European Security and Defence College
Doc: ESDC/2023/244
Date: 20 September 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Basics of cybercrime investigation	ECTS
Feb. 2025	217		1

Target audience	Aim
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. Open to: ▪ EU Member States and EU institutions ▪ Candidate countries ▪ Third countries and international and regional organisations	This course aims to: • Give an overview on strategic cybersecurity and the place of cybercrime among current threats. • Provide a comprehensive overview of the characteristics, types, future trends of cybercrime, its material, procedural and international legal aspects. • Introduce the tasks of international organizations in the context of cybercrime • Present the basics of digital forensics to record electronic data lawfully and professionally, and related knowledge of criminal procedure and criminalistics.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised cyber course, at tactical/technical levels* • *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)]*

Learning Outcomes	
Knowledge	LO1- Outline the principles of European cybersecurity strategies and norms, LO2- Understand the tasks of law enforcement agencies in case of attacks against public an private organizations, LO3- Be aware of national and international law in cyberspace, LO4- Know the basic rules of digital forensics.
Skills	LO5- Implement investigation practices, aligned with international legislation, LO6- Cooperate with law enforcement agencies in investigations of cybersecurity incidents, LO7- Report cybercrime related information for relevant stakeholders, LO8- Analyse digital evidence and attacking methods.
Responsibility and Autonomy	LO9- Integrate the global cybercrime legislation and practice within the organization, LO10- Manage and investigate cybercrime related incidents, LO11- Handle digital evidence lawfully, LO12- Decide on the proposed security mitigations measures.

Evaluation and verification of learning outcomes

The course is evaluated in accordance with the Kirkpatrick model, with level 1 evaluation (based on participants' satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated on the basis of their active contribution to the residential module, including syndicate sessions and practical activities, as well as on completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. There is active observation by the course director/lead instructor, and a feedback questionnaire is filled in by participants at the end of the course.

However, no formal verification of learning outcomes is planned; the proposed ECTS is based only on participants' work.

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
TOTAL	**25(10)**	

Materials

Required:

- AKU 2 on European Global Strategy

Recommended:

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

Prerequisite

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

Methodology

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

Additional information

A pre-course questionnaire on learning expectations and possibly a briefing topic from the specific area of expertise may be used.

All course participants must 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.

The Chatham House rule is applied during the residential phase 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'.