European Security and Defence College
Doc: ESDC/2022/ 060
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cybersecurity Basics for Non-Technical Experts	ECTS 1
Feb. 2024	203		EAB.CYBER N/A

Target audience	Aim
Participants should be non-technical end users (civilians or military personnel) that need to use IT equipment on a daily base and want to understand the cybersecurity basics from both the regulatory and technical perspective. Open to: ▪ EU Member States / EU Institutions Bodies and Agencies	This course aims to enable participants to: • Explain the current cybersecurity strategy and legislation from the European Union's perspective. • Document and in-depth understanding of current cyberattacks, threats, vulnerabilities and risks on an understandable and technical way for non-technical persons. • Move beyond the classic cybersecurity awareness training and let the participants to use their own IT defence in a real environment.

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 – Explain the complexity of cybersecurity, L03 – Define the basics of cyber-threats, L04 – List the basic technical controls. L05 – Explain the necessity of the recommended measures related to the cybersecurity protection
Skills	L06 – Implement Cybersecurity Best Practices, aligned with EU legislation, L07 – Develop cyber-security plans, select the appropriate security measures to establish the information security management L08 – Classify the cyber threats, and identify the domain-specific vulnerabilities, L09 – Analyse the cyberattacks (i.e fundamentals of malwares, information-based attacks) and attacking methods,
Responsibility and Autonomy	L10 – Propose measures for integration of the European cybersecurity legislation within the organization, L11 - Promote cybersecurity awareness activities in the organization, L12 – coordinate implementation a range of recommended counter-measures, L13 - Decide on the proposed security counter-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 feed-back* 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 non-specialised course, at awareness level, link with the Pillar 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.Cybersecurity from the European perspective	8(4)	1.1 European cybersecurity strategy 1.2 The interaction of the CFSP/CSDP with the EU CYBER Ecosystem (Institutions, Policies, Directives)
2. Cyber-attacks in practice	8	2.1 Cyberattacks (i.e Social engineering, Malware attacks, DoS and DDoS attacks etc.), 2.2 Study cases of known cyber incidents 2.3 Mitigation measures related with the cyber-attacks.
3. Workgroup work	10(4)	3.1 Information security management in the cyber field, 3.2 The usage of cybersecurity tools at the individual level (i.e firewalls, antivirus, secure procedures etc.), 3.3 Cybersecurity on networks (i.e IDS/IPS, firewalls, filters, network tools), 3.4 Cyber hygiene
TOTAL	**26(8)**	

Materials Required:

- AKU1- History and Context of ESDP/CSDP development, AKU2- The European Global Strategy (EGS), AKU3- Role of EU institutions in the field of CFSP/CSDP, AKU4- CSDP crisis management structures and the Chain of Command, AKU5- Civilian and military capability development, AKU6- CSDP Decision Shaping/Making, AKU107- Awareness course on Cyber Diplomacy

Recommended:

- AKU104- 10 modules from ENISA

Methodology

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

• AKU106- Hybrid modules • Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016) • European Parliament: Directive on security of network and information systems (2016) • E-learning material • Presentations • Case studies	