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

European Security and Defence College
Doc: ESDC/2022/065
Date: 1 April 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Diplomacy Advanced Course	ECTS
Feb. 2024	207b		1

Target audience

The participants should be mid to senior 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

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 advanced course, the participants will better understand the need to interact and be interoperable across the global cyber ecosystem, identifying actual challenges, capacity building actions, and confidence-building measures. The final purpose is to understand and practice Cyber Diplomacy Toolbox measures, increasing the resilience.

Furthermore, this course will allow the mid to senior 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 - Outline Cyber Diplomacy Concepts and Actors and interactions LO2 – Identify Rules, Norms and International Laws in place LO3 – Identify the emerging trends and Geopolitical Challenges in Cyber Diplomacy LO4 - Describe Confidence- Building Measures & Capacity Building rationale
Skills	LO5 - Classify the cyber diplomacy issues according to complexity and their impact in the external relations domain LO6 – Design Cyber Diplomacy approaches and best practices LO7 – Design strategies in Confidence Building Measures and Capacity Building based on the strengths and weaknesses of the cyber cooperation topics LO8 – Recognise Hybrid threats and Disinformation Operations

Responsibility and Autonomy	LO9 – Asses the potential impacts of cyber threats LO10 –Integrate appropriate Rules, norms and principles, when engaging in Confidence Building Measures in Cyberspace LO11 – Design or evaluate a Capacity Building Measures in Cyber Domain LO12 – Justify the usage of different measures in the Cyber Diplomacy Toolbox LO13 – position themselves regarding other actors within the context of the Cyber Diplomacy Toolbox LO14 – Contribute to the design of a Cyber strategy and its implementation

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
Concepts and Actors	3 (2)	• Evolution and relevance of cyber and digital diplomacy. • Role of multinational organizations, • Role of State and Non-State Actors • EU organisations, agencies and bodies involved in cyber diplomacy
Rules, Norms and International Law	3 (2)	• Principles of UN Charter • International laws: human rights, criminal law, Armed Conflict • International wrongful acts and attribution • Tallinn Manual
Emerging Trends and Geopolitical Challenges	3 (2)	• Risks and insecurity of using ICTs • Cyber-resilience against malicious activities • Disinformation and Influence Operations • Hybrid Threats, Hybrid Warfare and deterrence
Confidence Building Measures & Capacity Building	2 (2)	• Norms of international law and voluntary political norms • Recommendations of UN GGE, and OEWG • National/Local/regional initiatives
EU Cyber Diplomacy	5	• Use of the EU Cyber diplomacy Toolbox in practice • Governance of Cyber diplomacy in the EU • EU Cooperation initiatives in Cyberspace

TOTAL	16 (8)	

Materials	Methodology
Essential eLearning: • AKU 2 on European Global Strategy • AKU 107 – Awareness course on Cyber Diplomacy 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".