CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

# Operational Training Needs Analysis
# Cybercrime – Attacks against Information Systems

EDUCATE, INNOVATE, MOTIVATE

# Operational Training Needs Analysis
# Cybercrime – Attacks against Information Systems

## 2019

# Operational Training Needs Analysis. Cybercrime – Attacks against Information Systems

## Background

Preventing and fighting cybercrime, as well as enhancing cybersecurity forms a priority under the Internal Security Strategy 2015-2020 (ISS) of the European Union. The mid-term review of the ISS underlined the need to strengthen the fight against cybercrime by regularly analysing the threat picture as well as the evolving nature of cyber-enabled crimes, and adjusting the policy tools accordingly with a focus on prevention and improved operational cooperation, just as to ensure the availability of effective investigative tools, that correspond to the digital age and respond to the evolving Internet Governance challenges. The EU Policy Cycle on Serious and Organised Crime 2018-2021 also defines fighting cybercrime as one of the priorities.

Acknowledging the above mentioned, CEPOL has identified cybercrime as one of its key priorities for the upcoming years. Towards this end, a more detailed analysis (TNA) of the training needs has been performed in the area of cyber-attacks against information systems based on the Training Competency Framework (TCF).

Furthermore, in order to respond to the growing training demand in the area of cyber, CEPOL has strengthened its cyber-training portfolio and established the European Cybercrime Training Academy, which is properly equipped and configured to train 80 participants simultaneously and becomes fully operational in 2019. Throughout the year, CEPOL will implement 15 residential cyber-training activities aiming to reach over 400 participants from different Member States.

This research assesses training needs against the necessary competencies law enforcement officials should have in order to perform their duties. The level of necessary competencies is defined in the Training Competency Framework (Annex 1.) The analysis provides an understanding of training needs from two perspectives. On the one hand, it compares the current level of knowledge of law enforcement officials performing different roles in investigations of cyberattacks against information systems to the level of knowledge necessary to fulfil their obligations. On the other, it sheds light on where respondents see there is a need for training and gives a picture of the dimensions of training need such as the level, form, urgency and number of participants who would need training.

This paper is structured as follows. The Executive summary offers an overview of the priorities to be addressed by training of law enforcement officials in different profiles and competencies. Section two describes the methodology of the survey, the process of data gathering and the process of the analysis. The third part describes training needs related to each role defined by the Training Competency Framework with special focus on the competencies necessary to fulfil the given roles.

## Executive Summary

The training needs analysis (TNA) on Cybercrime – attacks against information systems was launched in December 2018 in the form of an online survey. This resulted in 24 responses from 17 Member

States[1], Iceland, Switzerland and Europol's EC3, reflecting a 60% response rate on behalf of EU Member States[2]. Most respondents (79%) are employed by police and three-quarters of respondents represent a cybercrime unit, mostly on national level.

The general level of knowledge of law enforcement is between basic and expert level in all competencies, therefore, a gap in knowledge can be traced where the training competency framework expects expert level knowledge. However, training need is indicated in all competencies, even in those where current level of knowledge exceeds the basic level set by the competency framework.

**In terms of profiles, law enforcement management has the largest gap between their current level of knowledge and the level set by the TCF and accordingly they indicated the highest rate of training need**.

**A significant gap in knowledge exists in the profiles of digital forensic investigators and examiners, cyber experts, general criminal investigators and first responders, however in the two latter profiles a lower level of training need was signalled by respondents.**

**The level of current knowledge of heads of cybercrime units and team leaders exceeds the level set by TCF. At the same time, they indicated quite a high level of training needs second in rank among all profiles**.

**The number of participants who need training is the highest among general criminal investigators followed by first responders and online investigators**.

As for competencies, the largest gap in knowledge is in the competency of first responder where the existing level of knowledge is 79% lower than the expected level of knowledge across all roles. Different gaps remain significant, but are meaningfully lower such as in the competencies of live data forensics (39%), analytical and visualisation (32%) interviewing and interrogation (31%), programming, scripting and SQL (30%) and cybercrime legislation (29%). In the competencies of open source intelligence and internet networking and tracing law enforcement officials investigating cyberattacks against information systems have higher level of knowledge than set by the TCF. Still, most participants would need training in these two latter competencies according to respondents, meaning that they feel necessary to improve their knowledge in these fields.

Altogether 39.718 law enforcement officials would need training in the different competencies and profiles. This would mean 144.209 law enforcement officials to be trained in the 26 Member States. This number in reality is probably lower since there should be overlaps among the target groups of the training. Webinar series are to be attended by most participants while only 10% of participants would take part in residential activities. Basic level of training should be delivered for 60% of participants and expert level to the remaining 16.071 law enforcement officials.

The training need is relatively urgent, in general, as it should be delivered between 6 months and 1 year. **The training is most urgent for cybercrime analysts, intelligence officers, digital forensic**

[1] Member States taking part in the survey were: Austria, Belgium, Cyprus, Czech Republic, Germany, Greece, Hungary, Ireland, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia and the United Kingdom.

[2] The terminology `Member States` hereinafter refers to 26 Member States of the European Union participating in CEPOL regulation, i.e. all EU Member States excluding Denmark and the United Kingdom.

**investigators and examiners while it can be delivered in a year to intermediate and advanced intelligence officers and to law enforcement management**.

Existing training is scarce in all roles and competencies, meaning that around 10% of respondents indicated available national level training activities. The profile where most training is available is of digital forensic investigators and examiners. The competency most targeted by training on national level is of open source intelligence. Less than 10% of respondents indicated available national level training in the competencies of programming, scripting, SQL, analytical and visualisation, cybercrime legislation and interviewing and interrogation. In the profiles of intermediate and advanced intelligence officers, online investigators, cyber experts and first respondents there is little training available on national level.

## Methodology

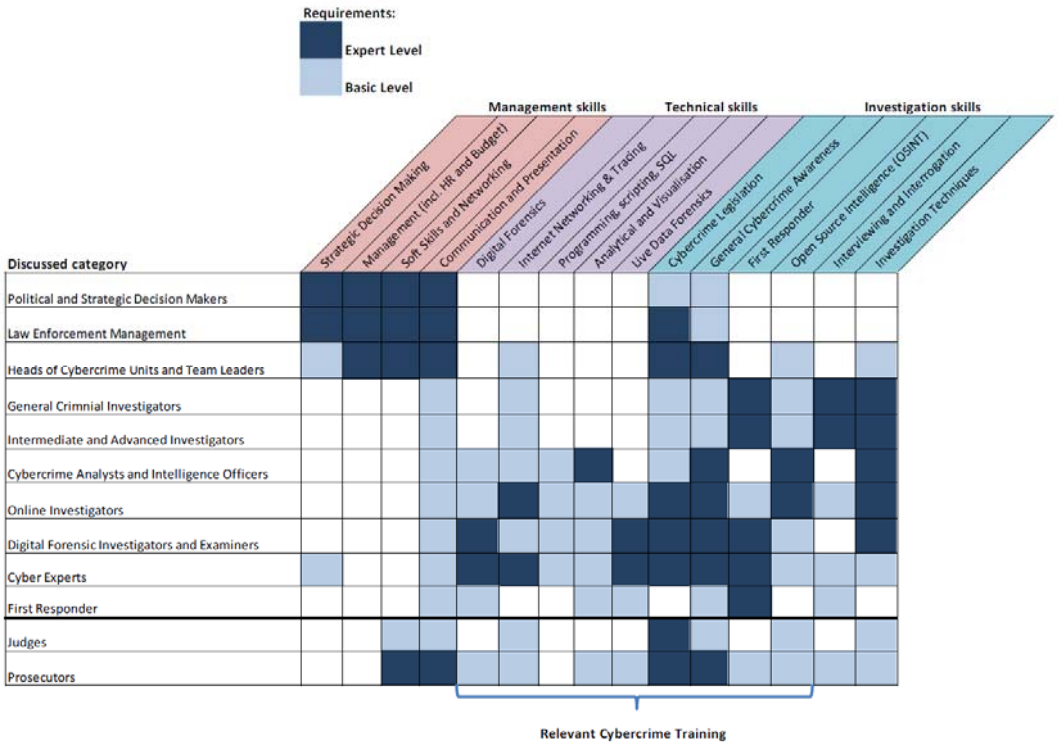
In order to ensure that a comprehensive training portfolio is also developed for 2020, CEPOL is conducting a TNA on attacks against information systems on European level with a blended methodology. The analysis as well as the consequent prioritisation of training needs and the design of the training portfolio is a joint effort coordinated by CEPOL in cooperation with Europol`s EC3, ECTEG, EUCTF, Eurojust, European Commission and EJTN – all organisations members of the so called Training Governance Model (TGM).

According to the applicable TNA methodology, the following steps have to be carried out:

| Design and launch questionnaire | → | Analyse data (interviews if necessary) | → | Validation workshop | → | Training portfolio design by an expert group |
|---|---|---|---|---|---|---|
| December 2018 | | April 2019 | | May 2019 | | June-July 2019 |

The TNA survey questionnaire was developed and launched by CEPOL in coordination with the TGM members in December 2018. The questionnaire was based on the Training Competency Framework and in line with Training Governance Model aims at gathering data on training needs of law enforcement officials across the European Union.

Image 1. Training Competency Framework




The questionnaire consists of two parts, the first analyses training needs and the second gathers data about existing training for each competency under each role.

The first part of the questionnaire asks respondents about training needs of law enforcement officials in each competency related to technical and investigation skills of each role defined by the TCF.

Competencies related to management skills and to roles of judges and prosecutors were not addressed in the survey.

Respondents were required to answer questions on

- the current level of knowledge in each competency under each role;
- whether they see a need for basic or expert level training;
- how urgent this training should be delivered with how many participants and in what form;
- the risks of not addressing the training need.

In the second part of the survey, respondents were asked to share details of existing training on national level, whilst referring to

- whether the training is a regular, an ad-hoc or a mandatory activity;
- the proficiency level of the training;
- the institution that delivers the training;
- the aim, target group and the number of participants taking part in the activity.

## Data gathering

The questionnaire was launched on an online platform, Limesurvey, in December 2018 and ended in January 2019. The questionnaire could be filled in through an open link that was forwarded to different target groups. In September 2018, CEPOL approached CEPOL National Units in 26 Member States to provide direct contact points in law enforcement agencies dealing with the subject of the cyberattacks against information systems of their respective countries. 20 MS and Europol responded to this initiative by providing contact points to 39 experts. Moreover, the questionnaire was sent to these nominated contact points. The questionnaire was also sent to members of the European Union Cybercrime Task Force by Europol and further distributed in the network of the ECTEG. Data gathering was closed in the end of January 2019.

## Analysis

Data analysis was performed by CEPOL between February and April 2019.

After eliminating some duplications text answers were translated into numeric codes as described in the table below.

Numeric values of texts

| **Text** | **Numeric value** |
|---|---|
| Yes | 1 |
| No | 0 |
| No knowledge | 0 |
| Basic level knowledge | 1 |
| Expert level knowledge | 2 |
| Urgency rate: Low (More than 12 months) – training would improve the performance, however, not significantly. | 1 |
| Urgency rate: Medium (6-12 month) – training is important to perform qualitatively. | 2 |
| Urgency rate: High (less than 6 months) – training is crucial for the successful performance of duties. | 3 |

First, the average of current level of knowledge indicated by respondents was calculated for each competency under each role and was compared to the level of knowledge set by the TCF, which resulted in a numeric value indicating the **gap in knowledge**.

Second, the ratio of respondents indicating that there is a need for training was calculated as follows. Number of 'yes' responses to basic level training needed/expert level training needed/no training is needed was divided by the overall number of responses to a given profile. This enables to understand how relevant respondents find training in each proficiency level for competency under each role. The **training need** in a given competency was calculated by subtracting the ratio of answers 'no training is needed' of 1.

Third, where training need on basic or expert level was indicated, the **urgency level** of training was defined by the maximum urgency level of training need specified by respondents in a given competency of a given role.

Fourth, the **number of participants** for each level of training and each form of training for each competency for every role was calculated by adding up the number of participants indicated by respondents. The median of these responses was calculated and multiplied by 26 to get an understanding of potential number of participants who would need training in a certain competency on EU level.

Fifth, the ratio of 'there is **national level of training**' in a certain competency in a certain role was calculated by diving the number of 'yes' responses by the number of all responses.

Sixth, **features of national level training activities** under each role were summed up in a table.

## Presentation of findings

Detailed findings for each profile of law enforcement officials are presented in a separate chapter in a structured format. Each chapter indicates the number of responses received in that particular role and the list of responding countries or organisations.

The starting point of data presentation is the level of expected knowledge in each competency fixed by the TCF, which is followed by showing the gap between the expected and existing level of knowledge indicated by respondents. The competency with the biggest observable gap in knowledge is ranked first, assuming that it has the highest training need.

The rank of competencies is followed by a graph where the blue stack area represents the gap in knowledge in each competency while the yellow line the training need set by respondents. Where the difference between the gap in knowledge and the indicated training need is striking, i.e., there is no gap, but the training need is high or there is a significant gap but low level of training need is indicated, a red bar is drawn to call the attention. Furthermore the graph contains a grey line to show the level of urgency of training needs.

The overview of gap in knowledge vs. training needs is followed by the description of the features of training needed, detailing the number of participants and form of training on basic and expert level set by respondents. Additionally, number of participants extrapolated to the 26 Member States also features for each role in the description. For easier overview, a summary graph presents the forms of training needed and the number of participants of basic and expert level training in the given profile.

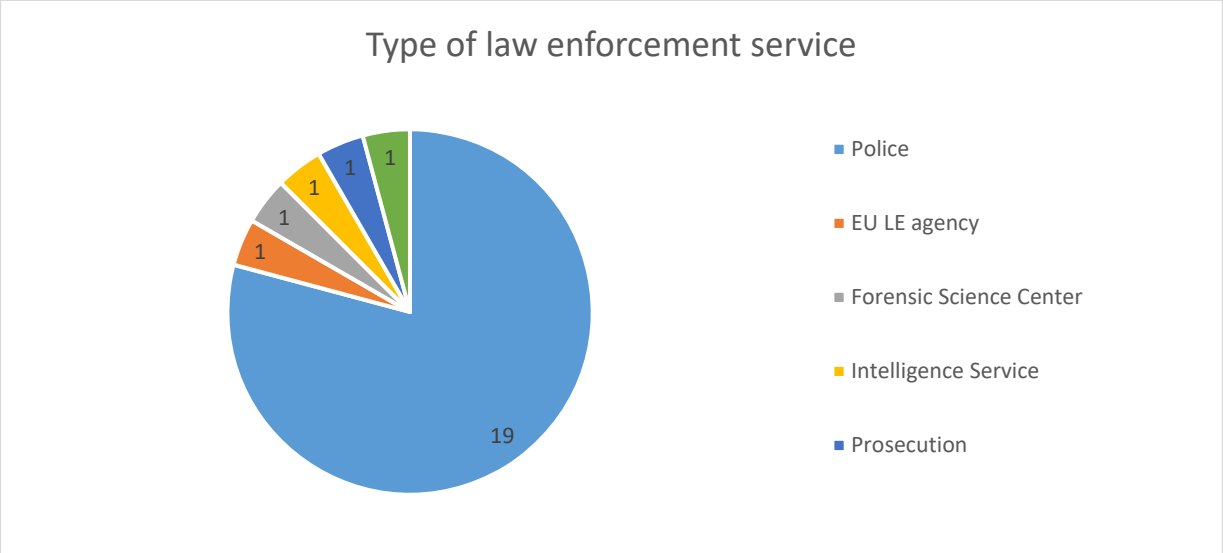
Existing training is scarce in each role and competency, so a summary paragraph on existing training activities described by respondents closes each chapter. The descriptive part is followed by the

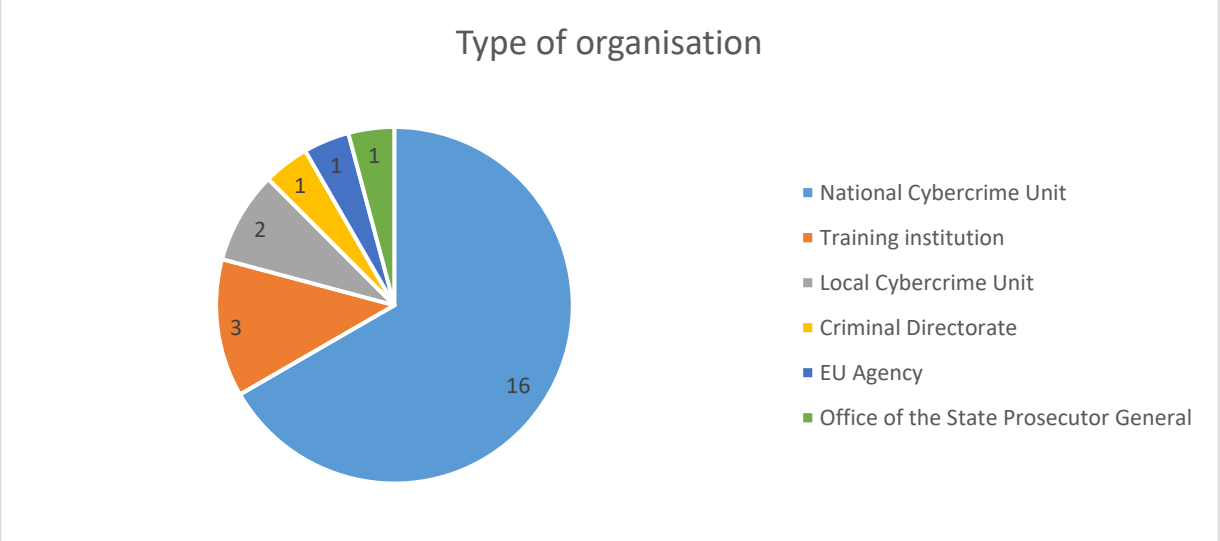
summary tables for each role. The first of such tables contains the current and expected level of knowledge as well as the gap in knowledge. The second one describes the overall urgency rate for each competency, number of participants who need training and the number of participants extrapolated to the EU. The next table gives details on the number of participants who need training in different forms while the last displays the features of exiting training such as its regularity, aim, target group, proficiency level and number of participants.

In the role of political and strategic decision makers only two respondents filled in the survey therefore training need related to this competency was not analysed further.

## Findings

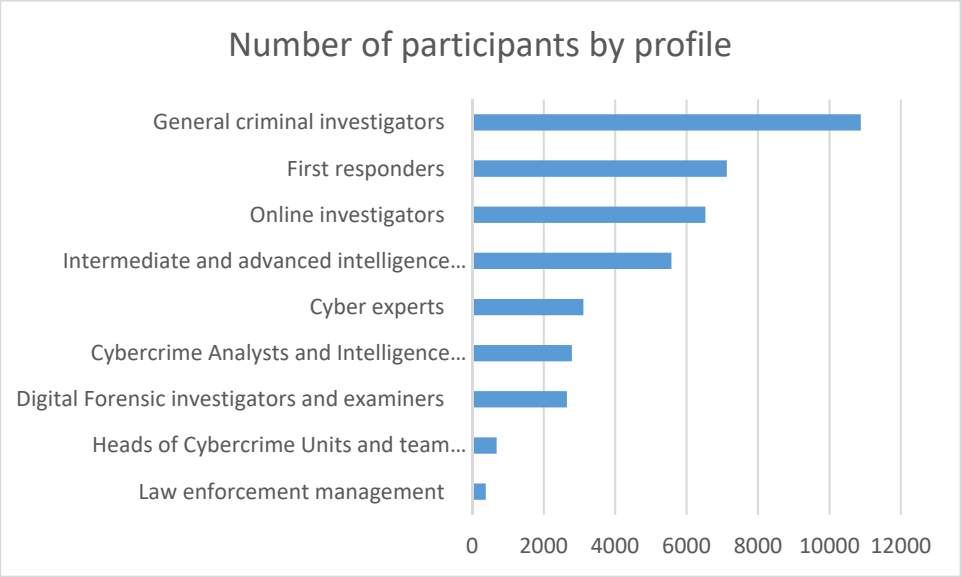
Findings of the first part of the survey on training needs are based on 24 responses from 17 Member States, Iceland, Switzerland and Europol's EC3. The following MSs took part in the survey: Austria, Belgium, Cyprus, Czech Republic, Germany, Greece, Hungary, Ireland, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia and the United Kingdom. This means that 60% of EU Member States are represented in the survey. Most respondents (79%) are employed by police and three-quarters of respondents represent a cybercrime unit, generally on a national level. The second part of the survey on existing training was filled in by 18 respondents.



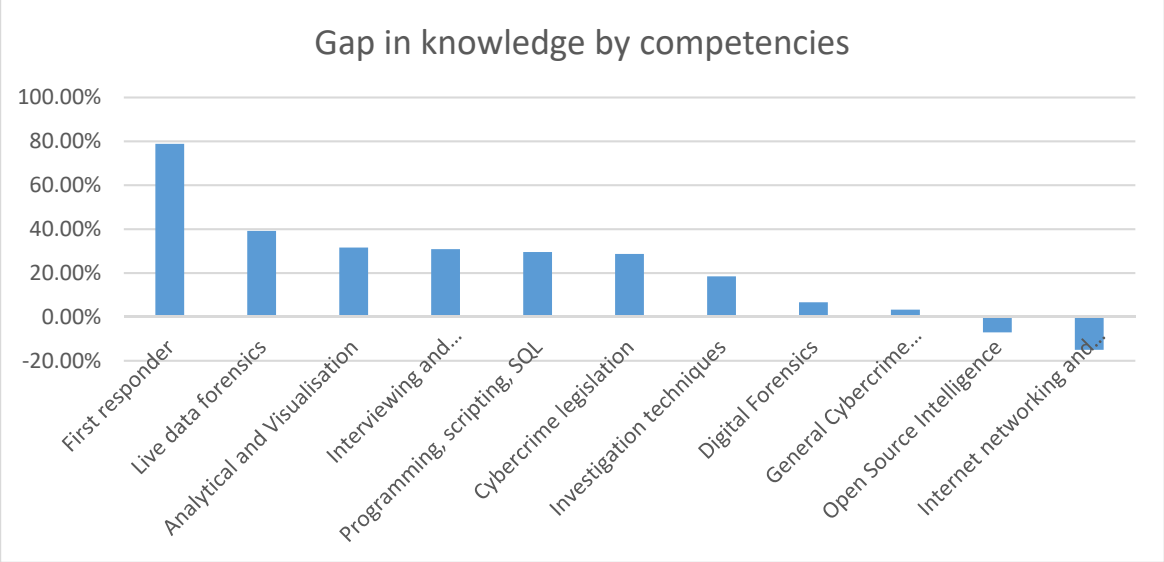


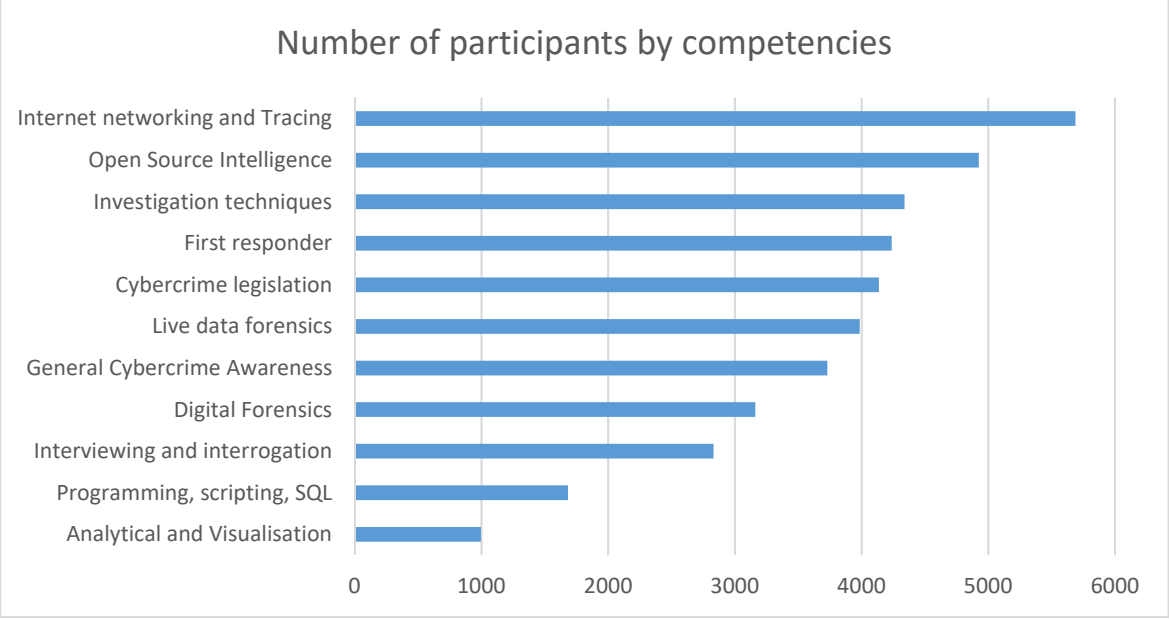

The general level of knowledge of law enforcement is between basic and expert level in all competencies, therefore, a gap in knowledge can be traced where the training competency framework expects expert level knowledge. However, training need is indicated in all competencies, even in those where current level of knowledge exceeds the basic level set by the competency framework.

In terms of profiles, law enforcement management has the largest gap between their current level of knowledge and the level set by the TCF and accordingly they indicated the highest rate of training need. A significant gap in knowledge exists in the profiles of digital forensic investigators and examiners, cyber experts, general criminal investigators and first responders however in the two latter profiles a lower level of training need was signalled by respondents. The level of current knowledge of heads of cybercrime units and team leaders exceeds the level set by TCF. At the same time, they indicated quite high level of training needs second in rank among all profiles. Number of participants who need training is the highest among general criminal investigators followed by first responders and online investigators.



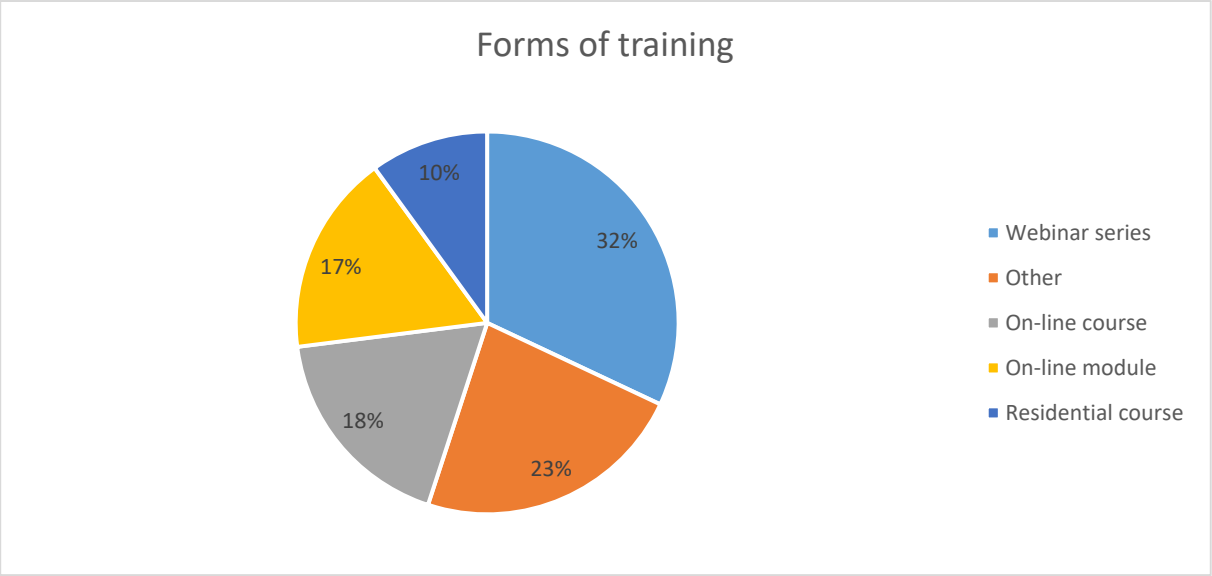
As for competencies, the largest gap in knowledge is in the competency of first responder where the existing level of knowledge is 79% lower than the expected level of knowledge across all roles. Other significant gaps are meaningfully lower concerning live data forensics (39%), analytical and visualisation (32%) interviewing and interrogation (31%), programming, scripting and SQL (30%) and cybercrime legislation (29%). In the competencies of open source intelligence and internet networking and tracing law enforcement officials investigating cyberattacks against information systems have higher level of knowledge than set by the TCF. Still, most participants would need training in these two latter competencies according to respondents, meaning that they feel necessary to improve their knowledge in these fields.




Altogether 39.718 law enforcement officials would need training in the different competencies under each profile. This would mean 144.209 law enforcement officials to be trained in the 26 Member States. This number in reality is probably lower since there should be overlaps among the target groups of the training. Webinar series are to be attended by most participants while only 10% of

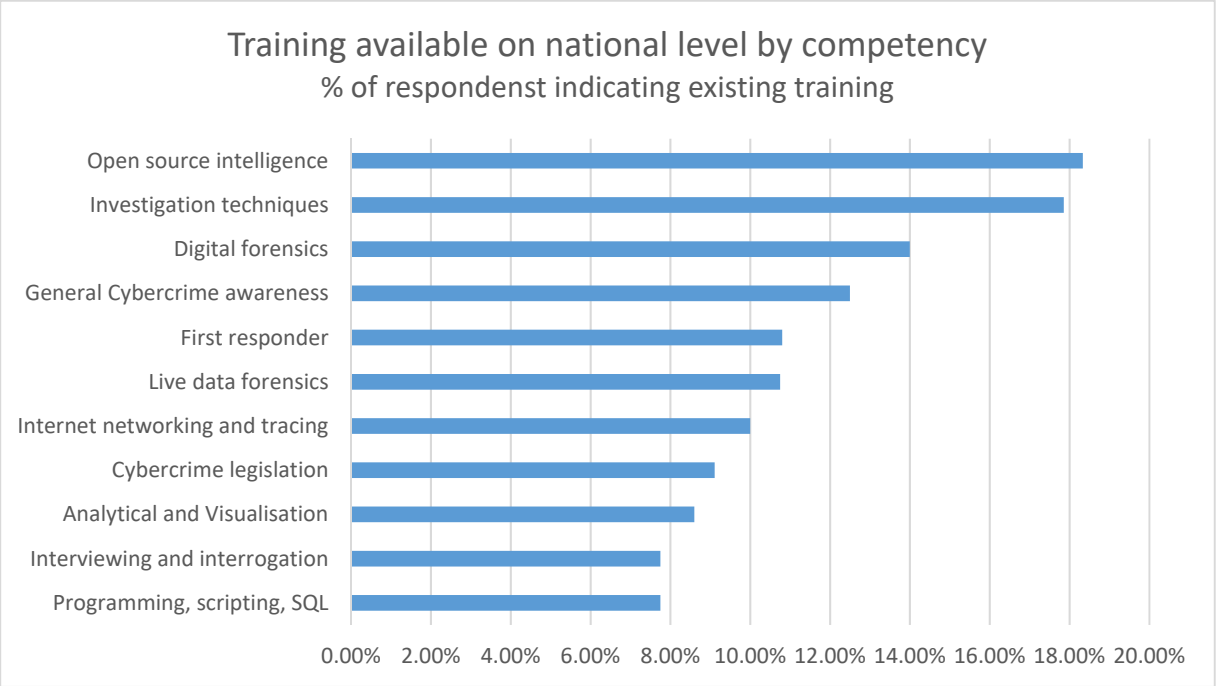
participants would take part in residential activities. Basic level of training should be delivered for 60% of participants and expert level to the remaining 16.071 law enforcement officials.

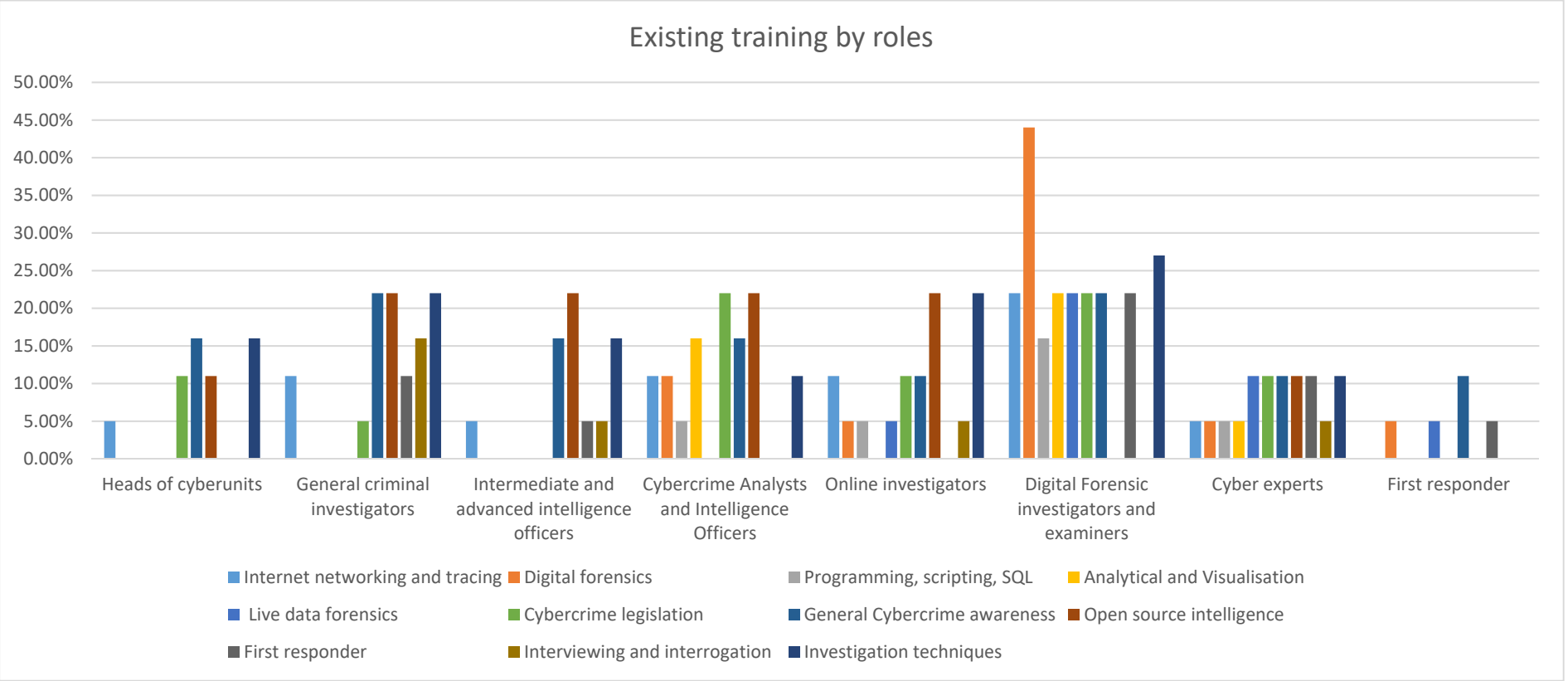


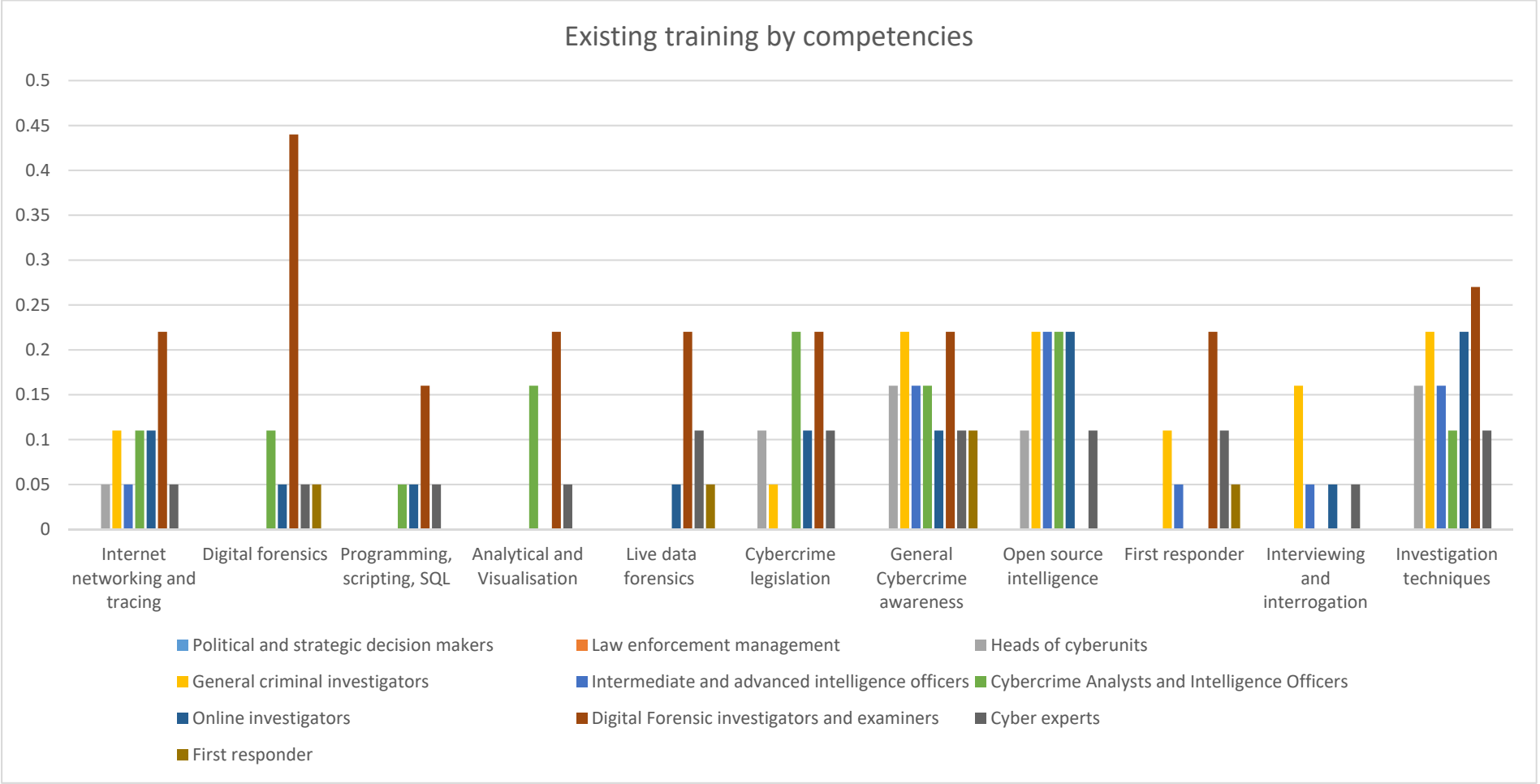

In general, the training need is relatively urgent, since it should be delivered between 6 months and 1 year. Training is most urgent for cybercrime analysts, intelligence officers and for digital forensic investigators and examiners while it can be delivered in a year to intermediate and advanced intelligence officers and to law enforcement management.

10% of respondents indicated available national level training activities which means that existing training is scarce in all roles and competencies. Most training opportunities are available for digital forensic investigators and examiners, most often targeting open source intelligence on a national level. Less than 10% of respondents indicated available national level training in the competencies of programming, scripting, SQL, analytical and visualisation, cybercrime legislation and interviewing and interrogation. In the profiles of intermediate and advanced intelligence officers, online investigators, cyber experts and first respondents, there is little training available on national level.


Training available on national level by role
% of respondenst indicating existing training
Digital Forensic investigators and examiners
General criminal investigators
Cybercrime Analysts and Intelligence Officers
Heads of cyberunits
Intermediate and advanced intelligence officers
Online investigators
Cyber experts
First responder
0.00%
5.00%
10.00%
15.00%
20.00%
25.00%
30.00%


Training available on national level by competency
% of respondenst indicating existing training
Open source intelligence
Investigation techniques
Digital forensics
General Cybercrime awareness
First responder
Live data forensics
Internet networking and tracing
Cybercrime legislation
Analytical and Visualisation
Interviewing and interrogation
Programming, scripting, SQL
0.00%
2.00%
4.00%
6.00%
8.00%
10.00%
12.00%
14.00%
16.00%
18.00%
20.00%


Existing training by roles
50.00%
45.00%
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
Heads of cyberunits
General criminal investigators
Intermediate and advanced intelligence officers
Cybercrime Analysts and Intelligence Officers
Online investigators
Digital Forensic investigators and examiners
Cyber experts
First responder
Internet networking and tracing
Digital forensics
Programming, scripting, SQL
Analytical and Visualisation
Live data forensics
Cybercrime legislation
General Cybercrime awareness
Open source intelligence
First responder
Interviewing and interrogation
Investigation techniques


Existing training by competencies
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
Internet networking and tracing
Digital forensics
Programming, scripting, SQL
Analytical and Visualisation
Live data forensics
Cybercrime legislation
General Cybercrime awareness
Open source intelligence
First responder
Interviewing and interrogation
Investigation techniques
Political and strategic decision makers
Law enforcement management
Heads of cyberunits
General criminal investigators
Intermediate and advanced intelligence officers
Cybercrime Analysts and Intelligence Officers
Online investigators
Digital Forensic investigators and examiners
Cyber experts
First responder

## Role: Political and strategic decision makers

Number of responses: 2

Countries, organisations represented: Austria, Germany, Ireland, Europol's EC3

For Heads of cybercrime units, the Training Competency Framework defines the following competencies:

| Competency | Level of knowledge |
|---|---|
| Cybercrime legislation | Basic |
| General Cybercrime Awareness | Basic |

No existing training was indicated under this profile.

No further analysis was performed due to the low response rate.

## Role: Law enforcement management

Number of responses: 4

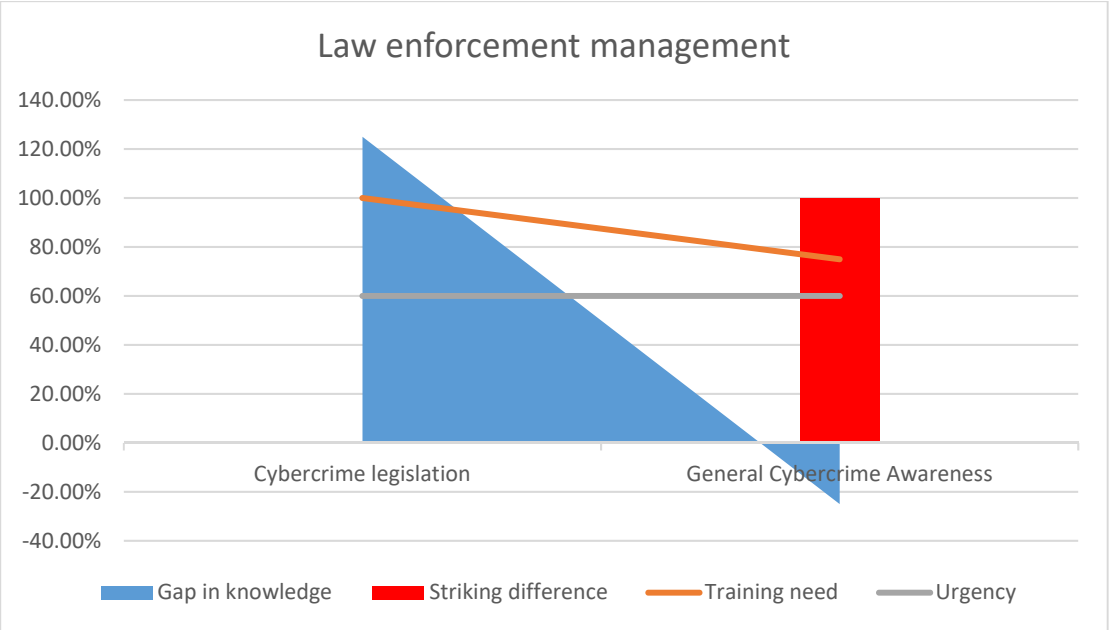
Countries, organisations represented: Austria, Switzerland

For Law enforcement management, the Training Competency Framework defines the following competencies:

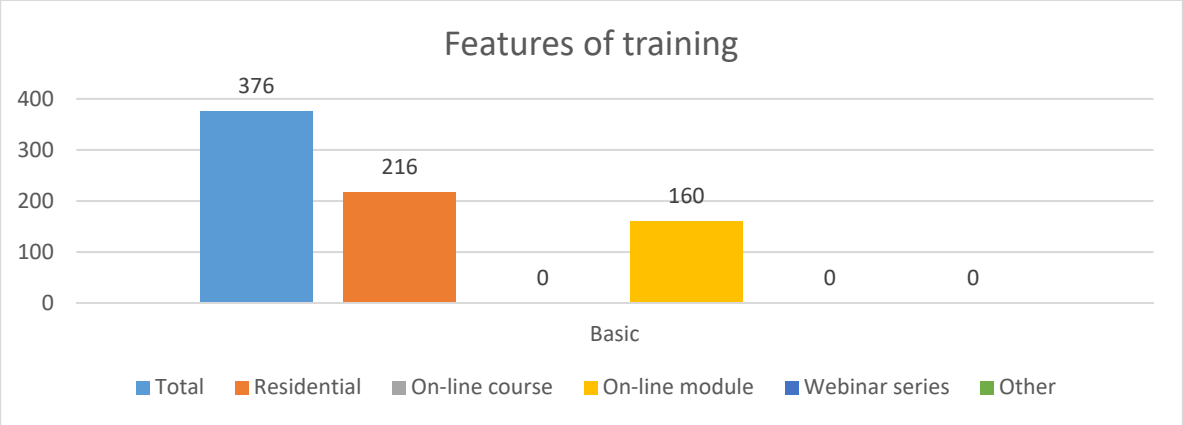
| Competency | Level of knowledge |
|---|---|
| Cybercrime legislation | Expert |
| General Cybercrime Awareness | Basic |

EU-level training needs in the order of gap between requested and existing level of competency:

1. Cybercrime legislation
2. General Cybercrime Awareness



In the competency of cybercrime legislation, law enforcement management has quite a significant gap in knowledge. While the TCF expects expert level of knowledge, their current level of knowledge is below basic level, consequently training need indicated by respondents is 100%. In case of cybercrime awareness the training need indicated is still high even though law enforcement management meets and exceeds the basic level the requirement set by the TCF.




Altogether 376 law enforcement managers would need training, all of them at basic level. According to the TCF these managers should have expert level of knowledge in the competency of cybercrime legislation, nevertheless these managers see basic level training as a first step to be completed. The most preferred training format is residential course (57%) followed by online modules (43%). This would mean 3510 law enforcement managers to be trained in the 26 EU Member States. Training need is in general mid-urgent, meaning that training should be delivered within 6-12 months.

For detailed information please see the tables below.

No existing training was indicated in this topic.

## Summary tables of training needs of General criminal investigators

### Training need

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| Cybercrime legislation | 0.75 | 2 | 1.25 |
| General Cybercrime Awareness | 1.25 | 1 | -0.25 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| Cybercrime legislation | 2 | 173 | 910 | | | |
| General Cybercrime Awareness | 2 | 203 | 2600 | | | |
| Total/Average for urgency | 2 | 376 | 3510 | | | |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| Cybercrime legislation | 113 | | 60 | | | 173 | | | | | | |
| General Cybercrime Awareness | 103 | | 100 | | | 203 | | | | | | |
| Total | 216 | 0 | 160 | 0 | 0 | 376 | | | | | | |

## Role: Heads of cybercrime units

Number of responses: 13

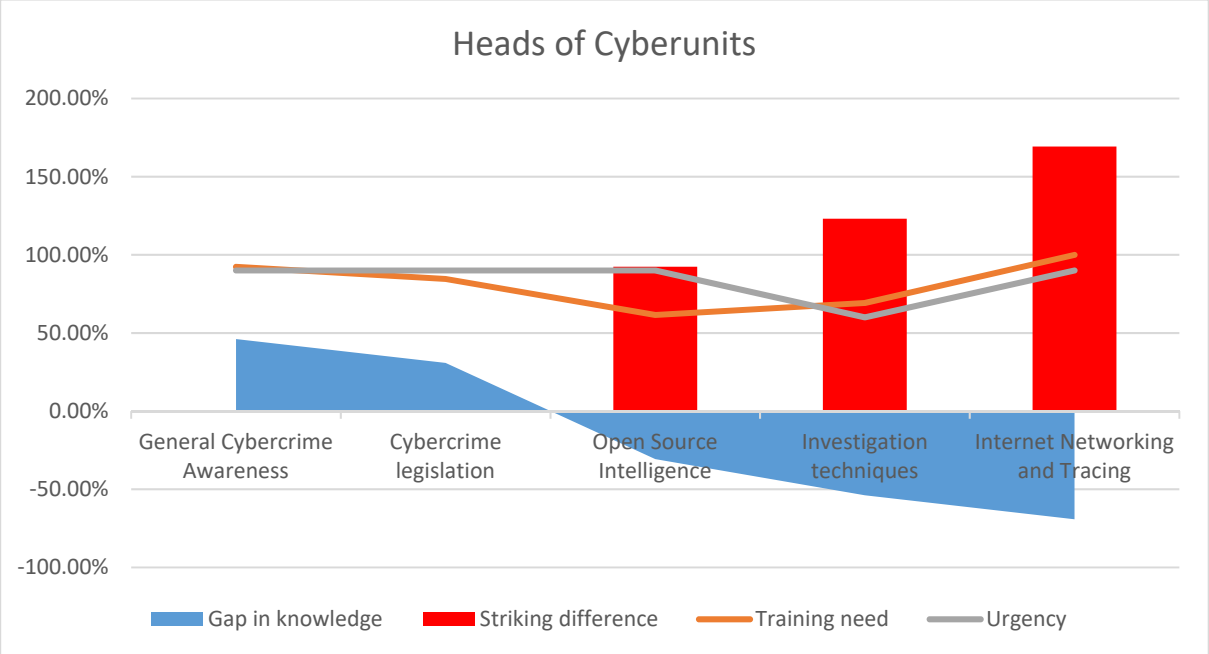
Countries, organisations represented: Austria, Belgium, Czech Republic, Europol-Ec3, Greece, Iceland, Ireland, Poland, Romania, Slovenia, Slovakia, Switzerland, United Kingdom.

For Heads of cybercrime units, the Training Competency Framework defines the following competencies:

| Competency | Level of knowledge |
|---|---|
| Internet Networking and Tracing | Basic |
| Cybercrime legislation | Expert |
| General Cybercrime Awareness | Expert |
| Open Source Intelligence | Basic |
| Investigation techniques | Basic |

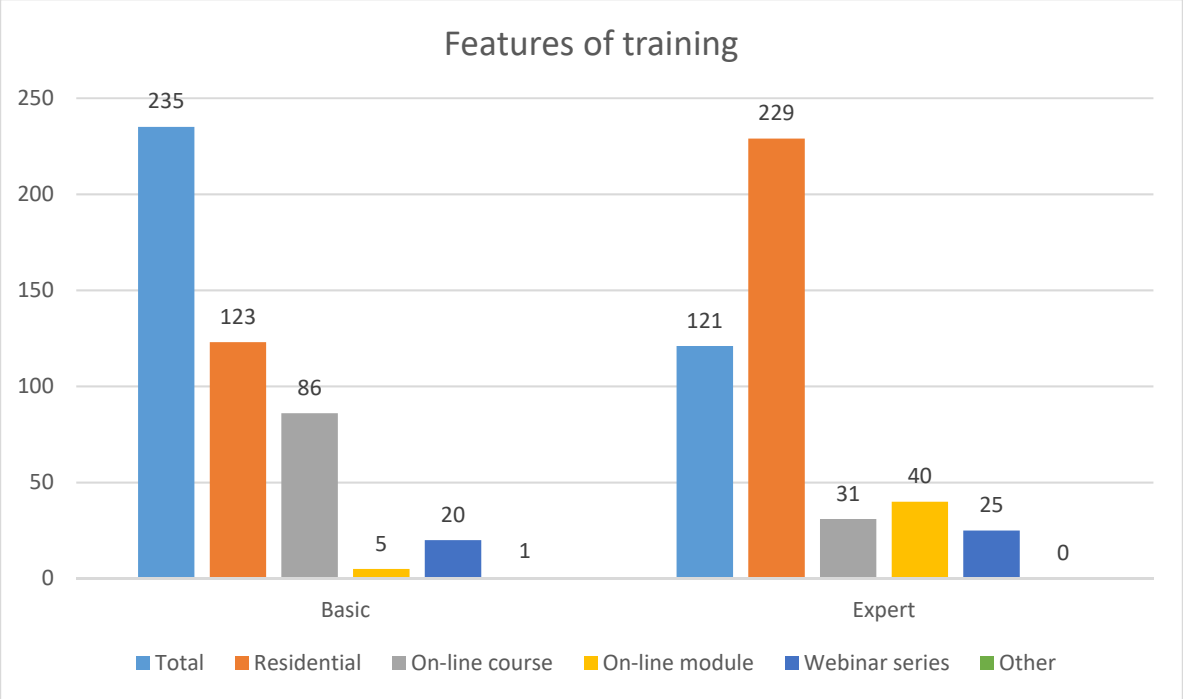
EU-level training needs in the order of gap between requested and existing level of competency:

3. General Cybercrime Awareness
4. Cybercrime legislation
5. Open Source Intelligence
6. Investigation techniques
7. Internet Networking and Tracing




The biggest gap in knowledge is in the competency of general cybercrime awareness where the TCF expects expert level knowledge. The current level of knowledge is between basic and expert level, therefore expert level training need is quite high in this competency. The other competency where the TCF defines expert level of knowledge for heads of cybercrime units is of cybercrime legislation. Here the current level of knowledge is closer to expert level, but still there is need for further training. In all competencies where the TCF defines only basic level of knowledge, like internet networking and

tracing, open source intelligence and investigation techniques, heads of cybercrime units have the required or even higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies, especially in the competency of internet networking and tracing where 100% of respondents indicated a need for training on basic or expert level.




Altogether 356 Heads of cybercrime units would need training, of which 66% would need basic level training. The most preferred training format is residential course (99%). This would mean 2977 heads of cybercrime units should be trained in the 26 EU Member States – if there were so many officers fulfilling this position. Training need in general is extremely urgent, meaning that training should be delivered within 6 month.

11.8% of respondents indicated that there is training available on national level. The competencies most addressed by training on national level are general cybercrime awareness and investigation techniques while internet networking and tracing is the topic least targeted on national level.

For detailed information please see the tables below.

## Summary tables of training needs of heads of cybercrime units

### Training needs

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| General Cybercrime Awareness | 1.538462 | 2 | 0.461538 |
| Cybercrime legislation | 1.692308 | 2 | 0.307692 |
| Open Source Intelligence | 1.307692 | 1 | -0.30769 |
| Investigation techniques | 1.538462 | 1 | -0.53846 |
| Internet Networking and Tracing | 1.692308 | 1 | -0.69231 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| Internet Networking and Tracing | 3 | 45 | 520 | 3 | 128 | 169 |
| Cybercrime legislation | 3 | 45 | 520 | 3 | 87 | 130 |
| General Cybercrime Awareness | 2 | 28 | 91 | 3 | 87 | 520 |
| Open Source Intelligence | 3 | 68 | 520 | 2 | 61 | 208 |
| Investigation techniques | 2 | 49 | 130 | 2 | 83 | 169 |
| Total/Average for urgency | 2.6 | 235 | 1781 | 2.6 | 446 | 1196 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| Internet Networking and Tracing | 25 | 20 | | | | 45 | 55 | 48 | 5 | 20 | | 128 |
| Cybercrime legislation | 25 | 20 | | | | 45 | 11 | 73 | 3 | | | 87 |
| General Cybercrime Awareness | 22 | | 5 | | 1 | 28 | 27 | 40 | 20 | | | 87 |
| Open Source Intelligence | 23 | 25 | | 20 | | 68 | 8 | 48 | | | 5 | 61 |
| Investigation techniques | 28 | 21 | | | | 49 | 20 | 20 | 3 | 20 | 20 | 83 |
| Total | 123 | 86 | 5 | 20 | 1 | 235 | 121 | 229 | 31 | 40 | 25 | 446 |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Internet networking and Tracing | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 6-30 |
| General Cybercrime Awareness | ad-hoc | basic | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 6-30 |
| General Cybercrime Awareness | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |
| General Cybercrime Awareness | Regular | Expert | Other | Heads of Cybercrime Units | Improvement | 5 |
| General Cybercrime Awareness | ad-hoc | expert | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 6-30 |
| General Cybercrime Awareness | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |
| Open source intelligence | Regular | Expert | Other | Heads of Cybercrime Units | Specialisation | 10 |
| Open source intelligence | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 6-30 |
| Investigation techniques | Regular | Expert | Other | Heads of Cybercrime Units | Improvement | 5 |
| Investigation techniques | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 6-30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Investigation techniques | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |

## Role: General criminal investigators

Number of responses: 20

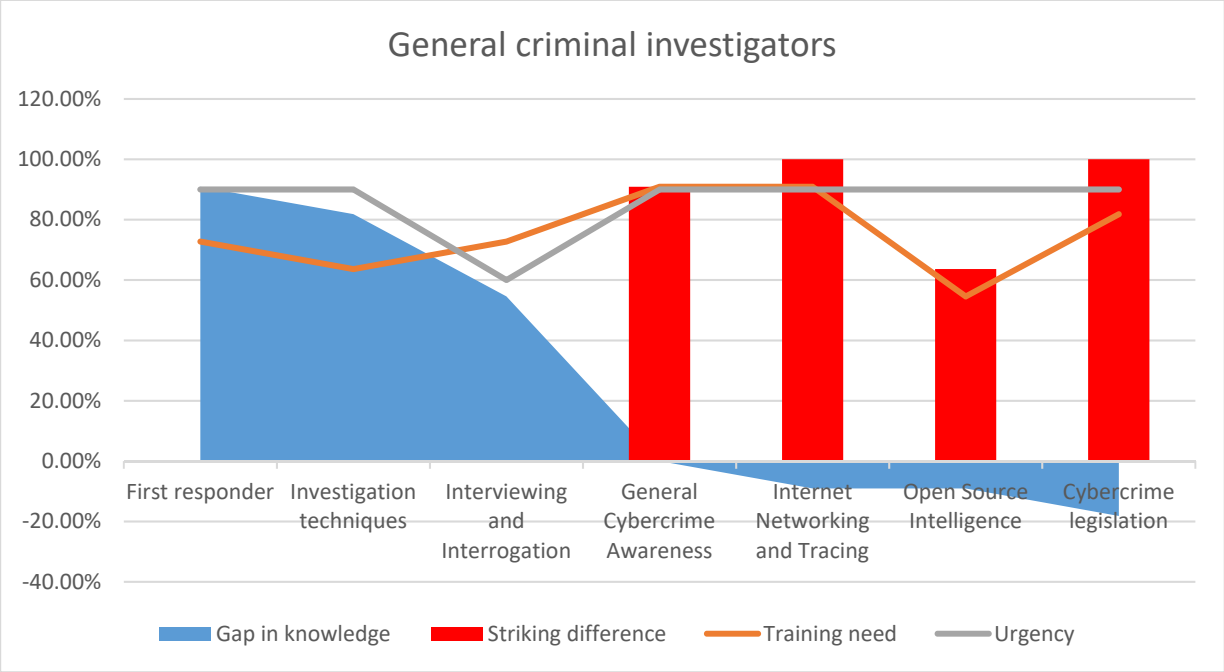
Countries, organisations represented: Austria, Belgium, Czech Republic, Europol-Ec3, Germany, Greece, Hungary, Iceland, Ireland, Latvia, Malta, Poland, Romania, Slovenia, Slovakia, Switzerland, United Kingdom.

For general criminal investigators, the Training Competency Framework defines the following competencies:

| Competency | Level of knowledge |
|---|---|
| Internet Networking and Tracing | Basic |
| Cybercrime legislation | Basic |
| First responder | Expert |
| General Cybercrime Awareness | Basic |
| Open Source Intelligence | Basic |
| Interviewing and Interrogation | Expert |
| Investigation techniques | Expert |

EU-level training needs in the order of gap between requested and existing level of competency:

1. First responder
2. Investigation techniques
3. Interviewing and Interrogation
4. General Cybercrime Awareness
5. Internet Networking and Tracing
6. Open Source Intelligence
7. Cybercrime legislation



The biggest gap in knowledge is in the competency of first responder where the TCF expects expert level knowledge while the current level of knowledge is around basic level. Only 11% of respondents indicated national level training for this competency. In the two other competencies, where the TCF expects expert level of knowledge, i.e. in the competencies of investigation techniques and interviewing and investigation significant knowledge gap can be traced with consequent training needs. In all competencies where the TCF defines only basic level of knowledge, like internet networking and tracing, general cybercrime awareness, cybercrime legislation and open source intelligence, general criminal investigators have the required or even higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies.

Altogether 10.880 general criminal investigators would need training, mostly (97%) on expert level and in the form of webinar series (66%). This would mean 32.019 general criminal investigators to be trained in the 26 EU Member States. Training need is in general extremely urgent, meaning that training should be delivered within 6 month.

15.57% of respondents indicated that there is training available on national level. The competencies most addressed by training on national level are general cybercrime awareness, open source intelligence and investigation techniques while cybercrime legislation is the topic least targeted on national level.

For detailed information please see the tables below.

## Summary tables of training needs of General criminal investigators

### Training needs

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| | 1.25 | 2 | 0.75 |
| First responder | 1.090909 | 2 | 0.909091 |
| Investigation techniques | 1.181818 | 2 | 0.818182 |
| Interviewing and Interrogation | 1.454545 | 2 | 0.545455 |
| General Cybercrime Awareness | 1 | 1 | 0 |
| Internet Networking and Tracing | 1.090909 | 1 | -0.09091 |
| Open Source Intelligence | 1.090909 | 1 | -0.09091 |
| Cybercrime legislation | 1.181818 | 1 | -0.18182 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| Internet Networking and Tracing | 3 | 1750 | 5200 | 3 | 50 | 195 |
| Cybercrime legislation | 2 | 1535 | 6760 | 3 | 45 | 260 |
| First responder | 2 | 1541 | 455 | 3 | 40 | 520 |
| General Cybercrime Awareness | 2 | 1220 | 390 | 3 | 113 | 520 |
| Open Source Intelligence | 3 | 1739 | 520 | 3 | 45 | 169 |
| Interviewing and Interrogation | 2 | 1020 | 13260 | 2 | 555 | 585 |
| Investigation techniques | 2 | 1725 | 2860 | 3 | 57 | 325 |
| Total/Average for urgency | 2.28 | 10530 | 29445 | 2.86 | 905 | 2574 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| Internet Networking and Tracing | 200 | | 1020 | 530 | | 1750 | 50 | | | | | 50 |
| Cybercrime legislation | 15 | | 1520 | | | 1535 | 30 | | 5 | 10 | | 45 |
| First responder | 3 | 15 | 523 | 1000 | | 1541 | 40 | | | | | 40 |
| General Cybercrime Awareness | | 17 | 3 | 1200 | | 1220 | 93 | | 20 | | | 113 |
| Open Source Intelligence | 2 | 15 | 22 | 1700 | | 1739 | 35 | | | 10 | | 45 |
| Interviewing and Interrogation | | | 20 | 1000 | | 1020 | | | | | | 0 |
| Investigation techniques | | | 23 | 1702 | | 1725 | 57 | | | | | 57 |
| Total | 220 | 47 | 3131 | 7132 | 0 | 10530 | 305 | 0 | 25 | 20 | 0 | 350 |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Internet networking and Tracing | regular | basic | Cybercrime Dept. Hungary | Hungarian police officers | to develop the personal skills | 30 |
| Cybercrime legislation | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |
| General Cybercrime Awareness | regular | basic | free online tools | all staff | upskill across the agency | 30+ |
| General Cybercrime Awareness | ad-hoc | basic | various | CPD with other subjects | Provide knowledge | 25 |
| General Cybercrime Awareness | regular | basic | every year 4 times | criminal police officers | Cybercrime Awareness | 120 |
| General Cybercrime Awareness | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |
| First responders | Regular | Basic | Office for Combating Cybercrime | Investigators | Basic Knowledge | 40 |
| Open source intelligence | regular | basic | Cybercrime Dept. Hungary | Hungarian police officers | to develop the personal skills | 30 |
| Open source intelligence | CEPOL/Hungary | basic/expert | CEPOL | Digital investigators | increase knowledge | 50 |
| Interviewing and interrogation | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |

| | | | | | | |
|---|---|---|---|---|---|---|
| Interviewing and interrogation | regular | basic | Police academies | Investigators and Intelligence Officers | to improve interviewing and interrogation techniques | 16 on each training |
| Investigation techniques | regular | basic | Cybercrime Dept. Hungary | Hungarian police officers | to develop the personal skills | 30 |
| Investigation techniques | mandatory | basic | PJ School | candidates | After a competition the training is mandatory to fulfil the inherent functions | depends on the number of accepted candidates |

