

Curriculum

| | | | |
|---|------------------------------|--|-------------------|
| To be reviewed by <i>February 2022</i> | Activity number 40 | EU facing “hybrid threats” challenges | ECTS 1 |
|---|------------------------------|--|-------------------|

| | |
|---|---|
| <u>Target audience</u> <i>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 and Finance). Participants are expected to have a basic knowledge on CSDP</i> | <u>Aim</u> The course is aimed to prepare military officers and civil servants from EU institutions and relevant Agencies and 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. |
|---|---|

| | | |
|--------------------------|-------------|--|
| Learning outcomes | Knowledge | <ul style="list-style-type: none"> Identify the extensive nature and diversity of threats. Define the basic notions and concepts related to hybrid threats. Evaluate the strategic impact or risks of hybrid threats on EU MS, missions and operations. Identify the EU and others institutions/agencies involved and their respective roles. Apply an integrated approach to conception and implementation of security strategies at EU level. Describe and apprehend the EU instruments to counter hybrid threats. Acknowledge the cooperation and coordination aspect's with partners. |
| | Skills | <ul style="list-style-type: none"> Identify and distinguish the most important civil and military options implemented, within the framework of CSDP. Analyse and take benefit from the role of the EU capability development and technology response to hybrid threats. Understand the constraints in the operating environment (democracy and rule of law). |
| | Competences | <ul style="list-style-type: none"> Be able to further critical views to EU approaches and to the options to overcome problems related to them. Develop a capability to make proposals to CSDP institutional management. |

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 | Recommended Working Hours (of that eLearning) | Contents |
| Definitions – What is “hybrid threats” – and State of play (legal and conceptual framework): improving the common understanding of “hybrid threats/warfare”. | 9 (6) | <ul style="list-style-type: none"> • Opening speech: “Hybrid threats/warfare” as a strategic warning? • Definition of “Hybrid threats/warfare”: an academic point of view • Legal aspects. Hybrid warfare and hybrid threats in the international law • Conceptual Framework on Hybrid Threats (JRC and CoE in Helsinki) |
| Challenges and multidimension of “hybrid threats/warfare”. | 4 (2) | <ul style="list-style-type: none"> • A wide range of dimensions and challenges: <ul style="list-style-type: none"> - Terrorism and criminality; - Maritime hybridation; - Information manipulation: counter propaganda/media; - Intelligence sharing; - “Hybrid threats/warfare” in the cyberspace; - Energy & critical infrastructures; - Use of financial leverage; - Artificial intelligence (AI); - Use of special forces. |
| Countering hybrid threats: which division of roles? Nations, EU, NATO. | 4 | <ul style="list-style-type: none"> • State level • EU level: <ul style="list-style-type: none"> - Presentation of the EU framework; - European Defence Agency’s contribution; - Improving awareness: situational awareness and early warning. Integrated approach: awareness, strategic communication, research and training - Building resilience. Implementation of an EU hybrid security policy. CSDP contribution to counter the hybrid threats. Building resilience in third states; preparedness and response. Adaptation defence capabilities for hybrid threats. Common tools for the protection of critical infrastructure (diversification of energy resources, promotion of safety and security standards, resilience of nuclear infrastructure, emerging threats in transport sector, resilience of space infrastructure/satellite communications) - Mobilising 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. Need for new instruments. Comprehensive reaction. - Energy Security Strategy & the protection of critical energy infrastructures. • NATO level |
| Cooperation and coordination with partners | 4 | <ul style="list-style-type: none"> • EU-NATO coordination. Cooperation, complementarity <ul style="list-style-type: none"> - Warsaw leaders' statement - Common Set of Proposals • Improving intelligence gathering and sharing: <ul style="list-style-type: none"> - NATO involvement in intelligence effort; - Role of the Hybrid Fusion Cell (HFC) - EU Intelligence and Situation Centre (INTCEN) • Improving strategic communication: <ul style="list-style-type: none"> - The Stratcom task forces: a communication tool for the EU; - 2018 EU action plan against disinformation; • Improving the partnerships to counter hybridity: <ul style="list-style-type: none"> - A collective cyberdefense in Europe: coordination of EU & NATO cyberdefenses. |

| | | |
|-------------------------------------|---------------|--|
| | | <ul style="list-style-type: none"> - A collective cybersecurity approach among EU agencies and civilian institutions. • Improving the resilience of the society and of EU partners: <ul style="list-style-type: none"> - The Center of Excellence (CoE): a structure serving the EU-NATO. - How to strengthen democracy against threats towards policy and political processes? • UN/OSCE and relevant partner countries. Cooperation with international organisations. • EU capability development and technology response to hybrid threats • Planning resistance and training. • EU - NATO PACE exercises: experience; lessons identified; next steps. |
| Case studies | 2 | <ul style="list-style-type: none"> • Case studies, real-life examples: <ul style="list-style-type: none"> - Russia and hybrid warfare; - Improving the resilience of the society; - How to strengthen democracy against threats towards policy and political processes? |
| "Hybrid threats/warfare" challenges | 3 | <ul style="list-style-type: none"> • Emerging security challenges in the EU • What are the key technological challenges? |
| TOTAL | 26 (8) | <i>NB: It does not include coffee and lunch breaks (+ 8 hours)</i> |

| | |
|---|---|
| <p style="text-align: center;"><u>Materials</u></p> <p><i>Essential eLearning:</i></p> <ul style="list-style-type: none"> - AKU 2: The European Global Strategy; - AKU 25: EU's Mutual Assistance Clause - 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 warfare - AKU 106f (H-CoE): Hybrid threats in Maritime Security <p><i>Recommended eLearning</i></p> <ul style="list-style-type: none"> - AKU 6: Decision making/shaping - AKU 7: Impact of Lisbon treaty in CSPD - AKU 21: Intercultural Competences <p><i>Supplemental material (selection)</i></p> <ul style="list-style-type: none"> - Joint Framework on countering hybrid threats - a European Union response (06/04/2016) - European Council conclusions on Security and Defence (22/06/2017) | <p style="text-align: center;"><u>Additional information</u></p> <p>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.</p> <p>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".</p> |
|---|---|