European Security and Defence College
Doc: ESDC/2023/050
Date: 23 Feb 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Challenges of European Cybersecurity	ECTS
Feb. 2025	**200**		**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 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. Open to: ▪ EU member States / Institutions ▪ Third countries ▪ Candidate countries	The course aims to enable participants to understand the extensive nature of the information society and to recognise its complexity and the different threats, the basic notions and concepts related to cyber security and cyber defence, as well as international cyber space issues and cyber diplomacy. Offering an overview on technological tools used in cyber security and cyber defence, the course aims at providing an opportunity to create a network of people working in the field.

Learning Outcomes	
Knowledge	LO1. Recognise the extensive nature of the information society we are living in LO2. Recognise the complexity of the information society LO3. Recognise the nature of the different cyber threats we are experiencing. LO4. Define the basic notions and concepts related to cyber security and cyber defence. LO5. Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles. LO6. Identify the challenges of cyber security at a European level and the way ahead. LO7. Reflect on the different trends in cyber threats LO8. Address international cyber space issues and cyber diplomacy
Skills	LO9. Identify technical as well as organisational tools related to cyber security. LO10. Consider the potential impacts of cyber threats in public policies. LO11. identify the challenges of industrial and public planning needed to face cyber threats LO12. Perceive the challenges of industrial and public planning needed to face cyber threats.
Responsibility and Autonomy	LO13. Evaluate the potential impacts of cyber security on public policies LO14. 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: it makes use of level 1 evaluation (based on participant's 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 the active contribution in the residential Module, including their syndicate session and practical activities as well as on their completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. Active observation by the course director/lead instructor and feedback questionnaire filled by course participants at the end of the course is used.

However, no formal verification of learning outcome 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. 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

Main Topic	Suggested Working Hours (Required for individual learning)	Suggested Contents
Cyber Space: Concepts and Strategies	4 (4)	Overall contextual framework: past, present and future trends Definitions and concepts of Cyber Security Trends in cyber threats and critical Infrastructure Towards a strategic autonomy for EU in Cyber-Space. European cyber security strategy; EU's implementation of cyber security National cyber-security policies: comparison and exchanges – point of view and strategies Cyber-Security of private infrastructure: role and responsibilities of Private Sector; issues of Cyber Security on private infrastructure
EU Capabilities and Requirements	4 (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 Strategy for Cyberspace EU Cyber Defence Policy Framework EU NIS Directive EU Cyber Resilience Act EU Cybercrime Framework
Legal Frameworks & Cyber War	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 digital combat 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 Cyber Co-operation	4	Preventing cyber war: role of confidence-building measures Cooperation in Cyberspace: partners and achievements Human resource capacity building Cyber diplomacy and international cyber issues Intelligence, interference
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	Additional information
Required: AKU 1 History and context of ESDP/CSDP development AKU 2 European Global Strategy AKU 3 The Role of EU institutions in the field of CFSP/ CSDP **Recommended:** AKU 7: Impact of Lisbon treaty in CSPD *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 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)	Pre-course questionnaire on learning expectations and possible briefing topic from the 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 supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular. The Chatham House Rule is applied during all 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".