European Security and Defence College
Doc: ESDC/2022/037
Date: 24 February 2022
Origin: Executive Academic Board

Curriculum

To be reviewed by	Activity number		ECTS
February 2024	*40*	**EU 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 to senior level staff from Member States and relevant EU institutions and agencies. The training audience coming from the MSs might include, but is not limited to, participants from different ministries (Foreign Affairs, Defence, Economy, Interior, Research, Technology and Finance). Participants are expected to have a basic knowledge on CSDP	The course is aimed to prepare military officers and civil servants from EU institutions and relevant Agencies as well as from Member States, 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 and moreover to security issues at strategic level.
Open to: ▪ EU member States / Institutions	

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 their syndicate session and practical activities as well as on their 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
1Improving the common understanding of "hybrid threats/warfare" (legal and conceptual framework).	9 (6)	1.1 "Hybrid threats/"Operations as a strategic warning? ~~1.2~~ Definition of "Hybrid threats/warfare"~~:~~ 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)
2. Challenges and multidimension of "hybrid threats/warfare".	4 (2)	2.1 A wide range of dimensions and challenges: - Terrorism and criminality; - Maritime hybridation; - Disinformation, misinformation, malinformation/media - Intelligence sharing; - "Hybrid threats/warfare" in the cyberspace; - Energy & critical infrastructures; - Use of financial leverage; - Use of special forces. - The weaponisation of irregular migrant flows
3. Countering hybrid threats: which division of roles? Nations, EU, NATO.	4	3.1 State level - Whole of Government and Whole of society approach" 3.2 EU level: - Presentation of the EU framework, organization and instruments. - Presentation of the EU framework; - European Defence Agency's contribution; - Improving awareness: situational awareness and early warning. - Building resilience. Implementation of an EU hybrid security policy. CSDP contribution to counter the hybrid threats - Mobilizing EU instruments to counter hybrid threats (EU Hybrid Playbook, crisis management mechanisms; ARGUS, CRM and IPCR). Hybrid threats vs integrated approach. Use and coordination of existing tools and instruments to counter hybrid threats. - Energy Security Strategy & the protection of critical energy infrastructures. 3.3 NATO level
4. Cooperation and coordination with partners	4	4.1 EU-NATO coordination. Cooperation, complementarity - Common Set of Proposals 4.2 Improving intelligence gathering and sharing: - NATO involvement in intelligence effort; - Role of the Hybrid Fusion Cell (HFC) - EU Intelligence and Situation Centre (INTCEN) 4.3 Improving strategic communication: - The Stratcom task forces: a communication tool for the EU; - 2018 EU action plan against disinformation; 4.4 EU policy to counter foreign information manipulation and disinformation 4.5 Improving the partnerships to counter hybridity: - A collective cyber defense in Europe: coordination of EU & NATO cyber defense. - A collective cybersecurity approach among EU agencies and civilian institutions. 4.6 Improving the resilience of the society and of EU partners: - The Center of Excellence (CoE): a structure serving the EU-NATO. - How to strengthen democracy against threats towards policy and political processes? 4.7 UN/OSCE and relevant partner countries. Cooperation with international organizations. 4.8 EU capability development and technology response to hybrid threats 4.9 Planning resistance and training. 4.10 EU - NATO PACE exercises: experience; lessons identified; next steps.

5. Case studies	2	5.1, Real-life examples: - Russia and/or Chinese hybrid warfare; - Improving the resilience of the society; How to strengthen democracy against disinformation -
6. "Challenges	3	6.1 Emerging security challenges in the EU 6.2 What are the key technological challenges?
TOTAL	**26 (8)**	

Materials

***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

Recommended
- 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 7: Impact of Lisbon treaty in CSPD
- AKU 21: Intercultural Competences

Supplemental material (selection)
- Joint Framework on countering hybrid threats - a European Union response (06/04/2016)
- European Council conclusions on Security and Defence (22/06/2017)

Methodology

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.

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".