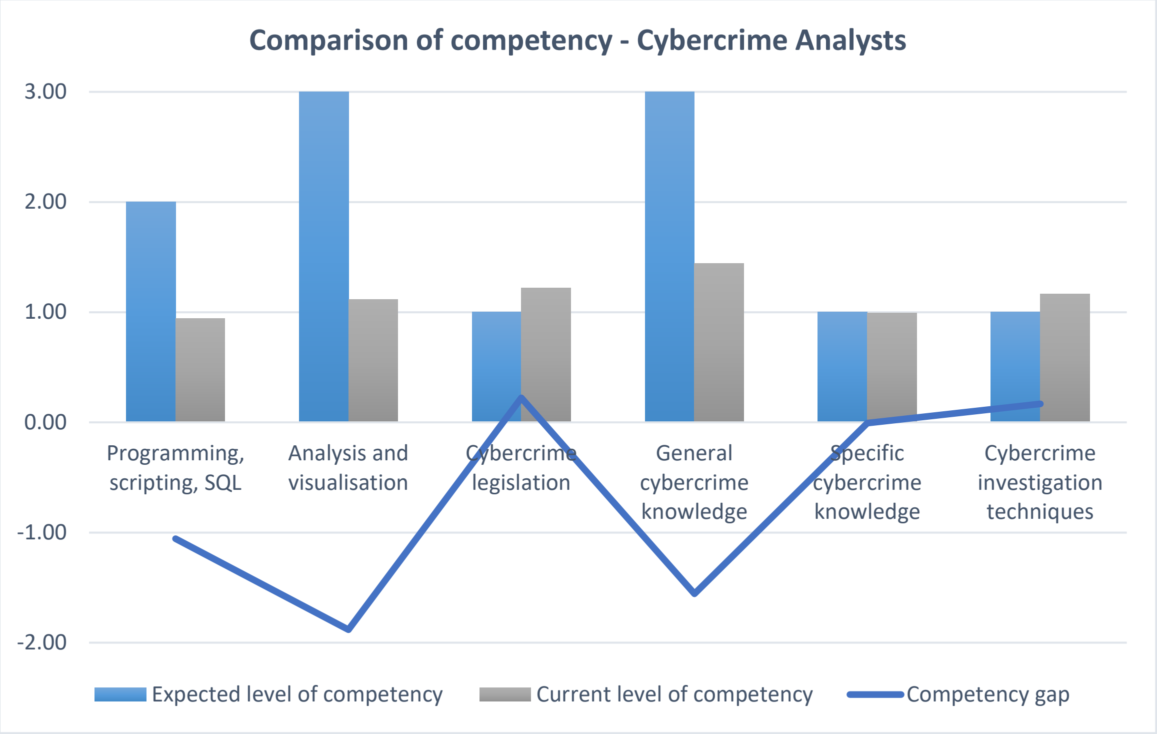

Figure 13. Competency level – Cybercrime Analysts

The training needs expressed are generally well in line with the need to improve competencies. Training on analysis and visualisation, general cybercrime knowledge and programming, scripting and SQL should be provided to narrow the gap between the current and expected competency. Regardless of the relatively large competency gap, the average urgency attributed to training within this area is relatively low: 29.60 % on average.

[23] A total of 18 responses, of which 50.00 % (n=9) were received from Poland and 27.78 % (n=5) from Portugal.

Table 12. Summary of competency development needs – Cybercrime Analysts

	Programming, scripting, SQL	Analysis and visualisation	Cybercrime legislation	General cybercrime knowledge	Specific cybercrime knowledge	Cybercrime investigation techniques	Average
Expected level of competency	2.00	3.00	1.00	3.00	1.00	1.00	**1.83**
Current level of competency	0.94	1.12	1.22	1.44	0.99	1.17	**1.15**
Competency gap	-1.06	-1.88	0.22	-1.56	-0.01	0.17	**-0.69**
Level of training required	1.50	2.22	1.83	1.89	1.85	2.06	**1.89**
Urgency of training required	23.61	27.78	20.38	34.72	30.69	40.28	**29.60**

Cybercrime Investigators

Table 13. Sample characteristics – Cybercrime Investigators

Number of responses:	19
Number of countries represented:	12
Share of responding countries:	52.17 %
Names of countries represented:	Austria, Finland, France, Germany, Greece, Latvia, Luxembourg, Malta, Poland, Slovakia, Spain, Sweden
Sectors represented:	100.00 % Police
Responses referring to:	47.37 % Organisation, 52.63 % Individual

Cybercrime Investigators' current level of competency is below the expected in all areas except digital forensics. The gap ranges between -0.16 and -1.26.

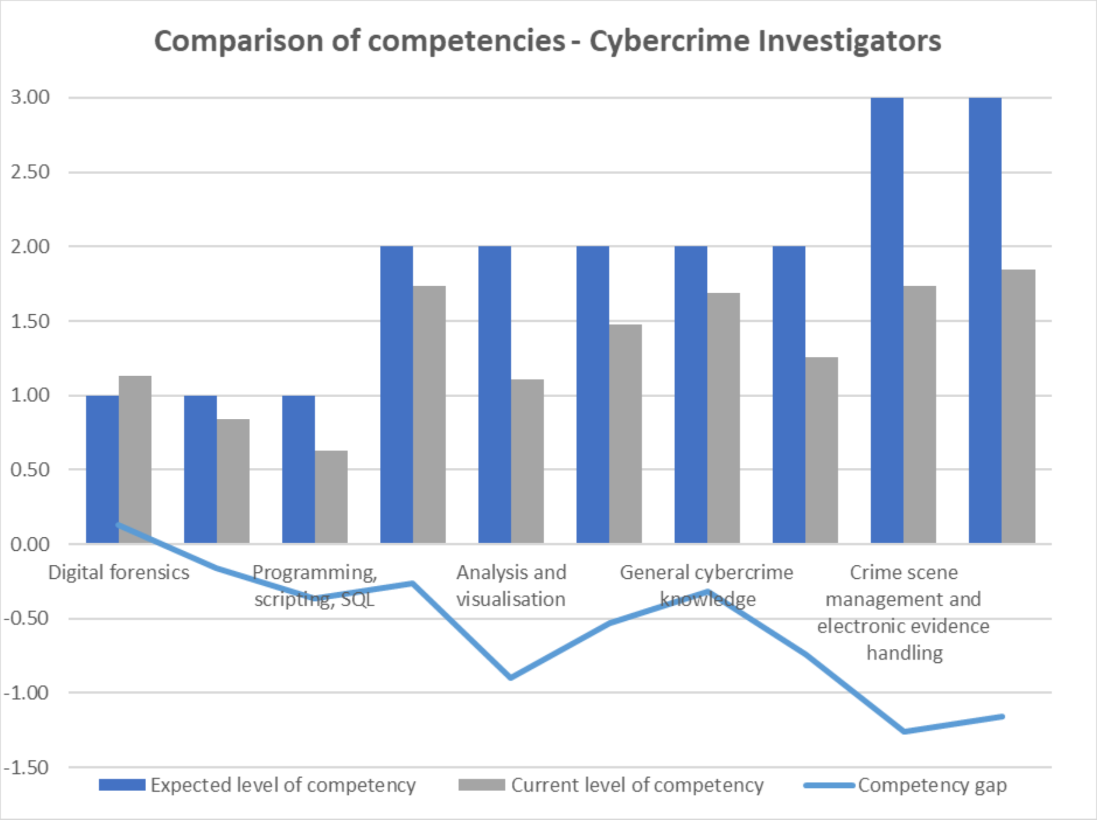

Figure 14. Competency level – Cybercrime Investigators

Training needs are in line with the competency gap, suggesting demand for intermediate-level training. The topics **of crime scene management and electronic evidence handling** and **cybercrime investigations techniques** would require priority attention in order to catch up on the expected competency levels in these areas. The average urgency is 31.12 %, which does not however suggest a primary urgency for training Cybercrime Investigators.

Table 14. Summary of competency development needs – Cybercrime Investigators

	Digital forensics	**Network management and tracing**	**Programming, scripting, SQL**	**Reporting and presenting cybercrime investigative**	**Analysis and visualisation**	**Cybercrime legislation**	**General cybercrime knowledge**	**Specific cybercrime knowledge**	**Crime scene management and electronic evidence**	**Cybercrime investigation techniques**	**Average**
Expected level of competency	1.00	1.00	1.00	2.00	2.00	2.00	2.00	2.00	3.00	3.00	**1.90**
Current level of competency	1.13	0.84	0.63	1.74	1.11	1.47	1.68	1.26	1.74	1.84	**1.34**

Competency gap	0.13	-0.16	-0.37	-0.26	-0.89	-0.53	-0.32	-0.74	-1.26	-1.16	**-0.56**
Level of training required	2.13	2.05	1.53	2.11	1.95	1.89	2.26	2.01	2.11	2.63	**2.07**
Urgency of training required	30.92	28.95	23.68	28	27.63	31.58	36.84	28.95	30.62	44.74	**31.12**

Cybercrime Experts

Table 15. Sample characteristics – Cybercrime Experts

Number of responses:	11
Number of countries represented:	8
Share of responding countries:	34.78 %
Names of countries represented:	Austria, Bulgaria, Czechia, Finland, Greece, Poland, Slovakia, Sweden
Sectors represented:	100.00 % Police
Responses referring to:	81.82 % Organisation, 18.18 % Individual

The responses from Cybercrime Experts indicate that among the sample, the current level of competency is generally below expected, with the most striking difference in competencies regarding **network management and tracing, specific cybercrime knowledge, cybercrime investigation techniques**, as well as **reporting and presenting cybercrime investigative data.** Currently, only general cybercrime knowledge meets the expected level of competency.

