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

**European Security and Defence College**
**Doc: ESDC/2022/075**
**Date: 1 April 2022**
**Origin:** ESDC Secretariat

# Curriculum

| To be reviewed by | Activity number | **Basic Analysis Course (BAC)** | ECTS |
|---|---|---|---|
| **Feb. 2024** | **268** | | **2** |

| 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.<br><br>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 operational/strategic-level training in Intelligence Analysis discipline.<br><br>This course aim to provide a forum for the exchange of knowledge and best practices among «All Source Analysts» by improving their knowledge, skills and competencies via structured methods of intelligence analysis and lab exercises.<br><br>Furthermore, this course will allow the participants to exchange their views and share best practices on related topics of Analysis by improving their knowledge, skills and competencies and better align with the overall objectives of CSDP.<br><br>By the end of this course the participants will be able to be more effective in Intelligence Analysis with the use of structured analytic techniques in order to create more accurate estimations. |
| Open to:<br>▪ EU Member States / EU Institutions Bodies and Agencies | |

| CORRELATION WITH CTG / MTG TRAs | EQUIVALENCES |
|---|---|
| CTG / MTG TRA on Cyber | • *Specialised cyber course, at technical and tactical levels*<br>• *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- Define the basic notions and concepts used in the EU Cyber Security Strategy<br>LO2- Identify the entities involved in the EU Intelligence Frame<br>LO3- Explain Cognitive Biases that affect Intelligence Analysis<br>LO4- Explain how Thinking and Memory works |

| | |
|---|---|
| **Skills** | LO5- Use Argumentation and Reasoning in Analysis<br>LO6- Use various structured analytic techniques<br>LO7- Create Scenarios and Indicators |
| **Responsibility and Autonomy** | LO8- Take advantage of collected information from various sources<br>LO9- Select the most accurate and appropriate information<br>LO10- Use a structure approach to answer an intelligence requirement<br>LO11- Create a structured report to present the collection results<br>LO12- Create a formal report to present the results of analysis |

## 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.*

| Main Topic | Suggested Working Hours (required for individual learning) | Suggested Contents |
|---|---|---|
| 1. Introduction to Analysis | 9(2) | 1.1 Analysis Principles-Definitions<br>1.2 EU – National Intelligence Agencies |
| 2. Mental Mechanism | 10(1) | 2.1 Introduction to Thinking<br>2.2 Mind Sets<br>2.3 Critical Thinking<br>2.4 Creative Thinking<br>2.5 Cognitive Biases<br>2.6 Aristotle's Rhetoric |
| 3. Structured Analytic Techniques | 5 | 3.1 Define the problem-Decomposition<br>3.2 Idea Generation-Visualization<br>3.3 Diagnostic Techniques<br>3.4 Foresight Techniques<br>3.5 Challenge Analysis<br>3.6 Support Decision |
| 4. Delivering Results | 11 | 4.1 Creating a formal Analysis Report |

| | | |
|---|---|---|
| 5. Practise | 13 | 5.1 Practise in Structured Analytic Techniques |
| 6. Major Exercise | 2 | 6.1 Work Teams in production of an Analysis Product based on a real case scenario |
| **TOTAL** | **68 (2)** | |

| Materials | Methodology |
|---|---|
| **Required:**<br>AKU on OSINT<br><br>**Recommended:**<br>• *Council Decision (2001/80/CFSP) on the Establishment of the EUMS*<br>• *HR Decision 013 on the Establishment of an ISA*<br>• *Intelligence-Counterintelligence and Analysis Training Guide by HNDGS* | The course is based on the following methodology: lectures, workshops, exercises, labs<br><br>Additional information<br><br>Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used.<br><br>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.<br><br>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". |