

## Curriculum

To be reviewed by <b>Feb. 2026</b>	Activity number <b>217</b>	<b>Basics of cybercrime investigation</b>	<b>ECTS</b>  <b>1</b>
---------------------------------------	-------------------------------	-------------------------------------------	-----------------------------

<p style="text-align: center;"><u>Target audience</u></p> <p>Participants should be law enforcement specialists with general knowledge on cybercrime and should use IT equipment on a daily base and want to understand cybercrime from both the regulatory and technical perspective.</p> <p><u>Open to:</u></p> <ul style="list-style-type: none"> <li>▪ EU Member States and EU institutions</li> <li>▪ Candidate Countries</li> <li>▪ Third countries and international and regional organisations</li> </ul>	<p style="text-align: center;"><u>Aim</u></p> <p>This course aims to:</p> <ul style="list-style-type: none"> <li>• Give an overview on strategic cybersecurity and the place of cybercrime among current threats.</li> <li>• Provide a comprehensive overview of the characteristics, types, future trends of cybercrime, its material, procedural and international legal aspects.</li> <li>• Introduce the tasks of international organizations in the context of cybercrime</li> <li>• Present the basics of digital forensics to record electronic data lawfully and professionally, and related knowledge of criminal procedure and criminalistics.</li> </ul>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	<ul style="list-style-type: none"> <li>• <i>Specialised cyber course, at tactical/technical levels</i></li> <li>• <i>Linked with the strategic objectives of Pillar 1 and Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]</i></li> </ul>

Learning Outcomes	
Knowledge	L01- Outline the principles of European cybersecurity strategies and norms, L02- Understand the tasks of law enforcement agencies in case of attacks against public and private organizations, L03- Be aware of national and international law in cyberspace, L04- Know the basic rules of digital forensics.
Skills	L05- Implement investigation practices, aligned with international legislation, L06- Cooperate with law enforcement agencies in investigations of cybersecurity incidents, L07- Report cybercrime related information for relevant stakeholders, L08- Analyse digital evidence and attacking methods.
Responsibility and Autonomy	L09- Integrate the global cybercrime legislation and practice within the organization, L010- Manage and investigate cybercrime related incidents, L011- Handle digital evidence lawfully, L012- Decide on the proposed security mitigations measures.

### Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly level 1 evaluation (based on participants' satisfaction with the course) and level 3 evaluation (assessment of participants' long-term change in behaviour after the end of the course). Evaluation feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to accomplish all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award certificates to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the final evaluation report, which is presented to the Executive Academic Board.

### **Course structure**

*The residential module is held over 3 days.*

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. The state of cybersecurity from the cybercrime perspective	12(8)	1.1 Trends of cybercrime 1.2 EU approach on cybercrime 1.3 International treaties and legislation of cybercrime, Budapest Convention on Cybercrime 1.4 International organizations related to cybercrime and internet governance
2. Cyberattacks in practice	9	2.1 Financially motivated cyberattacks (i.e Social engineering, Malware attacks, DoS and DDoS attacks etc.) 2.2 Case studies of known cybercrime incidents 2.3 Cyberdefence from the organizational perspective
3. Basics of digital forensics	4 (2)	3.1 Sources of digital evidence (i.e. IPS/IDS, log management, monitoring) 3.2 Principles of digital data gathering in a law enforcement process 3.3 Typical digital evidences in IT devices
<b>TOTAL</b>	<b>25(10)</b>	

#### Materials

**Prerequisite**

- Basic knowledge of IT: ECDL or similar knowledge,
- Professional law enforcement experience

**Required:**

- AKU 2 on European Global Strategy

**Recommended:**

- AKU 55: Strategic Compass
- AKU 3 Role of EU Institutions in the field of CFSP/ CSDP
- AKU 109 Open Source Intelligence Introduction Course

#### Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises

#### Additional information

Pre-course questionnaire on learning expectations and possible briefing topic form specific area of expertise may be used.

All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

<ul style="list-style-type: none"> <li>• Council Conclusion on EU Policy on Cyber Defence (22.05.2023)</li> <li>• EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022)</li> <li>• Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS 2)</li> <li>• COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States</li> <li>• EU's Cybersecurity Strategy for the Digital Decade (December 2020)</li> <li>• The EU Cybersecurity Act ( June 2019)</li> <li>• The EU Cyber Diplomacy Toolbox (June 2017)</li> </ul>	<p>The Chatham House Rule is applied during all residential modules of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------