European Security and Defence College
Doc: ESDC/2022/ 063
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2024**	Activity number **206**	**The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability**	ECTS **1**
			EAB.CYBER **N/A**

Target audience

Participants should be mid-ranking to senior officials dealing with aspects in the field of cyber security from Third Countries

Course participants must be available during the entire course and should be ready participate with their specific field of expertise and experience.

Open to:

- EU Member States / EU Institutions Bodies and Agencies
- Third countries
- International Organisations

Aim

This course presents the main pillars of the EU cyber ecosystem and how these pillars can reinforce the global security stability by strengthening the cyber resilience, built trust and upscaling the cooperation among the global actors.

Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on cyber-related topics by improving their knowledge, skills and competencies.

By the end of this course the participants will be able to be more interoperable across the global cyber ecosystem and to share some common views.

Learning Outcomes

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

Knowledge	L01- List the policies used in EU related with cyber L02- Identify the entities involved in the EU cyber ecosystem and their respective roles L03- Define the basic notions and concepts related to cyber security within EU L04- Identify the nature of the different cyber threats L05- Identify the challenges of cyber security at global level L06- Identify the international cyber space issues and their effect globally L07- Identify the specific sectors for cooperation globally L08- Define the basic notions and concepts related to hybrid threats

Skills	L09- Classify the cyber issues according to complexity L10- Classify the impact of the cyber threats in the global stability L11- Categorize the cooperation opportunities with the EU cyber ecosystem and the global cyber environment
Responsibility and Autonomy	L12- Evaluate the potential impacts of cyber threats in the global environment L13- Create opportunities for synergies with the EU cyber ecosystem and the global cyber environment L14- Select the appropriate trust building measures to broaden cooperation in cyber domains

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. It is a non-specialised course, at awareness level link with the Pillars 3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020).

Furthermore the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase].

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. The EU Cyber Ecosystem	8 (4)	1.1 Present the EU Agencies and bodies with cyber- related tasks
2. The EU Approach building resilience in cyberspace	12 12 (4)	1.1 Policies - Regulations Directives related with cyber within EU 1.1.1 EU Cybersecurity Strategy 1.1.2 Digital Single Market Strategy for Europe 1.1.3 Network and Information Security (NIS) Directive 1.1.4 Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', 1.1.5 The Cyber Security Act 1.1.6 The General Data Protection Regulation 1.1.7 The EU Coordinated Response to Large Scale Cybersecurity Incidents and Crises 1.2 The Communication on the EU Strategic Approach to Resilience defines
3. The EU's External Cyber Capacity Building	5	3.1 Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', 3.1.1 The EU Cyber Diplomacy Toolbox

4. The EU Approach in the Hybrid threats	2	4.1 The conceptual framework on hybrid threats and the interaction with cyber
TOTAL	**29(8)**	

Materials

Required:
AKU 2 on European Global Strategy

Recommended:

- *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*
- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *The EU Cybersecurity Act (June 2019)*
- *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*

Methodology

The course is based on the following methodology: lectures, panels, workshops

Additional information

The Chatham House Rule is applied during all residential modules of the HLC: "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".

The mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).