## Role: Intermediate and advanced investigators

Number of responses: 8

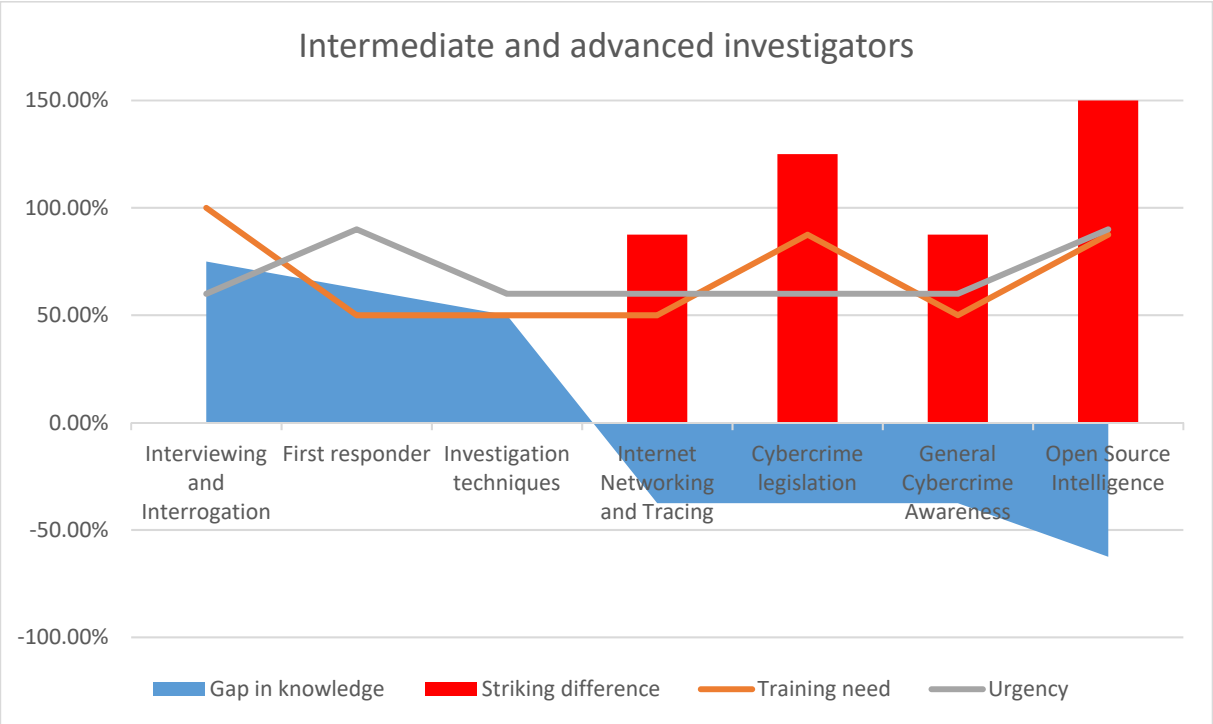
Countries, organisations represented: Austria, Czech Republic, Europol-Ec3, Ireland, Latvia, Romania, Slovakia, United Kingdom.

For Intermediate and advanced investigators, the Training Competency Framework defines the following competencies:

| Competency | Level of knowledge |
|---|---|
| Internet Networking and Tracing | Basic |
| Cybercrime legislation | Basic |
| First responder | Expert |
| General Cybercrime Awareness | Basic |
| Open Source Intelligence | Basic |
| Interviewing and Interrogation | Expert |
| Investigation techniques | Expert |

EU-level training needs in the order of gap between requested and existing level of competency:

1. Interviewing and Interrogation
2. First responder
3. Investigation techniques
4. Internet Networking and Tracing
5. Cybercrime legislation
6. General Cybercrime Awareness
7. Open Source Intelligence



The biggest gap in knowledge is in the competency of interviewing and investigation where the TCF expects expert level knowledge while the current level of knowledge is just a bit above basic level. In the two other competencies, where the TCF expects expert level of knowledge, i.e. in the competencies of first responder and investigation techniques a significant knowledge gap can be traced with consequent training needs. National level training in the competencies of first responders and interviewing and investigation was indicated only by 5% of respondents. In all competencies where the TCF defines only basic level of knowledge, like internet networking and tracing, general cybercrime awareness and open source intelligence, intermediate and advanced investigators have the required or even higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies.

Altogether 5577 intermediate and advanced investigators would need training, 88% of them basic level training, mostly in the format of webinar series (79%). This would mean that 19.747 intermediate and advanced investigators are to be trained in the 26 EU Member States. Training need is in general not very urgent, meaning that training should be delivered within one year.

Only 9.86% of respondents indicated that there is training available on national level. The competencies most addressed by training on national level are open source intelligence (22%), general cybercrime awareness (16%) and investigation techniques (16%) while there is no training available on cybercrime legislation on national level.

For detailed information please see the tables below.

## Summary tables of training needs of Intermediate and advanced investigators

### Training needs

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| Interviewing and Interrogation | 1.25 | 2 | 0.75 |
| First responder | 1.375 | 2 | 0.625 |
| Investigation techniques | 1.5 | 2 | 0.5 |
| Internet Networking and Tracing | 1.375 | 1 | -0.375 |
| Cybercrime legislation | 1.375 | 1 | -0.375 |
| General Cybercrime Awareness | 1.375 | 1 | -0.375 |
| Open Source Intelligence | 1.625 | 1 | -0.625 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| Internet Networking and Tracing | 2 | 1223 | 2860 | 2 | 56 | 325 |
| Cybercrime legislation | 2 | 580 | 1300 | 2 | 106 | 1378 |
| First responder | 3 | 532 | 780 | 2 | 5 | 130 |
| General Cybercrime Awareness | 2 | 517 | 390 | 2 | 110 | 1430 |
| Open Source Intelligence | 3 | 702 | 5200 | 3 | 170 | 780 |
| Interviewing and Interrogation | 2 | 515 | 260 | 2 | 106 | 1378 |
| Investigation techniques | 2 | 717 | 2795 | 2 | 138 | 468 |
| Total/Average for urgency | 2.28 | 4786 | 13585 | 2.14 | 691 | 5889 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| Internet Networking and Tracing | 20 | 3 | | 1300 | | 1323 | 36 | 20 | | | | 56 |
| Cybercrime legislation | | 30 | 50 | 500 | | 580 | 6 | | | 100 | | 106 |
| First responder | 2 | 30 | | 500 | | 532 | 5 | | | | | 5 |
| General Cybercrime Awareness | 2 | 15 | | 500 | | 517 | 10 | | | 100 | | 110 |
| Open Source Intelligence | 2 | | 500 | 200 | | 702 | 68 | 102 | | | | 170 |
| Interviewing and Interrogation | 15 | | | 500 | | 515 | | 100 | | 6 | | 106 |
| Investigation techniques | 17 | | | 700 | | 717 | 36 | 100 | | 2 | | 138 |
| Total | 58 | 78 | 550 | 4200 | 0 | 4886 | 161 | 322 | 0 | 208 | 0 | 691 |

## Existing training

| | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| General Cybercrime Awareness | Regular | Expert | Other | Advanced Intelligence Officers | Improvement | 10 |
| General Cybercrime Awareness | regular | basic | free online tools | Cybercrime unit intelligence officers | awareness for staff | 50 |
| General Cybercrime Awareness | ad-hoc | basic | various | CPD with other | Provide knowledge | 25 |
| First responders | Regular | Expert | Other | Advanced Intelligence Officers | Improvement | 5 |
| Open source intelligence | Regular | Expert | Other | Advanced Intelligence Officers | Improvement | 10 |
| Open source intelligence | L2/L3 | in house / external provider | Cybercrime Unit intelligence officers | awareness of techniques all staff | 50 | 50 |
| Open source intelligence | ad-hoc | basic | various | CPD with other | Provide knowledge | 25 |
| Open source intelligence | ad-hoc | expert | Domestic/International | Police officers | Development of knowledge | Depending on time period |
| Investigation techniques | Regular | Expert | Other | Advanced Intelligence Officers | Improvement | 10 |
| Investigation techniques | ad-hoc | expert | Domestic/International | Police officers | Development of knowledge | Depending on time period |

## Role: Cybercrime analysts and intelligence officers

Number of responses: 9

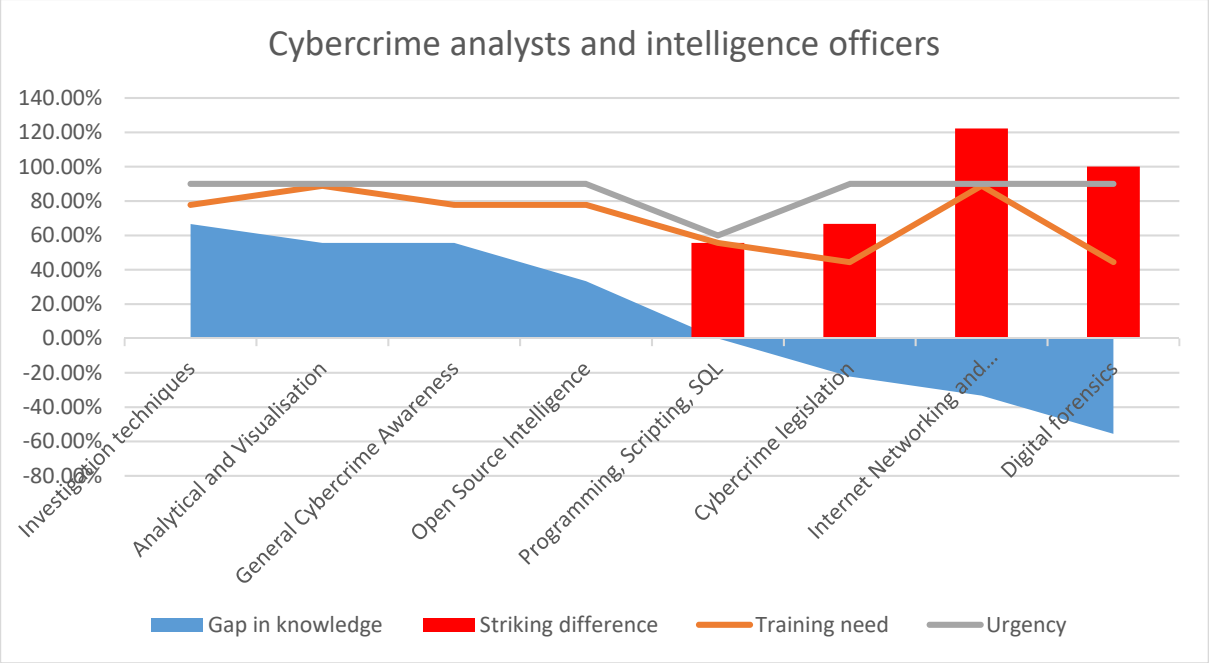
Countries, organisations represented: Cyprus, Czech Republic, Europol-Ec3, Iceland, Ireland, Latvia, Malta, Romania, United Kingdom.

For Cybercrime analysts and intelligence officers, the Training Competency Framework defines the following competencies:

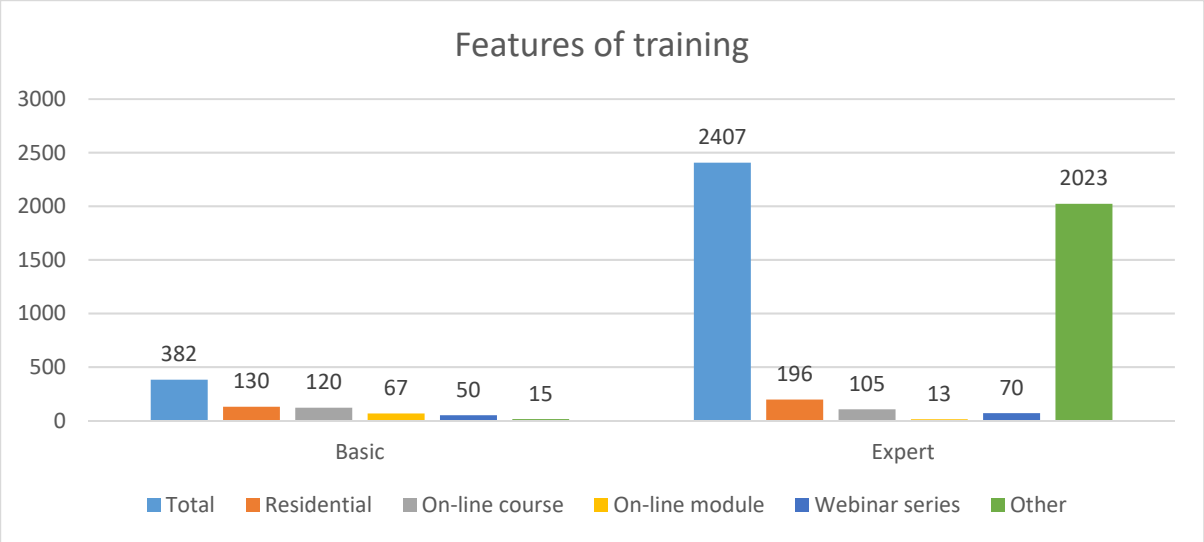
| Competency | Level of knowledge |
|---|---|
| Digital forensics | Basic |
| Internet Networking and Tracing | Basic |
| Programming, Scripting, SQL | Basic |
| Analytical and Visualisation | Expert |
| Cybercrime legislation | Basic |
| General Cybercrime Awareness | Expert |
| Open Source Intelligence | Expert |
| Investigation techniques | Expert |

EU-level training needs in the order of gap between requested and existing level of competency:

1. Investigation techniques
2. Analytical and Visualisation
3. General Cybercrime Awareness
4. Open Source Intelligence
5. Programming, Scripting, SQL
6. Cybercrime legislation
7. Internet Networking and Tracing
8. Digital forensics



The training need is higher than the gap between expected and current level of knowledge in all competencies. The biggest gap in knowledge is in the competency of investigation techniques where the TCF expects expert level knowledge while the current level of knowledge is just above basic level. In all competencies, where the TCF expects expert level of knowledge, i.e. in the competencies of analytical and visualisation, general cybercrime awareness and open source intelligence a significant knowledge gap can be traced with consequent training needs. In all competencies where the TCF defines only basic level of knowledge, like programming, scripting, SQL, cybercrime legislation, internet networking and tracing and digital forensics, Cybercrime analysts and intelligence officers have the required or even higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies.




Altogether 2789 cybercrime analysts and intelligence officers would need training, 86% of them expert level training, mostly in the format of residential courses and online courses. This would mean 5902 cybercrime analysts and intelligence officers ought to be trained in the 26 EU Member States. The training need is in general urgent, meaning that training should be delivered within 6 months.

14.25% of respondents indicated that there is training available on national level. The competencies most addressed by training on national level are open source intelligence (22%) and cybercrime legislation (22%) while programming, scripting and SQL is the competency least targeted by training on national level.

For detailed information please see the tables below.

