European Security and Defence College
Doc: ESDC/2024/056
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number		ECTS
Feb. 2026	**275**	**Cybersecurity and Smart Cities**	**1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised cyber course, at tactical/technical/strategic levels* • *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)]*

Target audience	Aim
Municipal staff and civil servants working for the national government at local agencies. All the engaged staff participate in smart city planning and smart service delivery in the urban space, while they are exposed to several types of threats. Priority is given to participants from EU Member States. However non-EU citizens as well as NATO staff are welcome.	This course aim to teach the engage audience about cyber security and IoT cyber security at a city level, especially in the smart city context, where several interventions are driven by local governments and stakeholders, which transform typical urban and business activities (e.g. mobility, transaction, supply chain, production etc.).
Open to: ▪ EU Member States / EU Institutions Bodies and Agencies	

Learning Outcomes	
Knowledge	LO1-Recognize smart facilities and smart services in the city LO2- Recognize the nature of the different cyber threats we are exposed in a city LO3- Define the basic notions and concepts related to cybersecurity and cyber defence LO4- Identify the local stakeholders that deal with cybersecurity and cyber defence LO5- Identify the EU institutions and agencies involved in cybersecurity and cyber defence and their respective roles LO6- Reflect the emerging trends in cyber threats LO7- Address international cyber space issues and cyber diplomacy LO8- Outline models and frameworks that asses cyber security LO9- Assess how much an individual has protected his own facilities

Skills	LO10 – Identify technical, personal and organizational tools related to cyber security LO11- Evaluate the protection level of an individual or an organization in the city context LO12- Outline the potential impacts of cyber threats for smart city growth LO13- Identify challenges for a local government to raise community awareness on cyber security in daily activities LO14- Describe the collaboration framework between stakeholders in a city to recover from cyber attacks
Responsibility and Autonomy	LO15 – Assess the safety level of an individual or an organization LO16- Outline the process that a city has to follow in order to enhance cyber security and resilience from cyber attacks LO17- Apply safety frameworks at an individual level

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 accomplish 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 residential module is held over 3 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Smart city: infrastructure and services	8(5)	1.1 Smart city terminology; stakeholders; strategic frameworks; architectures; standards for smart city development; trends and monitoring systems
2. Cyber security at a city level	7(3)	2.1 Smart city standards for cybersecurity; IoT and cyber security; smart service deployment and cybersecurity; resilience of smart infrastructure and services; exemplars
3. Cyber security and cyber defence	3	3.1 Cybersecurity / cyber defence needs of the EU and CSDP 3.2 Protection of critical infrastructure against cyber-attacks 3.4 Assessment of the EU's progress in cybersecurity and outlook 3.4 EU cyber defence policy framework 3.5 EU NIS 2 Directive 3.6 EU cybersecurity capacities
4. Monitoring, Mentoring & Advising	4(2)	4.1 Monitoring, mentoring and advising local stakeholders · Principles for individual and local cyber protection and resilience
5. Cyber war and cyber crime	3	5.1 Legal framework for cyber operations 5.2 UN Charter and international law in cyberspace

		5.3 Promoting the Budapest Convention 5.4 Cyber regulation in the EU and local best practices 5.5 Digital combat in the conduct of daily operations; specificity of incidence of digitisation and robotisation of typical business and urban processes 5.6 Cybersecurity and cross-domain warfare 5.7 Cybersecurity and supply chain management 5.7 Cyber-attack simulation
6. Urban policy making and community awareness	3	6.1 Raising awareness at a local level 6.2 Participation and collaboration 6.3 Resilience plans for cyber-attack response and recovery 6.4 Planning with responsibility against cyber threats
TOTAL	**28(10)**	

<u>Materials</u>

Required:

- AKU 55 – Strategic Compass
- AKU 01 - History and Context of ESDP/CSDP Development
- AKU 107 Awareness course on Cyber Diplomacy

Recommended:

- European standards for cybersecurity; ITU recommendations for Smart City and Cybersecurity; ISO/IEC CD TS 27570.2: Information Technology Security Techniques
- Privacy guidelines for Smart Cities
- 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)
- Council conclusions on Strengthening Europe's Cyber

<u>Methodology</u>

The course is based on the following methodology: lectures, panels, workshops, exercises, labs

<u>Additional information</u>

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".

Resilience System and Fostering a Competitive and Innovative • AKU104- 10 modules from ENISA • AKU106- Hybrid modules • AKU 02 - European Union Global Strategy • AKU 03 - Role of EU Institutions in the field of CFSP/ CSDP • Cybersecurity Industry (November 2016) • European Parliament: Directive on security of network and information systems (2016)	