Council of the European Union

Brussels, 20 May 2025
(OR. en)

9119/25

LIMITE

EUMC 184
COPS 227
POLMIL 127
CSDP/PSDC 303
CFSP/PESC 719

COVER NOTE

From:	European External Action Service (EEAS)
To:	Political and Security Committee (PSC) European Union Military Committee (EUMC)
Subject:	Military Advice on the Artificial Intelligence Practical Implementation Roadmap

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (02.07.2025)

Delegations will find attached the Military Advice on the Artificial Intelligence Practical Implementation Roadmap.

EEAS(2025) 430 REV3

EEAS(2025) 430 REV3

LIMITE

EUROPEAN EXTERNAL ACTION SERVICE

European Union Military Staff

Official document of the European External Action Service

Brussels, 19.05.2025

EEAS Reference	**EEAS(2025) 430 REV3**
Classification	**LIMITE**
To [and/or GSC distribution acronyms]	**EUMC, EUMCWG, EUMCWG/HTF, EUMS, MPCC**
Title / Subject	**Military Advice on the Artificial Intelligence Practical Implementation Roadmap.**
[Ref. prev. doc.]	**EEAS(2025) 430**

Delegations will find attached the Military Advice on the Artificial Intelligence Practical Implementation Roadmap, as agreed by the MS, under Written Consultation at 16:00 on 19 May 2025.

Military Advice on the Artificial Intelligence Practical Implementation Roadmap

References:

A. Council Conclusions on EU Digital Diplomacy (ST 11406/22, dated 18 July 2022).

B. Council Conclusions on EU Digital Diplomacy – Council approved by the Council at its meeting on 26 June 2023 (ST 11088/23, dated 26 June 2023).

C. The Future of EU Digital Policy - Council Conclusions (21 May 2024) (ST 9957/2024, dated 21 May 2024).

D. Regulation (EU) 2024/1689 of the EU parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L series, dated 12 July 2024).

E. Regulation (EU) 2025/38 of the EU Parliament and of the Council of 19 December 2024, laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L series, dated 15 January 2025).

F. Non-paper for PSC on Artificial Intelligence in the Common Foreign and Security Policy (CSFP) and the Common Security and Defence policy (CSDP), dated 12 February 2025.

G. PSC Conclusions, 19 February 2025.

A. INTRODUCTION AND AIM

1. On 18 July 2022 (Ref. A) and later on 26 June 2023 (Ref. B) Council Conclusions on EU Digital Diplomacy were issued, where the Council emphasized the EU's commitment to a human-centric and human rights-based approach to digital technologies, including Artificial Intelligence (AI) based on risk-driven approach preserving human dignity.
2. On 21 May 2024, with the Council Conclusions on the Future of EU Digital Policy (Ref. C), the Council reaffirmed the EU's dedication to a human-centric and human rights-based approach to digital technologies.
3. On 19 December 2024 (Ref. E), European Parliament and the Council issued measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents.
4. On 19 February 2025, the Political and Security Committee (PSC) had an exchange of views on this matter and provided guidance to the EEAS (Ref. G), in close consultation with the EU Member States (MS) in relevant Working Parties, for the development of a Practical Implementation Roadmap with concrete next steps and activities in the field of AI in Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP).
5. The aim of this Military Advice[1] is to provide military inputs, including a possible military Roadmap, to be properly considered in the developing EEAS AI Practical Implementation Roadmap in the area of CFSP and CSDP.

[1] Due to the complexity and amplitude of the topic, this Military Advice includes a detailed and technical annex for a comprehensive treatment of the topic.

B. CONSIDERATIONS

General approach to Artificial Intelligence (AI)

6. The EUMC considers that AI has become a strategic asset, transforming military operations/missions and geopolitical dynamics. Its rapid integration into autonomous systems and decision-making tools—evident in the Ukraine-Russia conflict—boosts speed, precision, and reach, but also empowers cyber and disinformation threats.

   The EUMC understands that the EU must adapt its strategic posture. AI's dual-use nature, when referring to commercial tools usable for both civilian and military purposes, demands civilian-military coordination. However, when AI is implemented within closed military systems and networks, the dual-use condition does not apply.

