



**GC REAIM**

GLOBAL COMMISSION ON RESPONSIBLE  
AI IN THE MILITARY DOMAIN



تريندز للبحوث والاستشارات  
TRENDS RESEARCH & ADVISORY



Foreign, Commonwealth  
& Development Office

# GC REAIM Expert Policy Note Series

## The Tactical Governance of Artificial Intelligence in the Military Domain

Giacomo Persi Paoli and Yasmin Afina

May 2025

POWERED BY



The Hague Centre  
for Strategic Studies

# GC REAIM Expert Policy Note Series

## The Tactical Governance of Artificial Intelligence in the Military Domain

**Authors:** Giacomo Persi Paoli and Yasmin Afina

May 2025

Cover photo: [unsplash](#)

The Global Commission on Responsible Artificial Intelligence in the Military Domain (GC REAIM) is an initiative of the Government of the Netherlands that was launched during the 2023 REAIM Summit on Responsible Artificial Intelligence in the Military Domain in The Hague. Upon request of the Dutch Ministry of Foreign Affairs, the Hague Centre for Strategic Studies acts as the Secretariat of the Commission.

The GC REAIM Expert Policy Note Series was funded by the Foreign, Commonwealth and Development Office (FCDO) of the United Kingdom. GC REAIM Experts maintained full discretion over the topics covered by the Policy Notes. The contents of the GC REAIM Expert Policy Note series do not represent the views of the Global Commission as a whole. The Policy Notes are intended to highlight some key issues around the governance of AI in the military domain and provide policy recommendations. This Policy Note was released during the Commission Meeting in Abu Dhabi, hosted and graciously supported by Trends Research and Advisory.

© The Hague Centre for Strategic Studies. All rights reserved. No part of this report may be reproduced and/ or published in any form by print, photo print, microfilm or any other means without prior written permission from HCSS. All images are subject to the licenses of their respective owners

HCSS  
Lange Voorhout 1  
2514 EA The Hague

Follow us on social media:  
[@hcssnl](#)

The Hague Centre for Strategic Studies  
Email: [info@hcss.nl](mailto:info@hcss.nl)  
Website: [www.hcss.nl](http://www.hcss.nl)



تريندز للبحوث والاستشارات  
TRENDS RESEARCH & ADVISORY



The Hague Centre  
for Strategic Studies

# 1. Introduction

Military adoption of artificial intelligence (AI) is accelerating. As with previous waves of military innovation – from precision-guided munitions to space-based navigation and cyber operations – the integration of AI presents both extraordinary potential and novel risks. Critical questions are thus being raised about how to govern AI in the military domain.

AI can bring novel governance challenges and make existing ones more complex. Much attention has focused on governance at the strategic level – such as international law and treaties. However, effective oversight must also extend across its entire life cycle of an AI technology<sup>1</sup> – from initial concept to decommissioning – including the systems, processes and institutional practices that shape how AI is actually developed, fielded and used by military forces.

The defence sector is already regulated through a combination of hard law and a constellation of other tools that may not be legally binding in nature but that play a decisive role in how military systems are conceptualized, developed, acquired, deployed and retired.<sup>2</sup> To ensure that innovation proceeds in a way that is not only operationally effective but also ethically and legally sound it is thus key that governance is embedded throughout the entire life cycle of military AI via these policy, doctrine, procurement, training and accountability tools.

This policy note examines these tools. Section 2 first provides a general introduction to existing governance tools for military technology. Section 3 then takes a deep dive into eight selected operational, procedural and institutional mechanisms already in use within military structures and shows how they could be used by the defence sector to influence, and at times regulate, the life cycle of a military AI system. Section 4 concludes by proposing a potential pathway to action.

---

<sup>1</sup> For the purpose of this policy note (and without prejudice to existing approaches), the life cycle of an AI technology includes the following phases: pre-design, design, development, testing, deployment, use, sale, procurement, operation and decommissioning. These align with those included in United Nations General Assembly resolution: UN General Assembly (79th Sess.: 2024-2025), 'Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security :: Resolution /: Adopted by the General Assembly, 31 December 2024, <https://digitallibrary.un.org/record/4071348>.

<sup>2</sup> It should be acknowledged that the strength or degree of sophistication of such internal governance mechanisms varies between states and that they only harmonize to the degree that such harmonization brings military advantage (e.g. within military alliances).

