EUROPEAN SECURITY AND DEFENCE COLLEGE
COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE

European Security and Defence College
Doc: ESDC/2024/051
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Open Source Intelligence (OSINT)	ECTS
Feb. 2026	**261**		**2**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Support ECSF Role 4. Cyber Threat Intelligence* • *Specialized cyber course, at technical and tactical – operational – strategic levels* • *Linked with strategic objectives of Pilar 1 and Pilar 2 of the Eu's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Target audience

Participants should be officials dealing with aspects in the field of intelligence, security and cyber security from Member States (MS), EU Institutions and Agencies.

Course participants must be available during the entire course and should be ready participate with their specific field of expertise and experience.

Open to:

- EU Member States / EU Institutions Bodies and Agencies

Aim

This course is intended to strengthen the establishment of the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC and widen the scope of its activities by addressing basic technical and strategic/operational-level training in OSINT discipline. This course aims to provide knowledge, skills and competencies via structured methods of collecting information from Open Sources, lab exercises and practise in various scenarios.
In addition, the course aims to provide a forum for the exchange of knowledge and best practices among «OSINT Operators» and allow the participants to exchange their views and share best practices on related topics of OSINT.

By the end of this course the participants will be able to be more effective in Intelligence collection from open sources with the use of structured analytic techniques and create more accurate estimations in order to fulfil an intelligence question.

Learning Outcomes	
Knowledge	LO1- List the principles of OSINT LO2- Define the basic types of OSINT Sources LO3- Define the basic notions and concepts used in the EU Cyber Security Strategy LO4- Explain webpage evaluation criteria LO5- Identify the entities involved in the EU Intelligence Frame LO6- Explain Cognitive Biases that affect Collection from Open Sources LO7- Explain how Thinking and Memory works

	LO8- Explain how the Internet works
Skills	LO9- Describe the basics about computer networks LO10- Use various search engines LO11-Use BOOLEAN operators LO12-Use Google advance search operators LO13-Use various OSINT tools
Responsibility and Autonomy	LO14- Take advantage of opportunities to collect information from Open Sources LO15- Select the most appropriate method to collect information form open sources LO16- Use a structure approach to answer an intelligence question

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 5 days

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Introduction to OSINT	7(2)	• OSINT Principles-Definitions • EU Intelligence Agencies • OSINT by level of Command • OSINT Sources • Sources Evaluation
2. Computer Networks and the Internet	7(1)	• Computer Networks • The Internet • Deep Web • Site Framework • IP Tools
3. Search Engines	12(1)	• Google Dorking • Custom Search Engine • IOT Search Engines • Metasearch Engines
4. OSINT Collection	10(1)	• Social Media (Exploitation) • Multimedia Tools • OSINT Advanced Tools • Metadata Tools

5. Structured Approach to OSINT Collection	10	• Introduction to Thinking • Human Memory • Mind Sets • Cognitive Biases • Critical-Creative Thinking • Critical Reading • Problem Decomposition • Structured Analytic Techniques • Query Lists
6. Delivering the OSINT collectables	2	• Email Services / Email Security • Creating an OSINT report
7. Major Exercise	18	• Work Teams in research of information from Open Sources, based on a real case scenario
8. Presentation of OSINT products	3	• Work Teams in research of information from Open Sources, based on a real case scenario
9. Course Review	1	• Course evaluation form
TOTAL	**70(5)**	

Materials

Required:
AKU on OSINT

Recommended:
- Council Decision (2001/80/CFSP) on the Establishment of the EUMS
- HR Decision 013 on the Establishment of an ISA
- OSINT Training Guide by HNDGS
- AKU 2: European Global Strategy
- AKU 55 - Strategic Compass
- 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)

Methodology

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

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. 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 phase 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".

• The EU Cyber Diplomacy Toolbox (June 2017)	