UNIDIR

RESEARCH BRIEF

AI in the Military Domain: A briefing note for States

GIACOMO PERSI PAOLI · YASMIN AFINA

Acknowledgements

Support from UNIDIR funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Security and Technology Programme (SECTEC), which is supported by Czechia, Germany, Italy, the Netherlands, Norway, Republic of Korea, Switzerland and Microsoft.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. This background paper is presented in the authors' independent capacity and does not necessarily reflect the views or opinions of the authors or of the organizations with which the authors work. They do not necessarily reflect the views or opinions of the United Nations or UNIDIR.

Authors

Giacomo Persi Paoli

Head of Programme, Security and Technology Programme, UNIDIR

Yasmin Afina

Researcher, Security and Technology Programme, UNIDIR

Citation

Giacomo Persi Paoli and Yasmin Afina, 'AI in the Military Domain: A briefing note for states', (Geneva: UNIDIR, 2025).

Cover Image: Generated with AI. Credit: KaihkoImages / Adobe Stock.

Table of Contents

1. Background

On 24 December 2024, the United Nations (UN) General Assembly adopted Resolution A/RES/79/239 on "Artificial intelligence in the military domain and its implications for international peace and security".[1] This resolution represents a pivotal moment for multilateral discussions on artificial intelligence (AI) for two reasons: (1) the first two resolutions on AI adopted earlier in 2024 excluded the military domain and international security from their remits,[2] and (2) for the first time, the international peace and security community was invited to reflect on the impact of the development, deployment and use of AI beyond lethal autonomous weapons systems (LAWS), in recognition of the wide range of military applications of this powerful technology.

Following Resolution A/RES/79/239 and with a view to submitting a report to the eightieth session of General Assembly, the UN Secretary-General invited Member States, observer States, international and regional organizations, the International Committee of the Red Cross, civil society, industry, and the scientific community to submit their views "on the opportunities and challenges posed to international peace and security by the application of artificial intelligence in the military domain, **with specific focus on areas other than lethal autonomous weapons systems**".[3]

The present briefing note aims to support States in the formulation of their national views on this important topic, with the objective of making the resulting report as comprehensive, diverse and geographically representative as possible. The note will include some contextual information on the topic of AI in the military domain, a set of considerations for States to refer to, and a list of suggested readings that draws on UNIDIR's own research and selected external publications.

---

1 Resolution A/RES/79/239, "Artificial intelligence in the military domain and its implications for international peace and security", as of 03.03.2025: **https://docs.un.org/en/A/C.1/79/L.43**

2 See Resolution A/78/L.49, "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development", as of 03.03.2025: **https://docs.un.org/en/A/78/L.49**; and Resolution A/78/L.86, "Enhancing international cooperation on capacity-building of artificial intelligence", as of 03.03.2025: **https://docs.un.org/en/A/78/L.86**

3 Resolution A/RES/79/239, "Artificial intelligence in the military domain and its implications for international peace and security", Operative Paragraphs 7 and 8. as of 03.03.2025: **https://docs.un.org/en/A/C.1/79/L.43**

2. Context

Until January 2023, multilateral discussions on AI in the military domain were confined to the remit of the **Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts (GGE) of the High Contracting Parties [to the Convention on Certain Conventional Weapons] related to emerging technologies in the area of LAWS.** In this context, AI has been discussed as a technology that could enable advanced levels of autonomy in weapons systems. These technological advances bring to the fore a host of legal and policy challenges, both pre-existing and novel, including compliance with international humanitarian law and international human rights law, ethical considerations, and wider policy questions.

A key instrument of international humanitarian law, the CCW was designed to ban or restrict the use of specific types of weapons which may be deemed to be excessively injurious, or to have indiscriminate effects.[4] As such, most of the **discussions related to AI occurring within the general framework of the CCW and the specific context of the GGE on LAWS focused on use of these systems in military targeting, with an emphasis on legal compliance**.

The use of AI as an enabler for more advanced and sophisticated levels of autonomy in weapons systems is certainly a very important issue, but it only represents a very small portion of the range of possible military applications of this technology.[5] The potentially transformative effect of AI on all aspects of society, including national security and defence, has become a mainstream topic of discussion among policymakers and the general public alike, particularly following the public release of ChatGPT in late 2022.

Championing the idea that the responsible development, deployment and use of AI in the military domain needed to be placed higher up the international agenda, the Government of the Netherlands hosted in February 2023 the **first Global Summit on Responsible Artificial Intelligence in the Military Domain (REAIM 2023).** The Summit, co-hosted with the Republic of Korea, provided a platform for all stakeholders to discuss the key opportunities, challenges and risks associated with military applications of AI.[6] A number of government representatives present at the first REAIM Summit subsequently put out a joint ***Call to Action*** on the responsible development, deployment and use of AI in the military domain.[7] The **second REAIM Summit** was held in Seoul in September 2024 and hosted by the Republic of Korea alongside the Netherlands, Singapore, Kenya and the United Kingdom. This second edition was able to build on the solid foundations of the first summit, integrating insights from a series of regional consultations on responsible AI in the military domain that were held in early 2024 in Singapore,

---

4 UNODA, https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/

5 See for example: Sarah Grand-Clément, "Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain", UNIDIR, Geneva, 2023. https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/

6 For more information on REAIM 2023, see: https://www.government.nl/ministries/ministry-of-foreign-affairs/activiteiten/reaim/about-reaim-2023

7 Government of the Netherlands, *REAIM 2023 Call to Action*, 16 February 2023. https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/publications/2023/02/16/reaim-2023-call-to-action

Image generated by AI, Credit: Adobe Stock.

Istanbul, Nairobi, Santiago and online.[8] The Summit was able to dig deeper into the topic and take an incremental, yet meaningful, step forward through the ***REAIM Blueprint for Action***.[9] A third iteration of the Summit is scheduled for September 2025 in Spain.

In February 2023, in parallel with the launch of the REAIM initiative, the United States launched the ***Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy***.[10] The Declaration outlines measures that should be implemented by States in the development, deployment and use of military AI capabilities - including those that enable autonomous functions and systems - and provides a basis for exchanging best practices and building States' capacities.[11] Endorsed by over 50 States, the Declaration has provided a framework for the creation of a number of State-led working groups in this area.

Initiatives such as REAIM and the Declaration provide useful context both to Resolution A/RES/79/239 and to the subsequent invitation extended by the UN Secretary-General to Member States to submit their views on the opportunities and challenges posed to international peace and security by the application of AI in the military domain.

---

8 Yasmin Afina, "The Global Kaleidoscope of Military AI Governance", UNIDIR, Geneva, 2024. https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/

9 Government of the Republic of Korea, *REAIM Blueprint to Action*, 10 September 2024. https://reaim2024.kr/home/reaimeng/board/bbsDetail.do?encMenuId=4e57325766362f626e5179454e6d6e4d4a-4d33507a773d3d&encBbsMngNo=366e794c7a644d756342425668444f393053755142673d-3d&encBbsNo=6f784e4542386f7735767465766a6531556f4b6149413d3d&ctlPageNow=1&schKind=bbsTtlCn&schWord=#this

10 U.S. Department of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, February 2023. As of 03.03.2025: https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy

11 For the full list of measures, see: https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/

3. Considerations for States preparing national views

Drawing on UNIDIR research, the following sections outline some important considerations for States as they begin the process of preparing their national views:

a. Unpack the military domain

The first step is to break down the concept of "military domain" into its various components, acknowledging that the range of operational contexts within which military forces might be required to operate is broad and subject to different legal, ethical and normative frameworks. This is particularly relevant as different regions and sub-regions may face different types of threats in inherently varied security contexts, therefore deploying military forces in different ways and within different frameworks. As such, it would be important for **States to articulate their views across the range of operations as appropriate and relevant to their national contexts**. As an example, States could consider differentiating the use of AI by military forces in the conduct of hostilities (international armed conflicts and non-international armed conflicts) from the use of AI by military forces in other types of operations, such as peacekeeping, emergency response or disaster relief, and support to national security and public safety (support to law enforcement, border security, counter-piracy, protection of critical infrastructure and so on).

b. Consider the full array of military applications of AI

Resolution A/RES/79/239 calls for States to focus **on military applications of AI in areas other than LAWS**. Within the wide range of operational contexts described in the previous point, it is important for States to consider the full array of military applications of AI. While there is no internationally agreed taxonomy of military applications, States could consider using a task-based approach similar to the one presented in UNIDIR's report *Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain*. This approach uses four key military tasks to group military applications of AI beyond weapon systems.[12]

- **Command and Control (C2):** C2 refers to the decision-making aspect of a military operation.
- **Information Management:** Information management refers to the collection, processing, exploitation and dissemination of information relating to a military operation. This includes, for example, applications in support of intelligence, surveillance and reconnaissance.

---

[12] The report provides a detailed breakdown of the activities and actions included in each of the four macro-level tasks, as well as an appraisal of the impact of AI on each of such activities. For more information see: Sarah Grand-Clément, "Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain", UNIDIR, Geneva, 2023. https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/

- **Logistics:** Logistics refers to the movement, supply and monitoring of personnel and equipment to sustain a military operation. This can include, for example, predictive maintenance.
- **Training:** Training refers to the instruction and preparation of military personnel.

The above tasks can be used to map AI use cases across the full spectrum of military operations, including those outside of combat, as described in point (a) above. Other potentially relevant applications of AI beyond the scope of LAWS include those that support or enable cyber operations, including influence operations, cognitive warfare and electromagnetic warfare.[13]

c. Assess the risks

While the discussion on AI risks in the civilian domain is more advanced, there is no universally agreed risk framework for AI in the context of international peace and security. This may partially be explained by the varying risk perceptions and assessments within and across regions.[14] However, it is important that States adopt a holistic approach to risk assessments. This in mind, **States could consider reflecting on two distinct categories of risk: risks related to AI technology itself and risks related to its diffusion and use.** UNIDIR's taxonomy of AI risks can provide States with a useful reference in this regard.[15]

Risks related to the technology itself could include:

- AI safety risks stemming from the inherent brittleness of the technology, including all data issues.
- AI security risks deriving from new cyber vulnerabilities that AI systems might introduce.
- Risks associated with the human-machine interaction, such as automation bias and trust-calibration risks.

Consideration of risks related to the diffusion and use of AI, meanwhile, could include issues such as nonproliferation or risks of miscalculation and escalation. Part of this assessment could include consideration of the challenges involved in deploying such technology in compliance with existing legal regimes, as relevant and applicable to the specific operational context and application.

---

13 Many of such applications were discussed during a set of four regional consultations conducted in 2024 in preparation for the second REAIM Summit. For more information on the outcomes of these consultations please see: Yasmin Afina, "The Global Kaleidoscope of Military AI Governance", UNIDIR, Geneva, 2024. https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/

14 Yasmin Afina, "The Global Kaleidoscope of Military AI Governance", UNIDIR, Geneva, 2024. https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/

15 Ioana Puscas (2023) "AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures", UNIDIR, Geneva, Switzerland. As of 03.03.2025: https://unidir.org/publication/ai-and-international-security-understanding-the-risks-and-paving-the-path-for-confidence-building-measures/

Image generated by AI, Credit: Adobe Stock.

d. Elaborate on the opportunities

Resolution A/RES/79/239 also invites States to express views on the potential benefits brought by the development, deployment and use of AI technologies in the military domain. These opportunities - which may be international, regional, national or even local in nature - may include operational, legal and policy considerations. For example, AI-enabled technologies could be used to expand data collection practices, consolidate proportionality assessments and adopt precautionary measures. In reflecting on such opportunities, States should consider any contributing factors and aspects that would be key to harnessing such opportunities. These may include the preservation of State and individual accountability and responsibility throughout the technology's life cycle, cross-pollination with responsible AI efforts in the civilian realm, careful consideration of dual-use technologies, and data governance for responsible AI.[16]

e. Take stock of national structures

As part of States' assessments of the scope of the military domain and the full array of military applications of AI, **States could also consider existing structures at the national level (including those under development) that frame and/or are relevant for the governance of AI in the military domain**. These include governance structures and documents, such as national policy and/or strategy, civil and criminal legislation, internal regulations, codes of conduct, procurement guidelines, military manuals, and concept documents. These national structures also include relevant ministries and government agencies (e.g. law enforcement, intelligence agencies) involved in the development, deployment and use of AI in the military domain, as well as the existence of other national bodies (e.g. AI agencies, industry chambers, judicial courts).[17]

---

16 Yasmin Afina, "The Global Kaleidoscope of Military AI Governance", UNIDIR, Geneva, 2024. https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/

17 On the development of national strategies on AI in security and defence, see: UNIDIR, "Draft Guidelines for the Development of a National Strategy on AI in Security and Defence", UNIDIR, Geneva, as of 24 October 2024. https://unidir.org/publication/draft-guidelines-for-the-development-of-a-national-strategy-on-ai-in-security-and-defence/

4. Additional cross-cutting issues for consideration

In addition to the specific points presented above, States should consider contributing also their reflections on three important cross-cutting issues: (1) life-cycle management of AI systems, (2) the importance of data, and (3) possible pathways towards greater confidence, trust and transparency.

Cross-cutting issue 1: The life cycle of AI systems

Resolution A/RES/79/239 focuses on the whole life cycle of artificial intelligence capabilities applied in the military domain, "including the stages of pre-design, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning". This is an important consideration for States to take into account as they develop their national views since it may also impact upon the assessment of both risks and opportunities. While most of the public debate is focused on the "visible" part of the life cycle - namely the deployment, use and operation of AI systems - taking a holistic approach is the key both to mitigating risks and to leveraging opportunities.[18] As such, **States should consider, as relevant and applicable to their national context, reflecting on the whole life cycle of AI systems**. This also includes the critical phases of capability acquisition (sale, procurement or other type of transfer), which are an important element of capacity building.

Cross-cutting issue 2: The pivotal role of data

Along with models and computing power, data is a necessary component of AI systems, which makes it also a determining factor in the assessment of both opportunities and risks. Data feeds models during their training, testing, evaluation and use. As such, understanding and unpacking data practices is paramount for the responsible development and deployment of AI in the military domain.[19] **States could consider including in their national views any reflections on how the discussion around data intersects with the discussion on military applications of AI**, potentially elaborating on how this relationship has been managed at the national level.[20] In addition, States could consider elaborating on the opportunities and challenges of bringing data discussions to the regional and multilateral level.

---

18 Yasmin Afina and Giacomo Persi Paoli (2024). "Governance of Artificial Intelligence in the Military Domain: A Multi-Stakeholder Perspective on Priority Areas", UNIDIR, Geneva, Switzerland. As of 03.03.2025: https://unidir.org/publication/governance-of-artificial-intelligence-in-the-military-domain-a-multi-stakeholder-perspective-on-priority-areas/

19 Ibid.

20 Yasmin Afina and Sarah Grand-Clement, "Bytes and Battles: Inclusion of Data Governance in Responsible Military AI" CIGI Paper No. 308, 2024. https://www.cigionline.org/publications/bytes-and-battles-inclusion-of-data-governance-in-responsible-military-ai/

Cross-cutting issue 3: Building confidence through trust and transparency

Trust and transparency will play a key role both in mitigating the risks of military applications of AI and in leveraging the opportunities. As such, **States could consider including in their submission reflections on how to establish a positive agenda that may contribute to both confidence- and capacity-building**. In relation to confidence-building, **States could consider elaborating their views on three pillars of trust**: (1) how trust among States and their respective approaches to AI in the military domain can be built and maintained, (2) how trust in the technology can be calibrated, and (3) how trust in the responsible use of technology by human decision-makers, users and operators can be established. UNIDIR's recent reports on confidence-building measures for AI[21] and multistakeholder perspectives on the governance of AI in the military domain[22] provide useful context on this cross-cutting issue.

5. Conclusion

Resolution A/RES/79/239 provides a unique opportunity for States to (1) share their views on a topic of increasing importance to peace, security and conflict, and (2) influence how this topic will be discussed at the multilateral level. As such, it is crucial that the report produced by the UN Secretary-General be informed by as many national contributions as possible. This will also favour the best possible representation of the full diversity of States in terms of their geography, economy, culture, technological advancement and military power. While this research brief provides a broad overview of the range of topics that States may want to consider addressing when preparing their views, this list should not be interpreted as exhaustive or mandatory. States may decide to focus on only a few of the items suggested and add others as relevant and appropriate to their national context.

---

21 Ioana Puscas, Confidence-Building Measures for Artificial Intelligence. A Multilateral Perspective, UNIDIR, Geneva, 2024. https://unidir.org/publication/confidence-building-measures-for-artificial-intelligence-a-multilateral-perspective/

22 Yasmin Afina and Giacomo Persi Paoli (2024). "Governance of Artificial Intelligence in the Military Domain: A Multi-Stakeholder Perspective on Priority Areas", UNIDIR, Geneva, Switzerland. As of 03.03.2025: https://unidir.org/publication/governance-of-artificial-intelligence-in-the-military-domain-a-multi-stakeholder-perspective-on-priority-areas/

List of recommend readings

Selected UNIDIR resources

Yasmin Afina, “The Global Kaleidoscope of Military AI Governance”, UNIDIR, Geneva, 2024. https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/

Yasmin Afina and Giacomo Persi Paoli (2024). “Governance of Artificial Intelligence in the Military Domain: A Multi-Stakeholder Perspective on Priority Areas”, UNIDIR, Geneva, Switzerland. As of 03.03.2025: https://unidir.org/publication/governance-of-artificial-intelligence-in-the-military-domain-a-multi-stakeholder-perspective-on-priority-areas/

Sarah Grand-Clément, “Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain”, UNIDIR, Geneva, 2023. https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/

Ioana Puscas (2023) “AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures”, UNIDIR, Geneva, Switzerland. As of 03.03.2025: https://unidir.org/publication/ai-and-international-security-understanding-the-risks-and-paving-the-path-for-confidence-building-measures/

Ioana Puscas, Confidence-Building Measures for Artificial Intelligence. A Multilateral Perspective, UNIDIR, Geneva, 2024. https://unidir.org/publication/confidence-building-measures-for-artificial-intelligence-a-multilateral-perspective/

UNIDIR, “Draft Guidelines for the Development of a National Strategy on AI in Security and Defence”, UNIDIR, Geneva, as of 24 October 2024. https://unidir.org/publication/draft-guidelines-for-the-development-of-a-national-strategy-on-ai-in-security-and-defence/

Selected external publications

UNODA occasional papers no. 42 “Governance of artificial intelligence in the military domain” by Dr. Beyza Unal and Ulysse Richard. https://digitallibrary.un.org/record/4062924?v=pdf

Yasmin Afina and Sarah Grand-Clement, “Bytes and Battles: Inclusion of Data Governance in Responsible Military AI” CIGI Paper No. 308, 2024. https://www.cigionline.org/publications/bytes-and-battles-inclusion-of-data-governance-in-responsible-military-ai/

Thomas Reinhold, Elisabeth Hoffberger-Pippan, Alexander Blanchard, Marc-Michael Blum, Filippa Lentzos and Alice Saltini, “Artificial Intelligence, Non-proliferation and Disarmament: A Compendium on the State of the Art” Non-Proliferation and Disarmament Papers No. 92, January 2025. https://www.sipri.org/publications/2025/eu-non-proliferation-and-disarmament-papers/artificial-intelligence-non-proliferation-and-disarmament-compendium-state-art

Ashley Deeks, Noam Lubell and Daragh Murray, “Machine Learning, Artificial Intelligence, and the Use of Force by States” 2019 Journal of National Security Law and Policy 10. https://heinonline.org/HOL/P?h=hein.journals/jnatselp10&i=6

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais des Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG