EUROPEAN SECURITY AND DEFENCE COLLEGE
COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE

European Security and Defence College
Doc: ESDC/2022/067
Date: 1 April 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Critical Infrastructure Protection Advanced Course	ECTS
Feb. 2024	208b		1

Target audience

Participants should be mid to senior level representatives of public authorities, diplomats, or CI owners/operators with responsibilities for the development and implementation of security strategies, policies and mechanisms for Critical Infrastructure Protection. Governmental and private companies involved in CI operation should participate.

Open to:

- EU Member States / EU Institutions Bodies and Agencies,

Aim

This course aims to enable participants to:

- systematizes knowledge in four specific critical infrastructure fields that are, nevertheless, inter-related
- increase the interaction between participants and experts through an engaging table top exercise (TTX)
- train the strategic foresight in the CIP and resilience planning activities, with a focus on trans border and European dimension
- develop a multidisciplinary view of CIP and the interdependencies that lead to an unpredictable and complex security environment, as well as a better understanding of the toolbox and conceptual framework which decision makers utilise to perform complex system governance in a multi-stakeholder setting.

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 and Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes

Knowledge	LO1 - Describe the CI interdependencies in emerging areas of CIP focus and global dimensions; LO2 - Match and apply the Critical Infrastructure Protection framework regulations at European level; LO3 – Tackle with the new realities of the complex security environment; LO4 - Classify the emerging trends producing new risks, vulnerabilities and threats; LO5 – Apply the perspectives of Complex Systems Governance; LO6 - Outline the available instruments tools and regulations in the CIP practitioners and policymakers toolbox;
Skills	LO7 - Classify technical, organizational and trans border coordination challenges related to CIP; LO8 – Analyse the potential systemic impact of European and global integration on CIP governance efforts; LO9 – Categorise the impact of new technologies (such as trusted AI) and new priorities (such as climate change) on public policy related to CIP; LO10 – Analyse and classify the challenges for policymakers, regulators and CIP practitioners stemming from the changing security environment

Responsibility and Autonomy	LO11 – Evaluate the impact of new technologies and other trends on CI system-of-systems risks; LO12 – Develop a systemic and complex understanding of the security environment, grounded in the CIP framework and its latest developments LO13 – Systematize complex systems from a CIP perspective in order to address security issues utilizing the CIP framework LO14 - Design a systemic and complex model of the security environment, grounded in the CIP framework and its latest developments.

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 module is held over 3 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
Critical Infrastructure Protection Theory	5(4)	Recapping the main elements of CIP theory; Elements of system-of-systems dynamics; Ancillary considerations – law, regulation, education; New tools and conceptual frameworks for CIP.
Key Dimensions of CIP	5(4)	Critical Energy Infrastructures and related subdomains; Critical Transport Infrastructures and related subdomains; Critical Cyber Infrastructures and related subdomains; Critical Space Infrastructures and related subdomains; Other Critical domains and their Crosscutting issues – sectoral, geographic, global.
Elements and practice of CIP Governance	6(4)	National CIP governance frameworks – theory and practice; The European framework for CIP, pre- and post- December 2020; Civil-military cooperation; NATO-EU cooperation dimensions The underlying security environment for CIP; Analysis of facts of security environment; Trends in risks, vulnerabilities and threats; Hybrid threats as an encompassing framework for multi-tier, multi-pronged destabilization; Evolutions in the legislative and administrative framework for CIP.
Practical Task	6	Table Top Exercise
TOTAL	22 (12)	16 hours residential or synchronous learning + 12 hours eLearning asynchronous sessions (e-earning modules and pre-recorded sessions)

Materials	Methodology
Essential eLearning: • AKU 2 on European Global Strategy • AKU 107 – Awareness course on CyberDiplomacy Supplementary materials: • AKU 106a, b, c, d, e – Hybrid threats modules Pre-requisites: • To follow the CIP basic course, or • to prove their basic knowledge in this domain, or • to work into a related CIP position *Reading material:* - EU Directives, Council Decisions, Council conclusions, Regulations, Joint declarations; - Documents and assessments of the security environment from EU and non-EU, Think Tanks; - The course documentation prepared by the organizers.	The course is based on the following methodology: lectures, panels, workshops, exercises **Additional information** 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. The Chatham House Rule is applied during all 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".