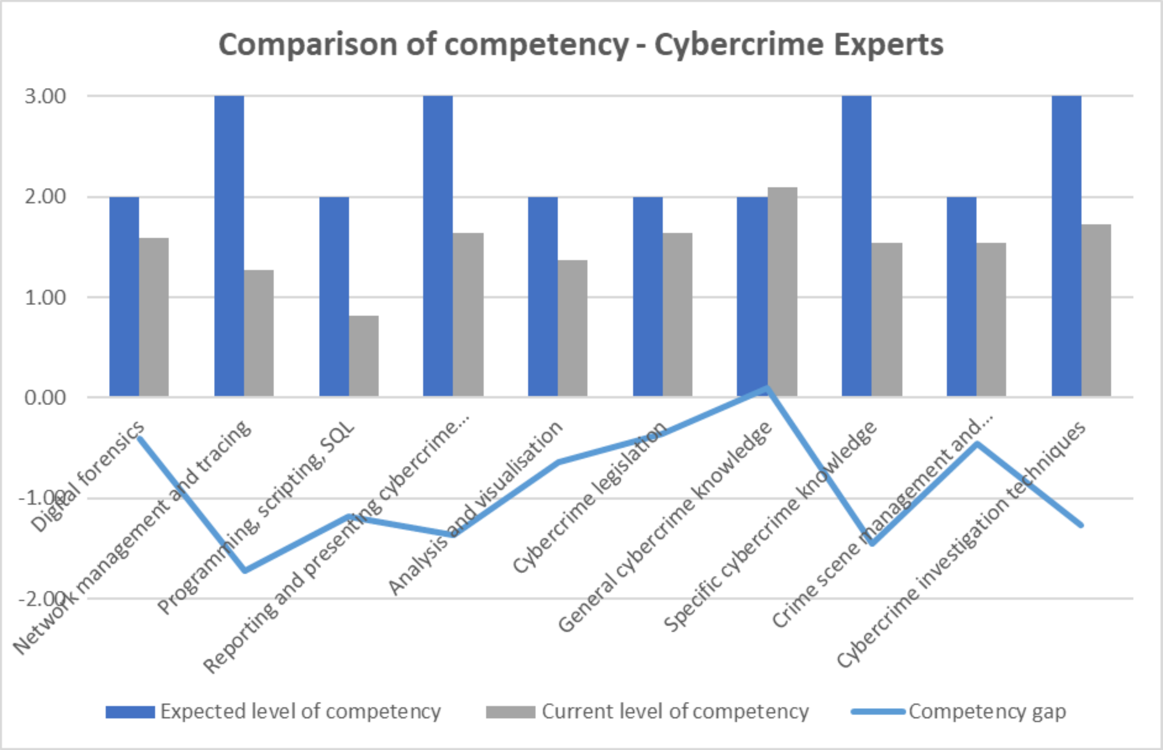

Figure 15. Competency level – Cybercrime Experts

The average demand is for intermediate-level training and, despite notable competency gaps, the urgency associated with training needs is only 27.73 %. The topic of cybercrime investigation techniques scored a higher urgency level (47.74 %) than others and points to moderate urgency, meaning it would be advantageous to receive training within a year, and this would improve performance significantly.

Table 16. Summary of competency development needs – Cybercrime Experts

	Digital forensics	Network management and tracing	Programming, scripting, SQL	Reporting and presenting cybercrime investigative data	Analysis and visualisation	Cybercrime legislation	General cybercrime knowledge	Specific cybercrime knowledge	Crime scene management and electronic evidence handling	Cybercrime investigation techniques	**Average**
Expected level of competency	2.00	3.00	2.00	3.00	2.00	2.00	2.00	3.00	2.00	3.00	**2.40**
Current level of competency	1.59	1.27	0.82	1.64	1.36	1.64	2.09	1.55	1.55	1.73	**1.52**
Competency gap	-0.41	-1.73	-1.18	-1.36	-0.64	-0.36	0.09	-1.45	-0.45	-1.27	**-0.88**
Level of training required	2.22	2.35	1.64	1.64	2.55	2.27	2.36	2.09	2.36	1.73	**2.12**
Urgency of training required	34.09	25.00	25.00	18.18	27.27	20.45	27.27	31.82	20.45	47.73	**27.73**

Digital Forensics Examiners

Table 17. Sample characteristics – Digital Forensics Examiners

Number of responses:	50[24]
Number of countries represented:	11
Share of responding countries:	47.83 %
Names of countries represented:	Austria, Czechia, Finland, France, Germany, Greece, Latvia, Malta, Poland, Portugal, Slovakia
Sectors represented:	92.00 % Police, 2.00 % Border police/border guard, 6.00 % Other
Responses referring to:	52.00 % Organisation, 46.00 % Individual, 2.00 % Unknown[25]

[24] 76% of responses (n= 38) represent Poland.

[25] The representativeness of the response was not specified by one respondent.

In the overall survey, the role of Digital Forensics Examiners was selected the most. It is worth noting that 76.00 % (n=38) of all responses were given by Polish professionals. Overall, the current competency of professionals is notably below the expected level in all topics except cybercrime investigations techniques, where the current average level nearly meets the expected with only a -0.02 unit difference.

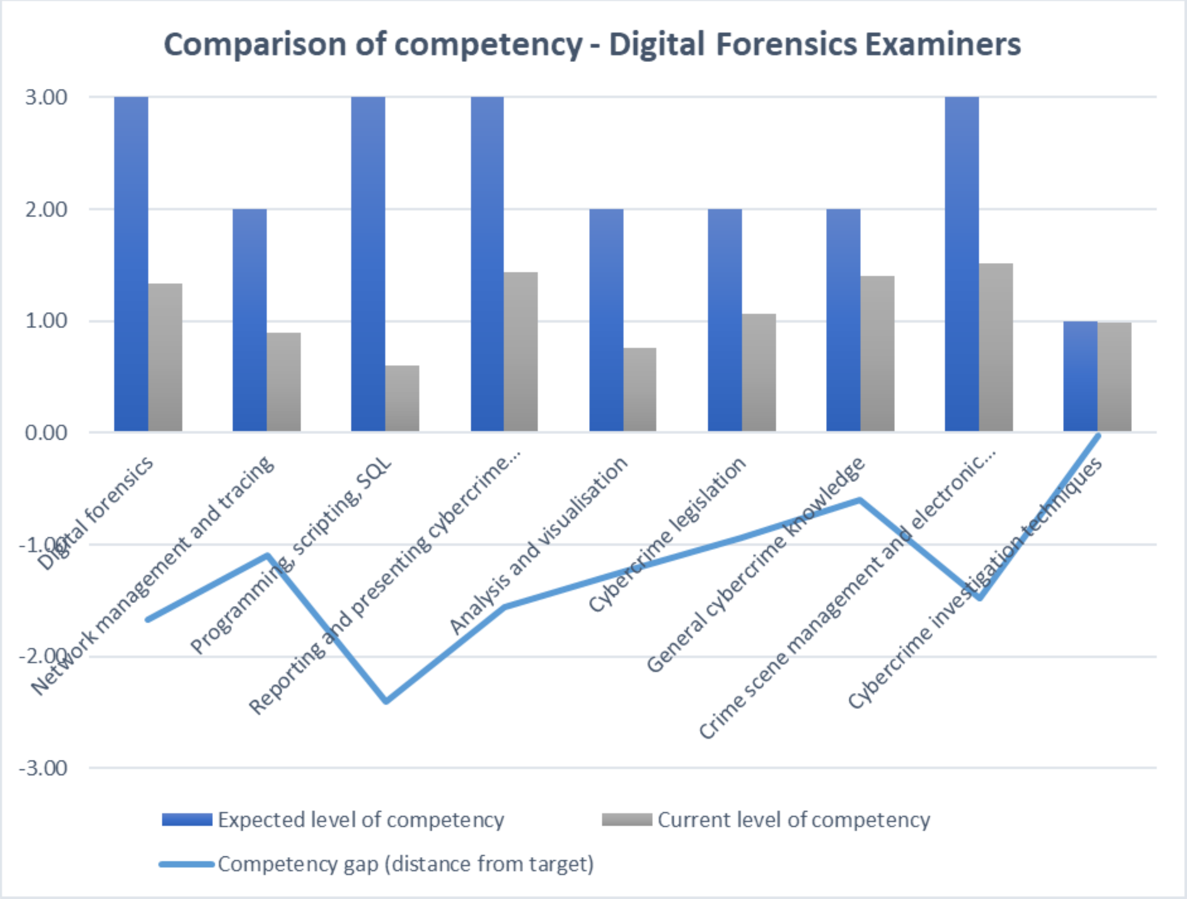

Figure 16. Competency level – Digital Forensics Examiners

A notable competency gap is found in all areas other than cybercrime investigation techniques. Across the topics, the respondents expressed the need for intermediate-level training, which is in line with the current competency remaining below target.

