# RESPONSIBLE PROCUREMENT OF MILITARY ARTIFICIAL INTELLIGENCE

NETTA GOUSSAC AND VINCENT BOULANIN

**STOCKHOLM INTERNATIONAL**
**PEACE RESEARCH INSTITUTE**

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

**STOCKHOLM INTERNATIONAL**
**PEACE RESEARCH INSTITUTE**

Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

# RESPONSIBLE PROCUREMENT OF MILITARY ARTIFICIAL INTELLIGENCE

NETTA GOUSSAC AND VINCENT BOULANIN

February 2026

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

DOI: https://doi.org/10.55163/YOLG1827

# Contents

# Acknowledgements

SIPRI and the authors express their sincere gratitude to the Mobilizing Insights in Defence and Security (MINDS) programme of the Canadian Department of National Defence and to the Ministry of Defence of the Netherlands for their generous financial support for this project.

The authors thank the interviewees and workshop participants from governments, think tanks and academia for generously giving their time and expertise during research for this report. The authors also thank SIPRI colleagues Alexander Blanchard, Laura Bruun, Rafael Lipcsey, Jules Palayer, Lorenzo Scarazzato and Caspar Trimmer for their insights and support throughout the project and the writing of this report.

# Abbreviations

| | |
|---|---|
| AI | Artificial intelligence |
| API | 1977 Protocol Additional to the 1949 Geneva Conventions, and Relating to the Protection of Victims of International Armed Conflicts |
| AUKUS | Australia–United Kingdom–United States of America |
| CCW | Convention on Certain Conventional Weapons (1981 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects) |
| CDAO | Chief Digital and Artificial Intelligence Office within the US DOD |
| CO | Component organization of the British MOD |
| CSO | Commercial solutions opening of the US DOD |
| CNAS | Center for New American Security |
| CRS | Congressional Research Service |
| CSIS | Center for Strategic and International Studies |
| DIU | Defense Innovation Unit of the US DOD |
| DIUx | Defense Innovation Unit Experimental |
| DOD | Department of Defense of the United States (also designated the Department of War) |
| DND | Department of National Defence of Canada |
| DSB | Defense Science Board within the US DOD |
| EU | European Union |
| GC REAIM | Global Commission on Responsible AI in the Military Domain |
| GGE on LAWS | Group of Governmental Experts on Lethal Autonomous Weapons Systems, under the auspices of the CCW |
| ICRC | International Committee of the Red Cross |
| IHL | International humanitarian law |
| IPM | Integrated Procurement Model of the British MOD |
| MOD | Ministry of Defence of the United Kingdom |
| NATO | North Atlantic Treaty Organization |
| REAIM | Responsible AI in the Military Domain |
| S&I | Strategy and implementation |
| SVDG | Silicon Valley Defense Group |
| TEVV | Testing, evaluation, validation and verification |
| UNIDIR | United Nations Institute for Disarmament Research |

# Executive summary

This report examines the intersection of military procurement and responsible military artificial intelligence (AI). The primary function of military procurement is to bridge a military's strategic needs and its operational capabilities through the identification of capability gaps, engagement with industry, solicitation and evaluation of proposals, and testing and acceptance of delivered capabilities. In practice, procurement is also a mechanism by which states implement policy commitments and legal obligations. For that reason, procurement can serve as a mechanism for implementing responsible military AI, but only if deliberately structured to do so.

This report investigates why and how states are adapting their procurement processes to accelerate military AI adoption, and why and how states should seize these opportunities to give effect to their legal obligations and high-level policy commitments related to responsible military AI.

In a tense geopolitical environment characterized by strategic competition and lessons drawn from contemporary armed conflicts, many militaries are under pressure to accelerate procurement, deployment and scaling of AI capabilities. The distinctive characteristics of AI capabilities are challenging traditional defence procurement processes. States are seeking to facilitate rapid acquisition of military AI by adapting procurement pathways, including by (*a*) deepening collaboration with suppliers to better match capability needs with products; (*b*) adopting more iterative procurement processes; and (*c*) trying different methods to achieve assurance about lawfulness, safety and reliability.

How these states are implementing their commitments to responsible military AI (where they exist) within adapted procurement processes remains difficult to establish. However, states' legal obligations and policy commitments to responsible military AI do have practical implications for procurement. These legal and policy frameworks require procurement authorities to interrogate whether and why a military AI capability is needed; maintain independent capacity to test supplier claims; and ensure clear lines of communication and responsibility in procurement decision-making.

States' efforts to adapt their procurement processes provide an opportunity to operationalize these obligations and commitments. Collaborative engagement with industry can become a mechanism for interrogating capability needs. Iterative processes can clarify lines of responsibility if accountability mechanisms are embedded at each decision point. Efforts to achieve trustworthy assurance can support the development of capacity and best practice in testing and evaluation.

