European Security and Defence College
Doc: ESDC/2024/61
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2026**	Activity number **224**	**Global security and hybrid warfare**	ECTS **1**

Target audience

The participants should be mid-ranking to senior military or civilian officials dealing with cyber and hybrid incident handling and security operation centres from EU Institutions, Bodies and Agencies as well as EU Member States, candidate countries.

Open to:

- EU Member States / EU Institutions Bodies and Agencies
- Candidate countries
- Third countries

Aim

The aim of the course is to demonstrate to the participants how to utilize strategy design methodologies to form policy options for senior leaders to respond/recover from a simulated cyber and emerging technology incident that poses a challenge to the United States and the European Union. In addition, the participants are informed how to structure a decision-making process and make strategic decisions based on situational variables, multiple alternatives, potential risks, time frames, and organizational capabilities, resource requirements.

Furthermore, this course will allow the participants to exchange their views and share best practices on hybrid warfare topics by improving their knowledge, skills and competencies.

By the end of this course, the participants will learn how to describe the national security governance frameworks for responding to hacktivist, criminal or nation-state cyber threat actors and to understand unique challenges the emerging technologies pose to national security..

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and the EU's Policy on Cyber Defence	• *Specialised cyber course, at tactical, operational, and strategic 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 the roles and responsibilities of US or European institutions involved with cybersecurity or emerging technology policy; LO2 – Describe the complexity of hybrid warfare; LO3 – Identify unique challenges the emerging technologies pose to national Security;

Skills	LO4 – Apply national security governance frameworks for responding to cyber threat actors; LO5 – Use strategy design methodologies to form policy options to respond / recover from a simulated cyber and emerging technology incident; LO6 – Structure decision-making process on cyber and emerging technology incidents;
Responsibility and Autonomy	LO7 – Make strategic decisions based on situational variables, multiple alternatives, potential risks, time frames, and organizational capabilities, resource requirements; LO8 – Use a comprehensive approach to responding to hybrid threats; LO9 – Build writing skills to communicate response to cyber and emerging technology incidents.

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, the 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 5 days.

Main Topic	**Suggested Working Hours (required for individual learning)**	**Suggested Contents**
1. Introduction to hybrid warfare	8(6)	1.1 Introduction to Hybrid Warfare 1.2 Overview of current global security challenges 1.3 Overview of hybrid warfare and tactics
2. Current Security Threats and Challenges	1.5	2.1 Case study example of a current security threat
3. Practitioner Experience	1.5	3.1 Case study example of a practitioner experience with hybrid warfare
4. Scenario Workshop Orientation and Introduction	1.5	4.1 Active learning and human-centered design principles 4.2 Group ice breakers 4.3 Norms setting 4.4 Introduction of the scenario
5. Understanding and Mapping the Operational Environment	1.5	5.1 Thematic module on Operational Environment and its relation to Hybrid Warfare and Crisis Management 5.2 Scenario analysis and identification of the relevant factors
6. Stakeholders	1.5	6.1 Thematic module on Stakeholders and their relation to Hybrid Warfare and Crisis Management 6.2 Stakeholder identification and mapping. Assessment of needs, goals, and interests

7. Problem Identification	2.5	7.1 Thematic module on Problem Identification and its relation to Hybrid Warfare and Crisis Management 7.2 Scenario analysis and identification of the relevant factors
8. Policy Response	5	8.1 Synthesize learning from previous modules to craft a policy response to the scenario 8.2 Present findings
TOTAL	23(6)	

Material

Required:

AKU 106a– Hybrid CoE Adversarial Behaviour
(b) AKU 106b Hybrid CoE The Landscape of Hybrid Threats
(c) AKU 106c Hybrid CoE The Changing security environment
(d) AKU 106d Hybrid CoE Introduction to Hybrid Deterrence
(e) AKU 106e Hybrid CoE Hybrid Warfare
(f) Hybrid Threats & Maritime Security

Recommended:

- *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**)*
- *EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022*
- *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*
- *The EU Cybersecurity Act (June 2019)*
- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*

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".