European Security and Defence College
Doc: ESDC/2024/046
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Diplomacy Fundamentals	ECTS
Feb. 2026	207a		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

The participants should be junior to mid-level diplomats or representatives of Member-States governmental or EU institutions, and any competent state agencies with a role in strategy formulation and implementation in the cyber realm.

Open to:

- EU Member States / EU Institutions Bodies and Agencies
- Candidate Countries

Aim

This activity will aim the participants with a sense of the momentous developments in the cyber external relations sphere and knowledge to understand, implement, actively understand and identify capacity building measures and increase resilience and stability.

During this basic course the participants will be able to understand why the need to interact and be interoperable across the global cyber ecosystem, understand and identify the basic notions, actual challenges, to find ways to implement capacity building measures, increase the resilience and share some common views, but also understand how to apply EU's Cyber Diplomacy Toolbox.

Furthermore, this course will allow the junior to mid-ranking officials to network, interact and exchange their views, share best practices on cyber-related topics by improving their knowledge, skills and competencies.

Learning Outcomes

Knowledge	LO1 - List the digital diplomacy strategies, policies, rules and norms in pursuit of broader EU cyber foreign policy objectives LO2 - List the entities involved in the EU cyber ecosystem and their respective roles LO3 - List the nature of the different cyber and hybrid threats and their impact in the external relations domain LO4 - List the key challenges of cyber security and cyber diplomacy at global level LO5 - List the key challenges of cyberspace governance and their effects LO6 - Define the basic notions, terminology and concepts related to cybersecurity, cyber defence, cybercrime and critical infrastructures
Skills	LO7 – Identify/Understand the cyber issues according to complexity and their impact in the external relations domain

	LO8 - Classify and distinguish the impact of the cyber threats in the cyber resilience and global stability LO9 - Categorize the cooperation opportunities with the EU cyber ecosystem and the global cyber environment LO10 – Analyse diplomatic approaches and best practices within the cyber domains LO11 – Analyse the strengths and weaknesses of the cyber cooperation topics
Responsibility and Autonomy	LO12 - Evaluate the potential impacts of cyber threats in the global environment LO13 - Develop opportunities for synergies with the EU cyber ecosystem and the global cyber environment LO14 - Distinguish between the different aspects of cybersecurity and the challenge they pose to the MS and within the society LO15 – Identify the main efforts at Cyber Diplomacy currently being implemented in the EU Cyber strategy LO16 - Design a Cyber external relations strategy and its implementation LO17 - Assess the impact of external relations on the organization security profile

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. The EU Cyber Ecosystem	9 (3)	1.1 The rationale for cyber diplomacy 1.2 Key concepts of the cyber-diplomacy, EU Cyber Ecosystem and the respective cyber domains 1.3 Local/regional initiatives and trends in cyber diplomacy 1.4 EU organisations, Agencies and bodies involved in cyber diplomacy
2. EU approach in bulding resilience and trust	8 (3)	2.1 EU cyber related strategies and actions 2.2 Policies and Regulations Directives related with cyber within EU 2.3 International cooperation 2.4 Resilience building trough fighting against Cybercrime, Cyberdefence and Critical Infrastructures Protection
3. The EU's model in External Cyber Capacity Building	8	3.1 Key Policies, Actors and initiatives 3.2 Cyber Governance in the EU and beyond. 3.3 The EU Cyber Diplomacy Toolbox and the EU Cyber Defense Policy 3.4 Coordinated Response to Large Scale Cybersecurity Incidents and Crises

Countering Hybrid Threats	4(2)	3.5 Existing and Emerging Threats; 3.6 Framework on hybrid threats, interaction with cyber
TOTAL	**29(8)**	

Materials

Required:
- AKU 55: Strategic Compass
- AKU 107 – Awareness course on CyberDiplomacy

Recommended:
- AKU 106a, b, c, d, e – Hybrid threats modules
- AKU 2 on European Global Strategy
- 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)
- Documents and assessments of the security environment from EU and non-EU, Think Tanks
- The course documentation prepared by the organizers.

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) 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".