Table 18. Summary of competency development needs – Digital Forensics Examiners

	Digital forensics	Network management and tracing	Programming, scripting, SQL	Reporting and presenting cybercrime investigative data	Analysis and visualisation	Cybercrime legislation	General cybercrime knowledge	Crime scene management and electronic evidence handling	Cybercrime investigation techniques	Average
Expected level of competency	3.00	2.00	3.00	3.00	2.00	2.00	2.00	3.00	1.00	**2.33**
Current level of competency	1.33	0.90	0.60	1.44	0.76	1.06	1.40	1.52	0.98	**1.11**
Competency gap	-1.67	-1.10	-2.40	-1.56	-1.24	-0.94	-0.60	-1.48	-0.02	**-1.22**
Level of training required	2.04	2.10	1.58	1.98	2.00	1.65	2.18	2.04	2.02	**1.95**
Urgency of training required	36.69	28.00	26.50	22.00	26.00	22.00	25.50	32.00	29.50	**27.58**

In order to validate the findings on the role of Digital Forensics Examiner, based on data with Poland representing 76.00 %, alternative testing was conducted by taking a statistical average of all the Polish responses (competency, training need, urgency), considering the average as one response, and then recalculating according to the established procedure. With this method, the current competency (average of all topics) increased slightly, but not drastically (1.54 instead of 1.11 – rounded up, this would indicate intermediate-level rather than basic-level competency). On average, training needs would still be for intermediate level, and the urgency attributed to training even slightly lower. While this additional test suggests a slightly lower competency gap, it does not have a major impact on overall capacity development needs.

Table 19. Additional summary of competency development needs – Digital Forensics Examiners

	Digital forensics	Network management and tracing	Programming, scripting, SQL	Reporting and presenting cybercrime investigative data	Analysis and visualisation	Cybercrime legislation	General cybercrime knowledge	Crime scene management and electronic evidence handling	Cybercrime investigation techniques	Average
Expected level of competency	3.00	2.00	3.00	3.00	2.00	2.00	2.00	3.00	1.00	**2.33**
Current level of competency	1.52	1.14	1.11	1.94	1.35	1.71	1.71	1.88	1.52	**1.54**
Competency gap (%)	-1.48	-0.86	-1.89	-1.06	-0.65	-0.29	-0.29	-1.12	0.52	**-0.79**
Level of training required	2.22	1.60	1.51	2.30	2.15	2.04	2.54	2.23	2.46	**2.12**
Urgency of training required (%)	32.98	21.56	21.40	15.33	23.23	20.94	17.56	33.27	34.83	**24.57**

Incident Response Experts

Table 20. Sample characteristics – Incident Response Experts

Number of responses:	12
Number of countries represented:	7
Share of responding countries:	30.43 %
Names of countries represented:	Finland, Germany, Greece, Italy, Poland, Portugal, Slovakia
Sectors represented:	50.00 % Police, 25.00 % Border police/border guard, 25.00 % % Other
Responses referring to:	41.67 % Organisation, 58.33 % Individual

Incident Response Experts remain below the expected level of competency in all areas apart from analysis and visualisation. The most notable gaps concern the competencies related to **crime scene management and electronic evidence handling, network management and tracing** and **general cybercrime knowledge,** in relation to which the current competency is at basic level, while professionals in this role are expected to reach advanced level in these topics.

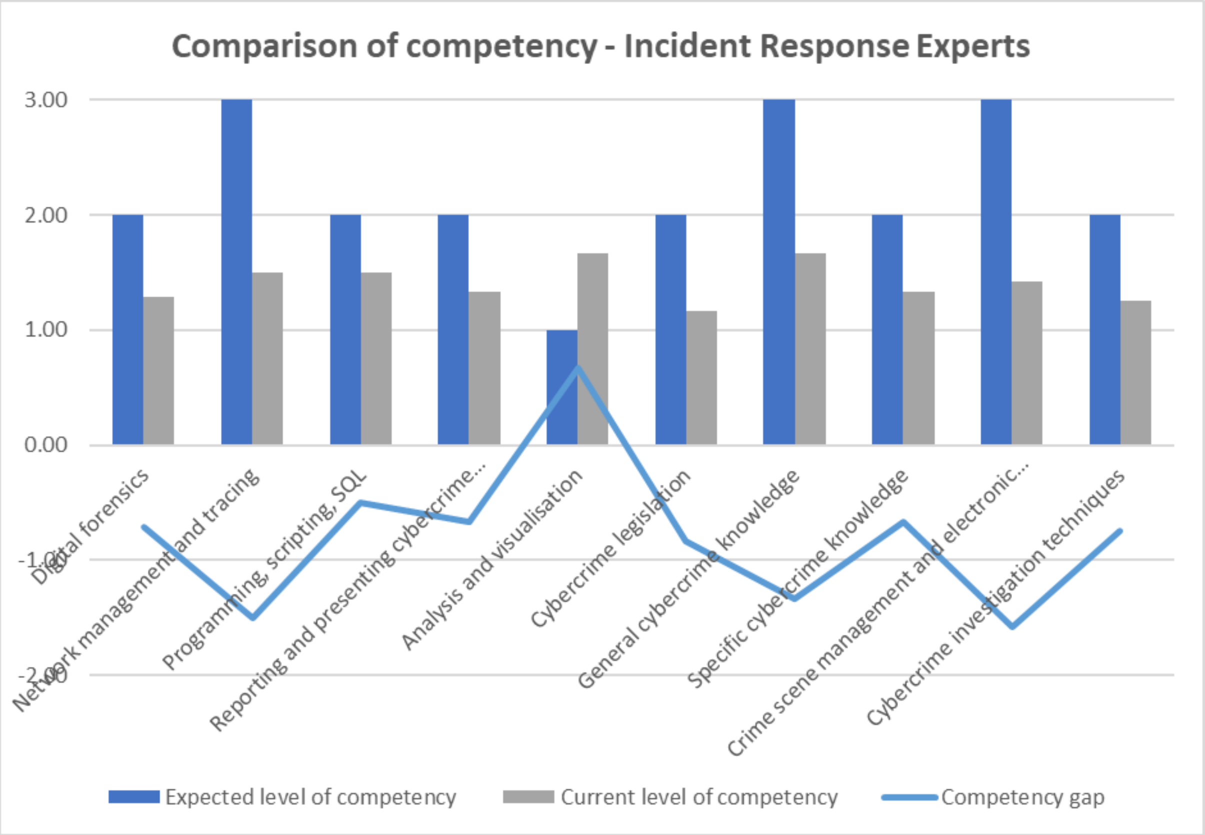

Figure 17. Competency level – Incident Response Experts

The findings suggest that the areas with the largest competency gaps should be addressed, but all other competency areas also requested advanced level training. However, respondents did not indicate a short timeline for training delivery, since only a secondary level of urgency is attributed to all topics. From this it can be inferred that training received within 2-3 years' time would be needed to stay up-to-date.

Table 21. Summary of competency development needs – Incident Response Experts

	Digital forensics	**Network management and tracing**	**Programming, scripting, SQL**	**Reporting and presenting**	**Analysis and visualisation**	**Cybercrime legislation**	**General cybercrime knowledge**	**Specific cybercrime knowledge**	**Crime scene management and electronic evidence**	**Cybercrime investigation**	**Average**
Expected level of competency	2.00	3.00	2.00	2.00	1.00	2.00	3.00	2.00	3.00	2.00	**2.20**
Current level of competency	1.29	1.50	1.50	1.33	1.67	1.17	1.67	1.33	1.42	1.25	**1.41**
Competency gap	-0.71	-1.50	-0.50	-0.67	0.67	-0.83	-1.33	-0.67	-1.58	-0.75	**-0.79**

Level of training required	1.99	2.17	2.08	1.92	2.17	2.08	2.00	2.11	1.83	2.00	**2.03**
Urgency of training required	24.74	29.17	20.83	25.00	27.08	22.92	27.08	32.44	27.08	31.25	**26.76**

First Responders

Table 22. Sample characteristics – First Responders

Number of responses:	6
Number of countries represented:	6
Share of responding countries:	26 %
Names of countries represented:	Finland, Greece, Malta, Poland, Portugal, Slovakia
Sectors represented:	83.33 % Police, 16.67 % Customs
Responses referring to:	83.33 % Organisation, 16.67 % Individual

The professionals that selected First Responders indicated that the current competency level among this group is at the expected level in the areas of **general cybercrime knowledge** and **cybercrime legislation**. **Digital forensics** is also very close to meeting the target.

