

AI in military decision-making: The global governance challenge

BY DENISE GARCIA

The race to integrate AI into military command systems is accelerating — and changing how warfare is conducted. International law and norms governing the use of force and war are being ignored. The global community remains unprepared to address serious threats to international security. Although efforts to develop global governance continue, they are too slow and fragmented to keep up with the rapid technological advancements.

The current state of play

Across the world's major military powers, AI is rapidly moving from experimental laboratories into operational command-and-control systems. Since 2017, advances in machine learning and other computational techniques, along with many countries' decisions to incorporate AI into their military operations, have accelerated the militarisation of AI. This has led to the gradual integration of Decision Support Systems (DSS) into the battlefield, with many already active in military missions. This is guided by the goal of improving situational awareness to gain a strategic military advantage.

The promise is tempting: AI systems can quickly analyse large amounts of battlefield data, identify patterns invisible to human analysts and allow commanders to act faster than enemies. Supporters say this could lower casualties and improve targeting accuracy. Critics argue that the speed and automation pose se-

rious new risks to peace, diplomacy and international stability by undermining long-standing ethical principles and conduct norms, resulting in blatant violations of international law.

Data to decision-making — AI's expanding role in the battlefield

As AI increasingly shapes decision-making in conflict, its rapid integration into military systems raises profound challenges for safety, accountability and ethics. AI-driven tools, especially DSS, often operate with limited predictability and transparency, making it difficult for users to understand and trust their analyses and outputs. The competitive drive among states and actors to adopt these technologies risks premature deployment before they are sufficiently tested, potentially leading to grave operational and humanitarian consequences. Moreover, as machine learning systems take on roles

“

AI-driven tools, especially Decision Support Systems, often operate with limited predictability and transparency, making it difficult for users to understand and trust their analyses and outputs.

traditionally held by humans, they risk eroding human judgment — the foundation of ethical and legal accountability in warfare.

Ultimately, determining responsibility for battlefield decisions must remain a human function, grounded in contextual understanding rather than technical indicators alone, to ensure compliance with international humanitarian law (IHL) and the preservation of moral agency in war.

The heightened escalation dynamics and nuclear AI dangers

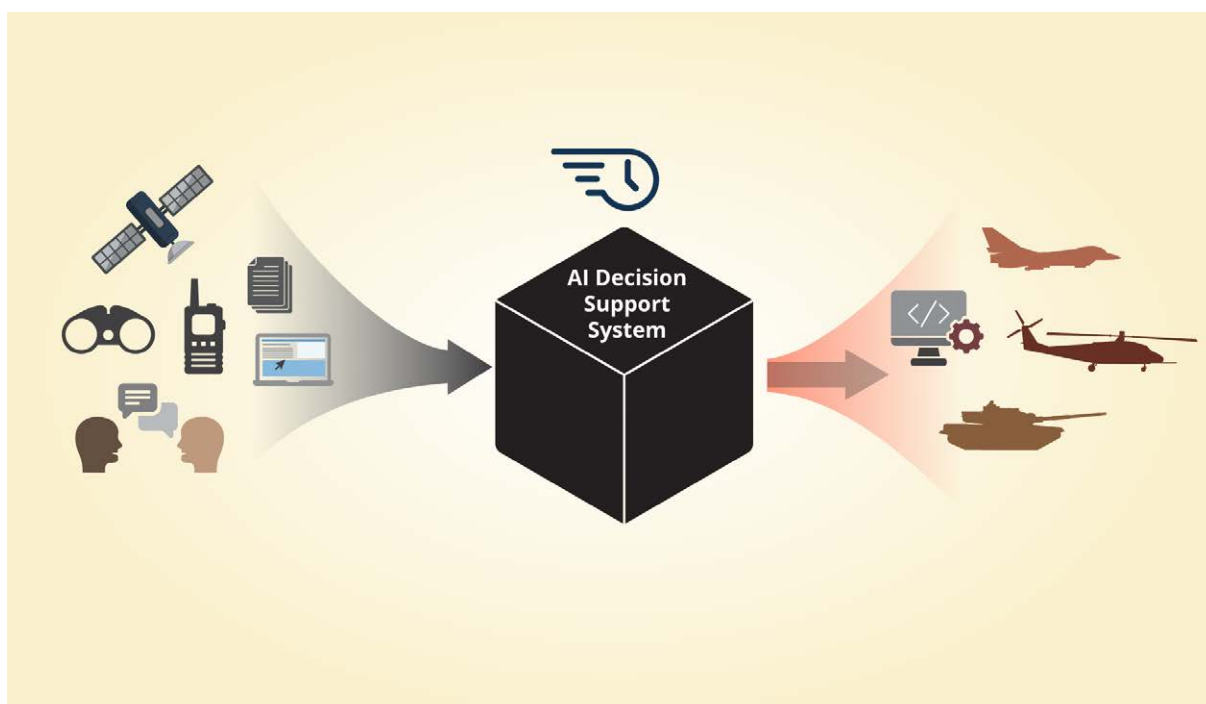
The integration of AI into military decision-making creates a dangerous paradox: while militarily advanced countries adopt these systems to reduce uncertainty on the battlefield, they simultaneously introduce new sources of unpredictability stemming from data vulnerabilities and the brittleness of algorithmic systems. This may lead to manipulation by adversaries and accidents. The gravest risk arises from the integration of AI into the command and control of nuclear arsenals and poses a governance challenge. The integration of AI in early warning systems, intelligence analysis and missile defense could threaten nuclear assets, creating multiple pathways for miscalculation and crisis instability as well as lowering their thresholds for nuclear use during a conflict.

Moreover, the speed at which AI systems operate compresses decision timelines. In a crisis scenario involving nuclear-armed states, AI-enabled systems might accelerate the tempo of operations to a pace where human leaders feel compelled to preemptively authorise responses before fully understanding the situation.

Accountability gaps and human oversight

IHL requires that human actors foresee, govern and constrain the use of weaponry. Yet, as AI systems evolve in sophistication and operate at unprecedented speeds, the scope for genuine human oversight diminishes significantly. Traditional legal frameworks presume human moral agency and deliberate decision-making; however, when an AI system is involved, assigning accountability becomes far more complex, compounding the risks of automation bias and over-reliance on AI-generated outputs.

The complexity of this issue is exacerbated by the inherent black box nature of many advanced machine learning systems. Despite their strong performance in testing environments, their underlying reasoning remains largely opaque. This lack of transparency in AI decision-making processes compromises the crucial human oversight required to uphold legal and ethical standards in military operations.



Military AI systems inherently depend on vast amounts of data for training, real-time operation and continuous learning. This dependence creates multiple vulnerabilities that adversaries can exploit. Consequently, an AI system that performs robustly in controlled testing environments may behave unpredictably in operational settings when confronted with manipulated or adversarial inputs. Data bias represents another critical concern. If AI systems are trained predominantly on data from specific operational environments or on particular adversary signatures, they may fail catastrophically when confronted with novel situations.

In sum, what is at risk is the erosion of moral and legal boundaries that limit the use of force, widening the gap between human accountability and emerging AI-driven military systems and creating destabilising effects.

The private sector: Blurring civilian-military boundaries

Military AI is primarily created by the private tech sector. Leading companies have made significant breakthroughs with both civilian and military applications. Private companies are creating sophisticated systems that the military then adapts for its needs. The dual-use and distributed nature of AI technology creates new challenges for establishing global governance.

The global nature of the AI industry further complicates governance and is leading to the militarisation of civilian AI research, potentially limiting academic freedom and international cooperation. These private companies control the development and deployment of AI, which could significantly alter global power dynamics. Power disparities between the advanced North and the developing South are likely to widen, as the vast majority of developing countries lack resources to compete for AI leadership or power to play a role in setting inclusive, just and fair rules for all.

Global governance: Significant gaps and concrete pathways forward

There are no universal rules or norms regarding the use of AI in military applications. However, efforts to regulate AI in the military began in 2017, following significant breakthroughs in machine learning and deep learning. There are three ongoing diplomatic processes.

“

The global nature of the AI industry further complicates governance and is leading to the militarisation of civilian AI research, potentially limiting academic freedom and international cooperation.

The first is state-led and focused on creating a new treaty on autonomous weapons at the UN in Geneva that involves all the major military powers. However, talks remain mired in definitional disputes and geopolitical tensions. The process is by consensus, so breakthroughs are hard to achieve. Two key questions that remain unresolved: (1) what constitutes meaningful human control over AI-enabled weapons?; and (2) how should IHL apply to AI decision-support systems? These talks could continue at the UN General Assembly which allows for a more inclusive process and require a two-thirds majority, but this approach may fail to get the major military powers' buy-in.

The second is led by middle power, small-state coalitions calling for the responsible use of AI in the military in two summits in 2023 and 2024. This process presents an innovative opportunity to forge new global governance that counts on the voices of more actors.

The third is the first resolution on autonomous weapons, a breakthrough event at the UN in New York in December 2023. The resolution received 164 votes in favour. Subsequently, on November 6, 2024, the second resolution, Resolution 79/239 *Artificial intelligence in the military domain and its implications for international peace and security*, received overwhelming support from UN Member States: 165 in favour and only two against. Middle powers and small states are likely to continue leading international efforts to develop norms.

However, several governance gaps remain unaddressed. First, there is no universally accepted risk framework for AI in military contexts. Second, confidence-building measures remain underdeveloped. Third, transparency around military AI development is severely limited. Nations keep their AI capabilities as closely guarded secrets, making it impossible for others to assess intentions or adjust their

own responses. This opacity fuels worst-case assumptions and promotes destabilising military race dynamics.

Pathways forward

Effective governance of AI in military decision-making requires a comprehensive approach across multiple domains and actors. Creating permanent institutional mechanisms to support global cooperation and permanent multi-stakeholder dialogue would foster trust through confidence-building measures and allow for lessons learned from high-stakes military AI applications and risk mitigation strategies. All of this could be guided by a responsibility by design framework that integrates ethical and legal compliance from the earliest development stages through the entire system lifecycle and into the socio-technical institutions where AI is used, while protecting human dignity.

“**The concrete governance framework for military AI should involve international confidence-building measures, transparency, legal accountability, technical safety safeguards and multi-stakeholder oversight.**”

References

General Literature

- The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, The Hague, 2025.
- Radin, A., Demus, A. and Evans, A. T., ‘A vocabulary of escalation: A primer on the escalation. Literature for military planners, RAND Corp., 2024.
- Vladislav Chernavskikh and Jules Palayer, *Impact of Military Artificial Intelligence on Nuclear Escalation Risk*, SIPRI Insights on Peace and Security, No. 2025/06 June 2025.
- ICRC, *Position on Autonomous Weapons Systems*, May 12, 2021, Geneva. Position and Background Paper.
- A/Res/78/241, Resolution adopted by the General Assembly on 22 December 2023, Lethal Autonomous Weapons Systems.
- United Nations General Assembly Resolution, First Committee, *Artificial intelligence in the military domain and its implications for international peace and security A/C.1/79/L.43*. 16 October 2024.
- Garcia, Denise. *The AI military race: Common good governance in the age of artificial intelligence*. Oxford University Press, 2024.
- Ancheta, Andrew. “U.S. Government Shutdown: How Will It Impact The Global Supply Chain?” *Forbes*, October 3, 2025. <https://www.forbes.com/sites/bernardmarr/2024/09/17/how-ai-is-used-in-war-today/>.
- Horowitz, Michael C. “Ukraine’s Operation Spider’s Web Shows Future of Drone Warfare.” *Council on Foreign Relations*, June 3, 2025. <https://www.cfr.org/expert-brief/ukraines-operation-spiders-web-shows-future-drone-warfare>.
- Humble, Kristian. “War, Artificial Intelligence, and the Future of Conflict.” *Georgetown Journal of International Affairs*, July 12, 2024. <https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict/>.
- Kirichenko, David. “Artificial Intelligence’s Growing Role in Modern Warfare.” *War Room - U.S. Army War College*, August 21, 2025. <https://warroom.armywarcollege.edu/articles/ais-growing-role/>.

The concrete governance framework for military AI should involve international confidence-building measures, transparency, legal accountability, technical safety safeguards and multi-stakeholder oversight. These steps aim to manage AI risks, prevent escalation, assign accountability and promote responsible development and deployment.

Conclusion

The integration of AI into military decision-making offers significant benefits, such as faster responses and fewer casualties, but also poses serious risks to stability and legal principles. The global community’s current governance systems are inadequate to manage these rapid technological advances, creating a troubling gap between AI development and regulatory frameworks.

Closing this gap requires sustained political will, creative institutional innovation and coordinated cooperation among nations with divergent interests and values. The stakes could not be higher. Left ungoverned, military AI could lower thresholds for conflict, compress decision timelines beyond human comprehension, blur the boundaries between peace and war, and ultimately undermine the institutions that have helped prevent great power war for eight decades.



