European Security and Defence College
Doc: ESDC/2021/147
Date: 23 June 2021
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Security/Defence Training Programme (CSDP TP CS/DC)	ECTS
February 2023	*201*		**5**

Target audience

The target audience of this specific training programme are officials from EU member states and EU institutions (incl. agencies) with no or limited experience of cyber security/cyber defence in relation to CFSP/CSDP.

If decided, the course can be opened for participants from international organisations such as the UN, OSCE and NATO.

Aim

The course aims to give participants an understanding of cyber security and defence aspects within the Common Security and Defence Policy, to provide a detailed overview of cyber security action at EU level and to enhance participants' knowledge and skills to mitigate risks and threats in the cyber domain at an individual and organisational level. During the course, the formation of networks among individuals will be encouraged.
The final goal of the course is to support the cyber-action within the EU institutions and EU member states.

Learning outcomes***		

	Knowledge	• Define the main goals of the Cyber Security Strategy and the Cyber Defence Policy;
		• Name the main principles of CSDP in the field of cyber security.
		• Identify
		  ○ the main actors and structures at EU level in relation to cyber defence and security,
		  ○ the required procedures in the cyber domain for CSDP operations
		• Recognise the main cyber vulnerabilities, including risks and threats for cyber security/defence/crime;
		• Define main principles in Cyber risk management and assessment for operational planning

	Skills	• Demonstrate the advantages and disadvantages of the current cyber security and defence structures and procedures; • Illustrate the roles and responsibilities of EU institutions and EU member states in relation to cyber defence and security. • Apply the Cyber Risk Management and Assessment principles for operational planning; • Categorise the various levels for operational planning;
	Competences	• Assess and manage the risks and threats at strategic and operational level; • Summarize the main achievements of the EU's Cyber Security Strategy and the Cyber Defence Policy Framework; • Assess the weak points of cyber defence in the planning phase for CSDP engagement; • Assess action-to-be-taken at EU and national level to mitigate the cyber risks and threats.

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 each of the three modules is used. An overall evaluation report will be drafted at the end of the course (3 modules). For the High Level Conference, a level 1 evaluation will take place.

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**
Module 1: Awareness/Basic Level	24 (+10)	• History and Development of CSDP • Structures and procedures • EU Global Strategy, the Cyber Security Strategy and the Cyber Defence Policy Framework • Cyber law, concepts and policies • Cyber security: Awareness, Hygiene, Forensic, Risks and Threats, Mainstreaming in CSDP missions and operations
Module 2A: Advanced Level	16 (+10)	• Cyber Security objectives • Strategic cyber threat and vulnerabilities assessment • EEAS and EC crisis response system, in particular in the cyber domain • Cyber risk management in CSDP missions and operations • Capability Development, including Research & Technology • Cyber Security and the EU's integrated approach
Module 2B: Operational Planning	24 (+10)	• Operational Risk Management • Cyber Risk Assessment in missions and operations • Integration of cyber elements in the operational and mission planning process • CIS Accreditation • Implementation of Cyber aspects for CSDP operations and missions • Implementation of the Cyber Diplomacy Toolbox
High Level Conference (HLC) - Alumni	16 (+6)	• New developments in the cyber environment • Strategies, laws, policies and concepts • New risks and threats • Regional and horizontal CSDP issues
TOTAL	**116 (+36)**	

Materials	Additional information
- Materials will be made available online on the eLearning platform of the ESDC; - on a case by case basis, the programme/conference director can distribute further information;	Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used. All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. In order to facilitate discussion between course participants and trainers/experts/guest speakers, the **Chatham House Rule** is used during the residential Module: "*participants to the CSDP HLC 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*"**.** ** The participants are invited to agree on being photographed or filmed during the training sessions; the pictures or films can be used by the ESDC or concerned ESDC network partners in relation with CSDP related training delivered within the Network*