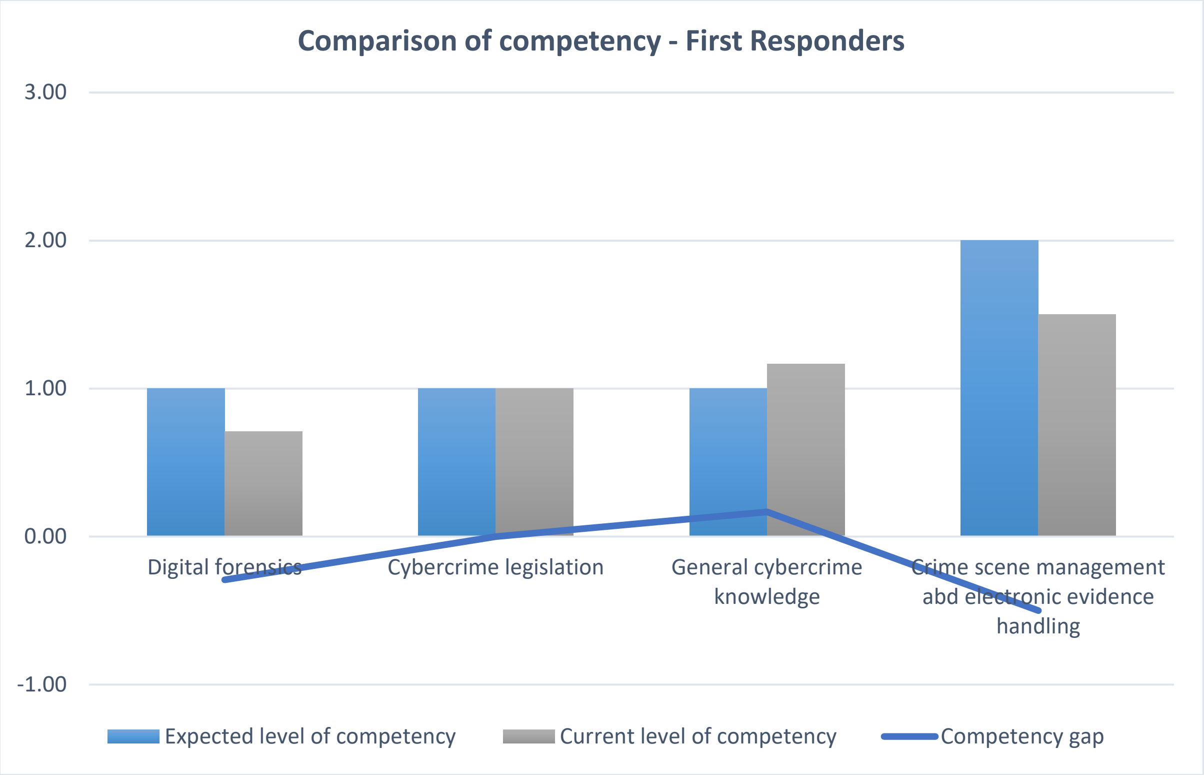

Figure 18. Competency level – First Responders

The average level indicted in terms of training required is basic level, which does not appear to be a very feasible response, especially for the areas where the expected level of competency has been already met. Based on the data, training for First Responders should focus on the topic of **crime scene management and electronic evidence handling**, primarily at intermediate level, and secondarily provide basic level training on **digital forensics** to close the remaining gap in that area.

Table 23. Summary of capacity development needs – First Responders

	Digital forensics	**Cybercrime legislation**	**General cybercrime knowledge**	**Crime scene management and electronic evidence handling**	**Average**
Expected level of competency	1.00	1.00	1.00	2.00	**1.25**
Current level of competency	0.71	1.00	1.17	1.50	**1.09**
Competency gap	-0.29	0.00	0.17	-0.50	**-0.16**
Level of training required	1.15	1.50	1.33	1.50	**1.37**
Urgency of training required	21.35	16.67	25.00	25.00	**22.01**

Trial and Appeal Judges

Table 24. Sample characteristics – Trial and Appeal Judges

Number of responses:	1
Number of countries represented:	0 countries, 1 agency
Share of responding countries:	N/A
Names of countries represented:	EUROJUST
Sectors represented:	100.00 % Judicial authorities
Responses referring to:	Unknown[26]

Only one respondent represented Trial and Appeal Judges. Furthermore, the received response did not specify whether it represented an individual or an organisation. Hence, the sample is not representative enough to draw conclusions concerning the wider population. The graph and table below summarise the results concerning competencies and training needs of Trial and Appeal Judges.

[26] The representativeness of the response was not specified by the respondent.

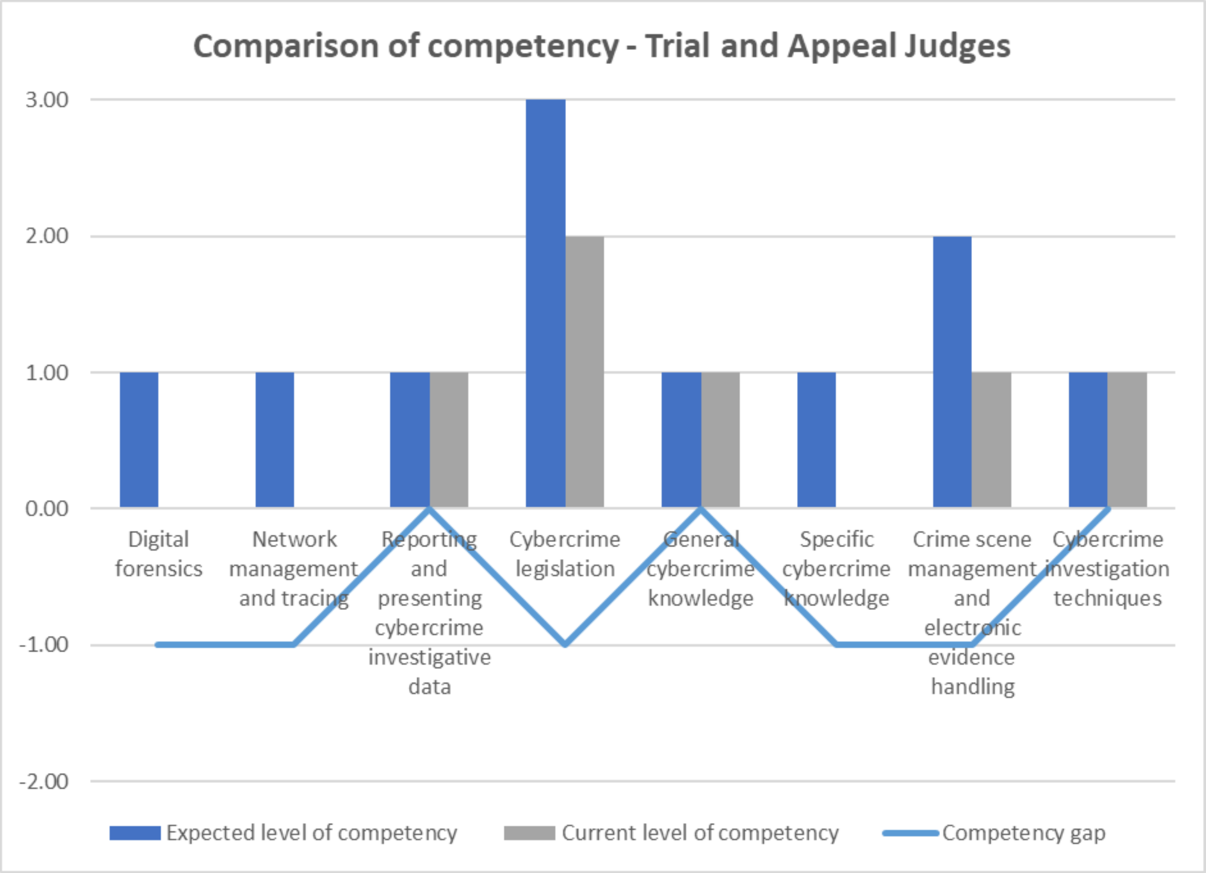

Figure 19. Competency level – Trial and Appeal Judges

Table 25. Summary of competency development needs – Trial and Appeal Judges

	Digital forensics	**Network management and tracing**	**Reporting and presenting cybercrime investigative data**	**Cybercrime legislation**	**General cybercrime knowledge**	**Specific cybercrime knowledge**	**Crime scene management and electronic evidence**	**Cybercrime investigation techniques**	**Average**
Expected level of competency	1.00	1.00	1.00	3.00	1.00	1.00	2.00	1.00	**1.38**
Current level of competency	0.00	0.00	1.00	2.00	1.00	0.00	1.00	1.00	**0.75**
Competency gap	-1.00	-1.00	0.00	-1.00	0.00	-1.00	-1.00	0.00	**-0.63**
Level of training required	1.00	1.00	1.00	2.00	1.00	1.14	1.00	1.00	**1.14**
Urgency of training required	25.00	25.00	25.00	25.00	25.00	25.00	25.00	25.00	**25.00**

Investigative Judges

Table 26. Sample characteristics – Investigative Judges

Number of responses:	8
Number of countries represented:	4 countries, 1 agency
Share of responding countries:	17.39 %
Names of countries represented:	Estonia, Latvia, Romania, Sweden, EUROJUST
Sectors represented:	87.50 % Police, 12.50 % Other, 12.50 % Unknown[27]
Responses referring to:	12.50 % Organisation, 75.00 Individual, 12.50 % Unknown[28]

Based on the results, the competencies of Investigative Judges remain below expected in all areas. The most notable gap concerns the topic of cybercrime legislation, where the expected level is advanced but the average current competency has not yet even met intermediary level. The current level in terms of reporting and presenting cybercrime investigative data is also -1.13 units below the expected level.

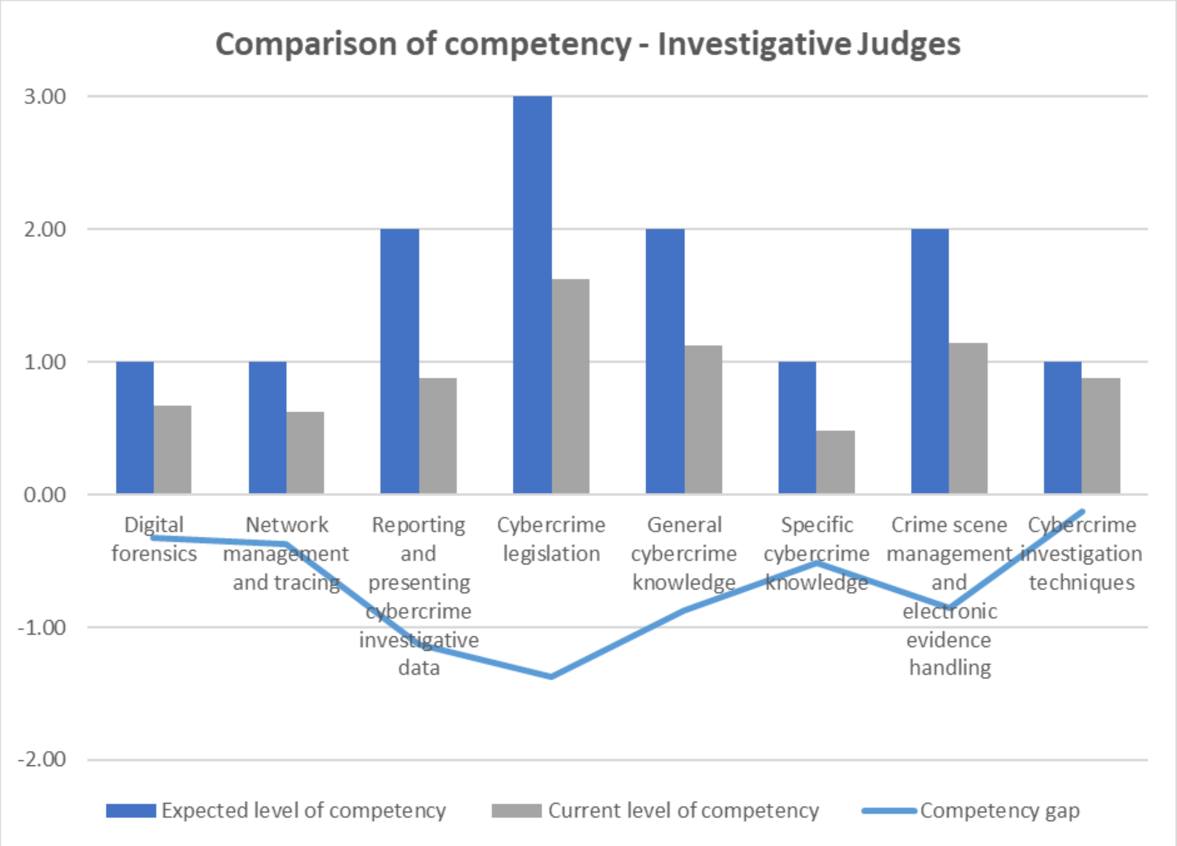

Figure 20. Competency level – Investigative Judges

[27] Sector not specified by one respondent.

[28] The representativeness of the response was not specified by one respondent.

Table 27. Summary of capacity development needs – Investigative Judges

	Digital forensics	Network management and tracing	Reporting and presenting cybercrime	Cybercrime legislation	General cybercrime knowledge	Specific cybercrime knowledge	Crime scene management and electronic	Cybercrime investigation techniques	Average
Expected level of competency	1.00	1.00	2.00	3.00	2.00	1.00	2.00	1.00	**1.63**
Current level of competency	0.67	0.63	0.88	1.63	1.13	0.48	1.14	0.88	**0.93**
Competency gap	-0.33	-0.38	-1.13	-1.38	-0.88	-0.52	-0.86	-0.13	**- 0.70**
Level of training required	1.58	1.63	2.13	2.25	2.00	1.68	2.25	2.00	**1.94**
Urgency of training required	24.22	21.88	31.25	37.50	34.38	27.68	28.13	31.25	**30**

For all competency areas, intermediary level training was requested. Considering the current level of skills, this might be necessary for the topics of **reporting and presenting cybercrime investigative data, crime scene management and electronic evidence handling,** and **specific cybercrime knowledge,** first at basic level. **In terms of digital forensics** and **network management and tracing,** the respondents indicate already being close to the expected (basic) competency level so these topics would not necessarily be a priority.

Conclusions

Considering the average of all cybercrime roles together[29], half of the competencies maintained a gap of more than >0.50[30] between the expected and current level of skills. In descending order, these include: **programming, scripting, SQL**; **reporting and presenting cybercrime investigative data**; **network management and tracing; specific cybercrime knowledge** as well as **crime scene management and electronic evidence handling.** In most roles, these topics, or some of them, are also among the most desired areas for further capacity development. However, further skills improvement concerns all competencies, and although the average gap for these is slightly less than 0.50, many professional roles will require training in digital forensics, analysis and visualisation and cybercrime legislation. Although with a smaller competency gap on average, training to improve general cybercrime knowledge and cybercrime investigation techniques also remains central for many roles. The key skills development needs for each role are summarised below.

Heads of Cybercrime Units' skills gap concerns three areas, namely **reporting and presenting cybercrime investigative data, cybercrime legislation and general cybercrime knowledge.** The results suggest that these competencies should be addressed as priority training for this cybercrime role, with training considered moderately urgent, so needed within a period of one year.

Team Leaders indicate the need for further capacity building in most areas, with the most notable competency gaps concerning **specific cybercrime knowledge** and **digital forensics**, where currently the average competency is closer to basic than the desired intermediate level. The need is for intermediate-level training, but with secondary urgency, meaning that training can be delivered in 2-3 years.

General Criminal Investigators responding to the survey currently possess a good level of competency in areas other than **crime scene management and electronic evidence handling.** The competency gap (-1.38 units) is notable, indicating that the experts serving in this role have not yet fully reached intermediate level, whereas the expectancy is they should be at advanced level. Results suggest that this competency area should be addressed through advanced-level training, although the need is of secondary urgency.

Cybercrime Analysts have considerable competency gaps related to **analysis and visualisation** and **general cybercrime knowledge;** the expected competency is advanced but it is currently closer to basic level. In these areas, intermediary-level training is required in order to build on competencies further and narrow the gap. **Programming, scripting and SQL** are also below the expected level, suggesting that experts in this role would request basic training. However, since the calculated average competency indicates that basic level has nearly been achieved, addressing this area at intermediary level might be the right training

[29] Including all roles associated with the different competency areas and based on the calculation of the average competency gap

[30] Gap ranging between -0.92 (programming, scripting, SQL) and -0.61 units (crime scene management and electronic evidence handling)

response. Regardless of the gaps in competencies, training is not considered more than secondarily urgent, and it is not crucial to be delivered sooner than during the coming 2-3 years.

Cybercrime Investigators' current level of competency is below the expected level in all areas except **digital forensics**. Intermediate-level training demand relates to all topics other than **cybercrime investigation techniques**, where training should be delivered for advanced-level professionals. Training needs are not more than secondarily urgent, apart from training on the topic of cybercrime investigation techniques, for which it would be advantageous to receive training within a year.

Cybercrime Experts are generally behind the expected level of competency, with currently only general cybercrime knowledge meeting the target. The largest gaps concern competencies related to **network management and tracing, specific cybercrime knowledge, cybercrime investigation techniques**, as well as **reporting and presenting cybercrime investigative data.** While advanced-level competency is expected for network management and tracing, actual competency is currently at basic level, and intermediary-level training is requested in order to gain advanced skills and knowledge. Competencies related to programming, scripting and SQL, and analysis and visualisation, are at basic level, but would require a level of intermediary training. Despite the centrality of the Cybercrime Experts role, the relatively high competency expectancy and the remaining competency gaps, the training needs do not indicate a high level of urgency. The need for training on cybercrime investigation techniques is moderately urgent; otherwise, it is considered sufficient if training is delivered with secondary urgency or even less. Regardless of the competency gap on the topic of reporting and presenting cybercrime investigative data, a low level of urgency is attributed to training needs, suggesting that training has a minor role in boosting performance.

