REAIM

4-5 February 2026
A Coruña / Spain 2026

Responsible AI in the Military Domain Summit

Co-hosted by the Netherlands and the Republic of Korea

REAIM Pathways to Action

1. We recognise that the responsible use and development of Artificial Intelligence (AI) in the military domain can and should contribute to international peace and security. When appropriately applied throughout their life cycles, military AI capabilities can help reduce the exposure of personnel to danger, improve the protection of civilians, and support more timely and better-informed decision-making, facilitating enhanced compliance with international law, including international humanitarian law, as applicable. At the same time, the use of AI can present risks across various facets of the military domain. Therefore, we also recognise the need for enhanced shared understandings of risks that may be presented throughout the life cycles of AI in the military domain, including miscalculation, bias, loss of control or escalation.

2. We underline that REAIM is a State-led, multistakeholder initiative that seeks to provide an agile, robust, and evidence-based platform to incubate and nurture ideas to complement and reinforce parallel initiatives for the promotion of responsible AI in the military domain.

3. We note related developments since the last 2024 REAIM Summit, in Seoul, including the UN Secretary-General´s report (A/80/78), particularly States' contributions included therein, and the adoption of UNGA Resolutions 79/239

and 80/58 on "Artificial intelligence in the military domain and its implications for international peace and security" , and the ongoing work of the Group of Governmental Experts (GGE) on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (LAWS) convened under the auspices of the Convention on Certain Conventional Weapons (CCW).

4. We also take note of the Global Commission REAIM´s report "Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain" and the recommendations therein, in particular its emphasis on responsibility by design, risk-based governance approaches, and the need for robust oversight and accountability mechanisms throughout the life cycles of the military AI capabilities.

5. We consider that REAIM's distinct added value lies in its multistakeholder character and its ability to leverage technical, industry, operational, legal, societal, ethical and regional expertise to generate, test, and refine practical ideas to harness the benefits of AI in the military domain while anticipating and addressing challenges to its implementation through foresight, forward-looking assessments, as well as the identification, sharing, and applications of lessons learned and good practices in this regard.

6. We stress the importance of capacity-building, and underline the role of REAIM to promote cooperation and to help bridge gaps between and within regions in the ability to, inter alia, develop policies, frameworks and guidelines, as well as create and sustain an environment conducive to the responsible design, development, testing, deployment, and use of AI in the military domain, through cooperation and knowledge-sharing.

7. Building on the Call to Action advanced at the REAIM Summit 2023 in The Hague and the Blueprint for Action advanced at the REAIM Summit 2024 in Seoul, convinced that the time has come to take steps towards operationalization of the principles reflected in these documents, we invite all stakeholders, as applicable - including States, industry, academia, civil society, and regional and international organizations - to:

Legal frameworks and general practices

8. Uphold compliance with applicable international law, including international humanitarian law and international human rights law, as required throughout the life cycles of AI capabilities in the military domain.

9. Develop and promote a "responsible by design" approach, integrating principles of responsible use of AI from the earliest planning stages through designing, developing, testing, deployment, monitoring and decommissioning.

10. Ensure that States and individuals remain accountable for decisions, including both actions and omissions, taken throughout the life cycles of AI military capabilities, consistent with their respective obligations under international law; recognizing that States and individuals (rather than machines and algorithms) bear legal and ethical responsibility; and avoiding the creation of "accountability gaps" in the use of AI in the military domain.

11. Recognise the challenges related to reliability, security, resilience, unintended biases, traceability and explainability, which can be addressed by advancing the field of AI assurance, including through assessments of reliability, security, and resilience. It is also critical to consider potential risks such as cyber threats and adversarial manipulation of data, models and outputs, while also anticipating

fast capability advances that may outpace assurance methods, including Artificial General Intelligence (AGI) or even Artificial Superintelligence (ASI).

12. Emphasise that AI-enabled decision support systems should support, not replace, the exercise of human judgement. The nature and degree of human involvement should be appropriate considering, among other factors, the operational context, the function performed, the technical characteristics and capabilities, as well as human factors such as training and fatigue, and the risks and benefits involved.

