European Security and Defence College
Doc: ESDC/2020/78
Date: 17/03/2021
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity Number	**The EU's Cybersecurity Strategy for the Digital Decade**	ECTS
February 2023	*209*		**1**

Target audience	Aim
Participants should be officials dealing with aspects in the field of cyber security from Member States (MS), EU Institutions and Agencies. 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's Cybersecurity Strategy for the Digital Decade. The course will act as a kind of forum where entities coming from MS, EU Institution and Agencies will have the chance to interact with the participants and inform them on the current and future developments at strategic, tactical and operational levels regarding the EU's Cybersecurity Strategy. Furthermore, this course will allow the participants to exchange their views and share best practices on related topics of the Strategy by improving their knowledge, skills and competencies and better align with the overall objectives of the Strategy. By the end of this course the participants will be able to be more interoperable across the EU cyber ecosystem and to share some common views.

	Knowledge	K1. List the three principal instruments of the EU action namely regulatory, investment and policy K2. Identify the entities involved in the objectives of the Strategy and their respective roles at Strategic, Tactical and Operational levels K3. Define the basic notions and concepts used in the EU Cyber Security Strategy
	Skills	S1. Analyse and Classify the related impacts of Pillar 1 of the Strategy (resilience, technological sovereignty and leadership) S2. Analyse and Classify the related impacts of Pillar 2 of the Strategy (building operational capacity to prevent, deter and respond) S3. Analyse and Classify the related impacts of Pillar 2 of the Strategy (the global and open Cyberspace) S4. Integrate the objectives of the Strategy into the related plan of the cyber ecosystem
	Competences	C1. Evaluate the potential impacts of cyber threats in the implementation of the strategy at Strategic, Tactical and Operational levels C2. Transform the expected outcome into opportunities and create synergies with the EU cyber ecosystem for the further development of the Strategy at Strategic, Tactical and Operational levels C3. Select the appropriate trust building measures to broaden cooperation for the purposes of the Strategy within the internal and external environment of the EU

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**
Stability in the Global Environment and	4	• Analysis of the impact of the cyber security in the global stability
The EU's Cybersecurity Strategy for the Digital Decade.	3(1)	• The overall objective of the EU's Cybersecurity Strategy for the Digital Decade and the EU Cyber Ecosystem
Pillar 1 : Resilience, technological sovereignty and leadership	8	• Resilient infrastructure and critical service • Building a European Cyber Shield • An ultra-secure communication infrastructure • Securing the next generation of broadband mobile networks • An Internet of Secure Things • Greater global Internet security • A reinforced presence on the technology supply chain • A Cyber-skilled EU workforce
Pillar 2 : Building operational capacity to prevent, deter and respond	6	• CSIRTs community Tackling cybercrime • EU cyber diplomacy toolbox • Boosting cyber defence capabilities • A Joint Cyber Unit •
Pillar 3 : Advancing a global and open Cyberspace	4	• EU leadership on standards, norms and frameworks in cyberspace (standardisation, international security, crime (&human rights) • Cooperation with partners and the multi-stakeholder community • Strengthening global capacities to increase global resilience
The EU Approach in the Hybrid threats	4(2)	• The conceptual framework on hybrid threats and the interaction with cyber
TOTAL	**29 (3)**	

Materials

Essential eLearning:
AKU 2 on European Global Strategy
AKU 4,6 on Hybrid Threats

Reading material [examples]:

- *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)*
- *EU Security Union Strategy: connecting the dots in a new security ecosystem*
- *The EU's Cybersecurity Strategy for the Digital Decade.*

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*".