European Security and Defence College
Doc: ESDC/2022/073
Date: 1 April 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number		ECTS
Feb. 2024	**262**	**Cyber Defence policy on national and international levels**	**1**

Target audience	Aim
Participants should be mid-ranking to senior officials from the defence and security sector dealing with strategic aspects of cyber security and cyber defence from EU MSs, relevant EU Institutions and Agencies. They should be either working in key positions or have a clear potential to achieve leadership positions, in particular in the field of Cyber Security or Defence. Course participants must be available for the entire course and should be ready to bring in their specific expertise and experience throughout the course.	The aim is to provide course participants with the conceptual framework to facilitate strategic thinking about cyber defence and develop understanding on how to integrate cyber considerations into national as well as international security policy and strategy formulation. The training will provide the participants with basic skills and knowledge to analyse and design proper policy framework and strategy for cyber defence. The curriculum has been designed to provide an integrated overview of contemporary geopolitical affairs and security issues to enable students to think creatively and critically about issues of strategic importance.
Open to: ▪ EU Member States / EU Institutions Bodies and Agencies	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised cyber course, at strategic and tactical levels* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes	
Knowledge	LO1– Quote key features of the modern/future security environment LO2- Define cyber domain as key enabler and tool of hybrid warfare LO3- Define the validity of cyberspace in the creation, storage, modification, exchange and exploitation of the information LO4- Define the dependency of the of the military domain on communication and information systems & networks LO5- Define the growing role of the cyberspace as a web of critical asset and its relation to the national security LO6- Understand basic technological aspects of cybersecurity

Skills	LO7- Classify the instruments of national power and relate them to the cyberspace effects LO8- Analyse the strategic aspects of cyber security in the national security environment LO9- Apply cyberspace terminology, concepts, issues, and components LO10- Relate cybersecurity considerations with the information environment LO11- Analyse various aspects of cybersecurity and relate their effects to national security
Responsibility and Autonomy	LO12- Evaluate cyber space policies and generate strategic concepts and approaches to cyber defence LO13- Assess the role of cyber defence in national and international security contexts LO14- Determine the appropriate measures to ensure the national security in digital era

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participants' satisfaction with the course*) and *level 3 evaluation* (*assessment of participants' long-term change in behaviour after the end of the course*). *Evaluation feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *Certificates* to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the *final evaluation report* which is presented to the Executive Academic Board.

Course structure

The residential module is held over 3 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. key concepts: Cyberspace, cybersecurity, cyber defence	6(6)	1.1 Terminology and key concepts 1.2 Digital revolution and its impact 1.3 Cyber as an operational domain 1.4 Threat actors in cyberspace 1.5 International relations in cyberspace 1.6 International law and inter-state relations in cyberspace 1.7 Cyber-enabled influence operations
2. Practical aspects of cybersecurity: vulnerabilities and responses	4	2.1 Anatomy of cyberattacks 2.2 Cyber targeting and layers of defence 2.3 CEMA - Cyber-Electromagnetic Activities 2.4 Examples of defensive measures 2.5 Cyber. considerations in real war
3. Cyber policy dilemmas: – deterrence, defence or defence foreword?	6(4)	3.1 Analysis of the cyberspace policy and strategy 3.2 Military aspect of cyber considerations 3.3 Definition of cyberspace superiority 3.4 Joint concept for cyberspace
4. Technology aspect of cyber defence and information security	4	4.1 Confidentiality, Integrity, Availability 4.2 Basics of security engineering 4.3 Information security risk 4.4 Reasons for Security Vulnerability Technology aspect

5. Cyber considerations in national and international security policy	8(4)	5.1 Cyber and other elements of national power 5.2 The role of private sector in cyber defence 5.3 Threat Environment 5.4 Private Sector Roles and Missions
TOTAL	**28(14)**	

Materials	Methodology
Required: AKU 2: European Global Strategy AKU 107: Awareness course on Cyber Diplomacy **Recommended:** • AKU 6: CSDP Decision Making, • AKU 106a: Adversarial behavior • AKU 106b: The landscape of hybrid threats • AKU106e: Hybrid warfare • Reading material [examples]: ○ Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016) ○ European Parliament: Directive on security of network	The course is based on the following methodology: lectures, panels, workshops, exercises Additional 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. The materials proposed for supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular. The Chatham House Rule is applied during all residential phase of the course: "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".