Recommendations for the operationalization of REAIM principles at the national level

13. Ensure relevant personnel are actively involved in the development and testing phases of AI systems in the military domain. Ensure as well that personnel operating military AI capabilities and those in the chain of command receive appropriate training and education, including a structured training and familiarisation phase before operational use, so they understand systems' capabilities as well as limitations.

14. Consider risk assessments, which take into account specific legal, humanitarian and operational risks of AI-enabled military systems, prior to deployment and use of AI-enabled systems in the military domain, and to regularly update such assessments as systems, operational environments and threat landscapes evolve. Recognise the need to consider the potential risks around unanticipated, emergent behaviours, and explainability.

15. Promote robust testing, evaluation, validation and verification (TEVV) and integrate TEVV requirements in relevant policies, doctrines, and procurement

processes. TEVV efforts should include qualification and/or certification, where appropriate, against requirements proportionate to intended benefits and risks, and the association of systems with defined use cases for which they have been tested and validated.

16. Conduct legal reviews of weapons, means, and methods of warfare enabled by AI, consistent with applicable international legal obligations and relevant national laws and procedures.

17. Strengthen measures to protect the integrity, availability and confidentiality of data and to mitigate risks of data compromise, poisoning or other manipulation, also by non-state actors, including terrorist groups.

18. Maintain audit trails and documentation across the life cycle, including mechanisms for incident reporting and lessons learned, to strengthen traceability, explainability and oversight.

19. Identify and adopt appropriate operational requirements and procedures to ensure accountability for decisions in the use of AI capabilities, including through doctrine, Tactics, Techniques and Procedures (TTPs), rules of engagement where relevant, and system/interface design and development.

20. Encourage the delineation of clear chains of command and control to ensure individual responsibility for operations involving AI-enabled systems and for relevant functions across the life cycles. Consider developing and implementing measures that could facilitate accountability, such as digital forensics, documentation, and clear processes for after-action reviews and investigations.

21. Encourage the designation of a national focal point within relevant departments (for example, a Chief Responsible AI Officer or equivalent) to facilitate whole-of-government coordination, the implementation of practices for the responsible use of AI, and international cooperation.

Recommendations for the operationalization of REAIM principles at the international level

22. Develop shared understandings regarding AI functions or capabilities across military applications.

23. Undertake confidence-building measures on a voluntary basis and as appropriate to strengthen trust and transparency where AI is applied in the military domain, that may complement existing multilateral mechanisms, to reduce possible risks of misunderstanding, miscalculation, and unintended escalation, including by:

    a. Sharing appropriate information on national policies, principles, governance structures and oversight arrangements, as well as frameworks, guidelines, approaches and methodologies for legal reviews and risk-assessment approaches and methodologies, where consistent with national security, including through the contribution of military academies.

    b. Encouraging outreach activities, regional cooperation, including through joint seminars, table-top exercises, inter-regional dialogue, workshops, and the exchange of lessons learned and good practices.

c. Exploring opportunities for visits or exchanges related to facilities or centres of excellence, where feasible and consistent with national security.

d. Considering crisis-communication arrangements to reduce risks of potential unintended escalation.

24. Promote capacity-building, including for developing countries, through regional centres of excellence, knowledge-sharing hubs, exchanges of best practices, point of contact directories, and technology cooperation taking into account different national contexts, needs and levels of technological development, and recognizing existing asymmetries.

Recommendations for engagement with industry, academia and civil society

25. Participate in and support initiatives between States, industry, and academia, aimed at promoting responsible AI in the military domain and advancing foundational research to enable AI security and reliability, including research on AI interpretability and robustness.

26. Further engage with our respective national industrial ecosystems and raise awareness of the approaches and principles advanced in the 2023 REAIM Call to Action, the 2024 REAIM Blueprint for Action, as well as the 2026 REAIM Pathways to Action.

27. Invite industry and other relevant stakeholders to address design challenges around human-machine interaction and user interfaces proactively.

28. Call on upcoming REAIM hosts and the wider REAIM community to build on these efforts to further strengthen links with industry aimed at jointly translating principles into practical recommendations and guidance.