Digital Forensics Examiners constituted the role that was most selected in the survey. Within this role, the current competency level of professionals is notably below the expected level in all topics except for cybercrime investigations techniques. The biggest gaps concern **programming, scripting and SQL**, **digital forensics**, and **reporting and presenting cybercrime investigative data**, where advanced competency is expected but the current level has barely met the requirements of basic level, and intermediate-level training in all competency areas is required. Current competencies related to **network management and** tracing and **analysis and visualisation** are also below basic, but the responses indicated the need for intermediary-level training. The training need is secondarily urgent in all areas, suggesting that while training would be useful for staying up-to-date, it is enough if that training is delivered within a few years' time.

Incident Response Experts' current level of competency remains below expected in all areas other than analysis and visualisation. The most notable gaps concern **crime scene management and electronic evidence handling, network management and tracing,** and **general cybercrime knowledge,** for which the current competency is at basic level, whereas professionals in this role are expected to reach advanced level on these topics. Training of professionals in this role is generally necessary at intermediate level, with secondary urgency – meaning no sooner than within a 2-3 year delivery cycle.

First Responders have reached a good competency level, meeting the targets established for **general cybercrime knowledge** and **cybercrime legislation**, and **digital forensics** is also very close to the expected level. In order to achieve the expected competency level, intermediate-level training is required on **crime scene management and electronic evidence handling**, but the training need is not urgent (secondary urgency).

Trial and Appeal Judges were represented by only one respondent; hence, the dataset is not representative enough to be able to draw conclusions about the wider population or cybercrime professionals serving in this role. A need for basic-level training was, however, indicated on most topics except for cybercrime legislation, which should be provided at intermediary level.

Investigative Judges are at below-expected level in all areas. The most notable gap concerns the topic of **cybercrime legislation,** where the expected level is advanced but the average current competency has not even reached intermediary level yet. The current level in **reporting and presenting cybercrime investigative data** is also below basic, whereas intermediate level was expected. The need for intermediary-level training is expressed for all areas. However, considering the existing competency gaps, **reporting and presenting cybercrime investigative data**, **crime scene management and electronic evidence handling**, as well as **specific cybercrime knowledge,** might also require training at basic level.

Annex 1. EU-STNA chapter on cyber-attacks

Cyber-attacks

Environmental challenges

Challenges identified in this area relate to the differences that exist in Member States' laws defining what constitutes a cyber-attack on information systems. These differences can obstruct the prevention, detection and sanctioning of cybercrime, as well as of other serious and organised crime related to and enabled by cybercrime. Furthermore, judicial cooperation becomes more complicated and therefore less effective, with negative consequences on cyber security. The admissibility of e-evidence originating from other countries is another legislative issue that needs improvement.

The private sector should be an ally of law enforcement authorities; however, there are several challenges hindering efficient cooperation. Private companies are in some cases reluctant to admit cyber-attacks, therefore criminal activities are largely underreported. Furthermore, private actors might face legal obstacles as regards sharing data with law enforcement or are unwilling to share them.

The number of cyber-attacks is growing while criminal methods are becoming more sophisticated. The rapidly increasing digitalisation of society and economy as well as the emergence of the Internet of Things create new vulnerabilities, which call for the strengthening of the capacity of law enforcement authorities. Unfortunately, high-cost forensic tools that could enhance the investigation of cyber-attacks remain unaffordable for law enforcement agencies in many Member States.

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

Challenges

Cybercrime services are increasingly offered online, being sold on the surface web and on the dark web, while criminals use cryptocurrencies to pay for them. The dark web also provides information on how to commit cybercrime. Since criminals use anonymisation, encryption and sophisticated techniques to cover digital traces, investigators of cyber-attacks should be aware of how to tackle these techniques.

The fact that criminal structures in this area are multifaceted, varying from organised groups and networks to lone offenders, developers, network administrators, intrusion specialists, mules or money launderers, poses a significant challenge in identifying and prosecuting offenders. Moreover, criminals quickly integrate technological developments into their operations, so law enforcement should have the capacity to keep pace.

The public and law enforcement officials not specialised in cyber-attacks lack situational awareness of the different types of cyber-attack, such as malware, web-based attacks, phishing, web application attacks, spam, distributed denial of service (DDoS), identity theft, data breach, insider threat, botnets, physical manipulation, damage, theft and loss, information leakage, ransomware, cyber-espionage, industrial espionage and cryptojacking. Therefore, the cybersecurity awareness of both law enforcement and the public needs substantial improvement.

The skills required by law enforcement agencies, prosecutors and the judiciary to combat cyber-enabled and cyber-dependent crime require significant development and adaptation to new technologies. Investigators of cyber-attack cases must have access to the latest online tools and develop alternative investigation techniques. It is imperative to develop the capacity of officials to perform big data and blockchain analyses, to deal with encryption, anonymisation and bulletproof hosting services, and to use new digital forensic tools.

Although the ability of law enforcement officials to properly manage digital evidence is key to the success of investigations, the capability gap related to identifying, handling, securing, preserving and analysing e-evidence remains a challenge.

Law enforcement should better understand and make use of the existing information exchange mechanisms as well as enhance its capacity to exchange e-evidence and use the SIRIUS platform. International cooperation between relevant law enforcement agencies and networks requires improvement. In addition, capacity building in non-EU countries experiencing rapid digital development seems highly necessary.

Training needs

Summary

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.

Awareness raising regarding cybersecurity, cyber-enabled and cyber-dependent crime, and cyber-attacks should target law enforcement, the judiciary and the public.

Member States indicated that 7 659 officials need training in this area.

Further details

Training covering the crime patterns and investigation techniques of cyber-attacks is imperative. It should focus primarily on the analysis of the latest cyber-attacks and the emergency response given by the EU as well as on how EU tools can be applied. Although ranked lower on the priority list, protocols to tackle large-scale cyber-attacks should also be included among the training topics.

Dealing with encryption, anonymisation and bulletproof hosting services is ranked high in terms of training priorities. Furthermore, it is important to cover the management of e-evidence from detection through handling, securing, preserving, analysing and exchanging to presentation in court.

In addition, training is required on the operation of criminal networks and on how crime-as-a-service is used by them. Although given slightly lower priority, training on criminal profiling and motivation analysis is also required.

According to the Member States, law enforcement officials also need training on EU cooperation and information exchange tools, such as the Joint Cybercrime Action Taskforce (J-CAT), the European Union Agency for Cybersecurity (ENISA), the Computer Emergency Response Teams (CERTs), Europol's European Cybercrime Centre (EC3), the European Cybercrime Training and Education Group (ECTEG) and the Computer Security Incident Response Teams (CSIRTs).

Raising awareness of cyber-attacks, cyber-enabled and cyber-dependent crime, cyber threats and cybercrime investigation is ranked seventh in terms of training priority; it should target law enforcement, the judiciary and the public.

Training on big data and blockchain analyses and on the use of AI, machine learning and deep learning in cybercrime investigation also seems necessary.

Guidance on ensuring respect for fundamental rights such as human dignity, liberty, non-discrimination, gender equality, privacy and data protection should form part of all training activities.

List of identified and prioritised training needs

The following list evidences the prioritisation, as carried out by the Member States, of topics in the area of training to combat 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

Annex 2. TCF Matrix[31]

	Digital Forensics	Network Management and Tracing	Programming, scripting, SQL	Reporting and Presenting Cybercrime Investigative Data	Analysis and Visualisation	Cybercrime Legislation	General Cybercrime Knowledge	Specific Cybercrime Knowledge	Crime Scene Management & Electronic Evidence Handling	Cybercrime Investigation Techniques
Heads of Cybercrime Units	🟩	🟩		🟧	🟩	🟦	🟦	🟩	🟩	🟩
Team Leaders	🟧	🟧	🟩	🟧	🟩	🟧	🟧	🟧	🟧	🟧
General Criminal investigators						🟩	🟩		🟦	🟩
Cybercrime Analysts			🟧		🟦	🟩	🟦	🟩		🟩
Cybercrime Investigators	🟩	🟩	🟩	🟧	🟧	🟧 *	🟧	🟧	🟦	🟦
Cybercrime Experts	🟧 *	🟦	🟧	🟦 *	🟧	🟧 *	🟧	🟦	🟧	🟦
Digital Forensic Examiners (Investigators)	🟦	🟧	🟦	🟦	🟧	🟧 *	🟧		🟦	🟩
Incident Response Experts	🟧	🟦	🟧	🟧	🟩	🟧 *	🟦	🟧	🟦	🟧
First Responders	🟩					🟩	🟩		🟧	
Trial and Appeal Judges	🟩	🟩		🟩		🟦	🟩	🟩	🟧	🟩
Investigative Judges and Prosecutors	🟩	🟩		🟧		🟦	🟧	🟩	🟧	🟩

LEGEND

🟩 **Basic**	Introductory understanding of the topic; knowledge of the main terms, areas and forms of application.
🟧 **Intermediate**	Above average understanding of the topic ; knowledge and skills to apply it in practice.
🟦 **Advance**	In-depth understanding of the topic ; highly developed knowledge/expertise and skills to perform complicated tasks.

[31] This is the latest draft of the TCF, not yet adopted.

Annex 3. Description of cybercrime roles[32]

Heads of cybercrime units

These professionals deal directly with cyber investigators and experts. They should take informed decisions in cybercrime cases and in other complex investigations involving cybercrime elements. Their role is to coordinate the structures under their command and their staff, allocate resources, prioritise policing activities and identify prevention activities in the area of cybercrime to be carried out by the responsible units. They should have a detailed overview of the capacity, capabilities and needs of the unit and provide it with the relevant training and tools that enable or facilitate the investigation and examination of the evidence. Their function is also to represent the unit when dealing with external stakeholders.

At least a minimum of hands-on practical experience to evaluate operational and strategic activities is recommended and so is the ability to communicate effectively with their staff and external experts. Knowledge of the English language is crucial for contributions and effective relationship management in the international environment involving stakeholders from different jurisdictions and organisations such as CEPOL, Eurojust or Europol.

Team leaders

These professionals engage directly with cybercrime investigations, investigators and experts (cybercrime, digital forensics) within the assigned area. They should take informed decisions in cybercrime cases or in other complex investigations involving cybercrime elements. Their role is to coordinate staff, allocate resources and prioritise policing activities. They should have a detailed overview of the capacity, capabilities and the needs of the team for strategic planning. They should also ensure that the team has relevant training and tools that enable or facilitate investigative activities and examination of the evidence.

Practical experience of evaluating operational and strategic activities is highly recommended as well as the ability to communicate effectively with their staff and external experts. Knowledge of the English language is important for international cooperation and exchanging of best practices.

Cybercrime investigators

These officials are law enforcement investigators specialised in cybercrime with an extra capacity to seize electronic data and support normal investigations with cyber-related activities. They should have a more in-depth understanding of data extraction and interpretation, including online information acquisition and seizure. They also lead cybercrime investigations, interviews and other investigative and judicial processes in cybercrime cases where the use of digital evidence is concerned. Their experience and expert knowledge make them suitable candidates for ‘train the trainer’ programmes.

[32] The descriptions of the roles are extracted from the latest draft of the TCF (not yet adopted).

Cybercrime experts

They are law enforcement officials who specialise in cybercrime and have specific cybercrime knowledge and skills in their area of expertise. They support the cybercrime investigation and other investigative and judicial processes in cybercrime cases where the use of digital evidence is concerned. The specialisation of cyber-crime experts can range from specific forms of intelligence gathering to in-depth understanding of specific technologies that are encountered in investigations.

Cyber-crime experts need to keep their competencies up-to-date by exchanging experience, lessons learned, and expertise with peers at the national and international levels. They also have the capacity to advise the authorities on potential threats and contribute to prevention.

Cybercrime analysts

These professionals either focus on strategic analysis, researching, analysing and presenting the latest threats and providing situational overviews, or they could be engaged in operational analyses to find patterns, trends and hotspots and create links between live cases. They need to be able to process large amounts of data from different sources and translate these into concise reports clearly outlining the issues in question while offering actionable recommendations. They should spread the relevant knowledge throughout the organisation through preparing written materials, training and their inclusion in strategic and operational meetings. They also need to be able to share information with wider audiences, such as in national or international reports of general interest.

Digital forensic examiners (investigators)

These professionals perform detailed forensic examinations of computer-based digital evidence. They should be familiar with different operating systems, know relevant commercial and open-source tools, have scripting/programming and database querying skills, understand forensic artefacts and data carving, have a basic understanding of cryptography and be able to prepare evidence for advanced decryption tasks, report and present their results. It is not necessary that they are multi-domain experts but they should be reference points for their own area of specialisation.

They should serve as a source of technical counsel and advice for investigators requiring forensic support. They should have skills to perform advanced forensic activities and keep them up to date.

Incident response experts

This role includes professional law enforcement representatives who facilitate cooperation with other entities (ENISA, CSIRT, CERT, related IT departments) when responding to cyber-attacks and incidents. They are responsible for initiating coercive technical countermeasures, as well as acquiring, preserving, analysing and documenting complex (digital) traces and electronic evidence.

Their actions guarantee quality and efficiency of the response to cyber-attacks in order to preserve digital evidence for investigation and prosecution, including international judicial cooperation from first response to presentation in front of judicial courts. They have a good command of the English language and are able to effectively communicate with the parties involved, different authorities and the public.

General criminal investigators

Investigators in other crime areas will increasingly encounter crimes facilitated by the internet and new technologies. To deal with that successfully they should at least obtain a fundamental understanding of the digital world.

One key issue will be how to integrate electronic evidence into a normal crime investigation process. In general, these professionals should become more digitally aware, particularly when it comes to seizing relevant electronic evidence at crime scenes. Their training should provide a clear list of dos and don'ts for digital seizures, handling digital material, basic legislation, and dealing with specialised colleagues.

In addition, investigators should be able to fully appreciate the amount of intelligence that may be generated by open-source intelligence and use the information effectively to complement their investigations.

First responders

A first responder is a law enforcement professional who is the first official to come into contact with potential electronic evidence. Patrol police officers, detectives and border and tax controllers are all examples of first responders. The first responder is an essential actor in the forensic process and can influence the efficiency and effectiveness of criminal investigations.

These professionals require basic knowledge of digital forensic features, including live data forensics, as well as general knowledge about cybercrime. The first responder's responsibilities may entail identifying, collecting, packaging, transferring and storing devices that can contain electronic evidence at a crime scene depending on national regulation and good practices. Depending on the country, a first responder could be expected to perform an urgent forensic intervention to preserve fragile or volatile electronic evidence. A first responder needs to understand which traces may be recovered by a specialised forensic examiner and how these traces may contribute to further investigation that will facilitate communication and reporting.

The first responder should also be able to gather information at the crime scene and document all findings, ensuring the correct chain of custody. They should also be able to provide basic advice to victims of cyber and cyber-enabled crimes.

Trial and appeal judges

This category includes judges who examine cybercrime cases. Judges play a key role in the justice system, assessing the evidence and adjudicating a case.

In most EU Member States, no judges specialise in 'cybercrime'. Thus, all judges should acquire a basic knowledge of cybercrime and e-evidence, which is kept up to date. One key issue will be how to integrate cyber evidence into a normal crime investigation process. These professionals should generally become more digitally aware, particularly regarding seizing relevant evidence at crime scenes, handling digital material, basic legislation, and dealing with specialised colleagues.

Given the increasing prominence of cyber-elements in general criminal cases and the proliferation of cybercrime, it is foreseen that a basic knowledge may not suffice for a proper and just application of the law by judges. For this reason, the competency framework for judicial authorities distinguishes between general practitioners and specialists.

Investigative judges and investigators

Depending on the jurisdiction, prosecutors and investigative judges may direct or oversee criminal investigations, assess the necessity, proportionality and subsidiarity of the collection of electronic evidence, and authorise special means of investigation. Prosecutors have the prerogative to bring criminal cases before the courts and present the case in court, assessing as a first filter the evidence of a case to be presented in court. To deal with that successfully, they should obtain a basic knowledge of the digital world.

Investigative judges direct the criminal investigation and assess the necessity, proportionality and subsidiarity of the collection of electronic evidence, authorising special means of investigation.

One key issue will be integrating cyber evidence into a normal crime investigation process. These professionals should generally become more digitally aware, particularly regarding seizing relevant evidence at crime scenes, handling digital material, basic legislation, and dealing with specialised colleagues.

In addition, prosecutors and investigative judges should be aware of the amount of intelligence that may be generated by open-source intelligence and use the information effectively to complement their investigations.

Annex 4. 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 has 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 (upcoming) 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.

Annex 5. List of national or international training attended

Profile	Topic or aim	Level	Target group	Organiser
Team Leaders	Malware analysis	Intermediate	EMAS	Europol
	Live Fire	Advanced	Information security	Cyberbit
General Criminal Investigators	New programs, analytics of malware	Basic	Experts	MediaRecovery
Cybercrime Analysts	New programs, analytics of malware	Basic	Experts	MediaRecovery
	Increased knowledge of network analysis	Intermediate	IT experts	The Norwegian Police University College
	Not specified	Intermediate	Cyber forensic analysts	CLKP
	Network forensics	Intermediate	Not specified	Police
	Ciber Perseu Threat Hunting	Intermediate	Government officials	Portuguese army
	Live Fire	Advanced	Information security	Cyberbit
Cybercrime Investigators	Tactical Reverse Engineering	Basic	Cyber Analyst	FBI
	Network forensics	Intermediate	Not specified	Police
	Investigations	Advanced	Cybercrime Investigators	Police College Baden-Wuerttemberg
	Dark web and cryptocurrencies	Advanced	Police	CEPOL
Cybercrime Experts	Cyber Intelligence	Intermediate	Cybercrime Experts	CEPOL
	Network forensics	Intermediate	Not specified	Police
Digital Forensics Examiners	Conducting searches on Various IT Devices	Basic	Not specified	CEPOL
	Cyberattack simulation, identifying the attacker	Basic	Not specified	Not specified
	Law enforcement agents; civil servants	Basic	Not specified	Multiple, CEPOL; CNCS; IPAI; CNCS; INA

	DFIR	Basic	Experts	Mediarecovery
	Improved skills in the field of obtaining data from mobile devices, image recording devices and computers[33]	Basic	Police	ForSec
	Pen testing eJPT	Basic	Everyone	eLearn Security
	Increasing the effectiveness of the police in obtaining data from image recording devices[34]	Basic	Specialist and experts	FORSEC
	Live data forensics	Intermediate	Not specified	CEPOL
	Innovative tools for the acquisition and protection of digital data	Intermediate	Police	Centralne Laboratorium Kryminalistyczne Policji
	Increased knowledge of network analysis	Intermediate	IT experts	The Norwegian Police University College
	Network forensics investigations	Intermediate	network forensics	CLKP
	Network forensics intermediate	Intermediate	IT Forensic Experts	Norwegian Police University College
	Network forensics intermediate	Intermediate	IT Forensic Experts	Norwegian Police University College
	Mobile Forensic	Intermediate	Experts	Forsec
	Increase skills	Intermediate	Civil servants	Global Network Systems, Inc (**GNS**)
	Classified Information	Intermediate	Not specified	Portuguese National Cybersecurity Centre (CNCS)

[33, 28] Inputs submitted in a national language (Polish) are machine translated into English.

