European Security and Defence College

European Security and Defence College
Doc: ESDC/2025/045
Date: 19 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed in	Activity number	**Advanced Research into Hybrid Threats**	ECTS
2027	***77***		**2**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
No correlation	No equivalence.

Target audience

Participants should be mid-ranking to senior officials, doctoral researchers, academics, and practitioners whose work is related to the implementation of prevention and countering of hybrid threats (ministries of foreign affairs, defence, intelligence, internal affairs). Priority is given to personnel from EU Member States and institutions involved in policy development, governance, and strategic security initiatives, who would benefit from acquiring the necessary knowledge to effectively manage and adapt to these emerging developments.

Open to:

- ESDC Doctoral School on CSDP fellows
- EU member States / Institutions
- Candidate Countries

Aim

Advanced Research into Hybrid Threats is an interactive course that examines the intersection of information manipulation tactics and cyber-attacks. It enhances experts' and practitioners' understanding of the tools and strategies used by hostile actors to spread disinformation and conduct covert operations at the EU level. The course also explores coercive and subversive strategies shaping geopolitical dynamics, particularly in the context of ongoing conflicts. Through lectures, debates, problem-solving exercises, and scenario-based activities, participants will analyse the impact of hybrid threats and anticipate future trends.

Learning Outcomes	
Knowledge	LO1. understand the main challenges to EU security, which emerged as a result of the changing landscape of hybrid threats and tactics LO2. be able to identify the elements of the EU integrated approach to situational awareness, resilience, response and cooperation against hybrid threats LO3. understand and map out the modus operandi that combines information manipulation with cyberattacks and learn to make a shared assessment LO4. comprehend the principles of an EU hybrid toolbox, focused on preventive, cooperative, stability-building, restrictive and support measures
Skills	LO5. identify lessons learnt and good practices in response options, from diplomatic engagement to crisis mitigation LO6. be able to create mechanisms of resilience from prevention to recovery LO7. learn how to mitigate identified risks and vulnerabilities through existing resources LO8. apply critical thinking, assessment and cooperation skills throughout the exercises and scenario making sections of the course

Responsibility and Autonomy	LO9. use tools and techniques to properly assess hybrid threats patterns, information manipulation and cyberattacks LO10. learn how to use cyber-diplomacy tools and interference mitigation mechanisms LO11. translate knowledge into practical oriented solutions to be shared, negotiated and advanced in multi-stakeholders' formats

Evaluation and verification of learning outcomes

The course follows the Kirkpatrick model for evaluation, incorporating level 1 assessment based on participants' satisfaction with the course. Evaluation feedback is collected through the level 1 evaluation module.

To successfully complete the course, participants must fulfil all learning objectives and actively contribute to the residential module, including teamwork sessions and practical exercises. They are also required to complete the mandatory eLearning phase and successfully finish the Autonomous Knowledge Units (AKUs), achieving a minimum score of 80% in the required tests or quizzes. Although the proposed ECTS credits are based on coursework completion, no formal verification of learning outcomes is conducted.

The Executive Academic Board takes these factors into account when deciding whether to award certificates. The Course Director, supported by the ESDC Secretariat, oversees the overall coordination of the course and is responsible for drafting the final evaluation report, which is then presented to the Executive Academic Board.

Course structure		
The residential module is held over four days		
Main Topic	**Suggested Working Hours (required for individual learning)**	**Suggested Contents**
1. The changing landscape of hybrid threats and their tactics - main challenges at EU level	6 (4)	1.1. Theories and concepts that can help map and understand hybrid threats 1.2. Hybrid warfare – main components and modus operandi 1.3. Role of information manipulation 1.4. Role of cyberattacks
2. The EU integrated approach to situational awareness, resilience, response and cooperation against hybrid threats	6 (4)	2.1. The EU integrated approach to hybrid threats 2.2. The EU perspective and priorities in countering information manipulation 2.3. The EU counter-hybrid threats policy and its line of action: situational awareness, resilience, response, cooperation 2.4. Main challenges ahead – AI impact and changing strategies in information manipulation
3. Cyberattacks – emerging trends, prospective threats	6 (4)	3.1 Emerging technologies and their role in cyber security 3.2 Main challenges in cyber security – perspectives for short and medium timeframe
4. Information manipulation and cyberattacks – intersectionality and interdependencies	6 (4)	4.1. New cyber tools, means and strategies used by enemy states in hybrid threats 4.2 The modus operandi that combines information manipulation with cyberattacks 4.3 Resilience building tools and mechanisms to counter hybrid threats
5.Syndicate assignment	6 (4)	5.1. Working groups 5.2. Case studies, simulation exercises, scenarios
TOTAL	**30 + (20) = 50**	

Materials	**Methodology**
Required: AKU 1 History and context of CSDP AKU 2 European Global Strategy AKU 55 Strategic Compass AKU 106a (H-CoE): Adversarial Behavior; AKU 106b (H-CoE): The Landscape of Hybrid Threats; AKU 106c (H-CoE): The changing security environment AKU 106d (HCoE): Introduction to Hybrid Deterrence AKU 106e (H-CoE): Hybrid warefare AKU 107 Awareness course on Cyber Diplomacy AKU 108 The Cyber Defence Policy Framework (CDPF) **Recommended:** AKU 4 CSDP crisis management structures and chain of command AKU 6 CSDP decision shaping/making AKU 25 EU Mutual Assistance Clause AKU 123 CYBER Cyber Policy Documents AKU 300 Intercultural competence Teamwork materials, scenario, other documents provided by Course director and the lecturers	The course will include lectures, workshops, problem-solving exercises and scenario-based discussions. Additional information A pre-course questionnaire may be used to assess participants' learning expectations and to identify potential briefing topics within their areas of expertise. All participants must complete the mandatory eLearning preparatory phase before attending the residential module. The supplementary eLearning materials will reflect the latest developments in hybrid threats and cybersecurity, ensuring participants arrive well-prepared for in-depth discussions. Participants are expected to attend the entire course and actively engage in lectures, discussions, scenario-based assessments, and workshops. The course will be conducted under the **Chatham House Rule**, meaning: *"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 disclosed."*

Coordinated by ESDC Training Manager, Maria PENEDOS, maria.penedos@eeas.europa.eu