# Operational Training Needs Analysis

## EU law enforcement training needs on digital skills and the use of new technologies

EDUCATE
INNOVATE
MOTIVATE

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

# 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 | Implementation 2022-2025

Desk research

Jan-Mar 2021

Expert group consultations

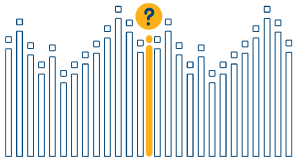
Mar-May 2021

Prioritisation, training volume estimation

Jun-Sep 2021

Report

Oct-Dec 2021



Mid-term review

Q3-4 2023

Evaluation

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.

CEPOL

# 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

CEPOL

# 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

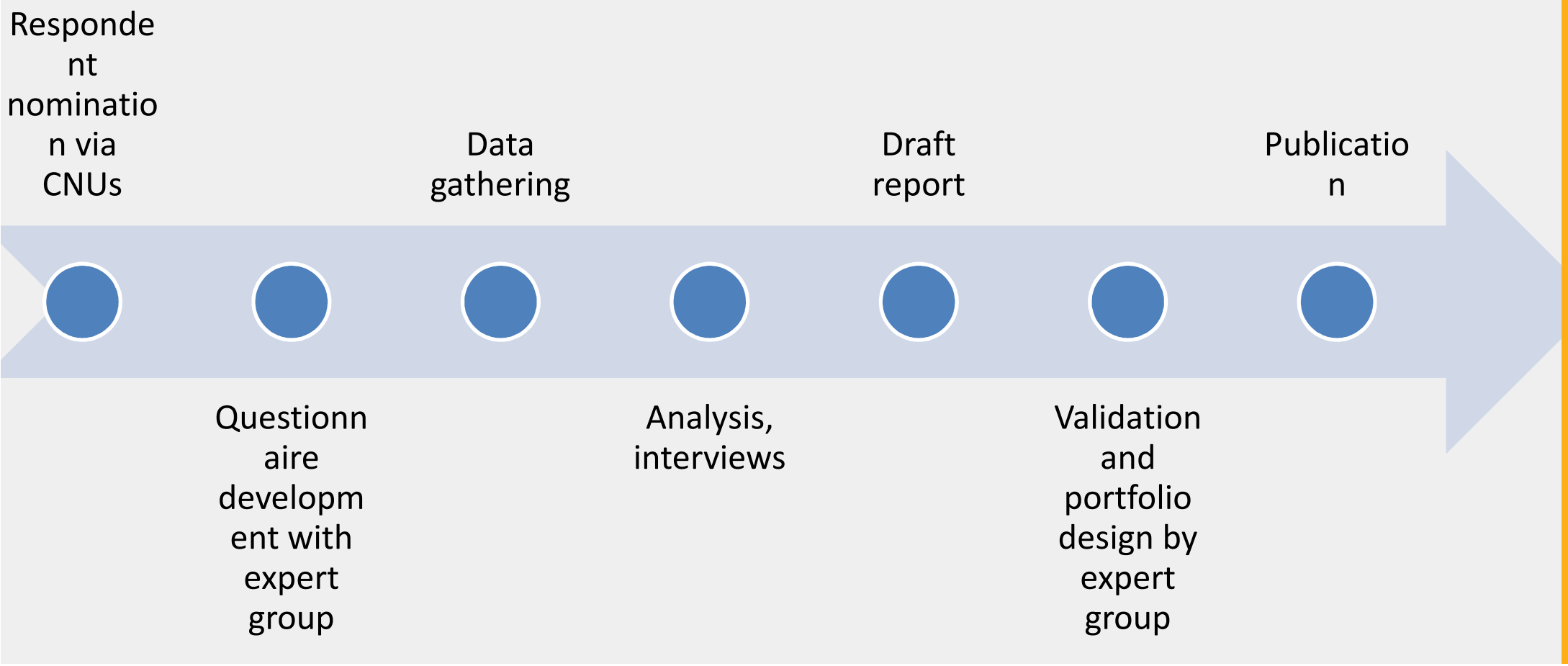
# OTNA

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



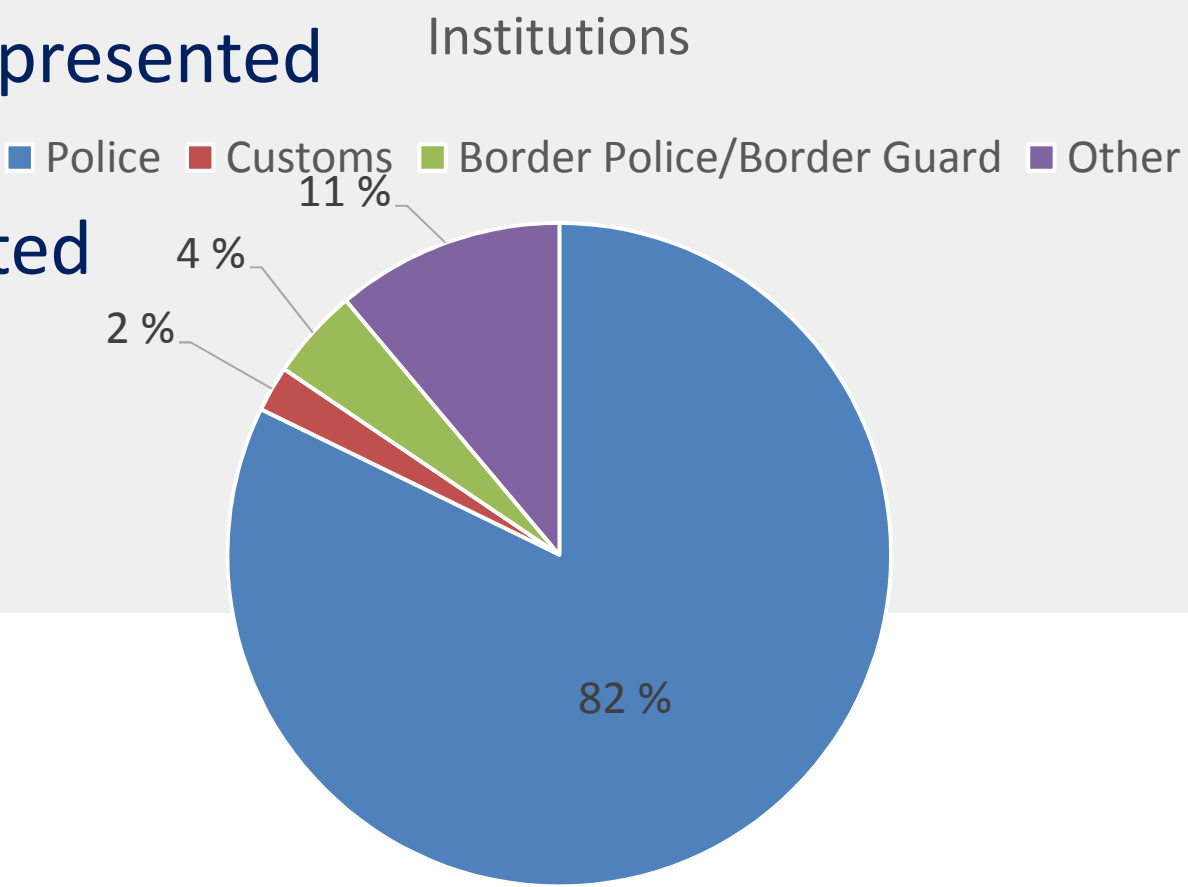
# OTNA 2023
# Digital skills and use of new technologies

| | | |
|---|---|---|
| EU-STNA topics | Relevance | Urgency |
| Proficiency level | Profiles | Number of participants |

