# International workshop on conducting criminal investigations of ransomware attacks

EDUCATE
INNOVATE
MOTIVATE

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

# CEPOL Cybercrime Academy


**Specialised law enforcement training centre (HU)**

- Opened in June 2019 in Budapest
- Capacity to host up to 85 participants
- Main cooperation partners:
  - EUROPOL, Interpol, ECTEG, EJTN, CoE, ENISA

- Excellent facilities to train ever growing demand for cyber training form EU & beyond

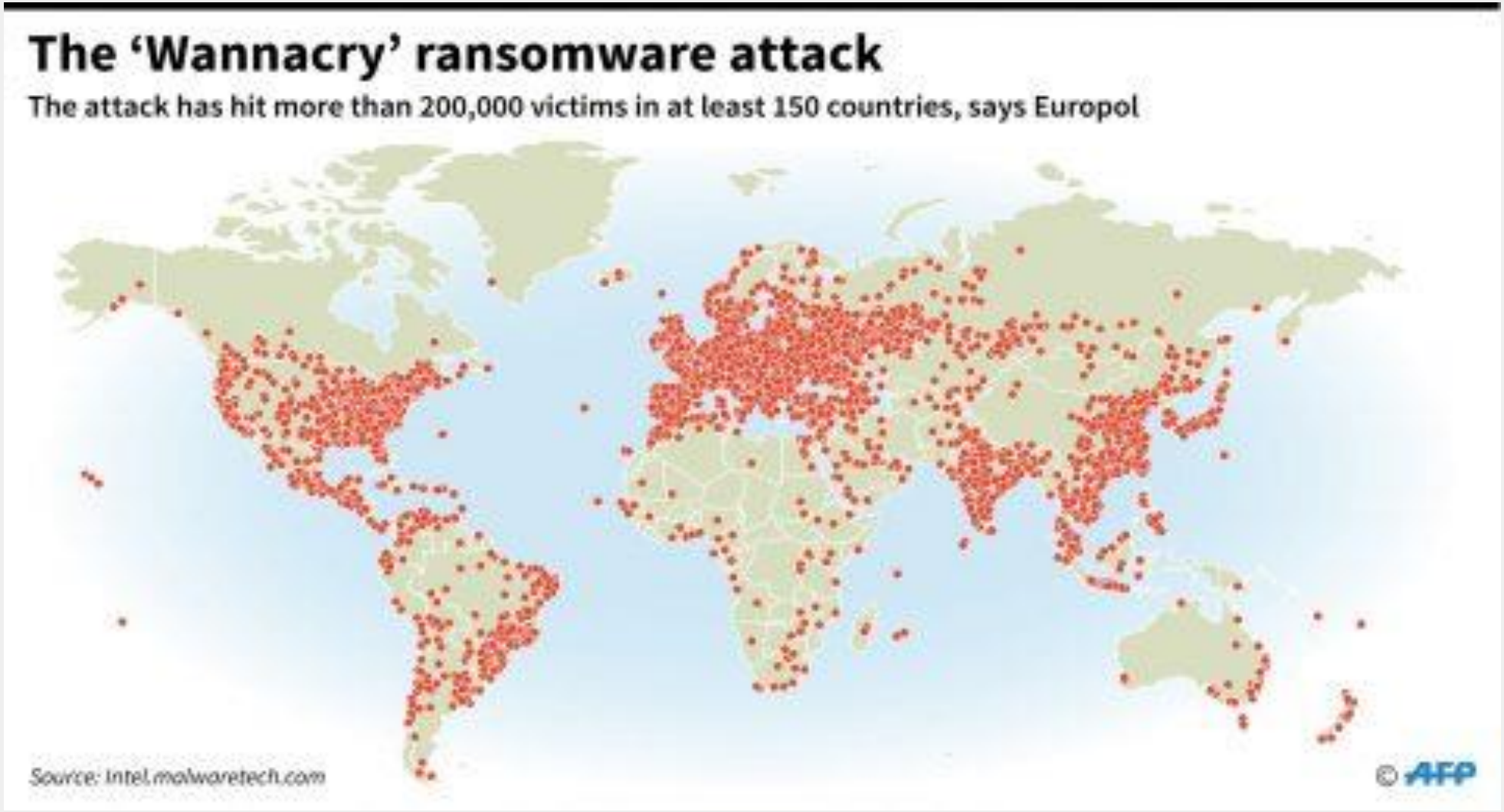
# EU STNA 2022-2025

## Relevance rate of subtopics from prioritised main topics

| Main topic | Subtopic | Relevance |
|---|---|---|
| Digital investigations | Open-Source Intelligence (OSINT) | 80 % |
| | Mobile devices for investigation | 78 % |
| | Cyberattacks (Ransomware, DDOS, Botnets) | 78 % |
| | Encryption, Anonymization techniques (VPN, Spoof calls, Sim boxes) | 77 % |
| | Software/tools developed to identify darkweb crimes | 75 % |
| | Darknet, what is darkweb, how to use darkweb | 74 % |
| | Digital fingerprints and metadata to identify persons and devices | 74 % |
| | Raw data analysis | 72 % |
| | Big data analysis, e.g. prediction of criminal behaviour with big data analysis | 71 % |
| | Analysis techniques/tools for many types of data (normalization, correlation, and fusion) including technical data from different domains | 70 % |
| | Information technology as a knowledge management enabler | 65 % |
| | Cloud platforms | 64 % |
| | Use of Artificial Intelligence, including AI risks towards fundamental rights, especially on face recognition systems | 63 % |
| | Internet of Things | 63 % |
| | Lawful interception | 62 % |

CEPOL

# Ransomware and Cryptocurrencies



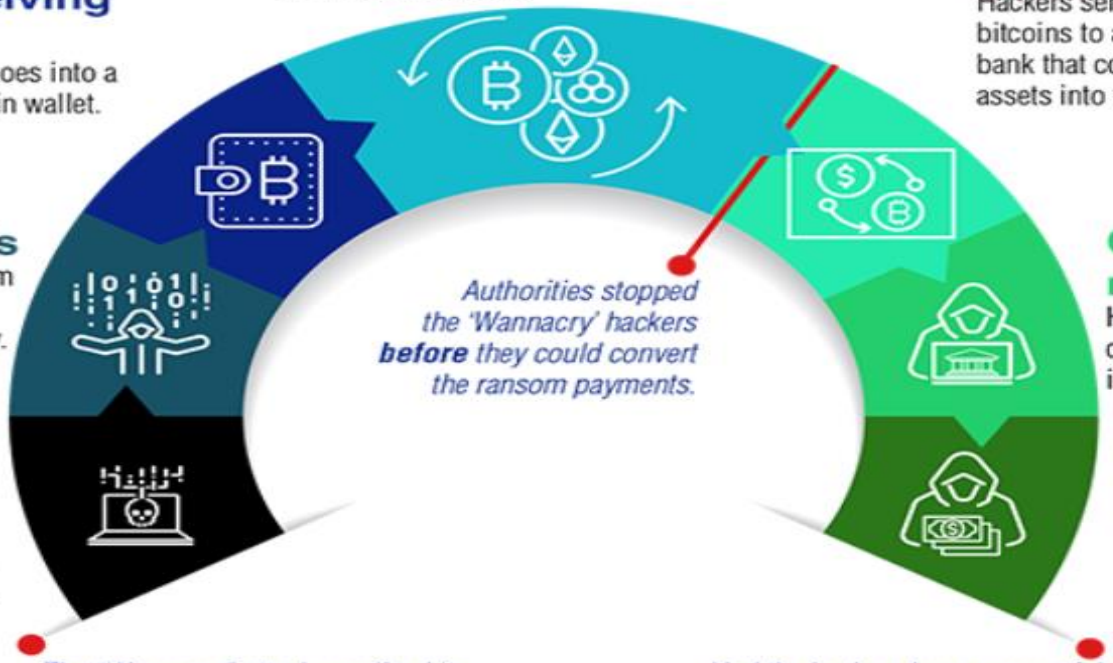
# Stages of a ransomware attack

**Layering**
Multiple transactions convert the payments from one virtual asset into another to remove all links to the crime.

