COMMUNICATION

EDA202203117/CAP/AS 28 March 2022

EDA documentation for Government use only

**Martin KONERTZ**
Director Capability, Armament and Planning
CAP@eda.europa.eu
T. +32 2 504 28 50

To: CAPABILITIES POCS, PT CYBER DEFENCE, EEAS, ENISA, EC3, CERT-EU, CH

# INVITATION TO THE PILOT COURSE "THE CONTRIBUTION OF CYBER IN HYBRID CONFLICT" PILOT COURSE, 12 – 16 SEP 2022

Annex: Course Schedule
Attachment: Hybrid CoE Admin Package

In 2019, EDA started the development of a Methodology for Developing Cyber Defence Training Courses and the conduct of several Cyber Defence Pilot Courses under the project 18.CAT.OP.205. The Methodology was delivered at the end of 2019 and is published at the EDA website.

In that context, EDA is pleased to invite MS, EU Institutions, Bodies and Agencies (including Missions and Operations) and Switzerland to nominate candidates for attending "**The Contribution of Cyber in Hybrid Conflict**" Pilot Course. This pilot activity is organised by EDA under the European Security and Defence College framework and follows the ESDC rules of nomination and selection for the participants.

The course is announced as **ESDC Activity No 22-23/274/1**.

Details can be found at https://goalkeeper.eeas.europa.eu/course/details.do?id=684, and ESDC website: https://esdc.europa.eu/courses

The pilot course will take place from **12 to 16 September 2022 at the HYBRID Centre of Excellence (HYBRID CoE)** in Helsinki, FI, as a physical course for a maximum of 35 participants.[1] The course starts on 12 September 2022 14:00 local Helsinki time and finishes on Friday 16 September 2022 13:00 local Helsinki time. The course will be held in English.

[1] If the evolution of the COVID-19 situation is to impact possibilities for physical attendance to the course, EDA is not in a position to reimburse potential costs incurred for both travel and accommodation.

EUROPEAN DEFENCE AGENCY

## COMMUNICATION

The objective of the Pilot Course is to educate participants about key elements of cyber defence and hybrid threats, and to provide them with individual training to enable them to address the implications of the nexus of cyber and hybrid. While applicable in a wider range of environments, the course focus is set to explicitly address implications in military operations. Furthermore, the course will provide participants with opportunities for networking and intellectual cross-fertilisation (potentially across communities that may not frequently interact).

Participants should be mid-to-senior rank military officers or civilian equivalents filling (or liable for) 'general staff' (ie non-Cyber Specialist) roles within the EU Institutions or in Member State and higher HQs who:

- engage in development of policies, strategies, concepts, or doctrine related to cyber defence or hybrid threats; and/or
- design or deliver professional education courses, individual training courses, or command post exercises related to cyber defence or hybrid threats, focused on military demands and needs.

The main activities for the Pilot Course are:

- **A foundation module embracing educational activities to impact knowledge and generate understanding**
- **An advanced module in which participants apply knowledge and understanding in a (synthetic) practical way through a matrix-style game/exercise**

You are kindly requested to provide names and contact details of nominees attending the pilot course[2] following the ESDC nomination process, **NTL 13 June 2022**.

For further information please contact the EDA Cyberteam (cyberteam@eda.europa.eu).

To identify your responsible ESDC nominator, please consult https://esdc.europa.eu/nominators/.

For registration and administrative aspects, please contact the ESDC Cyber Team: (EEAS ESDC CYBER ETEE ESDC-CYBER-ETEE@eeas.europa.eu and the Training manager, Mr Gregor SCHAFFRATH Gregor.Schaffrath@eeas.europa.eu)

Martin KONERTZ

[2] The European Defence Agency is committed to the protection of personal data. Personal data collected by EDA will be processed pursuant to Regulation (EU) 2018/1725. For more details, please consult the Privacy Statement.

Annex

Course Schedule

| Course structure | | |
|---|---|---|
| **Main Topic** | **Recommended Working Hours (of that eLearning)** | **Contents** |
| Module 1: Cyber fundamentals | 4 | • Introducing fundamental concepts related to the cyber domain, cybersecurity and cyber defence<br>• Cybersecurity and cyber defence in the European context<br>  o Roles and responsibilities within CSDP, the EU and other institutions |
| Module 2: Hybrid threat fundamentals | 4 | • Introducing fundamental concepts related to hybrid threats<br>• Mitigating and responding to hybrid threats in the European context<br>  o Roles and responsibilities within CSDP, the EU and other institutions |
| Module 3: The cyber-hybrid intersection | 4 | • Understanding the intersection between cyber and hybrid threats<br>  o Understanding cyber and hybrid threats for the military<br>• Embedding cyber considerations when planning for hybrid threats<br>  o Mapping potential cyber-hybrid threats to multi-national operations/missions |
| Module 4: Table-top exercise on the Contribution of Cyber in Hybrid Conflict | 12 | • Test knowledge and skill on cyber / hybrid threats and their intersection transferred to participants during previous modules in the context of a serious game / TTX<br>• Provide a forum for participants to explore insights, observations, and lessons related to challenges stemming from the intersection of cyber defence and hybrid threats<br>• Provide opportunities for participants to share awareness and experience of operating on issues at the intersection between cyber and hybrid threats<br>• Provide a networking and relationship development opportunity |