### Based on these findings, the report makes three recommendations.

*1. States should adapt their procurement processes to give effect to high-level obligations and commitments to responsible development and use of military AI.*

The procurement process offers significant opportunities for embedding responsible AI considerations. For example, the requirements specification stage—when a military's task is to develop explicit, testable and contractable requirements before issuing tenders or requests for proposals—should consider principles of responsible behaviour, rather than attempting to 'retrofit' them at a later stage. Similarly, the contracting stage is a critical opportunity for implementing principles of responsible behaviour because it determines what the supplier must deliver and prove (including claims about the results of testing and assurance processes), who is accountable for certain risks and failures, and what obligations and requirements are borne by the parties. An important first step is to ensure that policies, procedures and practices relating to military procurement explicitly refer to any national laws, policies and commitments related to responsible military AI. However, the specific measures necessary to give effect to high-level legal obligations and policy commitments to responsible military AI involve a number of challenges—such as the technical literacy needed to interrogate whether and why a military AI capability is needed and to assess supplier claims, the opacity of some AI capabilities, commercial sensitivities and the iterative nature of AI development—that demand further work.

*2. States should develop and publish documents articulating clear expectations for suppliers of military AI capabilities*.

Suppliers of military AI capabilities—from established defence industry companies to tech start-ups—need clarity and certainty about what military clients expect from the AI capabilities they procure. Without such guidance, procurement authorities and suppliers alike face a more complex process of pre-contract evaluation, back-and-forth requests for documentation and uncertainty around requirements. States should make public their expectations of suppliers, addressing the technical parameters and performance standards necessary to implement principles of equitability and bias mitigation, traceability and explainability, reliability and security, accountability and governability. Such documents should aim to translate abstract principles into concrete specifications regarding acceptable error rates, confidence thresholds, documentation requirements and testing protocols. Clear articulation of expectations offers potential benefits. It could enable suppliers to design systems that meet responsible military AI requirements from inception rather than requiring costly retrofitting; facilitate more efficient procurement processes by reducing ambiguity and iteration; and help states find alignment between national procurement processes and policy commitments to responsible military AI and relevant legal obligations.

*3. States should address the responsible procurement of military AI in international policy discussions.*

States adapting their procurement processes are currently navigating fundamental implementation questions independently, without the benefit of shared learning or common vocabularies. Making procurement practices an explicit component of international military AI governance discussions would strengthen both national implementation and broader international frameworks.

# 1. Introduction

Military adoption of artificial intelligence (AI) capabilities is challenging traditional procurement processes. In a tense geopolitical environment and amid an apparent AI arms race, many militaries are under pressure to accelerate procurement, deployment and scaling of novel AI capabilities (see box 1.1). Some militaries interested in AI capabilities are encountering challenges at the procurement stage. Challenges include lengthy acquisition processes, a shortage of skilled workers, a diverse market that includes traditional defence suppliers as well as newer tech start-ups, and hype surrounding AI that can obscure actual capabilities. States are therefore interested in adapting procurement pathways to facilitate accelerated acquisition of military AI capabilities.

This makes sense. Military procurement processes are intended to act as enablers of capability adoption that bridge a military's strategic needs and its operational capabilities (see box 1.2). They serve this process through the identification of capability gaps, engagement with industry, solicitation and evaluation of proposals, award and management of contracts, and testing and acceptance of delivered capabilities. They do this within a broader ecosystem of defence decision-making that encompasses strategic planning, capability development and budgetary allocation.

But, in practice, military procurement processes are also mechanisms by which states implement policy commitments and national and international legal obligations.[1] When it comes to AI in the military domain, militaries face the need to ensure fidelity to obligations under international law as well as principles of responsible development and use of AI adopted at the national or international level that, taken together, form the landscape of 'responsible military AI'. These include the national principles adopted by the United States, the United Kingdom, France and Japan, as well as principles set out in the (revised) AI strategy of the North Atlantic Treaty Organization (NATO), the European Parliament's guidelines for military and non-military use of AI, the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, the AI Safety Summit's Paris Declaration on Maintaining Human Control in AI Enabled Weapon Systems, and the Responsible Artificial Intelligence in the Military Domain (REAIM) Summit's Call to Action and Blueprint for Action (see table 3.1). While these initiatives may be disconnected institutionally from military procurement actors, they nonetheless bear on procurement activities. This is because responsible procurement of military AI capabilities is a precondition to the responsible use of these technologies. Fielding AI capabilities that have not been responsibly procured could lead to negative outcomes, undermining a principled approach to AI in the military domain.

These two functions of procurement—as a capability enabler and as an implementer of legal obligations and policy commitments—can therefore be in tension with one another. Procurement processes that act as important safeguards and facilitate international commitments may also impede rapid capability adoption and delivery. States may view this as a binary choice between rapid military procurement and fidelity to legal obligations and policy commitments. If so, it could mean that, in trying to expedite procurement through streamlined processes, states minimize processes that are integral to implementing legal obligations and policy commitments relevant to responsible behaviour.

This report argues that procurement reform can serve as a mechanism for implementing responsible military AI, but only if deliberately structured to do so. This ana-

[1] Migone, A., Howlett, A. and Howlett, M., *Procurement and Politics: Strategies of Defence Acquisition in Canada and Australia* (Palgrave Macmillan: Cham, 2023), p. 2.

**Box 1.1.** Military AI capabilities

Artificial intelligence (AI) enables military capabilities across a range of military activities. This report uses the term 'military AI capability' to denote AI used in operational military activities—those activities directly related to the planning, preparation and conduct of military operations. This includes AI applications in command, control and communications; intelligence, surveillance and reconnaissance; weapon systems; and cyber and information operations.

In this context, AI is typically an enabling technology, rather than a discrete capability or standalone item. AI may be embedded within platforms, systems, processes or functions. A single weapon system may integrate multiple AI-enabled components, such as decision support, sensor data fusion, pattern recognition, predictive maintenance or autonomous navigation.[a] Consequently, a military AI capability may be acquired through diverse pathways—as part of a new platform, upgrades to existing systems, or as software to be used across multiple capabilities.

In this report, the term 'military AI capability' deliberately excludes military use of AI in support or enterprise military functions such as logistics, health services, policy development and human resource management. This distinction matters for governance purposes: operational military AI capabilities raise specific concerns under international law that do not apply to most support or enterprise military functions.

[a] Persi Paoli, G. and Afina, Y., 'AI in the military domain: a briefing note for states', UNIDIR, 10 Mar. 2025, pp. 7–8.

lysis is based on the premise that procurement is not merely an administrative function but a critical juncture, prior to the use of military AI capabilities, where legal obligations and high-level policy commitments can be operationalized. The analysis in this report represents an added facet to discussions of responsible military AI, which have to date focused on the use of military AI. To this end, this report examines the intersection of military procurement and responsible military AI. It investigates why and how states are adapting procurement processes to accelerate the adoption of military AI, as well as why and how states should seize these opportunities to give effect to legal obligations and high-level policy commitments related to responsible military AI.

The analysis presented in this report is based on a review of public statements, policy documents, and applied and academic research literature related to military AI governance and defence procurement. It also relies on insights gathered from a closed workshop and interviews with selected government officials working on defence procurement and with other subject-matter experts.

The report is structured as follows. Chapter 2 examines the drivers for accelerated procurement of military AI. It analyses the strategic, operational and commercial pressures that are pushing states to consider expediting the adoption of AI capabilities, and the tensions these pressures create with traditional procurement processes. Chapter 3 surveys the international legal obligations and high-level policy commitments that constitute the governance framework for responsible military AI. Chapter 4 analyses why and how procurement can serve as a critical implementation point for responsible military AI. Chapter 5 presents the report's findings and recommendations.

**Box 1.2.** Military procurement

Procurement is the process by which militaries or defence authorities acquire goods and services they need to fulfil operational requirements.[a] While military procurement encompasses all defence-related acquisitions, this report focuses specifically on capability acquisition—the procurement of weapon systems, platforms (e.g. vehicle or structure) and services (e.g. technical support or upkeep of platforms) intended for military operations—rather than routine administrative goods and services.

Procurement processes are established at the national level and vary considerably across jurisdictions, though they may be shaped by supranational frameworks such as those of the European Union or the North Atlantic Treaty Organization; alliance interoperability requirements; and export control regimes.

Military procurement does not occur in isolation but rather implements priorities established through national defence and security strategies, capability planning processes and defence reviews. These upstream decisions concerning force structure, operational requirements and strategic posture shape what capabilities are sought through procurement. These strategic decisions are themselves constrained by government budgetary allocations, which determine the resources available for capability acquisition.

No single procurement model prevails. Approaches range from off-the-shelf acquisition of mature capabilities to developmental procurement in which the military leads or collaborates with suppliers in extensive research and design phases. Suppliers range from established defence industry actors (and their supply chains) to small and medium enterprises and, increasingly, technology companies that are relatively new to the defence market.

However, there are some commonalities (see figure 2.1). The procurement cycle typically comprises six phases: (*a*) assessment of operational requirements; (*b*) specification of technical requirements; (*c*) exploration of supplier options and solicitation of tenders; (*d*) evaluation, negotiation and selection; (*e*) contract and delivery management; and (*f*) review. The implementation of these phases also tends to vary depending on the nature of the systems. For instance, for software-intensive and artificial-intelligence-enabled systems, these phases are frequently concurrent and iterative rather than linear.

[a] Uttley, M., 'Defence procurement', eds D. J. Galbreath and J. R. Deni, *Routledge Handbook of Defence Studies* (Routledge: London, 2018), p. 15.

# 2. The need for speed: drivers for accelerated procurement of military AI

Military procurement systems are typically tailored for the acquisition of (complex) hardware platforms, a process that can take decades from the moment the desired capability is defined to the point where it is delivered. For instance, the US Air Force's F-35 programme was first conceptualized in the mid-1990s and the first aircraft were delivered in 2011.[2] For many militaries, the pace of the traditional military procurement process is at odds with the perceived imperative that AI capabilities need to be acquired quickly and iteratively. Many of them are now grappling with how to adapt their procurement processes to expedite the deployment and scaling of AI capabilities, as demonstrated by the January 2026 memorandum of the US Secretary of War directing his department to 'accelerate America's Military AI Dominance by becoming an "AI-first" warfighting force'.[3]

This chapter examines the pressures driving states to accelerate military AI procurement and the incompatibilities between these pressures and traditional acquisition frameworks. The analysis considers strategic competition dynamics, operational imperatives derived from contemporary conflicts, and the influence of industry advocacy. The chapter also assesses the specific points of friction between rapid procurement imperatives and established procurement processes, focusing on misalignments in temporal expectations, development methodologies and testing requirements. The chapter then explores how different states are navigating these tensions for maintaining responsible AI practices within military procurement processes.

## Drivers for faster adoption

### *Strategic and operational drivers*

States have long viewed harnessing the military benefits of AI as a strategic and operational imperative.[4] AI is seen as a force multiplier and strategic enabler that has the potential to shift the military balance of power and expand the potential domains of warfare.[5] That perception has only heightened in recent years with the central role that AI plays in the strategic competition between the USA and China, but also in the importance AI has had in recent armed conflicts.

For a decade now, the USA and China have been 'locked in a high-stakes competition for military technology' that positions AI at the centre of defence modernization efforts.[6] Both countries have been very explicit about their ambitions for military AI. In 2017 China declared that it was on a path to 'accelerate the development of military intelligentisation', meaning integrating AI, quantum computing, big data and other

[2] DiMascio, J., 'F-35 Lightning II: Background and issues for Congress', Congressional Research Service (CRS) Report No. R48304, 11 Dec. 2024.

[3] US Secretary of War, 'Accelerating America's military AI dominance', Memorandum, 9 Jan. 2026, p. 1.

[4] See e.g. 'Putin: Leader in artificial intelligence will rule world', AP News, 2 Sep. 2017; and US Department of Defence (DOD), '2017 DOD Artificial Intelligence Strategy: Harnessing AI to advance our security and prosperity', Fact Sheet, Feb. 2019. See also Boulanin, V. et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk* (SIPRI: Stockholm, June 2020).

[5] Stokes, J., 'Military artificial intelligence, the People's Liberation Army, and US–China strategic competition', Testimony before the US–China Economic and Security Review Commission, Hearing on Current and Emerging Technologies in US–China Economic and National Security Competition, 1 Feb. 2024, p. 7.

[6] Csernatoni, R., 'Governing military AI amid a geopolitical minefield', Carnegie Endowment for International Peace, 17 July 2024.

emerging technologies into a joint force.[7] It made clear that the enhanced sensing, relaying and processing capabilities that AI offers, and the autonomous capabilities it facilitates, are critical to China's strategy of 'multidomain precision warfare', a strategy predicated on attacking perceived 'weak points' in US systems such as internet, satellite or electromagnetic communication links or logistical supply chains.[8] The USA framed AI adoption as a competitive necessity as early as 2015 through its so-called third offset strategy.[9] That strategy made the case that the USA and its allies had to leverage AI and emerging technologies to maintain a competitive edge over Russia and China. The US Department of Defense (DOD) 2018 Artificial Intelligence Strategy confirmed that vision as it noted that failure to incorporate AI capabilities into weapon systems could hinder the ability of warfighters to defend the USA against near-peer adversaries. The strategy specifically mentions the significant investments of other nations in this area as threatening to erode US military technological and operational advantage.[10]

The strategic importance that the USA and China attribute to AI certainly impacted the views of many other states, not least the USA's NATO allies. Several NATO allies formalized their respective visions in national strategies for their militaries, including France, the UK and Canada , as did non-NATO ally Australia (through Pillar II of its Australia–UK–USA (AUKUS) agreement).[11] In these documents, these countries outline how they intend to leverage AI as part of their current or future military modernization programmes to variously enhance their deterrence capability, their preparedness and resilience against the risk of major conflict, or their ability to conduct decisive military operations against resourceful adversaries.

The reported use of AI in recent conflicts reinforces the view that military AI is central to the conduct of modern warfare—although the lack of precise information makes it difficult to evaluate the impact of the technology. In the 2020 armed conflict in the Nagorno-Karabakh region, Azerbaijan used a large number of AI-enabled loitering munitions to overwhelm Armenian air defences.[12] Israel relied extensively on AI to plan and conduct military operations in its most recent conflict with Hamas in Gaza.[13] Ukraine's response to Russia's 2022 invasion of its territory has also relied on innovative uses of robotics and AI.[14] Ukraine's use of AI capabilities has been viewed as proof of their significant operational value when integrated in modular 'attritable' systems—that is, systems designed to be affordable enough to lose without strategic, operational or tactical impact.[15] Ukraine's experience has also demonstrated the

[7] Xi Jinping, 'Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with Chinese characteristics for a new era', Speech at the 19th National Congress of the Chinese Communist Party, Beijing, 18 Oct. 2017; and Pollpeter, K. and Kerrigan, A., 'The PLA and intelligent warfare: A preliminary analysis', CNA, Oct. 2021.

[8] Stokes (note 5), p. 3.

[9] Work, B., 'The third US offset strategy and its implications for partners and allies', Speech at the Willard Hotel, Washington DC, 28 Jan. 2015.

[10] Stokes (note 5). See also US Secretary of War (note 3).

[11] French Ministry of Armaments, *L'Intelligence Artificielle au Service de la Défense* [*Artificial Intelligence in Support of Defence*], Report of the AI Task Force, Sep. 2019; British Ministry of Defence (MOD), *Defence Artificial Intelligence Strategy* (MOD: London, June 2022); Canadian Department of National Defence (DND), *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy* (DND: Ottawa, 2024); and AUKUS defense ministers meeting joint statement, 2 Dec. 2023.

[12] Shaikh, S. and Rumbaugh, W., 'The air and missile war in Nagorno-Karabakh: Lessons for the future of strike and defense', Center for Strategic and International Studies (CSIS), 8 Dec. 2020.

[13] McKernan, B. and Davies, H., ' "The machine did it coldly": Israel used AI to identify 37 000 Hamas targets', *The Guardian*, 4 Apr. 2024.

[14] Bondar, K., 'Ukraine's future vision and current capabilities for waging AI-enabled autonomous warfare', CSIS, 20 Mar. 2025.

[15] Fairfield, H., Hyde, D. and McCormick, J. T., 'Commoditizing AI/ML models', *Army AL&T Magazine*, 2 Oct. 2024. For a discussion of 'attritable' see Magnuson, S., 'The meanings of "attritable" and "expendable" ', *National Defense*, 9 Feb. 2022.

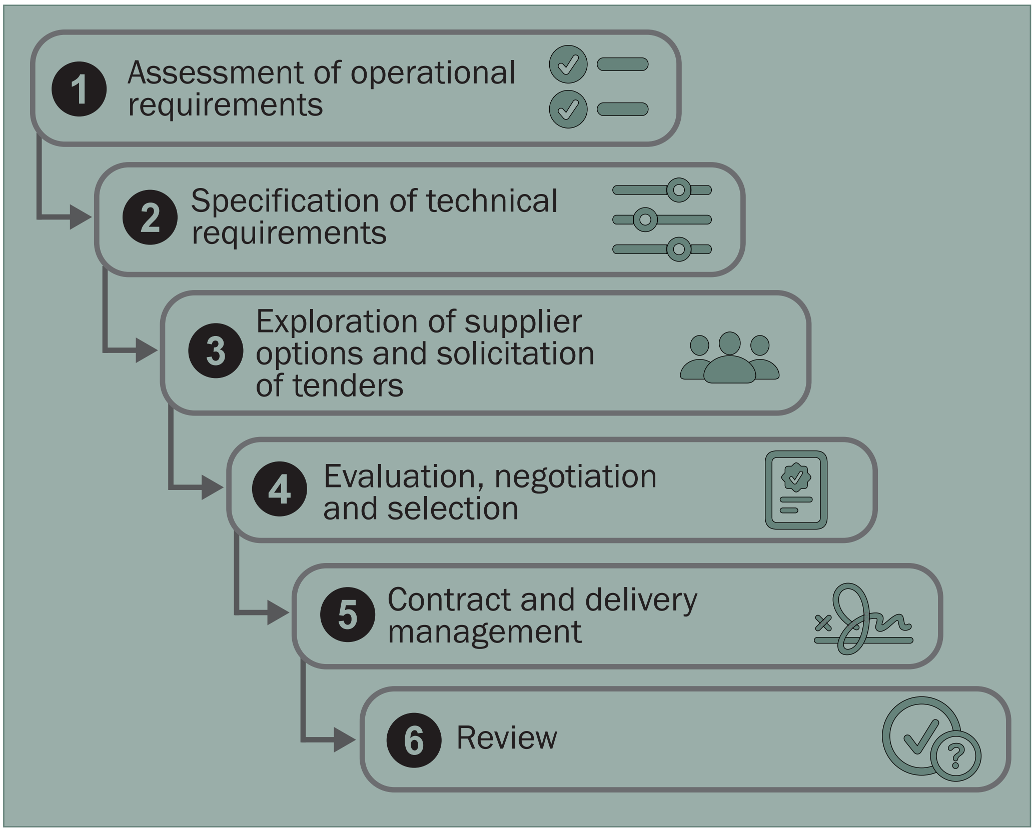
1 Assessment of operational requirements
2 Specification of technical requirements
3 Exploration of supplier options and solicitation of tenders
4 Evaluation, negotiation and selection
5 Contract and delivery management
6 Review

**Figure 2.1**. The  six phases of a typical military procurement cycle

importance of rapid innovation cycles and regular software updates. Any operational advantage that advances in AI offer can be lost within months as adversaries develop countermeasures.[16]

### *Advocacy from the industry*

Industry actors—whether traditional defence contractors, large technology companies or start-ups—have become increasingly influential in shaping state approaches to military AI procurement and driving initiatives to accelerate or streamline processes.[17] Industry actors have echoed and amplified state narratives emphasizing urgency and the strategic and operational imperatives for military AI adoption. US tech companies like OpenAI have stressed the need for the USA to keep a technological edge over China.[18] Industry has also positioned AI capabilities as essential solutions to a fundamental challenge confronting contemporary military operations: the problem of bandwidth.[19] Modern sensor networks, intelligence collection platforms and communications systems generate quantities of data that far exceed human analytical capacity, and industry actors have promoted AI as the means to process, synthesize and extract actionable intelligence from these information flows at the speed and scale that operational contexts demand.

[16] Bendett, S. and Kirichenko, D., 'Battlefield drones and the accelerating autonomous arms race in Ukraine', Modern War Institute at West Point, 10 Jan. 2025.

[17] González, R., 'How Big Tech and Silicon Valley are transforming the military-industrial complex', *Costs of War*, 17 Apr. 2024; Confino, P., 'Silicon Valley has been trying to shake up defense contracting for years. With Trump, they have a willing audience', *Fortune*, 3 May 2025; and Chatterjee, M., 'The AI lobby plants its flag in Washington', *Politico*, 6 June 2025.

[18] Ghaffray, S., 'OpenAI emphasizes China competition in pitch to a new Washington', *Financial Post*, 13 Jan. 2025; and Sigalos, M., 'OpenAI's Altman warns the US is underestimating China's next-gen AI threat', CNBC, 18 Aug. 2025.

[19] Elbaum, S. and Panter, J., 'DOD's AI balancing act', Council on Foreign Relations, 2 Dec. 2025; and O'Donnell, J., 'OpenAI's new defense contract completes its military pivot', *MIT Technology Review*, 4 Dec. 2024.

While there is long-standing consensus among stakeholders that existing procurement processes are excessively bureaucratic, industry actors have placed particular emphasis on the implications for innovation, arguing that cumbersome procedural requirements deter technology firms from engaging with defence markets and impede the rapid iteration cycles on which contemporary software development depends. Newer defence technology firms in the USA have been particularly active in positioning procurement reform as essential to national security. In 2024 Palantir and Anduril initiated the formation of a consortium explicitly designed to challenge incumbent contractors by offering 'a more efficient way to sell the government cutting-edge weapons and other tech'.[20] The 2025 Silicon Valley Defense Group's NatSec100 report explicitly advocates a focus on 'innovative adoption', that is, a shift of focus away from innovation and towards accelerating deployment of existing capabilities.[21]

## Tension with traditional procurement processes

As a result of these drivers, many states are now rushing to adopt military AI applications such as intelligence, surveillance and reconnaissance; maintenance and logistics; command and control (including targeting); information and electronic warfare; and autonomous systems.[22] In this rush, some states have indicated that traditional military procurement processes are not fit for the purpose of rapid adoption of novel AI technologies nor rapid iteration of such technologies once in service. Three main reasons have been cited for this misalignment.

### *Speed versus bureaucratic deliberation*

There is a mismatch between traditional procurement timelines and the pace of AI development. Traditional timelines are linked to extensive processes to define needs and documentation requirements, and sequential decision-making processes (or gateways) that assume stable procurement needs and predictable development arcs. These processes serve as important oversight and accountability mechanisms, but they span years or decades. The model and pace of bureaucratic deliberations that military procurement requires stand in sharp contrast with the timelines for AI products that are typically developed and deployed. In oral evidence to the UK's House of Commons Defence Committee inquiry into AI capacity and expertise, representatives of Palantir and Anduril pointed out that product timelines in the AI sector were measured in weeks or months.[23]

### *Iterative development versus linear process*

Traditional procurement models were developed for the acquisition of (complex) hardware rather than software. Traditional procurement follows a waterfall model, moving sequentially through formal stages (see figure 2.1).[24] This linear approach assumes that capability requirements remain static throughout. By contrast, the development of AI capabilities—whether in the military or civilian domain—requires

[20] Ha, A., 'Palantir and Anduril reportedly building a tech consortium to bid on defense contracts', Tech Crunch, 22 Dec. 2024.

[21] Silicon Valley Defense Group (SVDG), *NatSec 100: 2025 edition* (SVDG: Arlington, VA, 2025), p. 36.

[22] See analysis in Boulanin, V. (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume I—Euro-Atlantic Perspectives* (SIPRI: Stockholm, May 2019).

[23] British Parliament, House of Commons Defence Committee, *Developing AI Capacity and Expertise in UK Defence*, Second Report of Session 2024–25, HC 590, 10 Jan. 2025, p. 18.

[24] Wallin, J., 'Safe and effective: Advancing Department of Defense test and evaluation for AI and autonomous systems', Centre for New American Security (CNAS), 13 Mar. 2025; and Gansler, J. S., Lucyshyn, W. and Spiers, A., 'Using spiral development to reduce acquisition cycle times', University of Maryland Center for Public Policy and Private Enterprise, Sep. 2008.

continuous refinement through iterative training, testing and retraining.[25] Models may be updated as new data becomes available. This problem is not novel or unique to AI. The inadequacy of waterfall methodologies for software systems was identified as early as the 1980s, when Barry Boehm developed the spiral model in response to the demonstrated ineffectiveness of sequential development processes for complex software systems.[26]

Procurement agencies have been working to adapt their procurement processes to ensure that military equipment, when deployed, relies on state-of-the-art, rather than obsolete, software—with mixed success.[27] One approach that is considered for the integration of AI capabilities is 'AI as a service', where the supplier provides not only a 'product' (the AI capability) but also a service of continuous updates (usually through a cloud platform).[28] This model, however, raises several critical questions for procurement agencies as it requires shifting away from assumptions that underpin traditional procurement: conceptualization of a fixed and finished product that meets predetermined requirements, and the availability of existing models for testing, evaluation and certification.[29]

### *Opacity versus assurance*

This shift in assumptions pertains to the third reason: how procurement agencies typically assess the safety, security and reliability of the systems they acquire. Traditional procurement processes depend on testing and evaluation to verify that systems meet requirements and perform reliably. Acceptance testing protocols assume that system behaviours can be understood, performance standards defined, and failures identified through systematic evaluation. These assumptions derive from the characteristics of conventional military hardware, where testing and evaluation methodologies have been refined over decades to provide high confidence in system performance. Physical systems such as aircraft, missiles and vehicles exhibit deterministic behaviour; that is, given the same inputs and conditions, they produce predictable outputs that can be measured, replicated and verified.[30]

AI capabilities, which are now based on machine learning, challenge these assumptions. Formal methods to verify the reliability of hardware and systems are challenging to apply to machine-learning systems.[31] Reliability is therefore primarily evaluated through simulations and operational testing. Such empirical tests and evaluations can only provide a partial picture of how systems perform and potentially fail. The opacity of systems-based machine learning complicates the equation. In the absence of an explanation for how a system reaches its output from a given input, it can be difficult for engineers to identify where failures might stem from.