**Hackers' receiving wallet**
Each ransom payment goes into a publicly identified bitcoin wallet.

**Virtual Asset Service Provider**
Hackers send the 'cleaned' bitcoins to a service provider or bank that converts the virtual assets into fiat money.

**Ransom payments**
Victims pay the hackers a ransom in Bitcoin to decrypt their computer & resume their activity.



**Conversion into regulated currency**
Hackers receive the bitcoins in the currency of their choice, ready to invest in a bank.

and spend.

**Virus**
Computers are infected with a virus, disabling businesses, even hospitals, until a ransom is paid.

*Authorities stopped the 'Wannacry' hackers **before** they could convert the ransom payments.*

*The "Wannacry" attack paralised its victims' source of income, health care and other vital services, resulting in a total damage of **USD 8 billion.***

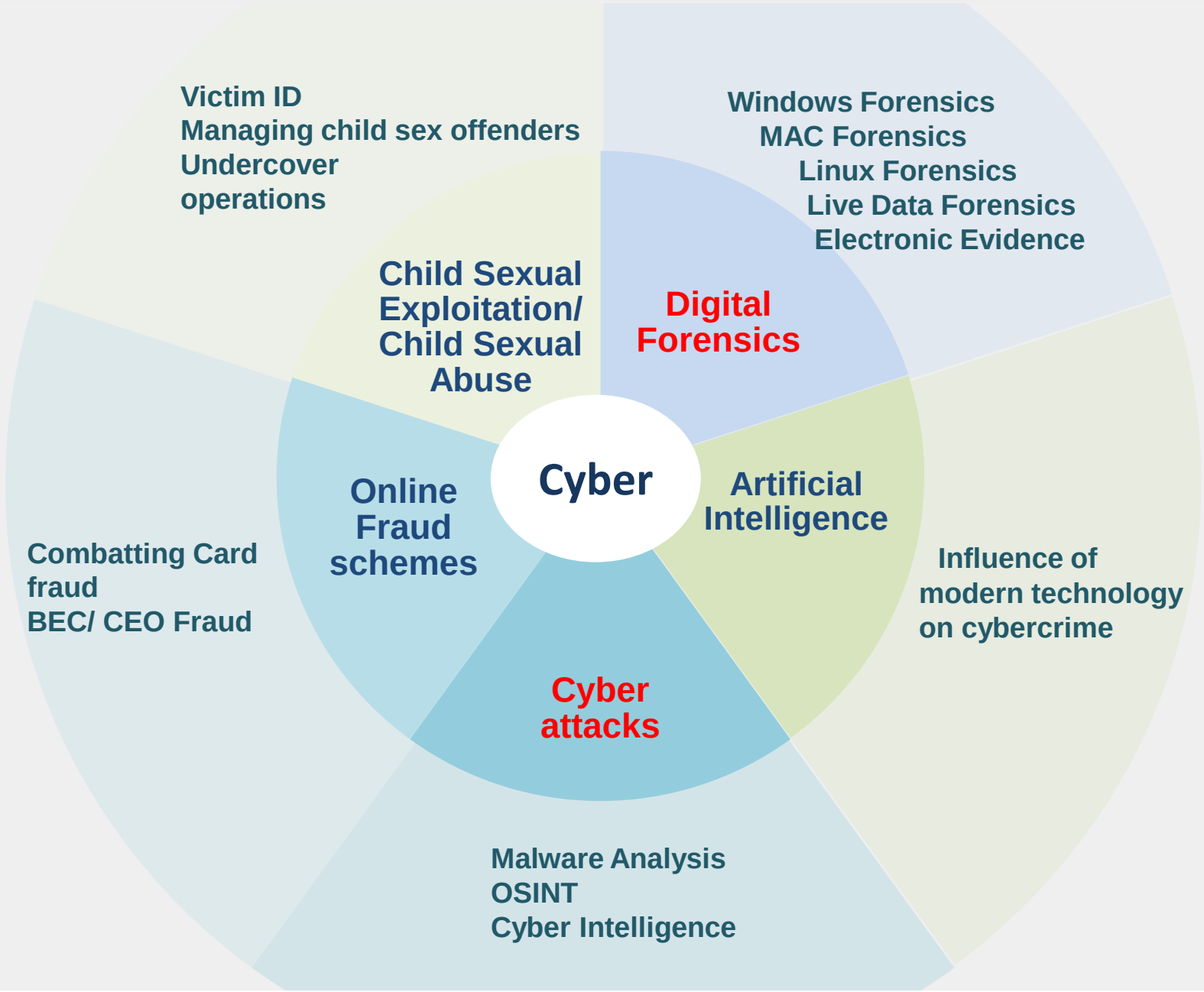
*Had the hackers been successful, they would have received a fraction of the amount of damage they ca... **USD 100 r...***

# Investigative techniques

## Follow the digital traces


## Follow the money

# Main areas of training



# 2022 Onsite Courses

- Open Source Intelligence (OSINT) and IT solutions (3 courses)
- Darkweb and cryptocurrencies (2 courses, basic and advanced)
- Cross Border exchange of Electronic Evidence
- Conducting Forensic searches in various IT devices
- Advanced Windows File System Forensics
- Digital Forensic Investigators Training
- First responders and cyber forensics
- Cyber-Intelligence
- Malware Investigation
- Live Data Forensics
- Mac Forensics
- Linux Forensics

**Digital Forensics/ Cybercrime Investigations**

- Strategies in Managing Child Sex Offenders
- Undercover Operations (CSE)
- Victim ID (CSE)

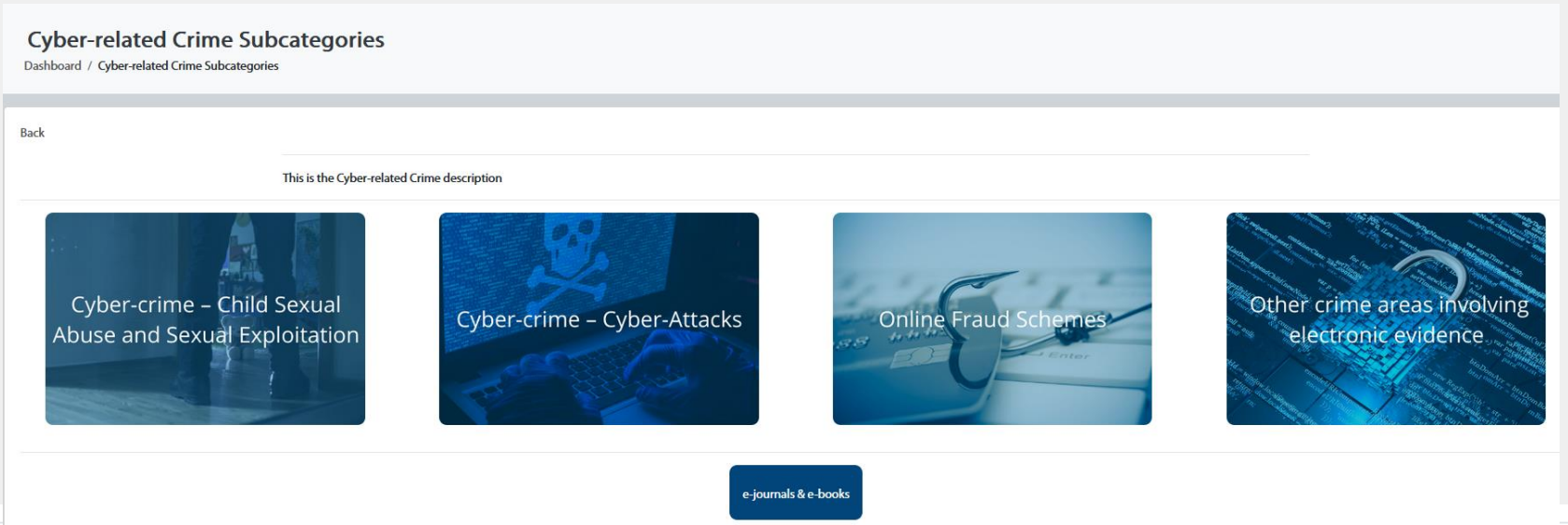
**CSE**

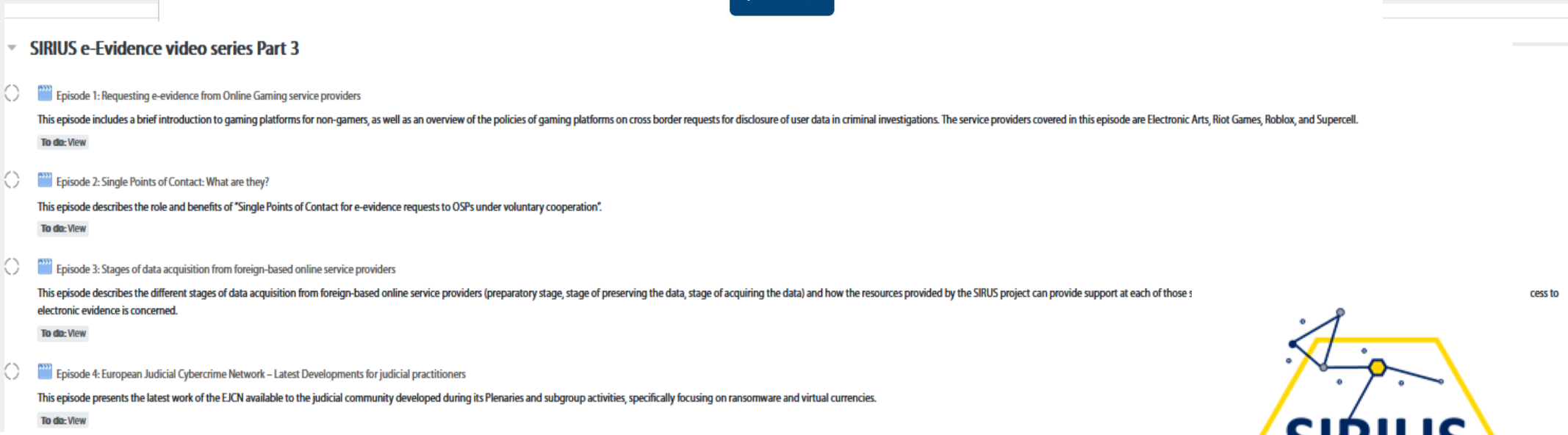
- Combating card fraud

**Non-cash means of payment**

CEPOL

# Online training materials available in Leed




CEPOL

LEEd

Law Enforcement Education

e-Platform by CEPOL the European Union Agency for Law Enforcement Training

SIRIUS

# New courses in 2023

- Ransomware investigations
- Decryption
- Mobile Forensics
- TOTs (Live Data Forensics, OSINT)

# CEPOL EXTERNAL EXPERTS ON CYBERCRIME

| Thematic area | Number of experts |
|---|---|
| CSA/CSE | 35 |
| NCMP | 36 |
| Cyber attacks | 58 |
| AI | 19 |
| **Total** | **148 expert** |

# Thank you for your attention!


ionut.stoica@cepol.europa.eu

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