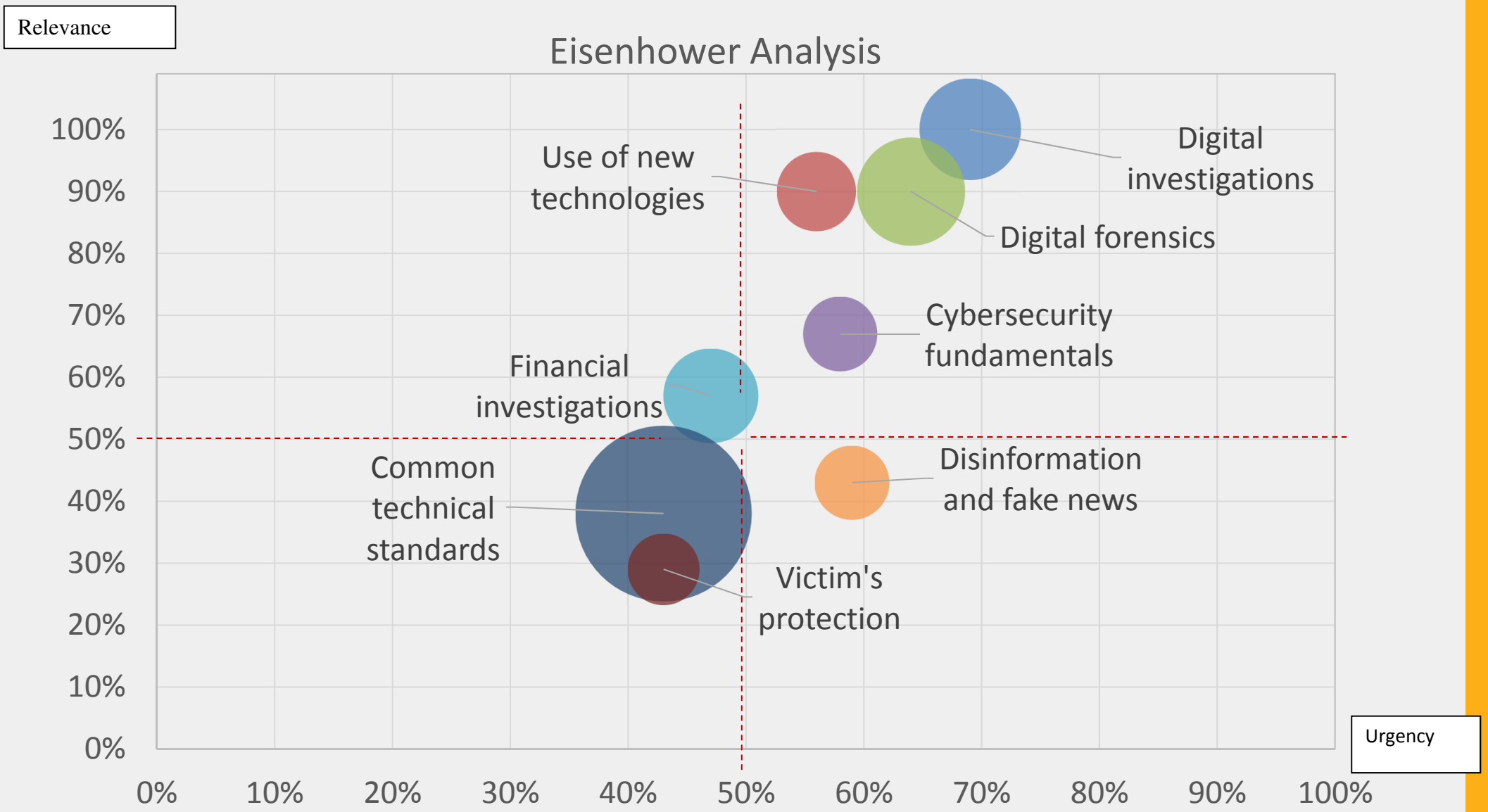
CEPOL

# Response rate

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



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


Relevance
Eisenhower Analysis
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Use of new technologies
Digital investigations
Digital forensics
Cybersecurity fundamentals
Financial investigations
Common technical standards
Disinformation and fake news
Victim's protection
Urgency

# NUMBER OF PARTICIPANTS

| Proficiency level | Number of participants |
|---|---|
| **Awareness** | 3081 |
| **Practitioner** | 2054 |
| **Advanced practitioner** | 2080 |
| **Expert** | 1469 |
| **Train-the-trainer** | 923 |
| **Total** | **9607** |

Profiles: investigators, experts on forensics and IT
analysts, intelligence officers, managers and cybersecurity officials
prosecutors, investigative judges and magistrates

# OTNA Conclusions

| Most relevant topics | Proficiency levels | New training needed |
| --- | --- | --- |
| • Digital investigations<br>• Use of new technologies<br>• Digital forensics | • Awareness<br>• Advanced practitioner<br>• Practitioner | • Use of new technologies<br>• Cybersecurity fundamentals<br>• IoT<br>• Disinformation & fake news |

