European Security and Defence College
Doc: ESDC/2025/033
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number		ECTS
Feb. 2027	**200**	**Challenges of European Cybersecurity**	**1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	•Specialised cyber course, at awareness level •Linked with the strategic objectives of Pillar 1,2,3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]

Target audience	Aim
Participants should be mid-ranking to senior officials dealing with strategic aspects in the field of cyber security and cyber defence from EU MSs, relevant EU Institutions and Agencies. They should be either working in key positions or have a clear potential to achieve leadership positions, in particular in the field of Cyber Security or Defence. Course participants must be available for the entire course and should be ready to bring in their specific expertise and experience throughout the course.	The course is designed to help participants understand the broad scope of the information society within the context of the European Union, recognizing its complexity, various threats, and foundational concepts related to cyber security and cyber defense. It also explores key EU policies on international cyberspace issues and cyber diplomacy. In addition to providing an overview of the technological tools used in cyber security and defense, the course offers participants the opportunity to network with professionals working in the field across the EU.
Open to: ▪ EU member States / Institutions ▪ Candidate countries ▪ Third countries and International organisations	

Learning Outcomes

Knowledge	LO1. Recognise the extensive nature and complexity of the information society we are living in LO2. Recognise the nature of the different cyber threats (threat landscape) we are experiencing and their trends LO3. Define the basic notions and concepts related to cyber security and cyber defence. LO4. Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles. LO5. Identify the challenges of cyber security at a European level and the way ahead. LO6. Address international cyber space issues and cyber diplomacy

Skills	LO7. Identify technical as well as organisational tools related to cyber security. LO8. Identify the challenges of industrial and public planning needed to face cyber threats
Responsibility and Autonomy	LO9. Evaluate the potential impacts of cyber security on public policies LO10. Assess and summarize the challenges of cyber security at European level and the way ahead

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 fulfil 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 course is held over 3 days.

Main Topic	**Suggested Working Hours + (Required for individual learning, eLearning etc)**	**Suggested Contents**
Cyber Space: Concepts and Strategies	5 + (4)	Overall contextual framework: past, present and future trends Definitions and concepts of cybersecurity Trends in cyber threats and critical Infrastructure National cybersecurity policies: comparison and exchanges – point of view and strategies Cybersecurity of private infrastructure: role and responsibilities of Private Sector; issues of Cyber Security on private infrastructure Emerging technologies (i.e Artificial Intelligence/Machine Learning, 5G, Quantum Computing)
EU Capabilities and Requirements	3 + (4)	Cyber Security / Cyber Defence needs for the EU and CSDP Critical infrastructure protection against cyber attacks Assessment and perspectives of EU’s progress in cyber security EU Capacities in cyber security EU Role in reinforcing member-states capacities Building a European cyber industry
EU Strategies & Policies	4	EU Cybersecurity Strategy for the digital decade; Towards a strategic autonomy for EU in Cyber-Space; EU’s implementation of cyber security EU Cyber Defence Policy Framework EU NIS Directive EU Cyber Resilience Act EU Cybercrime Framework

Legal Frameworks & Cyber Conflict	4	Legal framework for cyber operations UN Charter and International Humanitarian Law in cyberspace promoting the Budapest Convention Cyber regulation in the EU and national best practices Hybrid and cyber in the conduct of military operations; Specificity of military cyber space; incidence of digitization and robotisation of the battlefield. Cyber security and cross-domain warfare Cyber Attack simulation
Cyber Diplomacy and co-operation	4	Preventing cyber attacks: role of confidence-building measures Cooperation in Cyberspace: partners and achievements Capacity building Cyber diplomacy and international cyber issues Cyber threat intelligence Disinformation-Foreign Information Manipulation and Interference (FIMI)
Decision-making exercise (simulation/cyber range platform)	4	Table-top non-technical exercise Application of the acquired knowledge and individual experience. Simulation of a real situation
TOTAL	**24 + (8)**	

Materials

Required:

- AKU 1 History and context of ESDP/CSDP development
- AKU 3 The Role of EU institutions in the field of CFSP/ CSDP
- AKU 55 The EU Strategic Compass

Recommended:

- AKU 7: Impact of Lisbon treaty in CSPD
- AKU 2 European Global Strategy
- *AKUs 30-32, as soon as become available*
- EU's Cybersecurity Strategy for the Digital Decade (2020)
- EU Policy on Cyber Defence (2022)
- Council Conclusions on Cyber Defence (2023)
- 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 by the European Parliament (2016)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies

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.

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".