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

European Security and Defence College
Doc: ESDC/2024/60
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	The Contribution of Cyber in Hybrid Conflict	ECTS
Feb. 2026	**274**		**1**

Target audience

*The course is for **non-specialized and specialized on strategic–level** Mid-to-senior rank military officers and civilian officials equivalent in (or liable for) Cyber / Hybrid-related practitioner roles in EU Institutions, or in Member State ministries (e.g. MoDs; MoIs; MoFAs), relevant Agencies, or military HQs who:*

- *Engage in development of policies, strategies, concepts, or doctrine related to cybersecurity, cyber defence, hybrid threats/campaigns; and/or*
- *Design or deliver professional education courses, individual training courses, or command post exercises related to cybersecurity, cyber defence, or hybrid threats/campaigns.*

Open to:

- EU Member States and EU institutions

Aim

The course aims to educate participants about key elements of cyber and hybrid threats, and potential responses to them, and to provide them with an opportunity to deepen their understanding, via a decision-making exercise, of how to address the implications of the intersection of cyber and hybrid threats/attacks and campaigns.

Additionally, the course will provide participants with opportunities for networking and intellectual cross-fertilisation, including across communities that may not frequently interact.

Note: The Table-top exercise (TTX) is a decision-making exercise which will engage participants in a multi-turn adversarial contest in a high-level abstracted synthetic context.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *non-specialized and specialized on strategic level* • *Linked with the strategic objectives of Pillar 3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning outcomes	
Knowledge	LO01 – Explain the nature and terminology of digital technologies, cybersecurity, cyber defence, cyber threats, and how these interact in the real world. LO02 – Recount the institutional landscape and arrangements for cybersecurity, cyber defence, and countering hybrid threats at EU level. LO03 – Explain hybrid threats leveraging a bespoke conceptual framework and listing actors, domains and tools, and threat phases. LO04 – Explain the interaction between cyber and hybrid threats/ attacks / campaigns and its implication for contemporary conflicts (e.g. Russia's war against Ukraine)
Skills	LO05 – Recognise malicious activities in cyberspace and hybrid campaigns and their underlying tactics, techniques, and procedures. LO06 – Manage cyber-related considerations in planning for responding to hybrid threats. LO07 – Address potential cyber and hybrid threats / attacks and campaigns to multi-national operations and missions.
Responsibility and Autonomy	LO08 – Assess and design strategic and policy options for responding to cyber and hybrid threats / attacks and campaigns.

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 five days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Cyber fundamentals	2,5 (1)	1.1 Introducing fundamental concepts related to the cyber domain, cybersecurity and cyber defence 1.1.1 The cyber domain from the perspective of International Partner Organisations 1.1.2 Tallinn Manual (CCD COE) 1.2 Mitigating and responding to cyber threats /attacks and campaigns in the European context 1.2.1 Situational awareness and 1.2.2 Development of policy solutions at EU level 1.2.3 Development of Cyber Defence solutions at EU level (a.o. related Cyber Projects/Programmes at EDA, PESCO, and so on) 1.2.4 The impact of the EU Cyber Diplomacy Toolbox
2. Hybrid threat fundamentals	3,5 (1)	2.1 Introducing fundamental concepts related to hybrid threats 2.1.1 Frameworks and approaches for conceptualising hybrid threats 2.1.2 Hybrid threat landscape 2.2 Hybrid threat deep dives and case studies 2.2.1 Hybrid influencing (including disinformation) 2.2.2 Hybrid conflict and warfare by examples 2.2.3 Deterrence and resilience 2.3 Mitigating and responding to hybrid threats /attacks and campaigns in the European context 2.3.1 Situational awareness and 2.3.2 Development of policy solutions at EU level 2.3.3 The impact of the EU Hybrid Toolbox
3. The cyber-hybrid intersection	4,5 (1)	3.1 Understanding the intersection between cyber and hybrid threats 3.1.1 Function of cyber threats in hybrid attacks and campaigns (cognitive warfare, including

		examples from contemporary conflicts, e.g. Russia's war against Ukraine) 3.1.2 The role of information and strategic communication within the context of cyber and hybrid threats / attacks and campaigns 3.1.3 The interaction of the EU Hybrid Toolbox together with the EU FIMI Toolbox and EU Cyber Diplomacy Toolbox. 3.2 Understanding key emerging implications and lessons from the contemporary conflicts (e.g. Russia's war against Ukraine) with regard to cyber and hybrid threats / attacks and campaigns
4. Table-top exercise (TTX) on the Contribution of Cyber in Hybrid Conflict	17,5 (1)	4.1 The TTX is a decision-making exercise which will engage participants in a multi-turn adversarial contest and in a high-level abstracted synthetic context. 4.2 Test knowledge and skill on cyber / hybrid threats and their intersection transferred to participants during previous modules in the context of a decision-game 4.3 Provide a forum for participants to explore insights, observations, and lessons related to challenges stemming from the intersection of cyber and hybrid threats / attacks and campaigns
TOTAL	**28 (4)**	

Materials required:

- AKU 106 on Hybrid threats
  a) AKU 106a -H-CoE Adversarial Behaviour
  b) AKU 106B H-CoE The Landscape of Hybrid Threats
  c) AKU 106C H-CoE The changing security environment
  d) AKU 106D H-CoE Introduction to Hybrid Deterrence
  e) AKU 106E H-CoE Hybrid Warfare
- EU Policy on Cyber Defence , JOIN(22) 49 final, 10.11.2022
- Council Conclusions on the EU Policy on Cyber Defence, 22.05.2023

Recommended:

- AKU 55 – Startegic Cimpass
- AKU 2 on the EU Global Strategy
- AKU 4 CSDP Crisis Management Structures and the Chain of Command
- AKU 6 CSDP Decision Making
- 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)

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".

This curriculum has been opened to Switzerland, Hybrid CoE and opened to NATO CCD CoE on the condition of reciprocity for all EU Member States, as mandated by the ESDC SC decision during the 98th meeting on 02/07/2021, documented in ESDC/2021/183. The decision refers to the curriculum's initial working title "Cyber defence pilot course development, with a focus on cyber and hybrid".

• The EU Cybersecurity Act (June 2019) • The EU Cyber Diplomacy Toolbox (June 2017)	