## 2. Existing Tools for Governance of Military Technology

Militaries and governments have long used various mechanisms to govern the development, acquisition and use of advanced technologies and weapons. These range from hard law (i.e., formal rules that carry legal force) to soft law (i.e., measures, guidelines or processes that shape behaviour without strict legal mandates or enforcement). Understanding these existing tools is the first step in applying them in the context of AI in the military domain.

At the higher, strategic level is international law as embodied in the United Nations Charter and the Geneva Conventions. This is supplemented by a range of international and regional instruments, treaties and conventions, national laws and regulations as well as export control measures or other forms of limitations on the trade in specific (military or dual-use) technologies. In addition, the strategic level can include voluntary measures such as norms of responsible behaviour and confidence-building measures.<sup>3</sup>

Beyond these high-level instruments are governance mechanisms that military forces – and the defence sector more broadly<sup>4</sup> – develop, apply and leverage to guide development, acquisition and deployment of military capabilities. These mechanisms, which are more grounded in practice and operations, range from specific instruments designed to promote innovation to those that shape procurement and acquisition processes and the integration, use, review and disposal of technology.

These are referred to here as “tactical governance”<sup>5</sup> tools – understood as institutional and procedural mechanisms within the defence apparatus that shape the life cycle of technologies, distinct from but complementary to strategic-level governance such as international law or arms control treaties. While not always codified in law, these

---

<sup>3</sup> These include, for example, the norms and confidence-building measures agreed by consensus by all United Nations Member States in the context of international security of information and communications technology (ICT). See: ‘Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA’, accessed 6 May 2025, <https://disarmament.unoda.org/ict-security/>.

<sup>4</sup> For the purpose of this policy note, “military forces” refers specifically to the various services or front line commands of the armed forces (e.g., army, navy, air force, cyber command, joint command, special operations forces, etc.), while “defence sector” includes also those structures that are not part of the armed forces per se but are part of the broader national defence ecosystem (e.g., civilian ministries or departments of defence, national armaments directorates in charge of procurement, committees and other agencies). National intelligence services differ between states but can be part of the defence ecosystem.

<sup>5</sup> Tactical governance, as used in this policy note, is not to be confused with the military definition of “tactical,” which typically refers to short-term battlefield planning or unit-level operations. Rather, the term here captures the applied, operational character of governance tools situated between high-level legal frameworks and on-the-ground implementation.

instruments play a decisive role in ensuring accountability, safety and compliance with existing regulatory frameworks.

Tactical governance tools require deeper analysis for three main reasons. First, the current geopolitical context makes creation of new conventions or negotiation of treaties difficult. Yet, as AI technology continues to diffuse rapidly, it is important to highlight what states could do to mitigate risks. Second, even when focusing exclusively on existing legal obligations, there is an urgent need to illustrate how these can be translated into operational guidance and practice. Lastly, there is already an extensive scholarship covering the more strategic instruments such as international law and the different proposals for treaties, conventions and trade controls, while the potential benefits of tactical tools remain underexplored. Given the contemporary importance of such tools, the next section sheds additional light on them.



## 3. Unpacking Tactical Governance of AI in the Military Domain

This section examines how military forces and the national defence apparatus more broadly can influence and shape an AI capability throughout its life cycle.

### 3.1 Influencing Ideas and Concepts: The Importance of National Strategies and Principles

A **national AI strategy for defence** can be leveraged to set clear expectations on responsible innovation, procurement, integration and operational use. With such a strategy, governments can shape and frame the entire AI life cycle. Such a strategy could, for example, outline regulatory requirements, establish oversight bodies, and incentivize safe and ethical AI development, testing and evaluation through dedicated funding and research initiatives.<sup>6</sup> A second soft governance tool with potential benefits throughout the life cycle of an AI system consists of **ethical principles and guidelines** for the design and deployment of military applications of AI. They could emphasize, for example, transparency, accountability and bias mitigation.

**Ethical principles** can be part of the national AI strategy or can be released as a first, preparatory step towards the development of a strategy.<sup>7</sup> While not enshrined in law, these ethical principles influence the entire life cycle of AI: from pre-design (e.g., setting responsible use as a requirement), via development (e.g., asking engineers to document, ensure transparency in the training and testing data used, and test for biases, etc.), to deployment (e.g., requiring commanders to understand AI limitations and the preservation of accountability, and integrating monitoring and auditing solutions to detect possible new biases).

These ethical principles, agreed at high levels, can trickle down into military planning documents, training and best practices. They serve as a compass to guide officers and

---

<sup>6</sup> For more information on the development of national strategies for AI in defence, including procedural and substantive considerations, see: Yasmin Afina, 'Draft Guidelines for the Development of a National Strategy on AI in Security and Defence', 24 October 2024, <https://unidir.org/publication/draft-guidelines-for-the-development-of-a-national-strategy-on-ai-in-security-and-defence/>.

<sup>7</sup> See, for example, NATO's principles of responsible use included in its AI Strategy (released in 2021 and revised in 2024) or the five AI ethical principles released by the United States Department of Defense in 2020: 'DOD Adopts 5 Principles of Artificial Intelligence Ethics', U.S. Department of Defense, accessed 6 May 2025, <https://www.defense.gov/News/News-Stories/article/article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/>; 'NATO Review - An Artificial Intelligence Strategy for NATO', NATO Review, 25 October 2021, <https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html>; NATO, 'Summary of NATO's Revised Artificial Intelligence (AI) Strategy', NATO, accessed 6 May 2025, [https://www.nato.int/cps/en/natohq/official\\_texts\\_227237.htm](https://www.nato.int/cps/en/natohq/official_texts_227237.htm).

developers when formal law may not yet specify what to do. For example, member states of the North Atlantic Treaty Organization (NATO) have committed to a series of principles of responsible use, which form a key component of the alliance's AI Strategy. These principles, which fundamentally rest on ethical guidelines, include explainability and traceability, reliability, governability, and bias mitigation.

However, ethical principles must be more than slogans: they should be integrated into the daily work of AI developers and users. One way to achieve this is to establish **ethics review boards** or advisory committees for military AI projects.<sup>8</sup> This type of multidisciplinary body, comprising ethicists, legal experts and experienced officers, can evaluate proposed AI applications at the concept stage for alignment with principles. For example, a board can ask whether the project plan addresses bias mitigation and provides an appropriate degree of transparency. Its feedback can then guide procurement, design, testing and subsequent use requirements.

### 3.2 Shaping Innovation: Incentivizing Ethics, Safety and Security of AI through Targeted Funding Mechanisms

The defence sector can play a proactive role in shaping AI innovation by leveraging incentive-driven mechanisms such as **grand challenges, innovation prizes and targeted funding programmes**.<sup>9</sup> These initiatives, if applied to AI, could encourage and incentivize industry and academia to develop AI capabilities that align with military needs while embedding safety, security, ethics and operational requirements from the outset. They can do this by incentivizing, for example, reliability and explainability in AI and decision-support systems.

### 3.3 Steering the Market: Leveraging Procurement Processes for AI Development

Military organizations can use **procurement policies** to shape the design and development of AI systems. Calls for tender and defence contracts can specify requirements for transparency, explainability and safety in AI, thereby leveraging purchasing power as a governance tool.

---

<sup>8</sup> For example, the French Ministry of Armed Forces established a permanent Defence Ethics Committee in January 2020 to address ethical issues arising from new technologies in the defence field, providing the minister with insights on scientific and technical innovations.

<sup>9</sup> Examples in the military domain include the US Army's xTech AI Grand Challenge, Australia's Grand Challenges programme and the US Defense Advanced Research Projects Agency's Cyber Grand Challenge: 'Cyber Grand Challenge (CGC)', n.d., <https://www.darpa.mil/research/programs/cyber-grand-challenge>; Defence Science and Technology Group, 'Grand Challenges for Safeguarding Australia', 10 July 2014, <https://www.dst.defence.gov.au/grand-challenges>; 'XTech AI Grand Challenge – XTechSearch', n.d., <https://xtech.army.mil/competition/xtech-ai-grand-challenge/>.

Standard **military acquisition protocols** in many countries already demand extensive testing and validation for military systems.<sup>10</sup> In the case of AI, these processes should include rigorous bias detection, adversarial testing and explainability assessments to ensure reliable and ethical deployment. For example, the United States Department of Defense's updated directive on autonomy in weapon systems explicitly calls for "rigorous hardware and software verification and validation (V&V) and realistic system developmental and operational test and evaluation".<sup>11</sup> It even adds requirements for AI transparency and explainability in design, instructing that systems should be auditable and explainable to relevant personnel.

Finally, militaries should explore **standardized certification frameworks** for AI safety and reliability, modelled on existing military specifications for software and cybersecurity. Although these requirements are not laws, they function as internal standards that developers must meet in order to obtain military contracts.

In effect, procurement rules can embed ethical and safety expectations. This makes such rules a form of "soft law" that leverages contracting power to shape industry behaviour. For example, it can impose compliance with certain system safety and cybersecurity standards before a formal development decision is taken or can set specific testing and evaluation processes before fielding.

### 3.4 Conceptualizing Capability Development and Operations: The Role of Military Doctrine

In general terms, **military doctrine serves as a foundation for how a military organization prepares for and conducts warfare**. It encompasses everything from broad strategies to specific tactics and operational procedures. A doctrine establishes a shared understanding and language among military personnel, ensuring that everyone is on the same page when it comes to approaches to military operations. It also presents codified best practices on how to accomplish military goals and objectives based on analysis of experience and lessons learned.

A military doctrine is never static: it evolves and adapts to changing and novel threats, technologies and operational environments, reflecting ongoing learning and development within the military. In this spirit, existing military doctrines (e.g. for land, air and naval warfare) could, or should, be adapted to include specific guidance on the integration of AI in different domains of warfare and in multi-domain operations. Where relevant, other critical national doctrines (e.g. on nuclear or biological defence) could be reviewed to reflect the impact of AI, both as a threat and as a tool.

---

<sup>10</sup> See, for example, the US Department of Defense's standard practice MIL-STD-882E for system safety: 'System Safety Engineering – DoD Research & Engineering, OUSD(R&E)', accessed 6 May 2025, <https://www.cto.mil/sea/sse/>.

<sup>11</sup> 'DoD Announces Update to DoD Directive 3000.09, "Autonomy In Weapon Systems"', U.S. Department of Defense, accessed 6 May 2025, <https://www.defense.gov/News/Releases/Release/article/3278076/dod-announces-update-to-dod-directive-300009-autonomy-in-weapon-systems/><https://www.defense.gov/News/Releases/Release/article/3278076/dod-announces-update-to-dod-directive-300009-autonomy-in-weapon-systems/>.



In addition, military organizations could develop new doctrine dedicated to the integration of AI into operations by defining its role, capabilities and constraints, ensuring alignment with ethical principles and legal requirements. In recognition of the sensitivities associated with use of AI in the military domain, states may decide not to make such doctrines available in the public domain. However, to foster trust and transparency, they may instead consider the release of a shortened, sanitized and unclassified summary.

### 3.5 Guiding Operations: Standard Operating Procedures and Other Tools for Users of AI Systems

Militaries already use operational frameworks such as **standard operating procedures (SOPs), tactics, techniques and procedures (TTPs), logbooks, and after-action reviews (AARs)** to govern behaviour on the battlefield, including the use of systems and technology. These instruments ensure consistency in operations, document best practices and provide structured learning mechanisms to refine military applications over time. AI integration could follow this model:

- *SOPs for AI Systems*: Military AI systems should be governed by SOPs that detail roles and responsibilities, operational limits, verification steps and emergency disengagement procedures. For instance, several armies have developed detailed SOPs for the operation of unmanned aerial vehicles (UAVs), which include clear steps for handover procedures, loss-of-signal contingencies and emergency landing protocols. These serve as a model for how SOPs could govern AI-enabled systems by, for example, prescribing pre-mission system checks, defining approval authority for activation, specifying acceptable operational parameters, and outlining manual override protocols in the event of malfunction or target ambiguity.
- *TTPs for AI in Combat and Intelligence*: Military forces should develop AI-specific TTPs that outline how AI-driven decision aids, surveillance tools and autonomous systems interact with human operators in the field. For example, these procedures could outline how a human analyst should interpret AI-generated object-recognition alerts, validate targets and escalate decision-making.
- *Logbooks and Incident Reporting*: Pilots and cyber operators maintain detailed logs of system performance, actions and decisions taken, as well as incidents. Similarly, AI-driven systems should be required to generate detailed audit trails, and operation rooms should maintain a logbook detailing all orders and instructions related to the use of AI systems. These logs would serve both operational and accountability purposes, ensuring transparency and enabling forensic reviews when necessary (e.g., in the conduct of investigations for alleged violations of international humanitarian law).
- *AARs and Continuous Learning*: Militaries conduct AARs to evaluate missions, to analyse system performance, coordination gaps and technology limitations, to identify lessons learned, and to refine future operations. AI deployment should be subject to the same process, with structured AARs to assess AI performance, ethical compliance and unintended consequences.

By embedding AI governance in existing military documentation and operational review mechanisms, policymakers can ensure that AI technologies are integrated in a structured, responsible manner that aligns with existing military best practices.

