European Security and Defence College
Doc: ESDC/2024/034
Date: November 19-22.2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number		ECTS
February 2026	**76**	***Foreign Information Manipulation and Interference***	**2**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
No correlation	No equivalence.

Target audience

Participants should be mid-level professionals in MSs institutions involved in the implementation of prevention and countering disinformation and cyber security threats (ministries of foreign affairs, defence, intelligence, internal affairs). Practitioners with expert knowledge in the authorities of the MSs and from related EU Institutions and Agencies could be as well invited to join the course. Depending of the design of the course, senior decision makers could join the training, especially when the experts with field experience are invited to contribute with their expertise.

Open to:

- EU member States / Institutions
- International Organisations

Aim

Foreign Information Manipulation and Interference aims to provide an enhanced learning environment fostering the understanding and managing of current manipulation of information (hereby referred to as FIMI) and its underlying cybersecurity elements. It combines the best practices from both the counter-FIMI and the cybersecurity communities in order to expose the FIMI/disinformation creation and dissemination activities. By focusing on the emerging nexus created between information manipulation tactics and cyber-attacks, it aims to broaden the experts and practitioners' knowledge and understanding of the new tools, means and strategies used by enemy states to create and multiply non-illegal manipulative activities threatening/ having the potential to negatively impact values, procedures and political processes at EU level. The course also focuses on discussing and working with existing methodological frameworks (e.g. the open-source DISARM) currently used to identify and counter FIMI/disinformation, while introducing trainees to several showcases on how to combat FIMI/disinformation.
The course will also focus on setting the scene to better understand current FIMI actions' impact and future developments.
The course will include lectures, debates, problem-solving exercises, and mentorship.

Learning Outcomes	
Knowledge	LO1. Understand the main challenges to EU security, which emerged as a result of the changing landscape of FIMI/disinformation and tactics LO2. Be able to identify the elements of the EU integrated approach to situational awareness, resilience, response and cooperation against FIMI/disinformation *LO3.* Understand and map out the modus operandi that combines information manipulation with cyberattacks and learn to make a shared assessment *LO4.* Comprehend the principles of an EU FIMI/disinformation toolbox, focused on preventive, cooperative, stability-building, restrictive and support measures
Skills	LO5. Identify lessons learnt and good practices in response options, from diplomatic engagement to crisis mitigation LO6. Be able to create mechanisms of resilience from prevention to recovery

	LO7. Learn how to mitigate identified risks and vulnerabilities through existing resources LO8. Apply critical thinking, assessment and cooperation skills throughout the exercises and scenario making sections of the course
Responsibility and Autonomy	LO9. Use tools and techniques to properly assess manipulative actions patterns threatening/ having the potential to negatively impact values, procedures and political processes at EU level LO10. Learn how to use cyber-diplomacy tools and interference mitigation mechanisms LO11. Translate knowledge into practical oriented solutions to be shared, negotiated and advanced in multi-stakeholders' formats

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participant's satisfaction with the course*).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on the active contribution in the residential Module, including their syndicate session and practical activities (24 hours total) as well as on their completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz (26 hours total). Active observation by the course director/lead instructor and feedback questionnaire filled by course participants at the end of the course is used.

However, no formal verification of learning outcome is foreseen; proposed ECTS is based on participants' workload only.

Course structure		
The residential module is held over four days		
Main Topic	**Suggested Working Hours (required for individual learning)**	**Suggested Contents**
1. EU strategic environment	2 (2)	1.1 Multi-layered threats against the EU – an analysis of the Strategic Compass 1.2 European Democracy Action Plan – understanding the need to protect democracies
2. Emerging technology & evolving threats: information warfare as main challenge at EU level	4 (4)	2.1. Theories and concepts that can help map and understand information-based threats and warfare 2.2. Introducing FIMI – main components and modus operandi 2.3. Impact of information manipulation 2.4. Role of cyberattacks
3. The EU integrated approach to situational awareness, resilience, response and cooperation against FIMI/disinformation	2 (4)	3.1. The EU integrated approach to FIMI 3.2. The EU perspective and priorities in countering FIMI 3.3. Main challenges ahead – AI impact and changing strategies in information manipulation
4. Key FIMI actors and priority regions	2 (3)	4.1 Russia's modus operandi 4.2 China's modus operandi 4.3. Regions affected by FIMI activity of global actors, and local state/non-state actors
5. Managing the information security ecosystem: A practitioner's toolkit	4 (4)	5.1. The need for a structured approach: describing disinformation behaviours in order to identify and record disinformation attacks 5.2 Understanding the psychological aspects of FIMI 5.2. Introducing the DISARM framework 5.3 The modus operandi that combines information manipulation with cyberattacks

6.Syndicate assignment	6 (6)	6.1. Working groups 6.2. Case studies, simulation exercises 6.3. Showcases and mentorship
TOTAL	**20 + (21) = 41**	

Materials	**Methodology**
Required: AKU 2 on European Global Strategy AKU 6 CSDP decision shaping/making AKU 300 Intercultural competence **Recommended:** Syndicate materials, scenario, other documents provided by Course director and the StratCom expert/trainer AKU 1 History and context of ESDP/CSDP development AKU 4 CSDP crisis management structures and chain of command AKU 25 EU Mutual Assistance Clause	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. Depending on different audiences, the course can be organised as a familiarisation course or advanced course, with a corresponding change in focus regarding concepts, policies, planning and implementation. **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).