European Security and Defence College
Doc: ESDC/2022/059
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Critical Infrastructures in the Context Of Digitization**	ECTS **1**
Feb. 2024	**202**		EAB.CYBER **N/A**

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 / ▪ EU Institutions and Agencies	

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 - Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles, L02 - Recognize the challenges of cyber security at a European level, L03 - Define the basic notions and concepts related to Critical Infrastructures (CI) and associated operational technologies (OT), L04 - Summarize Strategies for Protecting CIs, L05 - Identify the best practices and standards in protection of CI, L06 - Identify the attack vectors on the protection CI, L07 - Identify the new Threats to CI, L08 - Identify mitigation approaches on the protection of CI, L09 - Identify response and mitigation measures for Cyber-Attack against CI,

Skills	L10 - Analyse information on risk management at National and/or Regional level related with the protection of CI L11 - Classify the technical as well as organisational tools related to the protection of CI L12 - Classify the potential impacts of cyber threats in the protection of CI L13 - Classify the critical risks for information security management L14 - Classify attack vectors on the protection CI L15 - Classify the potential impacts of cyber threats in CI policies L16 - Apply concepts and techniques related to risk management to the CI protection
Responsibility and Autonomy	L17 - Assess the potential impact of cyber threats, incidents on CI L18 - Determine cyber countermeasures on CI L19 - Assess the impact of the attack vectors to CI L20 - Assess the potential impact of cyber threats and incidents on cyber policies and systems L21 - 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: 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 residential module is held over 3 days. It is a specialised course, at technical and tactical levels, 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
1. Overview of Critical Infrastructure and Risk management in Critical infrastructures	12 (8)	1.1 EU institutions and Agencies involved in cyber security and their roles in CI 1.2 CI – norms and regulations 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	Methodology
Required: AKU 2 on European Global Strategy AKU 104b Information Security Management Implementation Course **Recommended:** • Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016) European Parliament: Directive on security of network and information systems by the European Parliament (2016)	The course is based on the following methodology: lectures, panels, workshops, Labs **Additional information** The Chatham House Rule is applied during all residential modules of the HLC: "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". The mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).