# Training needs – OTNA, Cybercrime 2020

## Most training should target

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

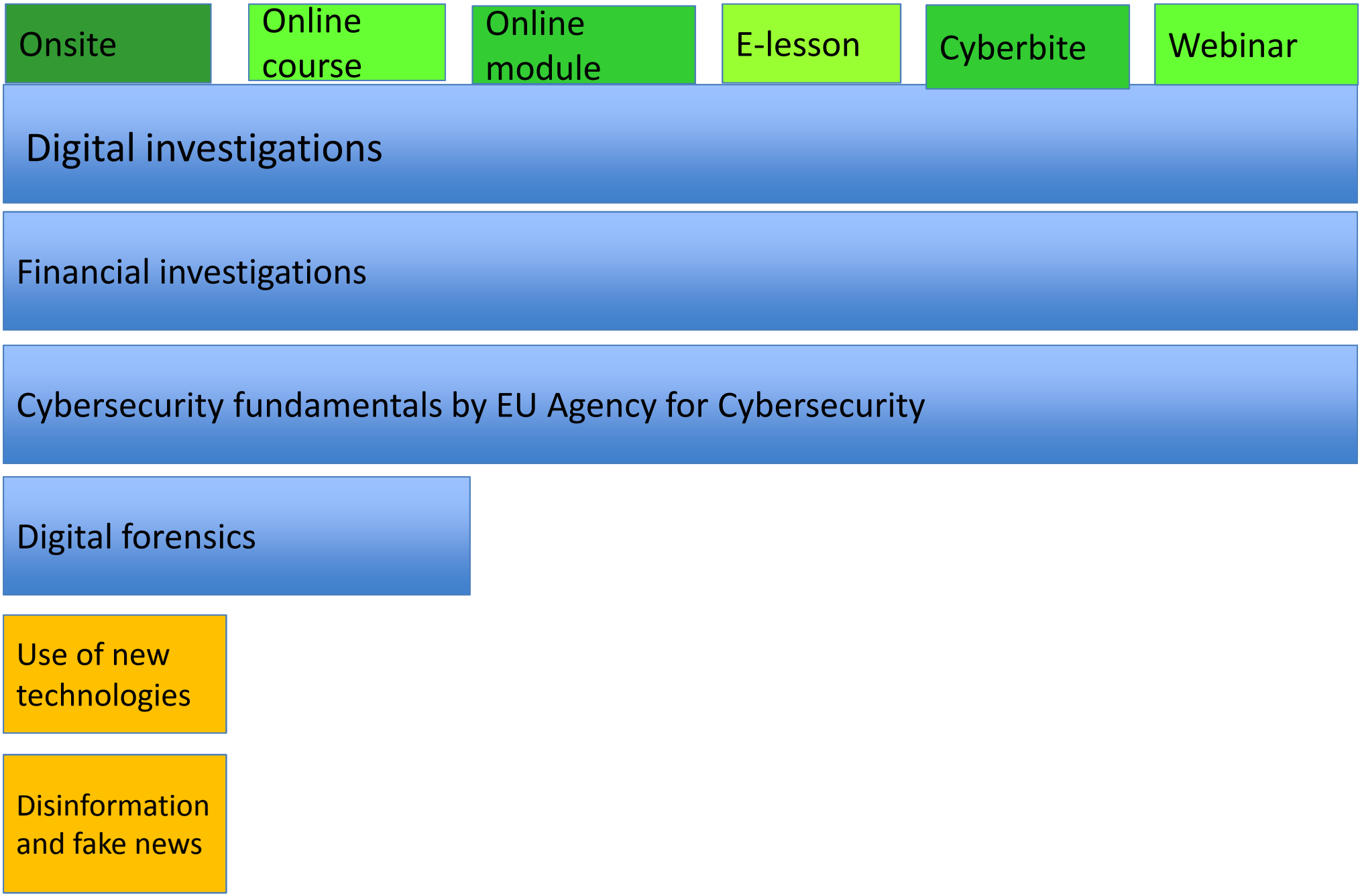
## Skills to be mostly developed

- First responder
- Live data forensic
- Cybercrime legislation

# CEPOL Training portfolio

2022

# CEPOL training portfolio



# Top priorities for new training

2023-2025

# Practitioners/advanced practitioner level (online modules or online courses)

## 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

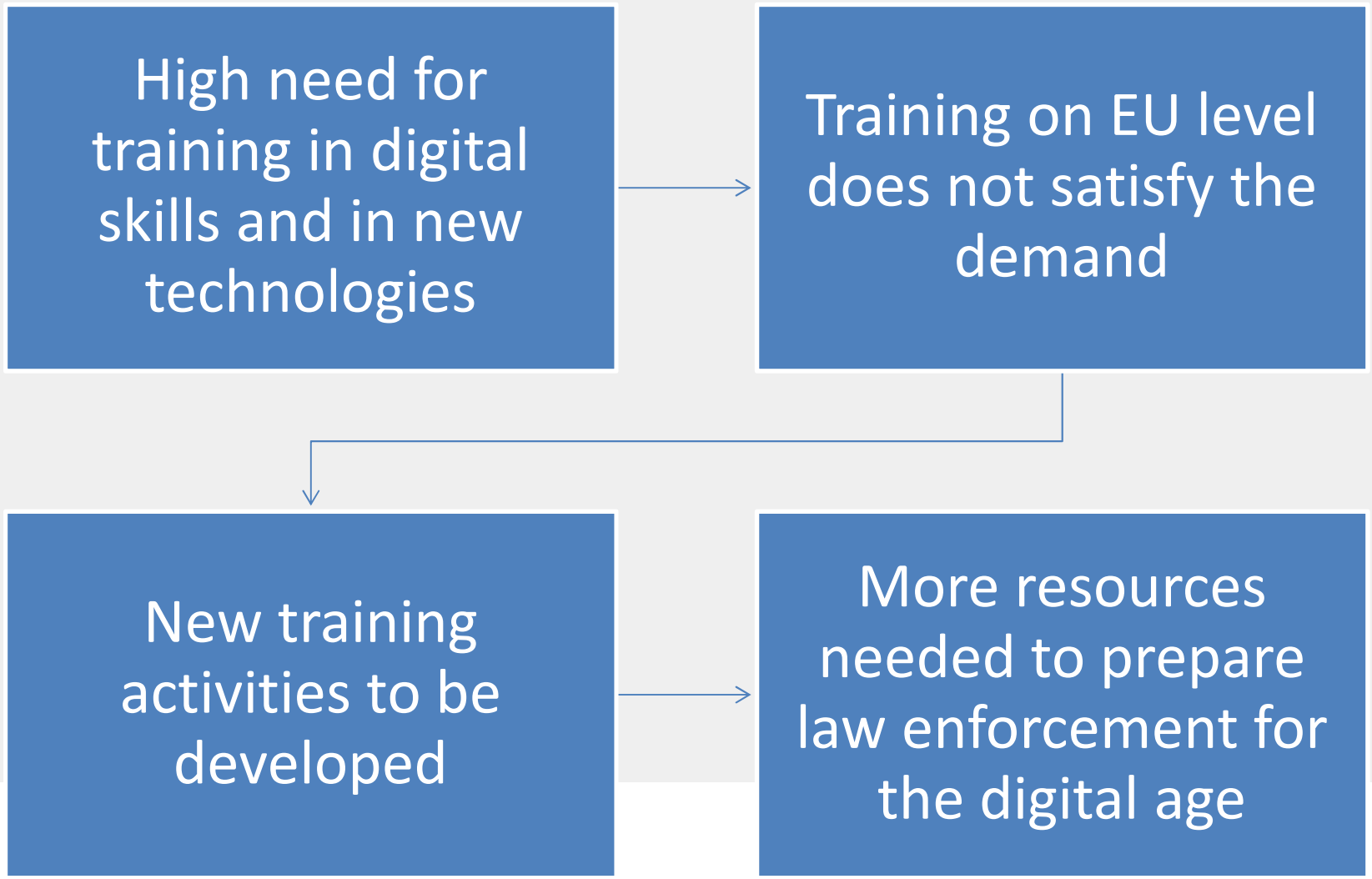
- Illegal use of drones by criminals, including aspects of fundamental rights and data protection
- Use of cameras –this is what we have, how to use, what to avoid, including aspects of fundamental rights and data protection
- 5G – use of 5G by criminals and by law enforcement, including aspects of fundamental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



# 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

CEPOL