## Summary tables of training needs of Cybercrime analysts and intelligence officers

### Training needs

| | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| Investigation techniques | 1.333333 | 2 | 0.666667 |
| Analytical and Visualisation | 1.444444 | 2 | 0.555556 |
| General Cybercrime Awareness | 1.444444 | 2 | 0.555556 |
| Open Source Intelligence | 1.666667 | 2 | 0.333333 |
| Programming, Scripting, SQL | 1 | 1 | 0 |
| Cybercrime legislation | 1.222222 | 1 | -0.22222 |
| Internet Networking and Tracing | 1.333333 | 1 | -0.33333 |
| Digital forensics | 1.555556 | 1 | -0.55556 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | **Urgency (1-low, 2-medium, 3-high)** | **Number of participants** | **Number of participants extrapolated to the EU** | **Urgency (1-low, 2-medium, 3-high)** | **Number of participants** | **Number of participants extrapolated to the EU** |
| Digital forensics | 3 | 55 | 715 | 3 | 69 | 260 |
| Internet Networking and Tracing | 3 | 80 | 455 | 3 | 52 | 130 |
| Programming, Scripting, SQL | 2 | 50 | 234 | 2 | 18 | 130 |
| Analytical and Visualisation | 3 | 30 | 234 | 3 | 50 | 260 |
| Cybercrime legislation | 3 | 57 | 325 | 3 | 17 | 221 |
| General Cybercrime Awareness | 3 | 70 | 910 | 2 | 21 | 208 |
| Open Source Intelligence | 3 | 30 | 780 | 3 | 1146 | 455 |
| Investigation techniques | 2 | 10 | 260 | 3 | 1034 | 325 |
| Total/Average for urgency | 2.75 | 382 | 3913 | 2.75 | 2407 | 1989 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other form | Total | Residential course | Online course | Online module | Webinar series | Other form | Total |
| Digital forensics | 55 | | | | | 55 | 64 | | | | 5 | 69 |
| Internet Networking and Tracing | 20 | 40 | 20 | | | 80 | 44 | | 3 | | 5 | 52 |
| Programming, Scripting, SQL | 45 | | | | 5 | 50 | 5 | 8 | | | 5 | 18 |
| Analytical and Visualisation | 10 | 10 | | | 10 | 30 | 30 | 10 | | | 10 | 50 |
| Cybercrime legislation | | | 47 | 10 | | 57 | 8 | 9 | | | | 17 |
| General Cybercrime Awareness | | 70 | | | | 70 | 8 | 3 | | 10 | | 21 |
| Open Source Intelligence | | | | 30 | | 30 | 27 | 60 | 10 | 50 | 999 | 1146 |
| Investigation techniques | | | | 10 | | 10 | 10 | 15 | | 10 | 999 | 1034 |
| Total | 130 | 120 | 67 | 50 | 15 | 382 | 196 | 105 | 13 | 70 | 2023 | 2407 |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Digital forensics | mandatory | basic/expert | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Digital forensics | regular | basic | CSI - Austria | LEA | unified methodologies | 200 |
| Internet networking and tracing | mandatory | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Internet networking and tracing | regular | basic | CSI - Austria | LEA | unified methodologies | 200 |
| Programming, scripting, SQL | ad hoc | expert | external partners e.g. QA / Learning Tree | Data Analysts and Cyber Engineering team | ability to manage and process bulk data | 20 |
| Analytical and Visualisation | ad-hoc | basic | Domestic/International | Police officers | Development of knowledge | Depending on time period |
| Cybercrime legislation | ad-hoc | basic | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Cybercrime legislation | regular | basic | CSI - Austria | LEA | unified methodologies | 200 |
| General Cybercrime Awareness | Regular | Basic | Other | Cybercrime analysts and officers | Improvement | 8 |
| General Cybercrime Awareness | regular | basic | free online tools | Analysts and Intelligence Teams | awareness for staff | 20 |
| General Cybercrime Awareness | mandatory | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Open source intelligence | Regular | Basic | Other | Cybercrime analysts and officers | Improvement | 10 |
| Open source intelligence | regular | L2/L3 | in house / external provider | Analysts and Intelligence Teams | awareness of techniques all staff | 20 |
| Open source intelligence | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Open source intelligence | ad-hoc | expert | Domestic/International | Police officers | Development of knowledge | Depending on time period |
| Investigation techniques | basic/expert | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 | |
| Investigation techniques | basic | CSI - Austria | LEA | unified methodologies | 200 | |

## Role: Online investigators

Number of responses: 13

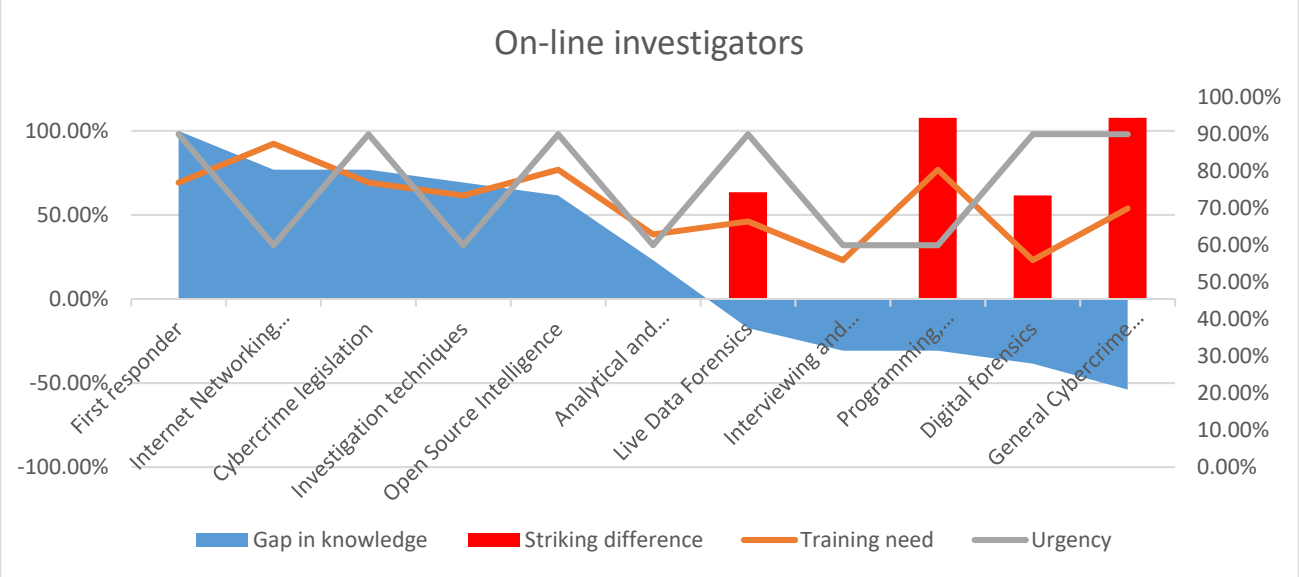
Countries, organisations represented: Austria, Cyprus, Czech Republic, Europol-Ec3, Hungary, Iceland, Ireland, Poland, Portugal, Slovakia, Switzerland, United Kingdom.

For Online investigators, the Training Competency Framework defines the following competencies:

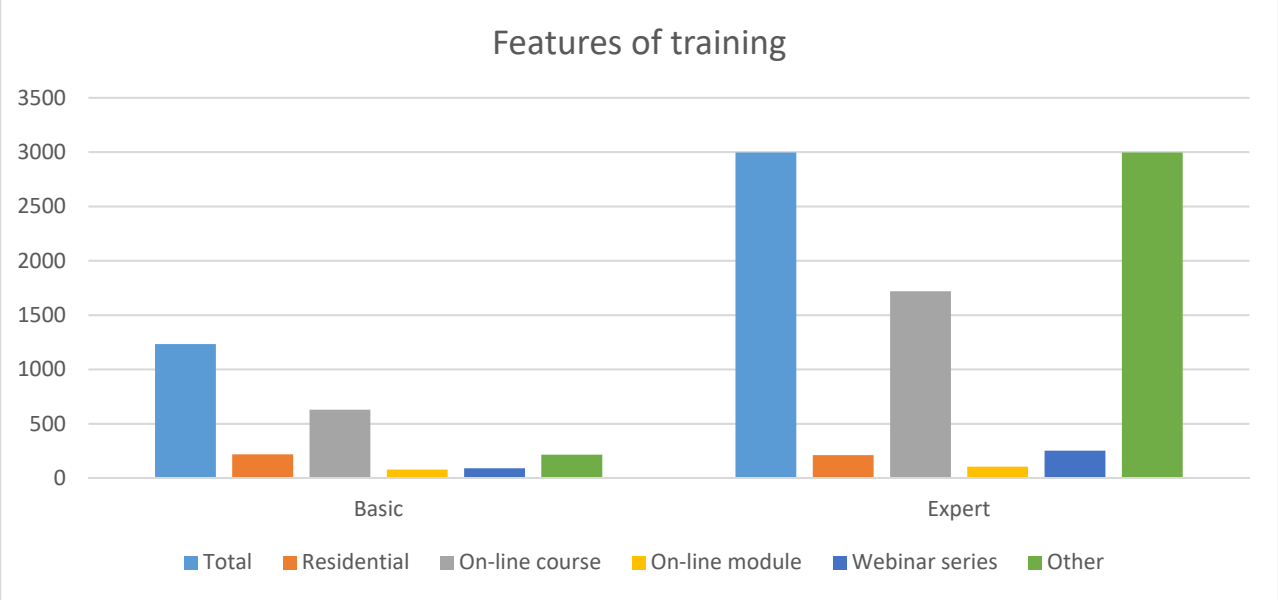
| Competency | Level of knowledge |
|---|---|
| Digital forensics | Basic |
| Internet Networking and Tracing | Expert |
| Programming, Scripting, SQL | Basic |
| Analytical and Visualisation | Basic |
| Live Data Forensics | Basic |
| Cybercrime legislation | Expert |
| First responder | Expert |
| General Cybercrime Awareness | Basic |
| Open Source Intelligence | Expert |
| Interviewing and Interrogation | Basic |
| Investigation techniques | Expert |

EU-level training needs in the order of gap between requested and existing level of competency:

1. First responder
2. Investigation techniques
3. Internet Networking and Tracing
4. Cybercrime legislation
5. Open Source Intelligence
6. Analytical and Visualisation
7. Live Data Forensics
8. Interviewing and Interrogation
9. Programming, Scripting, SQL
10. Digital forensics
11. General Cybercrime Awareness




The biggest gap in knowledge is in the competency of first responder where the TCF expects expert level knowledge while the current level of knowledge is at basic level. There was no training indicated on national level in this competency. In all competencies, where the TCF expects expert level of knowledge, i.e. in the competencies of investigation techniques, Internet networking and tracing, cybercrime legislation and open source intelligence a significant gap exists. In some competencies where the TCF defines only basic level of knowledge, like live data forensics, programming, scripting, SQL, Digital forensics and general cybercrime awareness, online investigators have the required or even higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies.




Altogether 4231 online investigators would need training, 71% of them expert level training, mostly in the format of online courses (55%). This would mean 10.127 online investigators are to be trained in the 26 EU Member States. The training need is in general urgent, meaning that training in most cases should be delivered either in 6 months or in a year`s time.

Only 9.7% of respondents indicated that there is training available on national level. The competencies most addressed by training on national level are open source intelligence and investigation techniques (22%) while digital forensics, programming, scripting and SQL, live data forensics and interviewing and interrogation are the competencies least targeted by training on national level (5%). There was no national level training indicated in the competency of analytical and visualisation.

For detailed information please see the tables below.

## Summary tables of training needs of online investigators

### Training needs

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| First responder | 1 | 2 | 1.00 |
| Internet Networking and Tracing | 1.230769 | 2 | 0.77 |
| Cybercrime legislation | 1.230769 | 2 | 0.77 |
| Investigation techniques | 1.307692 | 2 | 0.69 |
| Open Source Intelligence | 1.384615 | 2 | 0.62 |
| Analytical and Visualisation | 0.769231 | 1 | 0.23 |
| Live Data Forensics | 1.173077 | 1 | -0.17 |
| Programming, Scripting, SQL | 1.307692 | 1 | -0.31 |
| Interviewing and Interrogation | 1.307692 | 1 | -0.31 |
| Digital forensics | 1.384615 | 1 | -0.38 |
| General Cybercrime Awareness | 1.538462 | 1 | -0.54 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| Digital forensics | 2 | 260 | 650 | 3 | 1222 | 156 |
| Internet Networking and Tracing | 2 | 37 | 260 | 2 | 1331 | 780 |
| Programming, Scripting, SQL | 2 | 343 | 325 | 1 | 252 | 3276 |
| Analytical and Visualisation | 2 | 66 | 260 | 2 | 217 | 195 |
| Live Data Forensics | 3 | 96 | 520 | 2 | 1232 | 260 |
| Cybercrime legislation | 3 | 70 | 520 | 3 | 225 | 520 |
| First responder | 3 | 68 | 325 | 3 | 222 | 260 |
| General Cybercrime Awareness | 3 | 7 | 91 | 2 | 20 | 260 |
| Open Source Intelligence | 3 | 247 | 390 | 3 | 279 | 130 |
| Interviewing and Interrogation | 2 | 10 | 130 | 2 | 22 | 260 |
| Investigation techniques | 2 | 30 | 169 | 2 | 262 | 390 |
| Total/Average for urgency | 2.45 | 1234 | 3640 | 2.27 | 5284 | 6487 |

| Number of people who need training | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | **Total** | Residential course | Online course | Online module | Webinar series | Other | **Total** |
| Digital forensics | 40 | 210 | | 10 | | 260 | 14 | 200 | 3 | 6 | 999 | 1222 |
| Internet Networking and Tracing | 15 | 10 | 12 | | | 37 | 75 | 250 | 5 | 2 | 999 | 1331 |
| Programming, Scripting, SQL | 57 | 270 | | 16 | | 343 | | 250 | 2 | | | 252 |
| Analytical and Visualisation | 46 | 20 | | | | 66 | 12 | 200 | 5 | | | 217 |
| Live Data Forensics | 61 | 20 | | 15 | | 96 | 12 | 200 | 6 | 15 | 999 | 1232 |
| Cybercrime legislation | | | 30 | 40 | | 70 | | 200 | 20 | 5 | | 225 |
| First responder | | 65 | 3 | | | 68 | 5 | 200 | 15 | 2 | | 222 |
| General Cybercrime Awareness | | 5 | 2 | | | 7 | 10 | | 10 | | | 20 |
| Open Source Intelligence | | 20 | 10 | 2 | 215 | 247 | 43 | 212 | 24 | | | 279 |
| Interviewing and Interrogation | | | 5 | 5 | | 10 | | | | 22 | | 22 |
| Investigation techniques | | 10 | 17 | 3 | | 30 | 40 | 7 | 15 | 200 | | 262 |
| **Total** | **219** | **630** | **79** | **91** | **215** | **1234** | **211** | **1719** | **105** | **252** | **2997** | **4231** |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Digital forensics | ad hoc | expert | external partners e.g. 7safe | Cybercrime Unit Investigations Teams | ability to support DF teams and awareness of what they require | 60 |
| Internet networking and tracing | basic | EC3 | investigators | | 65 | |
| Internet networking and tracing | regular | basic | ECTEG | LEA | train the trainer | 1 |
| Programming, scripting, SQL | basic | ECTEG | LEA | train the trainer | 1 | |
| Programming, scripting and SQL | regular | basic | ECTEG | LEA | train the trainer | 1 |
| Live data forensic | regular | basic | ECTEG | LEA | train the trainer | 1 |
| Cybercrime legislation | regular | expert | free online tools | Cybercrime Unit Investigations Teams | awareness of legislation | 60 |
| Cybercrime legislation | ad-hoc | basic | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| General Cybercrime Awareness | regular | expert | free online tools | Cybercrime Unit Investigations Teams | awareness for staff | 60 |
| General Cybercrime Awareness | mandatory | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Open source intelligence | ad hoc | L2/L3 | in house / external provider | Cybercrime Unit Investigations Teams | awareness of techniques all staff | 60 |
| Open source intelligence | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Open source intelligence | regular | basic | ECTEG | LEA | train the trainer | 1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Interviewing and investigation | ad hoc | basic | In house | Cybercrime Unit Investigations Teams | awareness of techniques | 60 |
| Investigation techniques | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Investigation techniques | regular | basic | ECTEG | LEA | train the trainer | 1 |

