European Security and Defence College
Doc: ESDC/2019/130
Date: 29 March 2019
Origin: ESDC Steering Committee

Curriculum

To be reviewed by	Activity number	**Challenges of European Cybersecurity**	ECTS
February 2021	*200*		**1**

Target audience

Participants should be mid-ranking to senior officials dealing with strategic aspects in the field of cybersecurity and cyber defence from EU Member States and relevant EU institutions and agencies. They should either be working in key positions or have a clear potential to achieve leadership positions, in particular in the field of cybersecurity or cyber defence.

Course participants must be available for the entire course and should be prepared to contribute 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 cybersecurity and cyber defence, international cyber space issues and cyber diplomacy.

Offering an overview of the technological tools used in cybersecurity and cyber defence, the course aims to provide 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 cybersecurity and cyber defence ○ Identify the EU institutions and agencies involved in cybersecurity and cyber defence and their respective roles ○ Identify the challenges of cybersecurity at a European level and the way forward ○ 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 on public policies. ○ Identify the challenges of industrial and public planning needed to face cyber threats.
	Compe-tencies	○ Evaluate the potential impacts of cybersecurity on public policies. ○ Assess and summarise the challenges of cybersecurity at European level and the way forward.

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).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution in the residential module, including the 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 a feedback questionnaire filled in by course participants at the end of the course are also used.

However, no formal verification of learning outcomes is foreseen; the proposed European credit transfer system (ECTS) score is based on participants' workload only.

Developed by: ESDC Secretariat

Course structure		
Main topic	**Recommended Working Hours (of that eLearning)**	**Contents**
Cyberspace and cyber strategy	15 (8)	Overall contextual framework: past, present and future trends. Definitions and concepts of cybersecurity Trends in cyber threats and critical infrastructures Towards strategic autonomy for the EU in cyberspace. European cybersecurity strategy; the EU's implementation of cybersecurity National cybersecurity policies: comparison and exchanges – points of view and strategies Cybersecurity in private infrastructures: the role and responsibilities of the private sector; issues related to cybersecurity in private infrastructures
Cybersecurity and cyber defence	3	Cybersecurity / cyber defence needs of the EU and CSDP Protection of critical infrastructure against cyber-attacks Assessment of the EU's progress in cybersecurity and outlook EU cyber defence policy framework EU NIS Directive EU cybersecurity capacities
Cyber war and cybercrime	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 cyberspace; incidence of digitisation and *robotisation* of the battlefield Cybersecurity and cross-domain warfare Cyber-attack simulation
Cyber diplomacy and cyber cooperation	5	Preventing cyber war: the role of confidence-building measures. The EU's role in reinforcing Member States' capacities. EDA action. 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: 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 the Lisbon treaty in CSDP
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 (2016)

Additional information

A pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used.

All course participants must prepare for the residential module by completing the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity/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 in the course 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'***.**