European Security and Defence College
Doc: ESDC/2024/041
Date: 21 Feb 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2026**	Activity number **202**	**Critical Infrastructures in the Context of Digitization**	ECTS **1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• Specialised cyber course, at technical and tactical levels • Linked with the strategic objectives of Pillar 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]

Target audience	Aim
Participants should be mid-ranking to senior officials, dealing with technical and operational aspects in the field of cyber security related to Critical Infrastructures, from EU MSs, EU Institutions and Agencies. Course participants must be available during the entire residential course and should be ready participate with their specific field of expertise and experience.	This course aims to enable participants to: • Understand the current context of the CIP strategies in the EU Cyber Ecosystem. • Analyse the impact of CIP at regional level, and apply CIP strategies in the context of continuous digitization, • Understand, evaluate and mitigate the cyber risks, threats and attack vectors against CI. • Move beyond classic CIP and apply new technologies in the new Cyber Ecosystem.
Open to: ▪ EU member States, Institutions and Agencies ▪ Candidate Countries	

Learning Outcomes

Knowledge	LO1. Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles LO2. Recognize the challenges of cyber security at a European level LO3. Define the basic notions and concepts related to Critical Infrastructures (CI) and associated operational technologies (OT) LO4. Summarize Strategies for Protecting CIs LO5. Identify the best practices and standards in protection of CI LO6. Identify the attack vectors on the protection CI LO7. Identify the new Threats to CI LO8. Identify mitigation approaches on the protection of CI LO9. Identify response and mitigation measures for Cyber-Attack against CI,
Skills	LO10. Analyse information on risk management at National and/or Regional level related with the protection of CI LO11. Classify the technical as well as organisational tools related to the protection of CI LO12. Classify the potential impacts of cyber threats in the protection of CI LO13. Classify the critical risks for information security management

	LO14. Classify attack vectors on the protection CI LO15. Classify the potential impacts of cyber threats in CI policies LO16. Apply concepts and techniques related to risk management to the CI protection
Responsibility and Autonomy	LO17. Assess the potential impact of cyber threats, incidents on CI LO18. Determine cyber countermeasures on CI LO19. Assess the impact of the attack vectors to CI LO20. Assess the potential impact of cyber threats and incidents on cyber policies and systems LO21. Determine cyber countermeasures on cyber policies and systems related to CI

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly 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 feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to accomplish all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award 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

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Content
1. Overview of Critical Infrastructure and Risk management in Critical infrastructures	12 (8)	1.1 EU institutions and Agencies involved in cyber security and cyber defence and their roles in CI 1.2 CI – norms and regulations (i.e NIS2 framework) 1.3 CI operational technologies 1.4 Process control systems 1.5 Physical protection systems 1.6 Ci interdependencies 1.7 Risk management process, Roles, responsibilities 1.8 Risk identification, assessment, and response strategies, plans, actions, 1.9 Risk Monitoring
2. Threat Analysis	9	2.1 Threat modelling 2.2 Attack trees 2.3 Incident response on malware 2.4 Regional / National impact in case of CI failures 2.5 Regional / National Response in case of Cyber Attack
3. Workgroup work	6	3.1 Targetting and compromise a CI 3.2 Identification of cyber threat actors 3.3 Analysis of the cyber threats 3.4 Threat assessment and Hybrid threats 3.5 Attack tree development and analysis 3.6 National / Regional Response for Cyber-attack against CI
TOTAL	**27(8)**	

Materials

Required:

- AKU 55 - Strategic Compass
- AKU 104b Information Security Management Implementation Course

Recommended:

- Council Conclusion on EU Policy on Cyber Defence (22.05.2023)
- EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022)
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS 2)
- COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
- EU's Cybersecurity Strategy for the Digital Decade (December 2020)
- The EU Cybersecurity Act (June 2019)
- The EU Cyber Diplomacy Toolbox (June 2017)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic form 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. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

The Chatham House Rule is applied during all residential modules 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".