European Security and Defence College **Doc: ESDC**/2024/047 **Date:** 21 Feb 2024 **Origin:** ESDC Secretariat

Curriculum

To be reviewed by	Activity number		ECTS
Feb. 2026	**207.b**	**Cyber Diplomacy Advanced Course**	**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 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]

Target audience	Aim
The participants should be mid- to senior-level diplomats or representatives of Member States governmental or EU institutions, and any competent state agencies involved in the development and implementation of cyber policies or strategies.	This course aims to provide participants with understanding of the geopolitical dynamics in cyberspace, the current threat landscape as well as the different pillars of cyber diplomacy. This knowledge will notably enable to implement cyber policies, engage in regional and multilateral for a and engage in capacity building. During this advanced course, the participants will come to better understand the global cyber governance, current challenges, the EU's tools to prevent, deter and respond to cyber threats, capacity building activities and confidence-building measures. The final purpose is to understand and practice different Cyber Diplomacy Toolbox measures. 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.
Open to: ▪ EU member States, institutions and agencies	

Learning Outcomes

Knowledge	LO1. Outline cyber diplomacy concepts, and actors and interactions LO2. Understand the international rules based order in cyberspace, grounded in the application of international law and norms of responsible state behaviour in cyberspace. LO3. Identify the emerging trends and geopolitical challenges in cyberspace LO4. Describe Confidence- Building Measures & Capacity Building rationale LO5. Identify the full spectrum approach to resilience, response, conflict prevention, cooperation and stability in cyberspace.
Skills	LO6. Identify cyber diplomacy challenges and their impact in the external relations domain LO7. Design cyber diplomacy approaches and best practices LO8. Design strategies for the development and implementation of Confidence Building Measures and Capacity Building activities LO9. Recognise Hybrid threats and Disinformation Operations

Responsibility and Autonomy	LO10. Assess the potential impacts of cyber threats LO11. Integrate appropriate Rules, norms and principles, when engaging in Confidence Building Measures in Cyberspace LO12. Design or evaluate Capacity Building Measures in Cyber Domain LO13. Justify the use of different measures in accordance with the Cyber Diplomacy Toolbox LO14. Contribute to the design and implementation of a Cyber strategy

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

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1.Concepts and Actors	3 (2)	1.1 Evolution and relevance of cyber and digital diplomacy. 1.2 Role of multinational organizations, 1.3 Role of State and Non-State Actors 1.4 EU organisations, agencies and bodies involved in cyber diplomacy 1.5 Governance of Cyber diplomacy, including in the EU
2.Rules, Norms and International Law	3 (2)	2.1 Principles of UN Charter 2.2 International laws: human rights, criminal law, Armed Conflict 2.3 International wrongful acts and attribution 2.4 Tallinn Manual
3.Emerging Trends and Geopolitical Challenges	3 (2)	3.1 Cyber threat landscape 3.2 Cyber-resilience against malicious activities 3.3 EU's tool to prevent, deter and respond to cyber threats (EU Cyber 3.4 Diplomacy Toolbox and EU Cyber Defense Policy) 3.5 Disinformation and Influence Operations Hybrid Threats, Hybrid Warfare and deterrence
4.Confidence Building Measures & Capacity Building	2 (2)	4.1 Norms of international law and voluntary political norms 4.2 Recommendations of UN GGE, and OEWG 4.3 National/Local/regional initiatives
5.Case study	5	5.1 Use of the EU Cyber diplomacy Toolbox in practice
TOTAL	**16 (8)**	

Materials

Required:

- AKU 55 – Strategic Compass
- AKU 107: Awareness course on Cyber Diplomacy

Recommended:

- AKU 106a, b, c, d, e – Hybrid threats modules
- 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)

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".