Incident Response Experts	Simulated Cyber Attack	Intermediate	Security Team	CNCS
	Live Fire	Advanced	Information security	Cyberbit
Investigative Judges	Digital Evidence Workshop	Basic	Eastern European Judges and Prosecutors	DOJ ICHIP

Annex 6. Training proposed for accreditation or certification

Modules or programmes
Academically accredited study programmes: e.g. MSC in Cybersecurity
Cybercrime Managers' certification
First Responders' training
Computer Forensics Expert Certificate
All CEPOL training
Certified Forensic Analyst
Standalone topics or knowledge prospects
Blockchain
Cloud data analysis
Cloud forensics
Computer forensics: new technologies and chipsets
Cryptocurrencies
Cybercrimes involving programming by the perpetrator(s): basic coding languages
Cybersecurity and digital forensics (CSE)
Dark web
Data recovery
Digital Forensics, including investigations
Filesystem analysis and forensics
Forensics: all knowledge areas
General cybercrime knowledge; GDPR; analysis and visualisation
Handling digital evidence: all training
Identifying security breaches and threat prevention
Incident response
Internet of Things (IoT)
Live data forensics
Network analysis and forensics
Malware analysis
Mobile Forensics
Network analysis and forensics
Network security
OSINT, including investigations
Other suggestions
ACE – Access Data Certified Examiner
BTL1 – Security Blue Team Level 1
BTL2 – Security Blue Team Level 2
CAP – Certified Authorization Professional
CASP+ – CompTIA Advanced Security Practitioner
CAWFE – Certified Advanced Windows Forensic Examiner
CBCI – Certificate of Business Continuity Institute
CBCP – Certified Business Continuity Professional
CCE – Certified Computer Examiner
CCFE – Certified Computer Forensics Examiner
CDRP – Certified Data Recovery Professional
CEDS – Certified E-Discovery Specialist
CEH – Certified Ethical Hacker

CEH Master – Certified Ethical Hacker Master
Certified Reliability Professional
Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001
Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301
Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert
CFSR – Certified Forensic Security Responder
CGAP – Certified Government Auditing Professional
CGEIT – ISACA's Certified in the Governance of Enterprise IT
CHFI – Certified Hacking Forensic Investigator
CIA – Certified Internal Auditor
CISA – Certified Information Systems Auditor
CISM – Certified Information Security Manager
CISSP – Certified Information Systems Security Professional
CMFE – Certified Mobile Forensics Examiner
CNFE – Certified Network Forensics Examiner
COBIT Foundation
CPENT – Certified Penetration Testing Professional
CPT – Certified Penetration Tester
CRISC – ISACA's Certified in Risk and Information Systems Control
CSSLP – Certified Secure Software Lifecycle Professional
CySA+ – CompTIA CySA+
eCDFP – eLearnSecurity Certified Digital Forensics Professional
eCMAP – eLearnSecurity Certified Malware Analysis Professional
EnCE – EnCase Certified Examiner
GASF – GIAC Advanced Smartphone Forensics
GAWN – GIAC Assessing and Auditing Wireless Networks
GBFA – GIAC Battlefield Forensics and Acquisition
GCCC – GIAC Critical Controls Certification
GCDA – GIAC Certified Detection Analyst
GCFA – GIAC Certified Forensic Analyst
GCFE – GIAC Certified Forensic Examiner
GCIH – GIAC Certified Incident Handler
GCPM – GIAC Certified Project Manager
GCPN – GIAC Cloud Penetration Tester
GCSA – GIAC Cloud Security Automation
GCTI – GIAC Cyber Threat Intelligence
GDAT – GIAC Defending Advanced Threats
GISP – GIAC Information Security Professional
GMOB – GIAC Mobile Device Security Analyst
GMON – GIAC Continuous Monitoring Certification
GNFA – GIAC Network Forensic Analyst
GOSI – GIAC Open Source Intelligence
GPEN – GIAC Penetration Tester
GPYC – GIAC Python Coder
GREM – GIAC Reverse Engineering Malware
GSE – GIAC Security Expert
GSLC – GIAC Security Leadership
GSNA – GIAC Systems and Network Auditor
GSOC – GIAC Security Operations Certified

GSOM – GIAC Security Operations Manager

GSSP – GIAC Secure Software Programmer

GSTRT – GIAC Strategic Planning, Policy and Leadership

GWAPT – GIAC Web Application Penetration Tester

GWEB – GIAC Certified Web Application Defender

GXPN – GIAC Exploit Researcher and Advanced Penetration Tester

ITIL Foundation

ITIL Managing Professional

ITIL Master

LPT – EC Council Licensed Penetration Tester

OSCE3 – Offensive Security Certified Expert 3

OSCP – Offensive Security Certified Professional

OSED – Offensive Security Exploit Developer

OSEE – Offensive Security Exploitation Expert

OSEP – Offensive Security Experienced Penetration Tester

OSMR – Offensive Security macOS Researcher

OSWA – Offensive Security Web Assessor

OSWE – Offensive Security Web Expert

OSWP – Offensive Security Wireless Professional

PenTest+ – CompTIA PenTest+

Security+ – CompTIA Security+

SSCP – Systems Security Certified Practitioner

Annex 7. Digital forensics – details on subtopics

	Live Data Forensics	OS Forensics (Mac, Windows, Linux ...)	File System Forensics	Mobile Forensics	Network Forensics	IoT Forensics	Cloud Forensics	Cryptography (e.g. decryption)
Heads of Cybercrime Units								
Current competency	2.00	2.10	2.10	2.20	1.90	1.10	1.40	1.20
Level of training required	2.50	2.20	2.10	2.10	2.50	2.00	2.10	1.80
Urgency of training	7.50	10.00	7.50	20.00	22.50	22.50	25.00	20.00
Team Leaders								
Current competency	1.33	2.00	1.78	1.25	1.33	1.00	0.78	1.11
Level of training required	2.33	2.00	2.00	2.33	2.22	1.78	1.78	1.67
Urgency of training	11.11	8.33	8.33	27.78	13.89	16.67	16.67	22.22
Cybercrime Investigators								
Current competency	1.16	1.32	1.32	1.32	1.28	0.89	0.84	0.95
Level of training required	2.16	2.16	2.11	2.32	2.26	2.11	2.00	1.95
Urgency of training	28.95	26.32	26.32	32.89	28.95	34.21	34.21	35.53
Cybercrime Experts								
Current competency	1.91	1.64	1.64	1.73	1.82	1.27	1.18	1.55
Level of training required	2.27	2.18	2.00	2.27	2.36	2.27	2.18	2.18
Urgency of training	36.36	31.82	36.36	31.82	38.64	31.82	34.09	31.82
Digital Forensics Examiners								
Current competency	1.47	1.76	1.72	1.96	1.20	0.90	0.78	0.86
Level of training required	2.40	2.40	2.31	2.56	2.02	2.02	1.84	1.86
Urgency of training	35.50	40.00	35.00	49.00	33.00	30.50	35.50	35.00

Incident Response Experts								
Current competency	1.58	1.75	1.67	1.00	1.67	0.75	0.83	1.08
Level of training required	2.25	2.08	2.00	1.58	2.25	1.83	1.75	2.17
Urgency of training	35.42	27.08	22.92	22.92	25.00	20.83	20.83	22.92
First Responders								
Current competency	0.83	0.83	0.83	0.83	0.67	0.67	0.50	0.50
Level of training required	1.17	1.00	1.00	1.50	1.17	1.00	1.00	1.33
Urgency of training	20.83	16.67	16.67	29.17	16.67	20.83	20.83	29.17
Trial and Appeal Judges								
Current competency	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Level of training required	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Urgency of training	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Investigative Judges								
Current competency	0.75	0.75	0.75	0.75	0.75	0.50	0.75	0.38
Level of training required	1.50	1.50	1.38	1.75	1.75	1.38	1.88	1.50
Urgency of training	28.13	21.88	25.00	25.00	25.00	21.88	21.88	25.00

Operational Training Needs Analysis

Cyberattacks

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