European Security and Defence College
Doc: ESDC/2024/22
Date: 08 February 2024
Origin: Executive Academic Board

Curriculum

To be reviewed by	Activity number		ECTS
February 2026	*40*	**EU addressing and facing hybrid threats challenges**	**1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
Civilian Training Area n. 15: Hybrid threats and cyber	**N/A**

Target audience	Aim
Participants would be preferable mid-ranking to senior level officials from Member States and relevant EU institutions and agencies. The training audience coming from the Member States might include, but is not limited to, participants from different ministries (Foreign Affairs, Defence, Economy, Interior, Research, Technology and Finance) as well as agencies sub-ordinated to such ministries and relevant members of the private sector. Participants are expected to have a basic knowledge on CSDP.	The course aims to provide civilian and military officials from EU institutions and relevant Agencies as well as from Member States, with the skills and knowledge to effectively take positions on security policies, strategies and missions/operations at senior staff level but also on capabilities development matters. It facilitates to get acquainted with diplomatic, institutional, legal and operational issues related to hybrid threats at the strategic level. It also allows Member States, via their officials, to share national perspectives and strategic analyses on this topic. These exchanges help to reinforce common situational awareness on hybrid threats across the EU.
Open to: ▪ EU member States / Institutions	

Learning Outcomes	
Know-ledge	LO 1 Identify the extensive nature and diversity of threats LO 2 Define the basic notions and concepts related to hybrid threats LO 3 Evaluate the strategic impact or risks of hybrid threats on EU MS, missions and operations LO 4 Identify the EU and others institutions/agencies involved and their respective roles LO 5 Identify broadly which actors analyse and address hybrid threats in the Member States LO 6 Apply an integrated approach to conception and implementation of security strategies at EU level LO 7 Describe and apprehend the EU instruments to counter hybrid threats LO 8 Acknowledge the cooperation and coordination aspects with partners
Skills	LO 9 Identify and distinguish the most important civil and military options implemented, within the framework of CSDP LO 10 Analyse the role of the EU capability development and technology response to hybrid threats LO 11 Understand the constraints in the operating environment (democracy and rule of law)
Responsibility and Autonomy	LO 12 Be able to further critical views to EU approaches and to the options to overcome problems related to them

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participant's satisfaction with the course*).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on the active contribution in the residential Module, including group work and practical activities as well as on the completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. Active observation by the course director/lead instructor and feedback questionnaire filled by course participants at the end of the course is used.

However, no formal verification of learning outcome is foreseen; proposed ECTS is based on participants' workload only.

Course structure		
Main Topic	**Suggested Working Hours (required for individual learning)**	**Suggested Contents**
1. Improving the common understanding of Hybrid threats/warfare/ modus operandi (legal and conceptual framework).	9 (6)	1.1 Hybrid threats as a strategic challenge 1.2 Definition of Hybrid threats/warfare and foreign interference 1.3 Legal aspects. Hybrid warfare and hybrid threats in the international law 1.4 Conceptual Framework on Hybrid Threats (JRC and CoE in Helsinki) 1.5 CORE Model (JRC and Hybrid Center of Excellency - CoE)
2. Challenges and multidimension of hybrid threats/warfare	4 (2)	2.1 A wide range of dimensions summarized in the CORE Model: - 13 domains: culture, social, information, cyber, space, economy, infrastructure, military defence, diplomacy, intelligence, legal, public admin, political - 3 spaces: Civic, Governance, Services - 3 layers: local, national, international 2.2. A wide range of challenges: - Terrorism and criminality - Hybrid threats in the maritime domain - Foreign Information Manipulation and Interference (FIMI) - Intelligence sharing - "Hybrid threats/warfare" in the cyberspace - Energy & critical infrastructures - Use of financial leverage - Use of Special Forces - Instrumentalised irregular migrant flows - The weaponisation of space
3. Countering hybrid threats: which division of roles? Member States, EU institutions	4	3.1 State level - Whole of Government and Whole of society approach - What domains, if there are any, are reserved for MS to handle? - How MS coordinate their national policies with the EU level? 3.2 EU level - Presentation of the EU framework, organisation and instruments.

		- European Defence Agency's contribution - Role of the Hybrid Fusion Cell (HFC) and the EU Intelligence and Situation Centre (INTCEN) - Improving awareness: situational awareness and early warning - Building resilience. Implementation of EU's countering hybrid threats policy - CSDP contribution to counter the hybrid threats - Mobilising EU instruments to counter hybrid threats (EU Hybrid Protocol for countering Hybrid Threats , crisis management mechanisms; ARGUS, CRM and IPCR) - Hybrid threats vs integrated approach. Use and coordination of existing tools and instruments to counter hybrid threats - Assessment of threats and their perpetrators - Vulnerabilities and resilience of critical infrastructures (including Energy security): coordination between MS and the EU Improving strategic communication: The Stratcom task forces: a communication tool for the EU - the 2018 EU action plan against disinformation - EU policy to counter foreign information manipulation and disinformation: FIMI toolbox - EU capability development and technology response to hybrid threats - A collective cybersecurity approach among EU agencies and civilian institutions
4. Cooperation and coordination with partners	4	4.1 EU-NATO coordination. Cooperation, complementarity - Common Set of Proposals - The Hybrid Center of Excellence (CoE): a structure serving the EU-NATO societies - Coordination of EU & NATO on cyber defense - NATO involvement in intelligence effort 4.3 Improving the resilience of the society and of EU partners: How to jointly strengthen democracy against threats towards policy and political processes? 4.4 UN/OSCE and relevant partner countries. Added value of cooperation with international organisation 4.5 Planning resilience and training 4.6 EU - NATO PACE exercises: experience; lessons identified; next steps
5. Case studies	2	5.1, Real-life examples:- Russian, Chinese and/or Iranian hybrid threats and campaigns in different domains and targeting different audiences in Europe or abroad Responses and lessons learned from such threats and campaigns
6. Challenges	3	6.1 Emerging security challenges in the EU 6.2 What are the key technological challenges?
TOTAL	**26 (8)**	

Materials	Methodology
Required: - 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	The course is based on the following methodology: lectures panels and case studies. Additional information All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The number of AKU's included in the e-learning module is decided by the Course director, but should not be fewer than two.

Recommended - AKU 55 – Strategic Compass - AKU 2: The European Global Strategy; - AKU 25: EU's Mutual Assistance Clause - AKU 106f (H-CoE): Hybrid threats in Maritime Security - AKU 6: Decision making/shaping - AKU 21: Intercultural Competences *Supplemental material (selection)* - EU Security Union Strategy - 2020. - Joint Framework on countering hybrid threats - a European Union response (06/04/2016) - European Council conclusions on Security and Defence (22/06/2017)	In order to facilitate discussion between course participants and trainers/experts/guest speakers, the Chatham House Rule is enforced during the residential module: "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".