14 September 2022

# INVITATION TO THE "CYBER IMPLICATIONS FOR CSDP MILITARY CRISIS ACTION PLANNING" PILOT COURSE, 16 – 18 NOV 2022

Annex: Course Draft Agenda

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

With this invitation, ESDC and EDA are pleased to invite MS, EU Institutions, Bodies and Agencies and Switzerland to nominate candidates for attending the "**Cyber Implications for CSDP Military Crisis Action Planning**" Pilot Course (ESDC Activity No 22-23/271/1), following the attached ESDC course publication form. This pilot activity is organised under the European Security and Defence College framework and follows its rules of nomination and selection for the participants.

Details can be found at https://goalkeeper.eeas.europa.eu/course/details.do?id=864

The pilot course will take place from **16 – 18 November 2022** in Brussels, BE, as a presence course for a maximum of 50 participants. Course venue will be announced in due time. The course will be held in English.

The aim of the Pilot Course is to educate participants about the use of Cyberspace to plan and conduct missions and operations, and to provide them with individual training to enable them to address the implications of such use in their work related to CSDP CMO planning.

While applicable in a wider range of environments, the course focus is set to explicitly address implications in military operations. Additionally, the course will provide participants with opportunities for networking and intellectual cross-fertilization.

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 States and higher military HQs who:

(1) plan CSDP CMO;

(2) engage in development of policies, strategies, concepts, or doctrine related to CSDP CMO or:

(3) design or deliver professional education courses, individual training courses, or command post exercises.

The main topics for the Pilot Course are:

- **Preliminaries** (including a syndicate-based quiz to determine the collective input standard)

- **Cyber Fundamentals**: **Cyberspace, Cyber-attacks, Cybersecurity**
- **Cyber Operations: Principles, Concepts and Doctrine**
- **Cyber Considerations in CSDP Crisis Action Planning**
- **Close-out** (panel Q&A, then a syndicate-based quiz to determine the collective output standard)

You are kindly requested to provide names and contact details of nominees attending the pilot course[1] following the ESDC nomination process, **NTL 10 Oktober 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 SCHAFFRATH Gregor (EEAS) (Gregor.SCHAFFRATH@eeas.europa.eu))

Please note that this course was previously planned for June 2022 (see attached invitation letter EDA), but was shifted to the new date in November 2022.

Annex

## Course Schedule

| Course Schedule (Draft V0.3) | | | |
|---|---|---|---|
| **Serial** | **Main Topic** | **Recommended Working Hours (of which e-Learning)** | **Contents (Sub-Topics)** |
| A | Preliminaries | 0.5 (0) | A.1 Course Administration; Course Aim, Learning Outcomes & Programme; Trainer & Participant Introductions |
| | | 0.5 (0) | A.2 Syndicate-based Quiz (to determine collective input standard/baseline) |
| B | Cyber Fundamentals | 3.5 (2) | B.1 The nature and lexicon of digital technologies, cyber-attacks and cybersecurity measures, and how these interact in the real world (case studies) |
| | | 1 (0) | B.2 The EU landscape for Cybersecurity & Cyber Defence of CSDP Military Operations and Missions: Policies; Concepts; Strategies; Actors; Capabilities (Guest Speaker) |
| C | Cyber Operations: Principles, Concepts and Doctrine | 1 (0) | C.1. Information Assurance; Safety, Reliability & Availability of Information Assets; Cyber Threats; Cyber Vulnerabilities; Resilience; Mission Assurance; Operational Risks & Mitigations |
| | | 2 (1) | C.2. Cyberspace as an Operational Domain; Cyber Deterrence & Diplomacy; Legal frameworks for Cyber Operations; Military reliance on cyberspace; Cyber Operations, functions and actors; Cyber contributions to joint military campaigning; the Cyber Operations 'Value Chain'; the 'Cyberspace Contest'; the 'Cyber Defence Dilemma'; Cyber in Effects-Based Planning |
| | | 0.5 (0) | C.3. Syndicate Exercise: 'How do Cyber Operations fit within wider military activities?' |
| | | 1 (0) | C.4. Cyberspace & 'Hybrid' campaigning; Potential Cyber threats to military operations/missions; Additional Cyber vulnerabilities of multi-national operations; Cyber threats and Operational Risk Management |
| D | Cyber Considerations in CSDP Military Crisis Action Planning | 1 (0) | D.1 Cyber Considerations in Planning: All-source Intelligence; Threat Assessment; Command & Control Architecture; Logistics Posture; Cyber Defence Posture; Training Requirements |
| | | 1 (0) | D.2 The EU CSDP 'Planning Snake'; Cyber considerations in planning: Military Strategic Options (MSO - EUMS); Initiating Military Directive (IMD - EUMS) (Guest Speaker) |
| | | 1 (0) | D.3 Introduction to the 'REDLAND' scenario, followed by Syndicate Exercise: 'Cyber Threat Assessment' |
| | | 1 (0) | D.4 Cyber Considerations in Planning: Cyber-focused Centre of Gravity Analysis; Cyber and Battlespace Architecture (boundaries; key terrain etc); Cyber and Force Composition; Cyber & C2 Architecture; Cyber & Force Supply Chain; Cyber consequence analysis & contingency planning |
| | | 1 (0) | D.5 Update on the 'REDLAND' scenario, followed by Syndicate Exercise: 'Operation MORGANTIC Cyber-focused Centres of Gravity Analysis' |
| | | 1 (0) | D.6 Update on the 'REDLAND' scenario, followed by Syndicate Exercise: 'Operation MORGANTIC C2 Architecture' |
| | | 1 (0) | D.7 Cyber considerations in EU CSP Crisis Action Planning: Concept of Operations (CONOPS - OHQ); Operations Plan (OPLAN - FHQ) (Guest Speaker) |
| | | 1 (0) | D.8 Update on the 'REDLAND' scenario, followed by Syndicate Exercise: 'Operation MORGANTIC Force Supply Chain' |
| | | 1 (0) | D.9 Update on the 'REDLAND' scenario, followed by Syndicate Exercise: 'Operation MORGANTIC Cyber Risk Anlaysis' |
| E | Close-out | 1 (0) | E.1 Trainer & Speaker Panel Q&A |
| | | 0.5 (0) | E.2 Syndicate-based Quiz (to determine collective output standard) |
| | | 0.5 (0) | E.3 Closing administration & farewells |
| | **Total** | **21 (3)** | |