### 3.6 Regulating Deployment and Use: Rules of Engagement for AI Systems

**Rules of engagement (ROE)** define the circumstances and limitations under which military forces may engage adversaries, ensuring alignment with operational goals and legal frameworks. They cover a broad range of issues to ensure compliance with national and international laws, ranging from geographical limitations to specific requirements or thresholds for positive target identification and the use of force. ROE vary between peacetime and wartime; some are standing and others adapt dynamically to the specific operational context. Who has the authority to request and authorize the entry into force of such an adapted rule follows a specific hierarchical structure.

In the context of AI, once an AI system is fielded, rules of engagement can, and should, be used to govern the manner of its use. Militaries should thus update their ROE and targeting protocols to account for AI. For example, ROE might stipulate that an AI decision aid can flag targets, but that a human operator must always confirm before lethal engagement – encoding “human-on-the-loop” or “-in-the-loop” requirements into operational orders. Conversely, an additional ROE that requires a higher level of authorization to be granted could be used to determine the parameters to authorize a “human-off-the-loop” scenario. This could apply, for example, in the context of air defence such as when a warship or a military base is targeted by a swarm of UAVs or a large number of missiles. In the context of AI-enabled autonomous systems, ROE could impose limits such as geofences (i.e., an AI weapon may not operate outside a defined area) or time limits (i.e., an autonomous system may only act within a certain timeframe before requiring human check-in).<sup>12</sup> These operational frameworks would ensure that, even after deployment, AI behaviour stays within predictable and controllable bounds.

Another important aspect that ROE can reinforce is **accountability**: militaries should clarify that commanders, operators and users are fully responsible for outcomes of AI use. This reasserts the principle that legal responsibility under international law will always rest on states (e.g., under international humanitarian law) and individuals (e.g., under international criminal law), leaving in principle no room for accountability gaps. This may be codified in military justice systems or policy memos to prevent any de facto accountability gap.

---

<sup>12</sup> This is aligned with the updated DOD Directive 3000.09, which requires systems to be designed to complete engagements within a specified timeframe and geographic area, as well as with the position of the International Committee of the Red Cross (ICRC) on autonomous weapon systems: ‘ICRC Position on Autonomous Weapon Systems | ICRC’, 12 May 2021, <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems>.

It should, however, be noted that the entire military chain of command and control and decision-making architecture is built on the principle of delegated authority. This clearly regulates the dynamic distribution of power and authority from the political level, through the various echelons of military leadership, down to the operator. The processes are designed to be dynamic and to respond to the needs on the battlefield, with specific procedures governing each step. This is even more relevant to the use of force, where strict processes and procedures exist to request and delegate authority for weapons release (activation and use). As such, while a specific provision covering AI might be a useful clarification, the architecture to avoid an accountability gap is already in place.

### 3.7 Empowering Humans: Training and AI Competency Development

Implementing AI responsibly requires **comprehensive and structured training programmes** tailored to different roles within the military.<sup>13</sup> Financial and technical resources should be specifically dedicated for these programmes. Training should educate operators, developers and commanders on the limitations, risks, ethical considerations and system vulnerabilities of AI.

Training is a key component of calibrating the trust that humans put in technology. It is needed to avoid both automation bias (i.e., overly trusting the outputs of a machine) and algorithmic aversion (i.e., never trusting the outputs of a machine) as well as the misuse or disuse of the technology (i.e. used in the wrong way, or for the wrong purpose). AI literacy – beyond technical knowledge but also including ethics, security and operational safety – should be embedded in all strands of military education. This would ensure that personnel understand the principles of AI decision-making, data biases and adversarial threats.

Exercises and simulations should also incorporate AI-human teaming scenarios to refine best practices, validate oversight mechanisms and stress-test AI decision aids under realistic battlefield conditions. Live and virtual training environments should include AI-based tools to familiarize personnel with automation-assisted operations, develop rapid-response protocols, and establish criteria for human override and disengagement.

### 3.8 Managing Obsolescence: Decommissioning, Sale and Transfer of AI Systems in the Military Domain

**Obsolescence management** at the end of a technology's life cycle is an important aspect of any military system that is often overlooked. AI systems, like other military technologies, require structured policies for their decommissioning and end-of-life phase. Proper obsolescence management should ensure that outdated AI does not pose

---

<sup>13</sup> See for example the Reliable Artificial Intelligence (RAI) Toolkit launched by the US Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO): 'RAI Toolkit Executive Summary', Reliable AI Toolkit, n.d., <https://rai.tradewindai.com/executive-summary>.

security risks due to vulnerabilities, performance degradation or adversarial exploitation.<sup>14</sup>

Governments should establish **decommissioning protocols** that include the secure retirement of AI systems, ensuring compliance with cybersecurity standards and preventing unauthorized repurposing. Additionally, **maintaining records of AI performance and updates** throughout a system's life cycle will help evaluate when the system should be retired.

One key concern in AI decommissioning is the sale or donation of obsolete AI systems to less advanced militaries as a form of military support or engagement. While arms sales and other government-to-government transfers are common in defence cooperation, the transfer of outdated AI presents risks. These include potential misuse, failure in high-stakes environments or exploitation by an adversary that reverse-engineers the technology. Policymakers should establish **strict controls and monitoring frameworks for AI decommissioning** that ensure that transferred systems undergo security vetting, do not violate international norms and maintain built-in safeguards to prevent unauthorized modifications.

Additionally, AI systems with learning capabilities may retain biases or strategic patterns from their original deployments. If transferred without thorough reconfiguration, these legacy biases could lead to unintended consequences in new operational contexts. To mitigate this, defence organizations should implement **comprehensive AI revalidation and retraining protocols** before repurposing or selling AI-driven military technology.

By integrating decommissioning and obsolescence management into AI governance, militaries can minimize risks associated with outdated AI while ensuring responsible disposal, ethical resale and continued security compliance throughout the system's life cycle.

---

<sup>14</sup> Yasmin Afina and Giacomo Persi Paoli, 'Governance of Artificial Intelligence in the Military Domain: A Multi-Stakeholder Perspective on Priority Areas', 9 May 2024, <https://unidir.org/publication/governance-of-artificial-intelligence-in-the-military-domain-a-multi-stakeholder-perspective-on-priority-areas/>.

## 4. Conclusion: A Pathway for Action

Drawing on the analysis above, existing military governance tools provide a viable mechanism to strengthen the governance of AI in the military domain at a more operational level. This approach is intended to offer an impactful complement and supplement to the higher levels of governance and the associated obligations emanating from existing public international law (including its branches such as *jus ad bellum* and international humanitarian, human rights and criminal law and regional and national laws and regulations).

Based on the analysis in this policy note, and within the broader context of ongoing multilateral discussions on this issue, policymakers could consider implementing the following steps to strengthen AI governance in military contexts:

1. **Develop national AI strategies and principles** designed specifically to guide the entire life cycle of military AI systems. These strategies could also include the creation and establishment of dedicated oversight and governance bodies.
2. **Integrate ethical AI and legal principles** into defence innovation and acquisition processes by making them requirements for military AI projects. This should include strengthening AI assurance, testing, evaluation and certification processes.
3. **Adapt** existing, or develop new as required, **military documentation** – including doctrines, standard operating procedures, tactics, techniques and procedures, logbooks, and after-action reviews, among others – to account for the impact that AI will have on the conduct of warfare.
4. **Review** existing **rules of engagement** and develop new ones as required to ensure that the chain of accountability remains clear to operators and decision makers even with the introduction of AI, and that military operations can be conducted in full compliance with international and national legal frameworks.
5. **Invest in** the human by improving **knowledge and training** at the individual level as well as at the unit and force levels to promote better understanding of AI systems and how such systems may change the conduct of operations.
6. **Design** tailored approaches to **obsolescence management** for AI systems to ensure that outdated AI does not pose security risks due to vulnerabilities, performance degradation or adversarial exploitation. This includes a responsible approach to the transfer of outdated AI systems to third parties, domestically and internationally.

By taking these steps, policymakers can ensure that military AI development does not occur in a legal or ethical vacuum, but rather is guided by the same rigour that governs traditional military operations and has guided the integration of other transformative technologies. The dual promise and peril of AI will be best managed by **proactive governance embedded at every stage**, using the hard power of law and the influence of other tools together to steer military AI towards safe and principled use. Early governance will not stifle innovation; rather, it will foster **trustworthy innovation**, ensuring that militaries can leverage AI's advantages without compromising on the rule of law or losing public confidence.




# About the Authors

## Dr Giacomo Persi Paoli

Giacomo is the Head of the Security and Technology Programme at the United Nations Institute for Disarmament Research (UNIDIR). His expertise spans the science and technology domain with emphasis on the implications of emerging technologies for security and defence.

## Dr Yasmin Afina

Yasmin Afina is a Researcher for the Security and Technology Programme at UNIDIR, where her research covers the intersection between international security policy, international law and artificial intelligence.



HCSS  
Lange Voorhout 1  
2514 EA The Hague

Follow us on social media:  
[@hcssnl](#)

The Hague Centre for Strategic Studies