European Security and Defence College
Doc: ESDC/2024/048
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

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

Target audience	Aim
Participants should be mid to senior 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/ CI operation are invited to participate.	This course aims to enable participants to: • give an overview of the evolving nature of Critical Entities Resilience efforts and interdependencies. • enable a strategic foresight in the CER 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 CER 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 the integration of technologies such as AI and Blockchain and the achievement of new scales in data acquisition or processing • introduce developments in the toolbox available to CER practitioners and policymakers for understanding and addressing CER risks.
Open to: - EU Member States / EU institutions, bodies and agencies	

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	LO0 – Outline Critical Entities Resilience framework regulations at European level; LO1 - Outline critical infrastructure and sectors' interdependencies as well the emerging areas for CER focus; LO2 - Recognise the factors, elements and attributes of resilience as it pertains to complex systems; LO3 - Recognise the new realities of the complex security environment, considering the security, safety and cyber perspectives; LO4 - Describe the emerging trends producing new risks, vulnerabilities and threats; LO5 - Identify the new perspectives of Complex Systems Governance; LO6 - Recognise the impact of new technologies on the organization of the Critical Infrastructure system-of-systems, but also on the toolbox available to CER practitioners and policymakers;
Skills	LO7 - Recognise technical and organisational challenges related to CER; LO8 - Analyse the potential systemic impact of the adoption of new technologies on specific CI components; LO9 - Analyse the impact of various transformations on public policy related to CER; LO10 – Analyse/ identify key challenges for policymakers, regulators and CER practitioners stemming from the changing security environment;

Responsibility and Autonomy	LO11 - Evaluate the impact of new technologies and other trends on CE system-of-systems risks; LO12 - Assess the challenges ahead for CER efforts at national and European levels given the new security environment; LO13 - Outline a systemic and complex model of the security environment, grounded in the CIP framework and its latest developments. LO15- Recognize the factors that contribute to the resilience of critical entities. LO16 - Propose measures to enhance cooperation between the public sector, on the one hand, and the private sector and public and private entities, on the other.

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 feedback is given in the level 1 evaluation on 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 3 days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Critical Infrastructure Protection/ Critical Entities Resilience Theory	4(4)	1.1 Introduction to Critical Entities Resilience, overall framework; 1.2 Policy options for the EU and other EU decision makers; 1.3 Trans-border Critical Infrastructures, Networks and interdependencies; 1.4 Resilience and Complex System Governance theory;
2. Emerging Technologies and CER/CIP impact	4(2)	2.1 Overview of emerging technologies; 2.2 Systemic Resilience Complexity; 2.3 Decision Support Systems and Risk Forecast; 2.4 Impact of new technologies in CE and Serious Gaming; 2.5 Transformations in the security environment;
3. New Dimensions of CER/CIP	4(3)	3.1 Critical Infrastructures Initiatives and Projects; 3.2 Critical Infrastructures and Climate Change; 3.3 Regional and Global Integration Initiatives – impact on CER and on the security environment; 3.4 Critical Infrastructure Diplomacy;
4. CER/CIP Governance	7(3)	4.1 CER Governance models (National, EU and international levels); 4.2 Tools for CER practitioners and policymakers; 4.2 Geopolitics of CER transformations; 4.2 Resilience and Defence; 4.2 Impact of Hybrid Threats on CER/CI 4.2 Civil-Military Cooperation in Critical Infrastructure Protection; 4.2 Decision making under conditions of uncertainty; 4.2 Business Continuity and Disaster Recovery; 4.2 Managing change at the level of society and of organizations; 4.2 Critical Infrastructure/Entity Field Visit.
TOTAL	19(12)	

Materials	Methodology
Required: • AKU 2 European Global Strategy • AKU 107 Awareness course on Cyber Diplomacy • 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)	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".