European Security and Defence College
Doc: ESDC/2022/ 066
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Critical Infrastructure Protection Basic Course	ECTS 1
Feb. 2024	208a		EAB.CYBER N/A

Target audience	Aim
Participants should be junior to mid level representatives of public authorities 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,	This course aims to enable participants to: • Give an overview of the evolving nature of Critical Infrastructure Protection efforts • Enable a strategic foresight in the CIP and resilience planning activities at the level of the various competent regulatory or coordinating authorities or owners/operators of Critical Infrastructures. • Present the latest research in the CIP field and have a clear view of the systemic transformations underway from National to European and Global levels, leading to new risks, vulnerabilities and threats. • Present the basics of integration of technologies such as AI, Blockchain and the achievement of new scales in data acquisition or processing • Introduce the developments in the toolbox available to CIP practitioners and policymakers for understanding and addressing CIP risks.

Learning Outcomes

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

Knowledge	L01 - Outline the CI interdependencies an emerging areas of CIP focus; L02 - Recognize the facets and attributes of resilience as it pertains to complex systems; L03 - Recognize the new realities of the complex security environment; L04 - Describe the emerging trends producing new risks, vulnerabilities and threats; L05 - Identify the new perspectives of Complex Systems Governance; L06 - Recognize the impact of new technologies on the organization of the Critical Infrastructure system-of-systems, but also on the toolbox available to CIP practitioners and policymakers;
Skills	L07 - Identify technical as well as organisational challenges related to CIP; L08 - Classify the potential systemic impact of the adoption of new technologies on specific CI components; L09 - Analyse the impact of various transformations on public policy related to CIP; L10 - Identify the challenges for policymakers, regulators and CIP practitioners stemming from the changing security environment.
Responsibility and Autonomy	L11 - Evaluate the potential impact of new technologies and other trends on CI system-of-systems risks; L12 - Assess the challenges to CIP efforts at National and European levels moving forward given the new security environment; L13 - 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. It is a non-specialised course, at awareness level, link with the Pillar 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020). Furthermore the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase)

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
Critical Infrastructure Protection Theory	4(4)	Introduction to Critical Infrastructure Protection, overall framework; Transborder Critical Infrastructures, Networks and interdependencies; Resilience and Complex System Governance theory. Policy options for the EU and other EU decision makers;
Emerging Technologies and CIP impact	4(2)	Overview of emerging technologies Systemic Resilience Complexity; Decision Support Systems and Risk Forecast; Impact of new technologies in CI and Serious Gaming. Transformations in the security environment;
New Dimensions of CIP	4(3)	Critical Infrastructures Initiatives and Projects; Critical Infrastructures and Climate Change. Regional and Global Integration Initiatives – impact on CIP and on the security environment. Critical Infrastructure Diplomacy;
CIP Governance	4(3)	CIP Governance models (National, EU and international level), Tools for CI practitioners and policymakers; Geopolitics of CI transformations; Resilience and Defence; Impact of Hybrid Threats on CIs; Civil-Military Cooperation in Critical Infrastructure Protection; Decision making under conditions of uncertainty. Managing change at the level of society and of organizations
TOTAL	16(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 first module of this course • If not followed the first module, to prove their basic knowledge in this domain *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. 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 courses 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*".