## Role: Digital Forensic Investigators and Examiners

Number of responses: 15

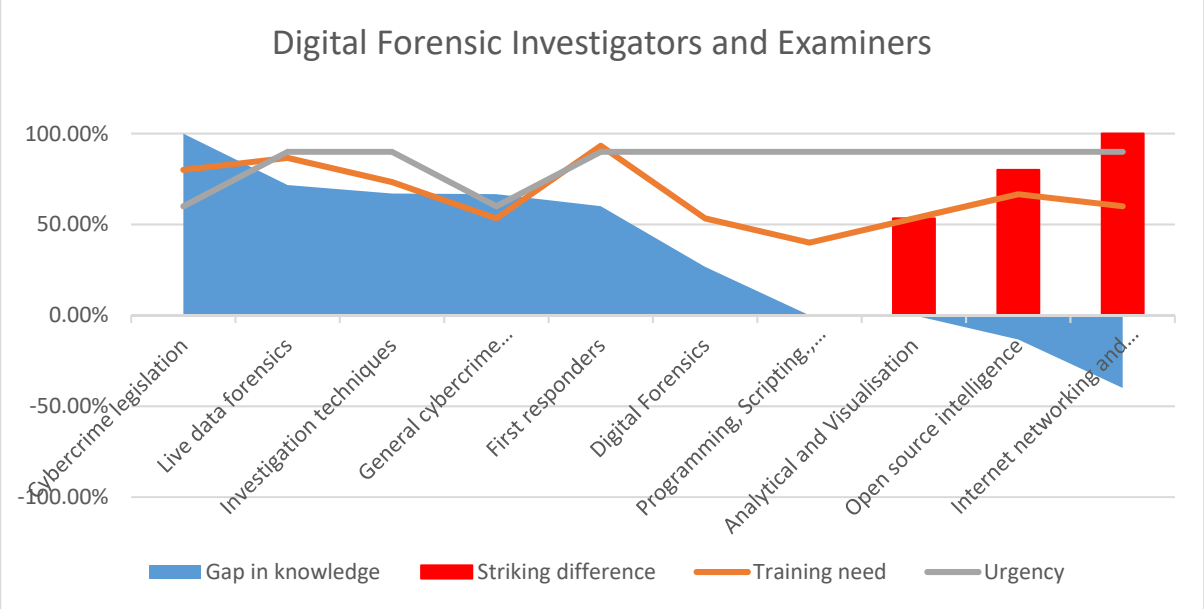
Countries, organisations represented: Belgium, Cyprus, Czech Republic, Europol-Ec3, Greece, Hungary, Iceland, Ireland, Latvia, Lithuania, Malta, Poland, Portugal, Slovakia, United Kingdom.

For digital forensic investigators and examiners, the Training Competency Framework defines the following competencies:

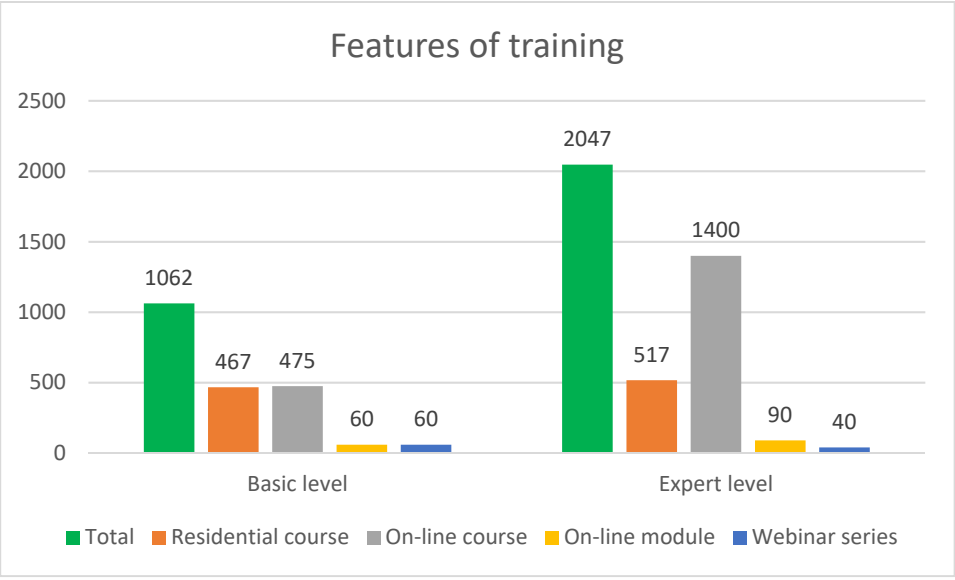
| Competency | Level of knowledge |
|---|---|
| Digital Forensics | Expert |
| Internet networking and Tracing | Basic |
| Programming, Scripting., SQL | Basic |
| Analytical and Visualisation | Basic |
| Live data forensics | Expert |
| Cybercrime legislation | Expert |
| General cybercrime awareness | Expert |
| First responders | Expert |
| Open source intelligence | Basic |
| Investigation techniques | Expert |

EU-level training needs in the order of gap between requested and existing level of competency:

1. Cybercrime legislation
2. Live data forensics
3. Investigation techniques
4. General cybercrime awareness
5. First responders
6. Digital Forensics
7. Programming, Scripting., SQL
8. Analytical and Visualisation
9. Open source intelligence
10. Internet networking and Tracing




The biggest gap in knowledge is in the competency of cybercrime legislation where the TCF expects expert level knowledge while the current level of knowledge is basic level. Not that large, but significant gaps exists in the competencies of live data forensics, Investigation techniques, general cybercrime awareness and first responders. In all these competencies there is national level training available, except for the competency of first responders. In the competencies where the TCF defines only basic level of knowledge, like analytical and visualisation, open source intelligence, internet networking and tracing digital forensic investigators and examiners have the required or even higher levels of knowledge. Still, the training need indicated by respondents is quite high in these competencies.




Altogether 2648 digital forensic investigators and examiners would need training, 63% of them at expert level training in the format of online courses. This would mean 3120 digital forensic investigators and examiners are to be trained in the 26 EU Member States. The training need is urgent in general, meaning that training in most cases should be delivered in 6 months.

24.33% of respondents indicated that there is training available on national level. The competency most addressed by training on national level is of digital forensics (44%) followed by investigation techniques (27%). Programming, scripting and SQL is the competency least targeted by training on national level (16%). There was no national level training indicated in the competency of first responders.

For detailed information, please see the tables below.

## Summary tables of training needs of digital forensic investigators and examiners

### Training need

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| First responders | 1.09 | 2 | 90.91% |
| Live data forensics | 1.18 | 2 | 81.82% |
| Cybercrime legislation | 1.27 | 2 | 72.73% |
| Digital Forensics | 1.45 | 2 | 54.55% |
| Internet networking and Tracing | 1.54 | 2 | 45.45% |
| General cybercrime awareness | 1.54 | 2 | 45.45% |
| Programming, Scripting., SQL | 0.81 | 1 | 18.18% |
| Analytical and Visualisation | 1.09 | 1 | -9.09% |
| Interviewing and investigation | 1.27 | 1 | -27.27% |
| Open Source Intelligence | 1.36 | 1 | -36.36% |
| Investigation techniques | 1.36 | 1 | -36.36% |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| Digital Forensics | 3 | 58 | 156 | 3 | 99 | 117 |
| Internet networking and Tracing | 3 | 36 | 117 | 3 | 329 | 130 |
| Programming, Scripting., SQL | 2 | 281 | 91 | 3 | 286 | 91 |
| Analytical and Visualisation | 3 | 44 | 104 | 3 | 52 | 260 |
| Live data forensics | 3 | 59 | 117 | 3 | 333 | 156 |
| Cybercrime legislation | 3 | 326 | 156 | 2 | 286 | 390 |
| General cybercrime awareness | 3 | 50 | 52 | 2 | 40 | 156 |
| First responders | 2 | 51 | 156 | 3 | 64 | 130 |
| Open source intelligence | 2 | 45 | 195 | 3 | 97 | 130 |
| Investigation techniques | 3 | 38 | 156 | 3 | 74 | 260 |
| Total/Average for urgency | 2.7 | 988 | 1300 | 2.8 | 1660 | 1820 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| Digital Forensics | 58 | | | | | 58 | 41 | 40 | 3 | 10 | 5 | 99 |
| Internet networking and Tracing | 11 | 20 | | | 5 | 36 | 47 | 274 | 3 | | 5 | 329 |
| Programming, Scripting., SQL | 24 | 250 | 4 | 3 | | 281 | 26 | 250 | 7 | 3 | | 286 |
| Analytical and Visualisation | 4 | 30 | 10 | | | 44 | 36 | | 16 | | | 52 |
| Live data forensics | 44 | 4 | | 6 | 5 | 59 | 62 | 250 | 6 | 10 | 5 | 333 |
| Cybercrime legislation | 1 | 254 | 31 | 40 | | 326 | | 250 | 6 | 30 | | 286 |
| General cybercrime awareness | 2 | | 2 | 46 | | 50 | 2 | 12 | | 26 | | 40 |
| First responders | 5 | 6 | 40 | | | 51 | 10 | 25 | 9 | 20 | | 64 |
| Open source intelligence | 10 | | | 35 | | 45 | 33 | 50 | 4 | 10 | | 97 |
| Investigation techniques | 2 | 10 | | 26 | | 38 | 27 | | 11 | | 36 | 74 |
| Total | 161 | 574 | 87 | 156 | 10 | 988 | 284 | 1151 | 65 | 109 | 51 | 1660 |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Digital forensics | Regular | Basic | Europol and CEPOL | Digital Forensic Investigators | The aim of the activity is to provide participants with an introduction to Open Source forensic software, file systems, data carving, evidential digital artefacts, networking, computer forensic strategies and live data forensics. It also aims to disseminate the latest investigation techniques and methods and to promote the mutual sharing of experience | 56 |
| Digital forensics | ad hoc | expert | External partners e.g. SANS | Cybercrime Unit Digital Investigations Teams | fully support cybercrime investigations and forensically examine digital evidence | 25 |
| Digital forensics | mandatory | basic/expert | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Digital forensics | regular | expert | International | Police officers | Development of knowledge | Depending on time period |
| Digital forensics | ad-hoc | basic | XRY | Digital Forensic investigators | Mobile Forensic | 2 |
| Digital forensics | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| Internet networking and Tracing | ad hoc | expert | External partners e.g. SANS | Cybercrime Unit Digital Investigations Teams | fully support cybercrime investigations and forensically examine digital evidence | 15 |
| Internet networking and Tracing | mandatory | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Internet networking and Tracing | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| Programming, scripting, SQL | ad hoc | expert | external partners e.g. QA / Learning Tree | Cybercrime Unit Digital Investigations Teams | fully support cybercrime investigations and forensically examine digital evidence | 10 |
| Programming, scripting, SQL | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| Programming, scripting, SQL | CEPOL/Online courses | basic/expert | CEPOL | digital investigators | increase knowledge | no information |
| Analytical and Visualisation | ad hoc | expert | external partners e.g. QA / Learning Tree | Cybercrime Unit Digital Investigations Teams | fully support cybercrime investigations and forensically examine digital evidence | 10 |
| Analytical and Visualisation | ad-hoc | basic | International | Police officers | Development of knowledge | Depending on time period |
| Analytical and Visualisation | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| Live data forensics | ad hoc | expert | External partners e.g. SANS | Cybercrime Unit Digital Investigations Teams | fully support investigations on scene | 10 |
| Live data forensics | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Live data forensics | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| Cybercrime legislation | ad hoc | basic | free online tools | Cybercrime Unit Digital Investigations Teams | awareness to ensure compliance and legality | 25 |
| Cybercrime legislation | mandatory | basic | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Cybercrime legislation | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| General cybercrime awareness | ad hoc | expert | free online tools | Cybercrime Unit Digital Investigations Teams | awareness for staff | 25 |
| General cybercrime awareness | mandatory | basic | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| General cybercrime awareness | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| First responders | ad hoc | basic | External partners e.g. SANS / 7safe | Cybercrime Unit Digital Investigations Teams | awareness to support investigations teams | 25 |
| First responders | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| First responders | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |
| Investigation techniques | ad hoc | basic | in house | Cybercrime Unit Digital Investigations Teams | awareness to support investigations teams | 25 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Investigation techniques | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Investigation techniques | mandatory | expert | The Polish Police | candidates for computer forensic experts | Computer Forensic Expert | Individual training |

## Role: Cyber experts

Number of responses: 17

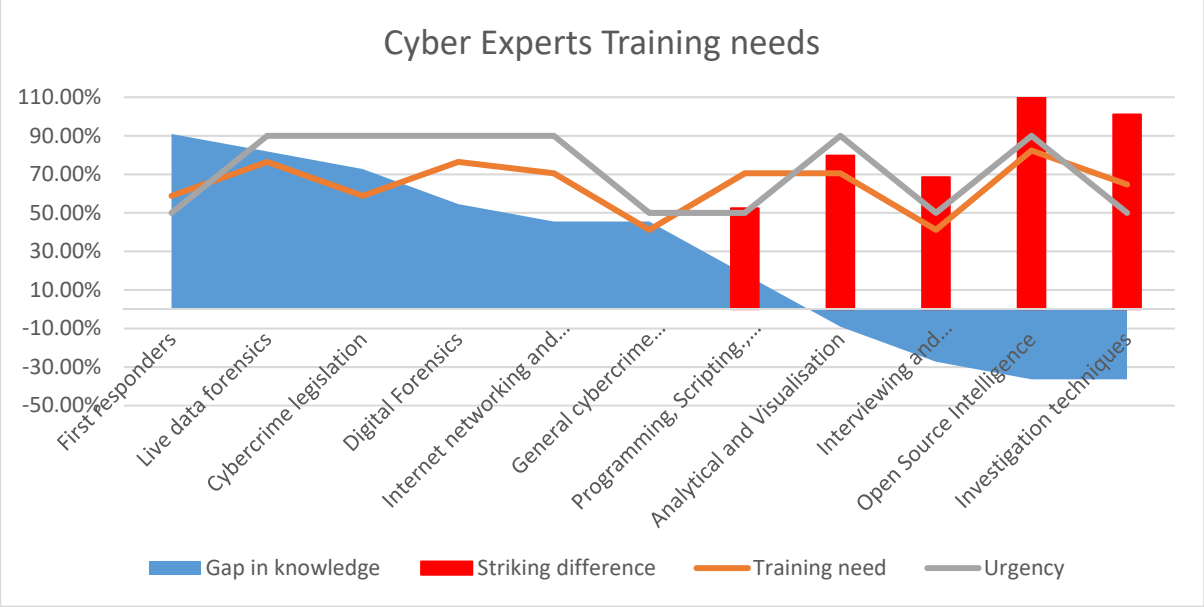
Countries, organisations represented: Austria, Belgium, Germany, Slovakia, Malta, Cyprus, Ireland, Czech Republic, Latvia, Slovenia, Poland, Greece, Hungary, Europol-Ec3, Switzerland, Iceland.

For cyber experts, the Training Competency Framework defines the following competencies:

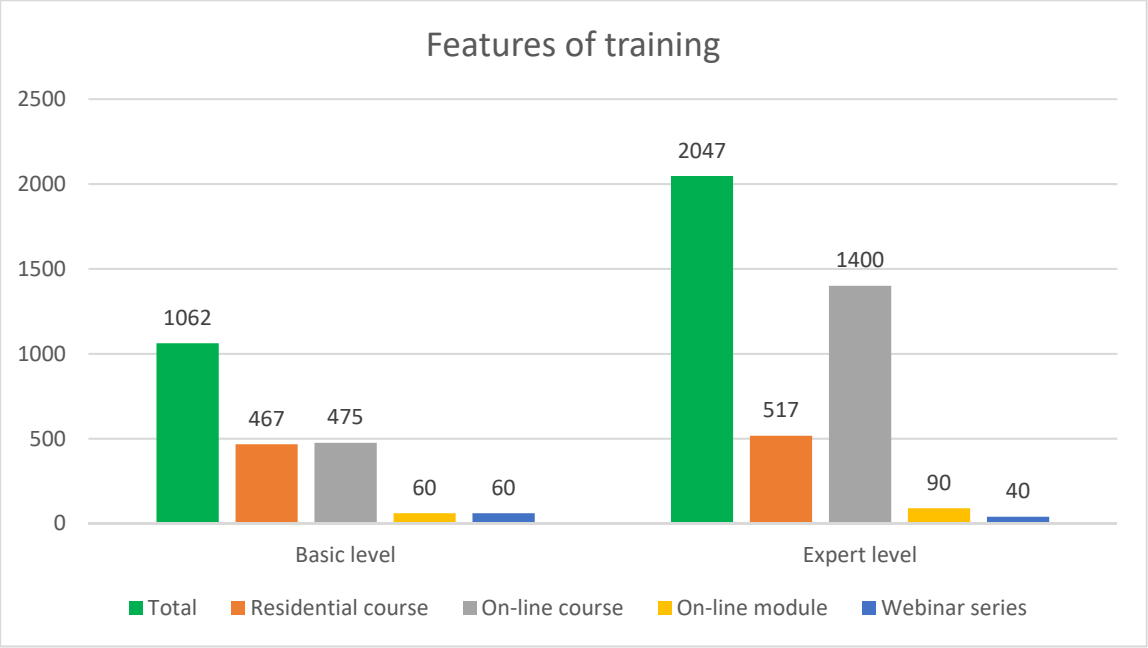
| Competency | Level of knowledge |
|---|---|
| First responders | Expert |
| Live data forensics | Expert |
| Cybercrime legislation | Expert |
| Digital Forensics | Expert |
| Internet networking and Tracing | Expert |
| General cybercrime awareness | Expert |
| Programming, Scripting., SQL | Basic |
| Analytical and Visualisation | Basic |
| Interviewing and investigation | Basic |
| Open Source Intelligence | Basic |
| Investigation techniques | Basic |

EU-level training needs in the order of gap between requested and existing level of competency:

1. First responders
2. Live data forensics
3. Cybercrime legislation
4. Digital Forensics
5. Internet networking and Tracing
6. General cybercrime awareness
7. Programming, Scripting., SQL
8. Analytical and Visualisation
9. Interviewing and investigation
10. Open Source Intelligence
11. Investigation techniques




The biggest gap in knowledge is in the competency of first responders where the TCF expects expert level knowledge while the current level of knowledge is just around basic level. Similarly, large gaps exist in the competencies of live data forensics and cybercrime legislation. In most of these competencies, 11% of respondents indicated the existence of training on national level. In the competencies where the TCF defines only basic level of knowledge, like programming, scripting, SQL, analytical and visualisation, interviewing and investigation, open source intelligence and investigation techniques cyber experts have the required or higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies.




Altogether, 3109 cyber experts would need training, 66% of them at expert level, generally in the format of residential activities or online courses. This would mean 17537 cyber experts are to be

trained in the 26 EU Member States. The training need is between low and high urgency meaning that training in most cases should be delivered in 6 months.

Only 8.27% of respondents indicated that there is training available on national level. The competencies where 11% of respondents indicated existing national level training are live data forensics, cybercrime legislation, general cybercrime awareness, open source intelligence, and first responder and investigation techniques. Internet networking and tracing, digital forensics, programming, scripting, SQL, analytical and visualisation and interviewing and interrogation are the competencies least targeted by training on national level (5%).

For detailed information, please see the tables below.

## Summary tables of training needs of cyber experts

### Training needs

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| First responders | 1.09 | 2 | 90.91% |
| Live data forensics | 1.18 | 2 | 81.82% |
| Cybercrime legislation | 1.27 | 2 | 72.73% |
| Digital Forensics | 1.45 | 2 | 54.55% |
| Internet networking and Tracing | 1.54 | 2 | 45.45% |
| General cybercrime awareness | 1.54 | 2 | 45.45% |
| Programming, Scripting., SQL | 0.81 | 1 | 18.18% |
| Analytical and Visualisation | 1.09 | 1 | -9.09% |
| Interviewing and investigation | 1.27 | 1 | -27.27% |
| Open Source Intelligence | 1.36 | 1 | -36.36% |
| Investigation techniques | 1.36 | 1 | -36.36% |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| First responders | 2 | 10 | 260 | 2 | 260 | 650 |
| Live data forensics | 3 | 17 | 221 | 3 | 256 | 195 |
| Cybercrime legislation | 3 | 250 | 1040 | 2 | 220 | 2860 |
| Digital Forensics | 3 | 215 | 2795 | 3 | 259 | 130 |
| Internet networking and Tracing | 3 | 215 | 2795 | 3 | 257 | 260 |
| General cybercrime awareness | 0 | 0 | 0 | 2 | 5 | 130 |
| Programming, Scripting., SQL | 2 | 213 | 52 | 2 | 241 | 1040 |
| Analytical and Visualisation | 3 | 52 | 156 | 2 | 201 | 2613 |
| Interviewing and investigation | 0 | 0 | 0 | 2 | 20 | 520 |
| Open Source Intelligence | 3 | 30 | 390 | 3 | 266 | 130 |
| Investigation techniques | 1 | 60 | 780 | 2 | 62 | 520 |
| Total/Average for urgency | 2.3 | 1062 | 8489 | 2.36 | 2047 | 9048 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| First responders | | | 10 | | | 10 | | 200 | 50 | 10 | | 260 |
| Live data forensics | 17 | | | | | 17 | 56 | 200 | | | | 256 |
| Cybercrime legislation | | 200 | 40 | 10 | | 250 | | 200 | 20 | | | 220 |
| Digital Forensics | 215 | | | | | 215 | 259 | | | | | 259 |
| Internet networking and Tracing | 215 | | | | | 215 | 60 | 200 | | | | 260 |
| General cybercrime awareness | | | | | | | | | | 5 | | 5 |
| Programming, Scripting., SQL | 3 | 210 | | | | 213 | 41 | 200 | | | | 241 |
| Analytical and Visualisation | 2 | 50 | | | | 52 | 1 | 200 | | | | 201 |
| Interviewing and investigation | | | | | | | | | 20 | | | 20 |
| Open Source Intelligence | 15 | 15 | | | | 30 | 61 | 200 | | 5 | | 266 |
| Investigation techniques | | | 10 | 50 | | 60 | 42 | | | 20 | | 62 |
| Total | 467 | 475 | 60 | 60 | 0 | 1062 | 520 | 1400 | 90 | 40 | 0 | 2050 |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Digital forensics | mandatory | basic/expert | various | Open to members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Internet networking and tracing | ad-hoc | basic/expert | various | Open to members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Programming, scripting, SQL | Regular | Expert | Other | Cyber experts | Specialisation | 5 |
| Analytical and visualisation | Regular | Expert | Other | Cyber experts | Specialisation | 5 |
| Live data forensic | Expert | Other | Cyber experts | Specialisation | 5 | |
| Live data forensic | basic/expert | various | Open to members working in the cybercrime bureau | Increase knowledge | 1-25 | |
| Cybercrime legislation | Regular | Expert | Other | Cyber experts | Improvement | 10 |
| Cybercrime legislation | mandatory | basic | internally | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| General cybercrime awareness | Regular | Expert | Other | Cyber experts | Improvement | 10 |
| General cybercrime awareness | mandatory | basic/expert | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| First responder | Regular | Expert | Other | Cyber experts | Improvement | 5 |
| First responder | ad-hoc | basic/expert | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Open source intelligence | Regular | Expert | Other | Cyber experts | Improvement | 10 |
| Open source intelligence | ad-hoc | basic | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |
| Interviewing and investigation | mandatory | basic | internally | Open to all members of An Garda Siochana | Increase knowledge | 1-25 |
| Investigation techniques | Regular | Expert | Other | Cyber experts | Improvement | 10 |
| Investigation techniques | ad-hoc | basic/expert | various | Open to all members working in the cybercrime bureau | Increase knowledge | 1-25 |

## Role: First responders

Number of responses: 11

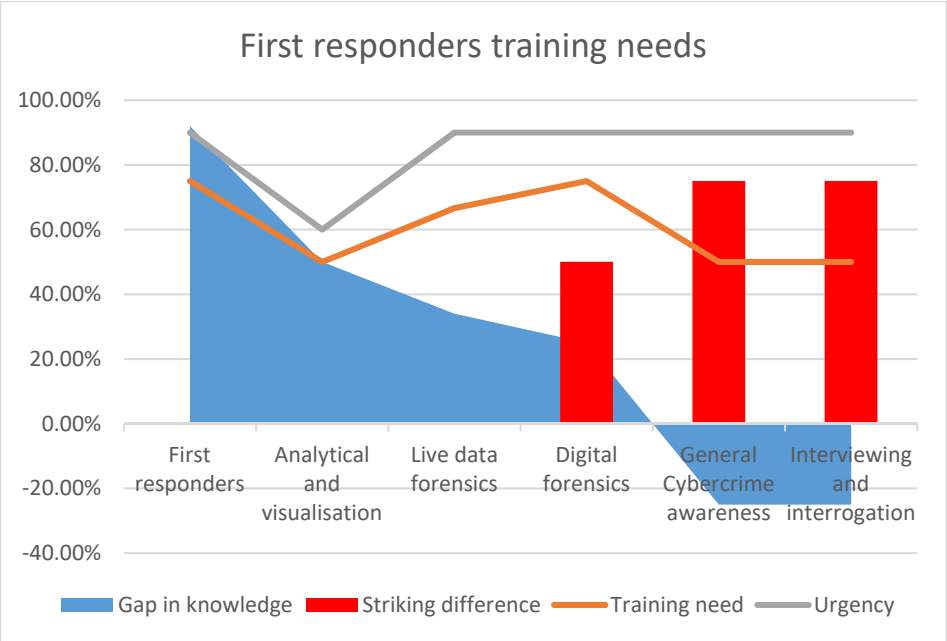
Countries, organisations represented: Cyprus, Czech Republic, Greece, Hungary, Iceland, Ireland, Malta, Poland, Portugal, United Kingdom, Europol's EC3

For first responders, the Training Competency Framework defines the following competencies:

| Competency | Level of knowledge |
|---|---|
| Digital forensics | Basic |
| Analytical and visualisation | Basic |
| Live data forensics | Basic |
| General Cybercrime awareness | Basic |
| First responders | Expert |
| Interviewing and interrogation | Basic |

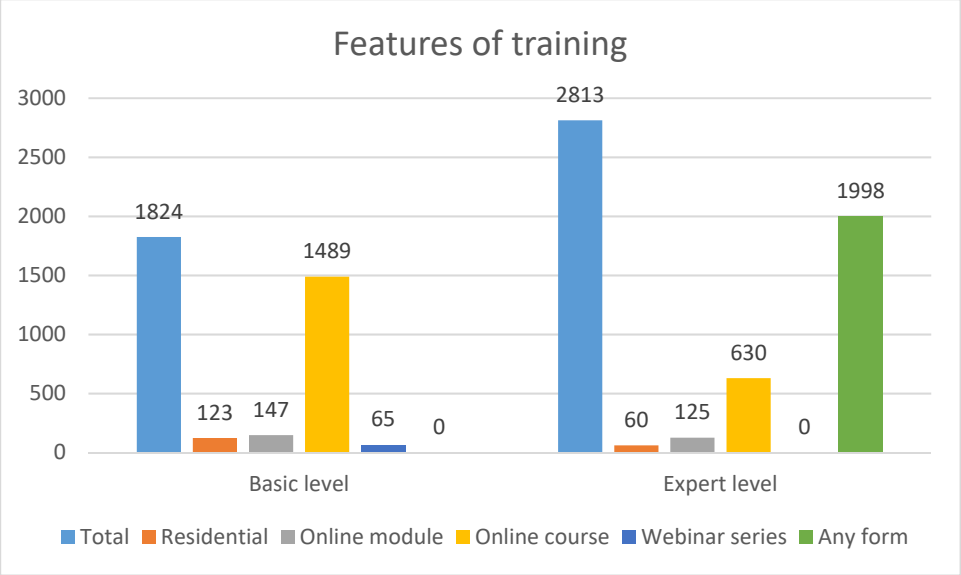
EU-level training needs in the order of gap between requested and existing level of competency:

1. First responders
2. Analytical and visualisation
3. Live data forensic
4. Digital forensics
5. Interviewing and interrogation
6. General cybercrime awareness




The biggest gap in knowledge is in the competency of first responders where the TCF expects expert level knowledge while the current level of knowledge is just around basic level. Similarly, large gaps exist in the competency of live data forensics and cybercrime legislation. In the competencies where

the TCF defines only basic level of knowledge, like programming, scripting, SQL, analytical and visualisation, interviewing and investigation, open source intelligence and investigation techniques cyber experts have the required or higher level of knowledge. Still, the training need indicated by respondents is quite high in these competencies.




Altogether 7130 first responders would need training, 63% at expert level training, generally in the format of online courses. This would mean 49.270 first responders are to be trained in the 26 EU Member States. The training need is urgent in general, meaning that training in most cases should be delivered in 6 months.

Only 5.2% of respondents indicated that there is training available on national level. The competency most addressed by training on national level is of general cybercrime awareness where 11% of respondents indicated existing training. In the rest of the competencies, either there is no training available or only 5% of respondents indicated the possibility national level training.

For detailed information on training needs please see the tables below.

## Summary tables of training needs of first responders

### Training needs

| Competency | Current level of competency | Expected level of competency | Gap in knowledge |
|---|---|---|---|
| First responders | 1.08 | 2 | 0.92 |
| Analytical and visualisation | 0.5 | 1 | 0.5 |
| Live data forensics | 0.66 | 1 | 0.34 |
| Digital forensics | 0.75 | 1 | 0.25 |
| General Cybercrime awareness | 1.25 | 1 | -0.25 |
| Interviewing and interrogation | 1.25 | 1 | -0.25 |

| Competency | Basic level | | | Expert level | | |
|---|---|---|---|---|---|---|
| | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU | Urgency (1-low, 2-medium, 3-high) | Number of participants | Number of participants extrapolated to the EU |
| First responders | 3 | 276 | 871 | 3 | 1169 | 2080 |
| Analytical and visualisation | 2 | 74 | 520 | 2 | 210 | 5460 |
| Live data forensics | 3 | 794 | 1560 | 2 | 1199 | 15587 |
| Digital forensics | 3 | 680 | 2860 | 2 | 235 | 3055 |
| General Cybercrime awareness | 3 | 1059 | 13767 | 2 | 295 | 1820 |
| Interviewing and interrogation | 3 | 1064 | 1300 | 3 | 75 | 390 |
| Total/Average for urgency | 2.83 | 3947 | 20878 | 2.33 | 3183 | 28392 |

| Number of participants | Basic level | | | | | | Expert level | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Residential course | Online course | Online module | Webinar series | Other | Total | Residential course | Online course | Online module | Webinar series | Other | Total |
| First responders | 4 | 17 | 205 | 50 | | 276 | 60 | 100 | 10 | | 999 | 1169 |
| Analytical and visualisation | 4 | 20 | 50 | | | 74 | | | 210 | | | 210 |
| Live data forensics | 60 | | 719 | 15 | | 794 | | | 200 | | 999 | 1199 |
| Digital forensics | 55 | 110 | 515 | | | 680 | | 25 | 210 | | | 235 |
| General Cybercrime awareness | | 60 | | | 999 | 1059 | | 10 | 215 | 70 | | 295 |
| Interviewing and interrogation | 50 | | | 15 | 999 | 1064 | 15 | | 10 | 50 | | 75 |
| Total | 173 | 207 | 1489 | 80 | 1998 | 3947 | 75 | 135 | 855 | 120 | 1998 | 3183 |

## Existing training

| Competency | Regularity | Proficiency level | Delivered by | Target group | Aim | Number of participants |
|---|---|---|---|---|---|---|
| Digital Forensics | Regular | Expert | Other | First responders | Specialisation | 10 |
| Live data forensics | Regular | Expert | Other | First responders | Specialisation | 10 |
| General Cybercrime Awareness | Regular | Expert | Other | First responders | Specialisation | 10 |
| General Cybercrime Awareness | ad-hoc | basic | CYBERCRIME DIVISION | cyber liaison officers | General Cybercrime Awareness | 104 |
| First responder | Regular | Expert | Other | First responders | Specialisation | 8 |

# Annex 1.

Training Competency Framework