- Lindelauf, Roy, and Herwin Meerveld. "Building Trust in Military AI Starts with Opening the Black Box." War on the Rocks, August 12, 2025.
- <https://warontherocks.com/2025/08/12/building-trust-in-military-ai-starts-with-opening-the-black-box/>.
- Mahon, Louis. "AI Ethics' Discourse Ignores Its Deadliest Use: War." Current Affairs, August 29, 2025. <https://www.currentaffairs.org/news/ai-ethics-discourse-ignores-its-deadliest-use-war>.
- Marr, Bernard. "How AI Is Used In War Today." Forbes, September 17, 2024. <https://www.forbes.com/sites/bernard-marr/2024/09/17/how-ai-is-used-in-war-today/>.

AI Governance and International Security Reports

- Afina, Yasmin, and Giacomo Persi Paoli. Governance of AI in the Military Domain. United Nations Institute for Disarmament Research (UNIDIR), 2024.
- Bode, Ingvild, et al. Global Governance Prospects for AI in the Military Domain. 2023.
- Bruun, Laura. Towards a Two-Tiered Approach to Regulation of Autonomous Weapon Systems: Identifying Pathways and Possible Elements. Stockholm International Peace Research Institute (SIPRI), August 2024.
- European Defence Agency. Trustworthiness for AI in Defence (TAID): White Paper - Developing Responsible, Ethical, and Trustworthy AI Systems for European Defence. Publication version 1.0, May 9, 2025.
- IEEE SA Research Group on Issues of Autonomy and AI in Defense Systems. A Framework for Human Decision Making Through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications. New York, NY: IEEE SA, 2024.
- Persi Paoli, Giacomo, Yasmin Afina, Sarah Grand-Clement, Ioana Puscas, Shimona Mohan, and Jessica Abowitz. Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security: An Evidence-Based Road Map for Future Policy Action. Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2025.
- Puscas, Ioana. AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures. United Nations Institute for Disarmament Research (UNIDIR), 2024.
- Veale, Michael, Kira Matus, and Robert Gorwa. "AI and Global Governance: Modalities, Rationales, Tensions." Annual Review of Law and Social Science 19 (2023): 255-275.

Conference Papers and Working Documents

- Bode, Ingvild, et al. "Global Governance of Autonomous Weapons: Prospects from the Stockholm Group." Paper presented at the International Studies Association (ISA) Conference, April 2023.

Magazine Articles

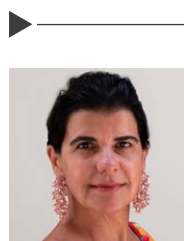
- Foreign Affairs. "The AI Power Paradox: Can States Learn to Govern AI Before It's Too Late?" Foreign Affairs 102, no. 5 (September/October 2023): 26-43.

Key Standards and Technical Documents Referenced

- International Organization for Standardization (ISO/IEC). ISO/IEC 22989:2022 Information Technology - Artificial Intelligence - Artificial Intelligence Concepts and Terminology. 2022.
- International Organization for Standardization (ISO/IEC). ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML). 2022.
- International Organization for Standardization (ISO/IEC). ISO/IEC TR 24029-(1-2-3):2021 Artificial Intelligence (AI) - Assessment of the Robustness of Neural Networks. 2021.
- International Electrotechnical Commission (IEC). IEC 61508:2010 Functional Safety Standard. 2010.
- European Standards (EN). EN 50129:2019 Railway Applications - Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling. 2019.
- IEEE Standards Association. IEEE 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being. New York, 2020.
- IEEE Standards Association. IEEE 7001-2021 IEEE Standard for Transparency of Autonomous Systems. 2021.

Regulatory Documents

- European Commission. Artificial Intelligence Act (Regulation (EU) 2024/1689). Official Journal, July 12, 2024.
- European Union Council. Council Decision (EU) 2022/2349 of 21 November 2022 Authorising the Opening of Negotiations on Behalf of the European Union for a Council of Europe Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. Brussels: Council of the European Union, 2022.
- European Union. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Preparation for COREPER). Interinst. File 2021/0106(COD), Brussels, 2022. <https://perma.cc/564K-RCKR>
- OECD. Explanatory Memorandum on the Updated OECD Definition of an AI System. 2024.
- U.S. Department of Defense. U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway. DoD Responsible AI Working Council, June 2022. https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf



About the author

Denise Garcia is a Professor of Political Science and International Affairs at Northeastern University and a founding faculty member of its Experiential Robotics Institute. She is also a Commissioner at the Global Commission on Responsible AI in the Military.