7. The EUMC deems that malicious actors exploit commercial AI for attacks and disinformation, while defence benefits from enhanced planning and threat detection—raising concerns on ethics and transparency. The EUMC underlines that military use of AI shall remain consistent with International Law, the Law of Armed Conflict, and the principles of Humanity, Necessity, Distinction, Proportionality and Precaution, as already governing the use of other weapons.

AI-Related Threats and Challenges

8. The EUMC highlights that Generative AI and foundational models are largely driven by civilian tech firms, marking a historical shift where a strategic military enabler lies mostly outside governmental control. This decentralization poses significant proliferation risks and weakens the EU's strategic autonomy. Moreover, commercially available AI tools may be weaponized, making their proliferation difficult to control.

   To mitigate these risks, the EUMC remarks that the EU must establish, when it is possible, clear boundaries between civilian and military AI applications. In particular:

- Defining dual-use AI categories within export control regimes;
- DELETED
- Preventing uncontrolled proliferation of AI tools that could be weaponized or used in military decision-making;
- Promoting responsible behaviour when using dual-used AI technology in military capabilities.

9. The EUMC considers that banning military AI systems prematurely—without fully understanding their strategic implications—could leave the EU vulnerable. While ethical and legal concerns are valid, banning certain capabilities too early could prevent EU forces from developing defences against AI-enabled threats from adversaries such as Russia or China. Any restriction or ban should follow a thorough legal, strategic and operational assessment, ensuring compliance with International Law, similar to other military capabilities.

AI-enabled Capabilities

10. The EUMC deems that the transformative impact of AI requires coordinated military leadership. The EUMC and EUMS must lead conceptual evolution and drive, with the support of European Defence Agency (EDA), EU-wide standardization efforts aligned with NATO frameworks.

DELETED

AI Global Governance

11. The EUMC suggests that the EU's AI posture must ensure full compliance with International Humanitarian Law (IHL), Human Rights Law, and the UN Charter, maintaining human control, especially in targeting. In particular, the EUMC highlights that AI offers potential to minimize collateral damage by enabling precision-targeted systems, such as smart munitions that avoid civilians or heritage sites. Research into such applications should be encouraged within international governance for including defensive-only systems and controls over Lethal Autonomous Weapons Systems (LAWS). The EUMC remarks that AI can support but not replace human judgment in targeting. Legal compliance and human validation, especially for estimations like Collateral Damage Estimation (CDE), remain essential to avoid operational risks.

Concreate Work with Partners, especially NATO

12. The EUMC considers that the EU's common effort should also focus on shaping international AI governance in cooperation with EU MS. This includes building bridges between existing frameworks such as the Convention on Certain Conventional Weapons – Group of Governmental Experts (CCW-GGE), UN General Assembly (UNGA) resolutions, the Responsible AI in the Military Domain (REAIM) principles, and NATO AI Strategy. The EU and NATO should jointly promote a dedicated forum to define norms, enhance transparency and compliance with International Law, in particular International Humanitarian Law (IHL), and support implementation of UNGA Resolution 79/239—while maintaining operational freedom in AI capabilities and research. Military AI systems must be designed with resilience and robustness in mind throughout their lifecycle. In particular, EU MS should align with NATO based on a more focused AI EU-NATO Structured Dialogue on EDT to avoid duplications.

Tentative Military Roadmap

13. The EUMC proposes that a tentative military Roadmap for the introduction of AI in the military field, part of the overall EEAS Practical Implementation Roadmap, could be, as follows[2]:
    - **Phase 1**: Situational awareness, threat analysis, pilot projects scoping, and data standardisation;
    - **Phase 2**: Launch or support of flagship projects under PESCO/EDF, AI-specific conceptual updates, and international engagement;
    - **Phase 3**: Integration of AI across EU-led CSDP operations/missions, full posture review, updates to legal and procurement frameworks.

C. RECOMMENDATIONS

14. The EUMC deems that all the above mentioned considerations and those more detailed reported in the annex are relevant and should be taken into proper examination, including a possible military Roadmap, in view of the development of the EEAS AI Practical Implementation Roadmap.

15. The PSC is invited to:
    - Consider this Military Advice and its annex, and;
    - Agree to its recommendations.

[2] Timeframes to be established by the EEAS in harmonization with the overall Practical Implementation Roadmap.

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 17)