European Security and Defence College **Doc: ESDC/2023/35** **Date: 21/02/2023** **Origin:** ESDC Secretariat

Curriculum

To be reviewed by *February 2025*	Activity number *209*	**The EU's Cybersecurity Strategy for the Digital Decade**	ECTS **1**

Target audience	Aim
Participants should be officials dealing with aspects in the field of cybersecurity from Member States (MS) or EU institutions and agencies. Course participants must be available during the entire course and should be ready to participate based on 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 from MS and EU institutions and agencies will have the chance to interact with participants and inform them about current and future developments at strategic, tactical and operational levels regarding the EU's Cybersecurity Strategy. Furthermore, this course will allow participants to exchange their views and share best practices on topics related to the Strategy, improving their knowledge, skills and competencies and better aligning with the overall objectives of the Strategy. By the end of this course participants will be more interoperable across the EU cyber ecosystem.
Open to: • EU Member States and EU institutions	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Non-specialised cyber course, at awareness level* • *Linked with the strategic objectives of Pillar 1,2,3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning outcomes

Knowledge	LO01 - List the three principal instruments of EU action, namely regulatory, investment and policy LO02 - Identify the entities involved in the objectives of the EU Cybersecurity Strategy and their respective roles at strategic, tactical and operational levels LO03 - Define the basic concepts used in the Strategy
Skills	LO04 - Analyse and classify the impacts of Pillar 1 of the Strategy (resilience, technological sovereignty and leadership) LO05 - Analyse and classify the impacts of Pillar 2 of the Strategy (building operational capacity to prevent, deter and respond) LO06 - Analyse and classify the impacts of Pillar 3 of the Strategy (the global and open cyberspace) LO07 - Integrate the objectives of the Strategy into the related plan of the cyber ecosystem

Competences	LO08 - Evaluate the potential impacts of cyber threats in the implementation of the Strategy at strategic, tactical and operational levels LO09 - 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 LO10 - 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 in accordance with the Kirkpatrick model, with 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 to the residential module, including syndicate sessions and practical activities, as well as on the 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. There is active observation by the course director/lead instructor and a feedback questionnaire is filled in by participants at the end of the course.

However, no formal verification of learning outcomes is planned; the proposed ECTS is based on participants' workload only.

Course structure

The residential module is held over three days.

Main topic	Recommended working hours (of eLearning)	Content
1. Stability in the global environment	4	1.1 Analysis of the impact of cybersecurity on global stability
2. The EU's Cybersecurity Strategy for the Digital Decade	3(1)	2.1 The overall objective of the EU's Cybersecurity Strategy for the Digital Decade and the EU Cyber Ecosystem
3. Pillar 1: Resilience, technological sovereignty and leadership	8	3.1 Resilient infrastructure and critical service 3.2 Building a European Cyber Shield 3.3 An ultra-secure communication infrastructure 3.4 Securing the next generation of broadband mobile networks 3.5 An Internet of Secure Things 3.6 Greater global Internet security 3.7 A reinforced presence on the technology supply chain 3.8 A cyber-skilled EU workforce
4. Pillar 2: Building operational capacity to prevent, deter and respond	6	4.1 CSIRTs community 4.2 Tackling cybercrime 4.3 EU cyber diplomacy toolbox 4.4 Boosting cyber defence capabilities 4.5 A joint cyber unit
5. Pillar 3: Advancing a global and open cyberspace	4	5.1 EU leadership on standards, norms and frameworks in cyberspace (standardisation, international security, crime & human rights) 5.2 Cooperation with partners and the multi-stakeholder community 5.3 Strengthening global capacities to increase global resilience
6. The EU approach to hybrid threats	4(2)	6.1 The conceptual framework on hybrid threats and the interaction with cyber
TOTAL	**29(3)**	

Materials *Essential eLearning:* AKU 2 on the EU Global Strategy AKU 4, and AKU 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*	Methodology The course is based on the following methodology: lectures, panels, workshops, exercises Additional information

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*	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 supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular. The Chatham House rule is applied during the residential phase of the course: "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".