European Security and Defence College
Doc: ESDC/2021/146
Date: 23 June 2021
Origin: ESDC Secretariat

Curriculum

To be reviewed by *February 2023*	Activity Number *200*	**Challenges of European Cyber Security**	ECTS **1**

Target audience

Participants should be mid-ranking to senior officials dealing with strategic aspects in the field 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.

Aim

The course aims to enable participants to understand the extensive nature of the information society and to recognise its complexity and the different threats, as well as the basic notions and concepts related to cyber security and cyber defence, as well the international cyber space issues and the cyber diplomacy.

Offering an overview on technological tools used in the cyber security and cyber defence, the course aims at providing an opportunity to create a network of people working in the field.

Learning outcomes	Knowledge	○ Recognise the extensive nature of the information society we are living in ○ Recognise the complexity of the information society ○ Recognise the nature of the different cyber threats we are experiencing. ○ Define the basic notions and concepts related to cyber security and cyber defence. ○ Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles. ○ Identify the challenges of cyber security at a European level and the way ahead. ○ Reflect on the different trends in cyber threats ○ Address international cyber space issues and cyber diplomacy
	Skills	○ Identify technical as well as organisational tools related to cyber security. ○ Consider the potential impacts of cyber threats in public policies. ○ identify the challenges of industrial and public planning needed to face cyber threats ○ Perceive the challenges of industrial and public planning needed to face cyber threats.
	Competences	○ Evaluate the potential impacts of cyber security on public policies ○ Assess and summarize the challenges of cyber security at European level and the way ahead

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
Cyber Space and Cyber Strategy	15 (8)	Overall contextual framework: past, present and future trends Definitions and concepts of Cyber Security Trends in cyber threats and critical Infra-structures Towards a strategic autonomy for EU in Cyber-Space. European cyber security strategy; EU's implementation of cyber security National cyber-security policies: comparison and exchanges – point of view and strategies Cyber-Security on private infra-structure: role and responsibilities of Private Sector; issues of Cyber Security on private infra-structure
Cyber Security and Cyber Defence	3	Cyber Security / Cyber Defence needs for the EU and CSDP Critical infra-structure protection against cyber attacks Assessment and perspectives of EU's progress in cyber security EU Cyber Defence Policy Framework EU NIS Directive EU Capacities in cyber security
Cyber War and Cyber Crime	4	Legal framework for cyber operations UN Charter and International Humanitarian Law in cyberspace promoting the Budapest Convention Cyber regulation in the EU and national best practices Digital combat in the Conduct of Military Operations; specificity of military cyber space; incidence of digitization and robotisation of the battle field Cyber security and cross-domain warfare Cyber Attack simulation
Cyber Diplomacy and Cyber Co-operation	5	Preventing cyber war: role of confidence-building measures EU Role in reinforcing member-states capacities Actions of EDA Human resource capacity building Building a European cyber industry Cyber diplomacy and international cyber issues Intelligence, interference and cyber diplomacy
TOTAL	**27 (8)**	

Materials

Essential eLearning:
AKU 1 History and context of ESDP/CSDP development
AKU 2 on European Global Strategy
AKU 3 : The Role of EU institutions in the field of CFSP/ CSDP

Recommended study on voluntary basis:
AKU 7: Impact of Lisbon treaty in CSPD
AKUs 30-32, as soon as become available

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 and information systems by the European Parliament (2016)

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.

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*"**.**