European Security and Defence College
Doc: ESDC/2025/044
Date: 19 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2027**	Activity number ***80***	**Course on Artificial Intelligence, Security, and Cooperation in the European Union**	ECTS **2**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on	(i.e SQF MILOF equivalence)

Target audience	Aim
Participants should be mid-ranking to senior officials, doctoral researchers, academics, and practitioners whose work intersects with or is expected to be impacted by the integration of AI in security, defence, and cooperation within the EU. Priority is given to personnel from EU Member States and institutions involved in policy development, governance, and strategic security initiatives, who would benefit from acquiring the necessary knowledge to effectively manage and adapt to these emerging developments.	This course aims to provide a comprehensive overview of the role of Artificial Intelligence (AI) in European security and cooperation, focusing on its strategic implications, the most prominent threats, ethical considerations, and operational applications. Participants will explore AI's impact on national security, cybersecurity, hybrid threats, disinformation, diplomacy, and gender-related security issues. The course facilitates networking among policymakers, academics, and practitioners, fostering an interdisciplinary approach to AI in security governance.
Open to: ▪ Fellows ESDC Doctoral School on CSDP ▪ EU member States / Institutions ▪ Candidate countries ▪ Non-EU countries and International organisations	

Learning Outcomes	
Knowledge	LO1. Describe the role of AI in shaping the EU's strategic environment and security policies. LO2. Explain the impact of AI on hybrid threats, cybersecurity, and predictive analytics in security operations. LO3. Identify AI-driven disinformation strategies and their effects on democratic processes. LO4. Assess AI's implications in diplomacy, cyber diplomacy, and international cooperation. LO5. Discuss the ethical dimensions of AI research and policy development, particularly in the security domain. LO6. Examine the intersection of AI, gender-based violence, and security.

Skills	LO7. Apply scenario-based assessments to evaluate AI’s role in national security and defence strategies. LO8. Develop strategies to identify and counter AI-enabled disinformation in European security contexts. LO9. Participate in discussions focused on developing AI governance strategies and AI-driven policy frameworks within the European Union LO10. Examine methods for incorporating AI into security research and policy development.
Responsibility and Autonomy	LO11. Work with stakeholders from diverse fields to promote interdisciplinary discussions on AI and security. LO12. Critically reflect on the governance challenges and lessons learned from AI implementation in European security and defence policies.

Evaluation and verification of learning outcomes

The course evaluation follows the **Kirkpatrick model**. The first level aims to assess the participants' initial reactions to the training through surveys to determine their satisfaction and perceived relevance of topics like AI's role in the EU's strategic security environment. The practical exercises and the eLearning activities will contribute to the evaluation of the participants' understanding of subjects such as AI-driven disinformation and ethical dimensions in AI policy development. The ultimate goal is to help participants integrate the third and fourth levels of the Model, namely contribute to positive behavioural changes in the participants' work environments through the application of the new knowledge acquired, and ultimately achieve a broader organizational impact through improvements in security strategies, international cooperation on AI issues, and ethical policy considerations.

To successfully complete the course, participants must fulfil all learning objectives and actively contribute to the residential module, including teamwork sessions and practical exercises. They are also required to complete the mandatory eLearning phase and successfully finish the Autonomous Knowledge Units (AKUs), achieving a minimum score of 80% in the required tests or quizzes. Although the proposed ECTS credits are based on coursework completion, no formal verification of learning outcomes is conducted.

The Executive Academic Board takes these factors into account when deciding whether to award certificates. The Course Director, supported by the ESDC Secretariat, oversees the overall coordination of the course and is responsible for drafting the final evaluation report, which is then presented to the Executive Academic Board.

Course structure

Main Topic	Suggested Working Hours + (Required hours for individual learning)	Suggested Contents
AI in the EU’s Strategic and Security Environment	5 + (6)	**The EU's Strategic Environment:** Collaboration with security organisations, AI’s role in addressing hybrid threats. **AI & National Security:** Use of AI in threat detection, predictive analytics, and operational security strategies. **Cybersecurity & AI:** AI-driven cybersecurity practices, challenges, and solutions for European security.
AI, Disinformation, and Democratic Resilience	4 + (5)	**Countering Disinformation:** AI’s role in detecting and mitigating disinformation threats. **AI, Disinformation, and the Threat to Democracy:** The impact of AI on democratic processes and societal stability.

AI in Diplomacy and Governance	4 + (6)	**AI Diplomacy & Cyber Diplomacy:** The role of AI in international security cooperation and cyber diplomacy. **Ethical AI Research & Policy:** Governance, best practices, and ethical considerations in AI-driven security policies.
AI's Societal Implications and Emerging Challenges	4 + (3)	**AI-Enabled Gender-Based Violence:** Examining AI's intersection with security and gender-related threats. **Mapping Challenges & Lessons Learned:** Identifying key takeaways, challenges, and future directions for AI in security. **Ethical Considerations in A.I. Research and Policies** Identifying ethical challenges and standards and frameworks related to AI in security. This could include case studies on ethical dilemmas and resolutions.
Interactive Learning and Application	5 + (2)	**Interactive Workshop –** National Security & AI: Scenario-based exercises to assess AI applications in security contexts. The specific focus can vary depending on the audience and scope. For instance it can be related to disinformation, A.I.-driven cyber attacks, A.I. driven gray zone tactics, etc. **Roundtable Discussion –** Research & Policy Integration: Exploring methodologies for AI research and policy implementation.
TOTAL	**22 + (22)**	

Materials

Required:

AKU 1 History and context of CSDP

AKU 2 European Global Strategy

AKU 55 Strategic Compass

AKU 106 H-CoE
AKU 107 Awareness course on Cyber Diplomacy

AKU 108 The Cyber Defence Policy Framework (CDPF)

Recommended:

AKU 123 CYBER Cyber Policy Documents

Syndicate materials, scenarios and other documents provided by the course director

Methodology

- Lectures and Panels: Expert-led discussions on AI's role in security.
- Workshops & Case Studies: Scenario-based learning on AI applications.
- Interactive Discussions: Engaging roundtables on ethical AI and policy development.
- Networking & Doctoral Research Sessions: Facilitating collaboration between academics and practitioners.

Additional information

A pre-course questionnaire may be used to assess participants' learning expectations and to identify potential briefing topics within their areas of expertise.

All participants must complete the mandatory eLearning preparatory phase before attending the residential module. The supplementary eLearning materials will reflect the latest developments in cybersecurity and AI, ensuring participants arrive well-prepared for in-depth discussions.

Participants are expected to attend the entire course and actively engage in lectures, discussions, scenario-based assessments, and workshops.

The course will be conducted under the **Chatham House Rule**, meaning: *"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 disclosed."*

Coordinated by ESDC Training Manager, Maria PENEDOS, maria.penedos@eeas.europa.eu