European Security and Defence College
Doc: ESDC/2022/064
Date: 1 April 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Diplomacy Basic Course	ECTS
Feb. 2024	207a		1

Target audience	Aim
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	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 CyberDiplomacy 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.

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)]*

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 challenges of cyber security and cyber diplomacy at global level LO5 - List the key problems 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 - Classify 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 – Classify 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: 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.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
The EU Cyber Ecosystem	9 (3)	The rationale for cyber diplomacy; Key concepts of the cyber-diplomacy, EU Cyber Ecosystem and the respective cyber domains Local/regional initiatives and trends in cyber diplomacy EU organisations, Agencies and bodies involved in cyber diplomacy
EU approach in bulding resilience and trust	8 (3)	EU cyber related strategies and actions Policies and Regulations Directives related with cyber within EU International cooperation Resilience building trough fighting against Cybercrime, Cyberdefence and Critical Infrastructures Protection,
The EU's model in External Cyber Capacity Building	8	Cyber Governance in the EU and beyond. Cyber Diplomacy Toolbox

		Coordinated Response to Large Scale Cybersecurity Incidents and Crises
Countering Hybrid Threats	4(2)	Existing and Emerging Threats; Framework on hybrid threats, interaction with cyber
TOTAL	**29(8)**	

Materials	Methodology
Essential eLearning: • AKU 2 on European Global Strategy • AKU 107 – Awareness course on CyberDiplomacy Supplementary materials: • AKU 106a, b, c, d, e – Hybrid threats modules • *Reading material:* - EU Directives, Council Decisions, Council conclusions, Regulations, Joint declarations; - Documents and assessments of the security environment from EU and non-EU, Think Tanks; - The course documentation prepared by the organizers.	The course is based on the following methodology: lectures, panels, workshops, exercises **Additional information** Additional information 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".