European Security and Defence College Doc: ESDC/2022/072
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Open Source Intelligence (OSINT)**	ECTS **2**
Feb. 2024	**261**		EAB.CYBER **N/A**

Target audience	Aim
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.	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 tactical/operational-level training in OSINT discipline. This course aim to provide a forum for the exchange of knowledge and best practices among «OSINT operators» by improving their knowledge, skills and competencies via lab exercises. Furthermore, this course will allow the participants to exchange their views and share best practices on related topics of OSINT by improving their knowledge, skills and competencies and better align with the overall objectives of CSDP. By the end of this course the participants will be able to be more effective in Intelligence Collection from Open Sources and to share some common views.
Open to: ▪ EU Member States / EU Institutions Bodies and Agencies	

Learning Outcomes

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

Knowledge	L01- List the principles of OSINT L02- Define the basic types of OSINT Sources L03- Define the basic notions and concepts used in the EU Cyber Security Strategy L04- Explain webpage evaluation criteria L05- Identify the entities involved in the EU Intelligence Frame L06- Explain Cognitive Biases that affect Collection from Open Sources L07- Explain how Thinking and Memory works L08- Explain how the Internet works

Skills	L09- Describe the basics about computer networks L10- Use various search engines L11- Use BOOLEAN operators L12- Use Google advance search operators L13- Use various OSINT tools
Responsibility and Autonomy	L14- Take advantage of opportunities to collect information from Open Sources L15- Select the most appropriate method to collect information form open sources L06- Use a structure approach to answer an intelligence requirement L17- Create a structured report to present the collection results

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 3 days. It is a specialised course, at technical and tactical levels, link with the Pillars 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020).

Furthermore the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase).

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Introduction to OSINT	9(2)	1.1 OSINT Principles-Definitions 1.2 EU Intelligence Agencies 1.3 OSINT by level of Command 1.4 OSINT Sources 1.5 Sources Evaluation
2. Computer Networks and the Internet	10(1)	2.1 Computer Networks 2.2 The Internet 2.3 Deep Web 2.4 Site Framework 2.5 IP Tools
3. Search Engines	5	3.1 Use of various search engines 3.2 Google Operators 3.3 BOOLEAN Operators

		3.4 Internet of Things
4. OSINT Collection	11	1.1 Social Media 1.2 Multimedia Tools 1.3 OSINT Tools 1.4 Metadata Tools - Deep Web tools
5. Structured Approach to OSINT Collection	13	5.1 Introduction to Thinking 5.2 How memory works 5.3 Mind Sets 5.4 Cognitive Biases 5.5 Critical-Creative Thinking 5.6 Critical Reading 5.7 Problem Decomposition 5.8 Structured Analytic Techniques 5.9 Query Lists
6. Delivering the OSINT collectables	2	6.1 Email Services / Email Security 6.2 Creating an OSINT report
7. Major Exercise	18	7.1 Work Teams in research of information from Open Sources, based on a real case scenario
TOTAL	**68 (3)**	

Materials	Methodology
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*	The course is based on the following methodology: lectures, workshops, exercises, labs Additional information The Chatham House Rule is applied during all residential modules of the HLC: "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 mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).