European Security and Defence College
Doc: ESDC/2022/070
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2024**	Activity number **217**	**Basics of cybercrime investigation**	ECTS **1**
			EAB.CYBER **N/A**

Target audience

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 / EU Institutions Bodies and Agencies
- Third countries
- International Organisations

Aim

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.

Learning Outcomes

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

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 an 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, L10- Manage and investigate cybercrime related incidents, L11- Handle digital evidence lawfully, L12- Decide on the proposed security mitigations measures.

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *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 on the residential modules.

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their 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. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *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. It is a specialised course, at tactical/technical levels link with the Pillars 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020).

Furthermore, the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase].

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:

- E-learning material

Prerequisite

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

Methodology

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

Additional information

The Chatham House Rule is applied during all residential modules of the HLC: "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".

The mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).