**European Security and Defence College**
**Doc: ESDC/2020/038**
**Date: 14/02/2020**
**Origin:** ESDC Secretariat

# Curriculum

| To be reviewed by | Activity Number | **The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability** | ECTS |
|---|---|---|---|
| *February 2022* | *206* | | **1** |

| Target audience | Aim |
|---|---|
| Participants should be mid-ranking to senior officials dealing with aspects in the field of cyber security from Third Countries<br><br>Course participants must be available during the entire course and should be ready participate with their specific field of expertise and experience. | 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.<br><br>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.<br><br>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** | Knowledge | K1 - List the policies used in EU related with cyber<br>K2 - Identify the entities involved in the EU cyber ecosystem and their respective roles<br>K3 - Define the basic notions and concepts related to cyber security within EU<br>K4 - Identify the nature of the different cyber threats<br>K5 - Identify the challenges of cyber security at global level<br>K6 - Identify the international cyber space issues and their effect globally<br>K7- Identify the specific sectors for cooperation globally<br>K8 - Define the basic notions and concepts related to hybrid threats |
| | Skills | S1 - Classify the cyber issues according to complexity<br>S2 - Classify the impact of the cyber threats in the global stability<br>S3 - Categorize the cooperation opportunities with the EU cyber ecosystem and the global cyber environment |
| | Competences | C1 - Evaluate the potential impacts of cyber threats in the global environment<br>C2 - Create opportunities for synergies with the EU cyber ecosystem and the global cyber environment<br>C3 - Select the appropriate trust building measures to broaden cooperation in cyber |

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 sessions and practical activities as well as on the 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. At the end of the course, there is active observation by the course director/lead instructor and a feedback questionnaire is filled by the course participants.

**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** |
| The EU Cyber Ecosystem | 8 (4) | • Present the EU Agencies and bodies with cyber-related tasks |
| The EU Approach building resilience in cyberspace | 12 (4) | • Policies - Regulations Directives related with cyber within EU<br>  ○ EU Cybersecurity Strategy<br>  ○ Digital Single Market Strategy for Europe<br>  ○ Network and Information Security (NIS) Directive<br>  ○ Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU',<br>  ○ The Cyber Security Act<br>  ○ The General Data Protection Regulation<br>  ○ The EU Cyber Security Toolbox<br>  ○ The EU Coordinated Response to Large Scale Cybersecurity Incidents and Crises<br>• The Communication on the EU Strategic Approach to Resilience defines |
| The EU's External Cyber Capacity Building | 5 | • Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU',<br>  ○ The EU Cyber Security Toolbox<br>  ○ The EU Coordinated Response to Large Scale Cybersecurity Incidents and Crises |
| The EU Approach in the Hybrid threats | 2 | • The conceptual framework on hybrid threats and the interaction with cyber |
| Stability in the Global Environment | 4 | • Analysis of the impact of the cyber security in the global stability |
| **TOTAL** | **29 (8)** | |

| Materials | Additional information |
|---|---|
| *Essential eLearning:*<br>AKU 2 on European Global Strategy<br><br>*Reading material [examples]:*<br>• *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*<br>• *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)*<br>• *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*<br>• *The EU Cyber Diplomacy Toolbox (June 2017)*<br>• *The EU Cybersecurity Act ( June 2019)* | Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used.<br><br>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.<br><br>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*"**.** |