European Security and Defence College
Doc: ESDC/2024/049
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2026**	Activity number **208b**	**Critical Entities Resilience Advanced Course**	ECTS **1**

Target audience	Aim
Participants should be mid- to high- level representatives of public authorities, Critical Entities or CI owners/operators (private and state) (Critical Entities) with responsibilities for the development and implementation of security strategies, policies and mechanisms for Critical Entities Resilience. EU Member States, Governmental and private companies involved in CER or CI operation are invited to participate. Open to: - EU Member States / EU institutions, bodies and agencies	This course aims to enable participants to: • systematise knowledge in specific critical entities resilience fields, interdependencies and dynamics; bolstering the interconnectivity and cross-border nature of their operations • enhance the interaction between participants and experts through an engaging table top exercise (TTX) • train the strategic foresight in the CER and resilience planning activities, with a focus on cross-border and European dimension • develop a multidisciplinary view of CER 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 use to perform complex system governance in a multi-stakeholder setting.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised cyber course at strategic 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 CER focus, national, European and global dimensions; LO2 - Describe the Critical Entities Resilience framework regulations at European level; LO3 – Identify challenges of the complex security environment; LO4 - Identify emerging trends producing new risks, vulnerabilities and threats; LO5 – Explain the perspectives of Complex Systems Governance; LO6 - Outline the available instruments tools and regulations in the CER practitioners and policymakers toolbox;
Skills	LO7 - Classify technical, organisational and trans border coordination challenges related to CER; LO8 – Analyse the potential systemic impact of European and global integration on CER governance efforts; LO9 – Categorise the impact of new technologies (such as trusted AI) and new challenges (such as climate change) on public policy related to CER; LO10 – Analyse and classify the challenges for policymakers, regulators and CER practitioners stemming from the changing security environment; LO11 – Evaluate the impact of new technologies and other trends on CI system-of-systems risks;

Responsibility and Autonomy	LO12 – Develop a systemic and complex understanding of the security environment, grounded in the CER framework and its latest developments; LO13 – Systematise complex systems from a CER perspective in order to address security issues utilizing the CER framework; LO14 - Design a systemic and complex model of the security environment, grounded in the CER framework and its latest developments; LO15- Share knowledge on the factors that contribute to the resilience of critical entities; LO16 - Exchange best practices with regard to the transposition of CER directive into national laws.

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 fulfil 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

The module is held over 5 days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Critical Infrastructure Protection Theory	7(4)	1.1 Recapping the main elements of CER theory and framework; 1.2 Elements of system-of-systems dynamics; 1.3 Ancillary considerations – law, regulation, education; 1.4 New tools and conceptual frameworks for CER. 1.5 Traditional measures and modern technologies, legislative use of such technologies
2. Key Dimensions of CIP/CER	7(4)	2.1 Critical Energy Infrastructures and related subdomains; 2.2 Critical Transport Infrastructures and related subdomains; 2.3 Critical Cyber Infrastructures and related subdomains; 2.4 Critical Space Infrastructures and related subdomains; 2.5 Other Critical domains and their Crosscutting issues – sectoral, geographic, global.
3. Elements and practice of CER/CI Governance	10(4)	3.1 National CER/CI governance frameworks – theory and practice; 3.2 The European framework for CIP, pre- and post- December 2020; 3.3 Civil-military cooperation; 3.4 NATO-EU cooperation dimensions 3.5 The underlying security environment for CER; 3.6 Analysis of facts of security environment; 3.7 Trends in risks, vulnerabilities and threats; 3.8 Risk assessment; 3.10 Hybrid threats as an encompassing framework for multi-tier, multi-pronged destabilization; 3.11 Evolutions in the legislative and administrative framework for CER.
4. Practical Task	10	4.1 Table Top Exercise 4.2 Critical Infrastructure/Entity Field Visit.
TOTAL	34 (12)	

Materials

Required:

- AKU 2 European Global Strategy
- AKU 107 Awareness course on CyberDiplomacy
- AKU 106– Hybrid threats modules
- Directive (EU) 2022/2557 on the resilience of critical entities (CER)
- AKU 55 - Strategic Compass

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)
- 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.

Pre-requisites:

- To follow the CIP basic course, or to prove knowledge in this domain, or to work into a related CER position

Methodology

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

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".