EUROPEAN SECURITY AND DEFENCE COLLEGE
COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE

European Security and Defence College
Doc: ESDC/2024/042
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cybersecurity Fundamentals for Non-Technical Experts	ECTS
Feb. 2026	203		1

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Non-specialised cyber course, at awareness level* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Target audience

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
- Candidate Countries
- Third Countries and international or regional organisations

Aim

This course aims to enable participants to:

- Explain the EU cybersecurity strategy, its legislation and its governance
- Document and in-depth understanding of the current cyber threat landscape, vulnerabilities and risks with 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

Knowledge	LO1 – Outline the principles of European cybersecurity strategies and norms, LO2 – Explain the complexity of cybersecurity, LO3 – Define the basics of cyber-threats LO4 – List the basic technical controls. LO5 – Explain the necessity of the recommended measures related to the cybersecurity protection LO6 – Understand Risk Management
Skills	LO6 – Implement Cybersecurity Best Practices, aligned with EU legislation, LO7 – Develop cyber-security plans, select the appropriate security measures to establish the information security management LO8 – Classify the cyber threats, and identify the domain-specific vulnerabilities, LO9 – Analyse the cyberattacks (i.e fundamentals of malwares, information-based attacks) and attacking methods, L10 – Identify Assets, assess and prioritize Risks, selecting countermeasures

Responsibility and Autonomy	LO10 – Propose measures for integration of the European cybersecurity legislation within the organization, LO11 - Promote cybersecurity awareness activities in the organization, LO12 – coordinate implementation a range of recommended counter-measures, LO13 - Decide on the proposed security counter-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.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

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)

• AKU6- CSDP Decision Shaping/Making • AKU107- Awareness course on Cyber Diplomacy Recommended: • AKU104- 10 modules from ENISA • AKU106- Hybrid modules • Council Conclusion on EU Policy on Cyber Defence (22.05.2023) • EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022) • 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) • 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 • EU's Cybersecurity Strategy for the Digital Decade (December 2020) • The EU Cybersecurity Act (June 2019) • The EU Cyber Diplomacy Toolbox (June 2017) • E-learning material • Presentations • Case studies	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. 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".