EU law enforcement training needs on digital skills and the use of new technologies
Assessment and Analyses of Training Needs

EU-STNA ➔ OTNA ➔ micro TNA

CEPOL training portfolio
To provide the most suitable training for law enforcement officials across the EU
EU-STNA

2022-2025
Methodology

Analysis and reporting 2021

Desk research
Expert group consultations
Prioritisation, training volume estimation
Report
Mid-term review
Q3-4 2023

Implementation 2022-2025

Implementation

Jan-Mar 2021
Mar-May 2021
Jun-Sep 2021
Oct-Dec 2021
Q1-2 2024
Findings

- **8 core capability gaps**
  where law enforcement officials need capacity building through training

- **230 training needs**

- **17 thematic areas**

- **9 other specific training needs**

Member States indicated

- **110,368 law enforcement officials**
  needing EU-level training in these areas
Findings: core capability gaps

- Digital skills and use of new technologies
- High-risk criminal networks
- Financial investigations
- Cooperation, information exchange, and interoperability
- Crime prevention
- Document fraud
- Forensics
- Fundamental rights and data protection
Detailed list of training priorities

Cybersecurity fundamentals for EU officials’ everyday use (cyber hygiene, cybersecurity guidelines, secure exchange of information, physical security).

Raising awareness of the most important cyber-threats (e-mail based attacks, web-based attacks, DDoS attacks, social media scams). Understanding the cybersecurity challenges from the modern technologies, like AI or 5G.

Better, modern and validated tools and training materials for tackling activities related to disinformation and fake news that are considered as crime or could lead to crime and are supported by advanced digital technologies.
### Detailed list of training priorities

**Digital investigation:** OSINT, dark net, cyber threat intelligence (CTI) knowledge management, decryption, use of AI, big data analysis, quantitative and qualitative analysis methods, internet of things, advanced use of camera systems, drones, exoskeletons and speech processors, big data analysis for prediction of criminal behaviour, cryptocurrencies

**Digital forensics**

**Victims’ protection**

**Fundamental rights and data protection**
Findings: thematic areas

- Cyber-attacks
- Criminal finances, money laundering and asset recovery
- Counter-terrorism
- Trafficking of human beings
- Drug trafficking
- Migrant smuggling
- Child sexual exploitation
- Online fraud schemes
- Organised property crime
Cyber-attacks

1. Investigating cyber-attacks on information systems and modus operandi: analysing latest cyber-attacks and EU emergency response; developing alternative investigation techniques and EU tools, including their use
2. Latest challenges for dealing with encryption, anonymisation and bulletproof hosting services
3. Identifying, handling, securing, preserving, analysing and exchanging e-evidence
4. Combatting crime-as-a-service used by criminals and criminal groups in illegal activities
5. Effective international cooperation
6. Protocols to tackle large-scale cyber-attacks
Cyber-attacks

7. Raising awareness of cyber-attacks for EU agencies, law enforcement agencies and the public, including a coordinated approach for prevention; cyber-enabled and cyber-dependent crime awareness, cyber threats and cybercrime investigation

8. Big data analysis

9. Blockchain analysis

10. Using artificial intelligence, machine learning and deep learning in cybercrime investigation

11. Cybercriminal profiling and motivation analysis

12. Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection
OTNA

2023-2025 and 2020-2022
OTNA methodology

• Developed by CEPOL (32/2017/MB, 9/2020/MB)
• Respondents: MS experts
• Via on-line survey and interviews
• Valid for 3 years
OTNA methodology

- Respondernt nominatio
  n via CNUs
- Questionnaire development with expert group
- Data gathering
- Analysis, interviews
- Draft report
- Validation and portfolio design by expert group
- Publicatio
OTNA 2023
Digital skills and use of new technologies

<table>
<thead>
<tr>
<th>EU-STNA topics</th>
<th>Relevance</th>
<th>Urgency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiles</td>
<td>Number of participants</td>
<td></td>
</tr>
<tr>
<td>Proficiency level</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Response rate

- 45 responses
- 21 MS, Europol and Frontex
- 15 252 LE officials represented
- 81% of MS represented

Institutions:
- Police: 82%
- Customs: 11%
- Border Police/Border Guard: 4%
- Other: 2%
<table>
<thead>
<tr>
<th>Main Topic</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital investigations</td>
<td>100 %</td>
</tr>
<tr>
<td>Use of new technologies</td>
<td>90 %</td>
</tr>
<tr>
<td>Digital forensics</td>
<td>90 %</td>
</tr>
<tr>
<td>Cybersecurity fundamentals for EU law enforcement official’s everyday use and awareness raising</td>
<td>67 %</td>
</tr>
<tr>
<td>Financial investigations</td>
<td>57 %</td>
</tr>
<tr>
<td>Disinformation and fake news</td>
<td>43 %</td>
</tr>
<tr>
<td>Common technical standards</td>
<td>38 %</td>
</tr>
<tr>
<td>Victim’s protection (how to protect victim’s rights during investigations)</td>
<td>29 %</td>
</tr>
</tbody>
</table>
Profiles: investigators, experts on forensics and IT analysts, intelligence officers, managers and cybersecurity officials, prosecutors, investigative judges and magistrates

<table>
<thead>
<tr>
<th>Proficiency level</th>
<th>Number of participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>3081</td>
</tr>
<tr>
<td>Practitioner</td>
<td>2054</td>
</tr>
<tr>
<td>Advanced practitioner</td>
<td>2080</td>
</tr>
<tr>
<td>Expert</td>
<td>1469</td>
</tr>
<tr>
<td>Train-the-trainer</td>
<td>923</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>9607</strong></td>
</tr>
</tbody>
</table>
## OTNA Conclusions

### Most relevant topics
- Digital investigations
- Use of new technologies
- Digital forensics

### Proficiency levels
- Awareness
- Advanced practitioner
- Practitioner

### New training needed
- Use of new technologies
- Cybersecurity fundamentals
- IoT
- Disinformation & fake news
Training needs – OTNA, Cybercrime 2020

Most training should target

- General criminal investigators
- Digital forensic investigators and examiners
- Cyber experts

Skills to be mostly developed

- First responder
- Live data forensic
- Cybercrime legislation
CEPOL training portfolio

Digital investigations

Financial investigations

Cybersecurity fundamentals by EU Agency for Cybersecurity

Digital forensics

Use of new technologies

Disinformation and fake news
Top priorities for new training

2023-2025
Use of new technologies

- Artificial Intelligence – combine data protection and tools with big data analysis; legal framework and constraints once the AI Act is adopted
- Big data analysis – hands on training on tools, analysis, etc., methodology, approach; various types of data can be retrieved and you need the proper tools to correlate data

Disinformation and fake news

- Deep fakes – some practical tools on how to find information, how to detect manipulation
Awareness level (webinars or e-lessons)

Use of new technologies

- Illegal use of drones by criminals, including aspects of fundamental rights and data protection
- Use of cameras – this is what we have, how to use, what to avoid, including aspects of fundamental rights and data protection
- 5G – use of 5G by criminals and by law enforcement, including aspects of fundamental rights and data protection
- Use of automotive by law enforcement, including aspects of fundamental rights and data protection
- Automotive forensics search, including aspects of fundamental rights and data protection

Disinformation and fake news

- Detecting tampered evidences, including aspects of fundamental rights and data protection

Update of Cyberbites
Conclusions

- High need for training in digital skills and in new technologies
- Training on EU level does not satisfy the demand
- New training activities to be developed
- More resources needed to prepare law enforcement for the digital age
Questions?

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, Ó utca 27., Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu