European Security and Defence College
Doc: ESDC/2020/037
Date: 14/02/2020
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity Number	**Critical Infrastructures in the Context Of Digitization**	ECTS
February 2022	*202*		**1**

Target audience	Aim
Participants should be mid-ranking to senior officials. dealing with technical and tactical aspects in the field of cyber security related to Critical Infrastructures, from EU MSs, relevant EU Institutions and Agencies. They should have a clear background related to the technical and tactical aspects of cybersecurity and critical infrastructures. 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.

Learning outcomes	Knowledge	K1 - Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles, K2 - Recognize the challenges of cyber security at a European level, K3 - Define the basic notions and concepts related to Critical Infrastructures (CI), K4 - Summarize Strategies for Protecting CIs, K5 - Identify the best practices and standards in protection of CI, K6 - Identify the attack vectors on the protection CI, K7 - Identify the new Threats to CI, K8 - Identify mitigation approaches on the protection of CI, K9 - Identify response and mitigation measures for Cyber-Attack against CI,
	Skills	S1 - Analyse information on risk management at National and/or Regional level related with the protection of CI S2 - Classify the technical as well as organisational tools related to the protection of CI S3 - Classify the potential impacts of cyber threats in the protection of CI S4 - Classify the critical risks for information security management S5 - Classify attack vectors on the protection CI S6 - Classify the potential impacts of cyber threats in CI policies S7 - Apply concepts and techniques related to risk management to the CI protection
	Compe-tences	C1 - Assess the potential impact of cyber threats, incidents on CI C2 - Determine cyber countermeasures on CI C3 - Assess the impact of the attack vectors to CI C4 - Assess the potential impact of cyber threats and incidents on cyber policies and systems C5 - 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 participant's satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on the active contribution in the residential Module, including their syndicate sessions and practical activities as well as on the completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. At the end of the course, there is active observation by the course director/lead instructor and a feedback questionnaire is filled by the course participants.

However, no formal verification of learning outcome is foreseen; proposed ECTS is based on participants' workload only

Course Structure		
Main Topic	**Recommended Working Hours (of that eLearning)**	**Contents**
Overview of Critical Infrastructure Risk management in Critical infrastructures	12 (8)	• EU institutions and Agencies involved in cyber security and their roles in CI • CI – norms and regulations • CI operational technologies • Process control systems • Physical protection systems • Ci interdependencies • Risk management process, Roles, responsibilities • Risk identification, assessment, and response strategies, plans, actions, • Risk Monitoring
Threat Analysis	9	• Threat modelling • Attack trees • Incident response on malware • Regional / National impact in case of CI failures • Regional / National Response in case of Cyber Attack
Workgroup work	6	• Target and compromise a CI • Identification of cyber threat actors • Analysis of the cyber threats • Threat assessment and Hybrid threats • Attack tree • National / Regional Response for Cyber-attack against CI
TOTAL	**27 (8)**	

Materials

Essential eLearning:
AKU 2 on European Global Strategy
AKU 104b Information Security Management Implementation Course

Reading material [examples]:
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)

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 HLC 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*"**.**