Procurement agencies face a dilemma: should they wait for the procurement of a desired capability until it can be firmly established that it meets the established stand-

[25] US DOD, Defense Science Board (DSB), *The Role of Autonomy in DoD Systems*, DSB Task Force Report (Office of the Secretary of Defense: Washington, DC, July 2012); and US DOD, *Report of the Defense Science Board Summer Study on Autonomy* (Office of the Under Secretary of Defense: Washington, DC, June 2016).

[26] Boehm, B. W., 'A spiral model of software development and enhancement', *Computer*, vol. 21, no. 5 (1988).

[27] Strong, J. et al., 'In machines we trust: AI enters the dogfight', *MIT Technology Review Narrated* (Podcast), season 3, episode 29, 22 Feb. 2023.

[28] Microsoft, 'What is AIaaS?', *Cloud Computing Terminology*, [n.d.].

[29] US Office of Management and Budget, Cloud Information Center, 'Acquisition challenges', [n.d.]; and US DOD, Office of the Under Secretary of Defense, 'Revision 1, Pilot program for anything-as-a-service contracts or agreements', Memorandum, 21 Aug. 2025.

[30] Panwar, R. S., Li Q. and Shanahan, J. N. T. (eds), 'Military artificial intelligence test and evaluation model practices', INHR, Dec. 2024; and Wallin (note 24).

[31] Urban, C. and Miné, A., 'A review of formal methods applied to machine learning', *arXiv*, 21 Apr. 2021.

ards of safety and security, or should they revisit their standards of assurance to identify new performance metrics suitable for military AI capabilities?

## Efforts to accelerate military AI procurement: case studies from Ukraine, the USA and the UK

The following case studies examine three states that have recently undertaken significant initiatives to accelerate military AI procurement. These examples are not intended as representative of global practice, but rather as illustrations of how different states are navigating the imperative for speed.

### *Ukraine*

Many states are looking to Ukraine as an example of how rapid adoption and scaling of military AI capabilities can be achieved under wartime conditions.

Ukraine's efforts to procure military AI capabilities quickly have been driven by an existential need to leverage low-cost drones to compensate for shortages in its military tanks and artillery.[32] As Russian electronic warfare can disrupt the communication and navigation systems on which remote-controlled drones depend, Ukraine has been using AI-enabled drones that can conduct part of an attack autonomously.[33]

In the early phase of the war, Ukraine pursued the acquisition of AI-enabled drones and other military AI capabilities primarily through imports. It purchased and repurposed commercial off-the-shelf systems and received donations from international partners. Over time, Ukraine shifted to a strategy prioritizing domestic production (still mostly based on foreign components) and domestic research and innovation.[34]

This growth in industrial capacity has been driven in part by Brave1, a state-led initiative established in April 2023 that aims to (*a*) connect the military with technology providers; (*b*) foster collaboration between industry stakeholders, including investors; and (*c*) facilitate rapid research and development as well as operational testing of new capabilities.[35] A key feature is that it enables decentralized procurement through its online Defence Technology Marketplace. Military units can buy directly from this market, choosing from a catalogue of over 1000 innovations, from autonomous drones and ground robots to AI-driven surveillance and intelligence systems.[36] This procurement model is intended to allow military units to easily identify and quickly acquire technology solutions that fit their operational needs.[37]

Ukraine's efforts to accelerate the procurement of AI—and new technology more broadly—have been guided primarily by operational needs and consideration for military effectiveness. Ukraine is still committed to aligning such efforts with international norms. Reportedly, technologies that are to be funded or marketed through Brave1 must go through a legal and ethical review process intended to demonstrate how they comply with Ukrainian law, international humanitarian law (IHL) and NATO-compatible standards.[38] Details about how that review process is conducted remain

[32] Bondar (note 14).

[33] Bondar (note 14).

[34] Prots, Y., 'Ukraine shifts defense procurement to domestic suppliers, nearly all drones now Ukrainian-made', *Kyiv Independent*, 28 July 2025; and Ruitenberg, R., 'Ukraine to hand combat units $60 million monthly for new drones', *Defense News*, 23 Jan. 2025.

[35] Kuzmuk, K. and Scarazzato, L., 'The transformation of Ukraine's arms industry amid war with Russia', SIPRI Backgrounder, 21 Feb. 2025.

[36] 'Brave1 Market: Ukraine launches marketplace for cutting-edge defense technologies', Ukrinform, 29 Apr. 2025.

[37] 'Ukraine launches Brave1 market for defense innovation', Digital State UA, 28 Apr. 2025.

[38] Mysyshyn, A., 'Governing AI under fire in Ukraine', *Cairo Review of Global Affairs*, no. 54 (Spring/Summer 2025).

limited.[39] Ukraine has made clear that it is wary of regulatory development that could slow down its adoption of decisive technological solutions. The Ukrainian Ministry of Digital Transformation recently stated that Ukraine does not intend to propose any regulation of AI systems within the defence sector, emphasizing the need for rapid innovation without regulatory constraints.[40]

### *The United States*

The USA has been working on adapting its military procurement system to facilitate the acquisition of AI-related capabilities for more than a decade. As early as 2012, a report from the Defence Science Board of the US DOD recommended drastic changes in procurement procedures to accelerate the acquisition of autonomous capabilities in military systems.[41] In 2015 the USA created the Defense Innovation Unit Experimental (also called Unit X or DIUx) to facilitate the military adoption of commercial off-the-shelf technologies by enabling direct connection between the DOD and Silicon Valley.[42] The USA's effort to make the procurement process more 'AI-ready' has only intensified as both the 2015 third offset strategy and the 2022 national security strategy made clear that innovation in AI was central to the USA's pacing challenge with China.[43] The conflict in Ukraine also reinforced this strategic orientation. US DOD officials have explicitly referenced Ukrainian operational experience as demonstrating 'the advantages that technologies like these can have on the modern battlefield at scale' and what industry can produce under wartime conditions.[44]

One of the latest and most significant targeted efforts to speed up the acquisition of AI capability within the US armed forces was the US DOD's Replicator initiative from August 2023. Inspired by Ukraine's deployment of low-cost drones, the initiative mandated the fielding of 'multiple thousands' of attritable autonomous systems within 18 to 24 months.[45] To achieve this, the initiative aimed to compress the procurement process timeline, which usually takes several years, to 18–24 months, using an open solicitation process known as a commercial solutions opening (CSO).[46] The US DOD's CSO uses a form of agreement that bypasses the traditionally lengthy Federal Acquisition Regulations, allowing the DIU to find and rapidly prototype commercially available technologies to address specific operational needs.[47]

The US DOD has emphasized that the Replicator initiative operates within established policies on ethical use of military AI. These include the US DOD's Directive 3000.09,

[39] Copeland, D. and Liivoja, R., 'Progressing the legal review of autonomous weapon systems', Report of an expert meeting, Geneva, 10–11 Mar. 2025, Asia-Pacific Institute for Law and Security, Sep. 2025, pp. 8–9.

[40] Ukrainian Ministry of Digital Transformation, 'White paper on artificial intelligence regulation in Ukraine: Vision of the Ministry of Digital Transformation of Ukraine', Consultation paper, June 2024, p. 10. See also Nover, S., 'In Ukraine's AI-enabled war against Russia, humans still call the shots', GZERO, 11 Mar. 2025.

[41] US DOD, DSB (note 25), p. 10.

[42] Pellerin, C., 'DoD's Silicon Valley innovation experiment begins', DOD News, 29 Oct. 2015.

[43] Gentile, G. et al., 'A history of the third offset, 2014–2018', RAND Research Report RR-A454-1, 2021; and Hicks, K., US Deputy Secretary of Defense, 'The urgency to innovate', Keynote address, NDIA Emerging Technologies for Defense Conference, Washington, DC, 28 Aug. 2023.

[44] US Defense Innovation Unit (DIU), 'Implementing the Department of Defense Replicator initiative at speed and scale', 30 Nov. 2023.

[45] Sayler, K. M., 'DOD Replicator initiative: Background and issues for Congress', CRS In Focus IF12611, 19 Sep. 2025; and US DOD, 'Deputy Secretary of Defense Hicks announces first tranche of Replicator capabilities focused on all domain attritable autonomous systems', Press release, 6 May 2024.

[46] US DOD, 'Secretary of Defense Hicks announces first tranche of Replicator capabilities focused on all domain attritable autonomous systems' (note 45).

[47] See US DIU, 'Work with us', [n.d.]; and US Defense Innovation Unit Experimental (DIUx), *DIUx Commercial Solutions Opening: How-to Guide* (Defense Technology Information Center: Fort Belvoir, VA, 30 Nov. 2016).

the DOD's ethical principles for AI and the DOD Responsible Artificial Intelligence Strategy and Implementation Pathway.[48]

Directive 3000.09 mandates that systems will go through 'rigorous hardware and software verification and validation, and realistic system developmental and operational test and evaluation', and must be approved by a host of senior DOD officials before formal development and fielding.[49] The directive explicitly requires that the 'design, development, deployment, and use of AI capabilities in autonomous and semi-autonomous weapon systems will be consistent with the DOD AI Ethical Principles and the DOD Responsible Artificial Intelligence Strategy and Implementation Pathway'.[50]

The DOD's AI ethical principles, which were adopted in February 2020, state that AI should be responsible, equitable, traceable, reliable and governable.[51] The DOD Responsible Artificial Intelligence Strategy and Implementation Pathway establishes six foundational tenets, the third of which includes the goal to 'exercise appropriate care in the AI product and acquisition lifecycle to ensure potential AI risks are considered from the outset of an AI project, and effects are taken to mitigate or ameliorate such risks and reduce the likelihood of unintended consequences, while enabling AI development at the pace the Department needs'.[52] The responsible AI S&I pathway calls for development of an acquisition toolkit including 'operationally-relevant [responsible AI]-related evaluation criteria'; guidance on how industry can meet the DOD's AI ethical principles; and 'standard AI contract language' addressing independent test and evaluation, remediation when capabilities cannot be used in accordance with ethical principles, and performance monitoring.[53]

Combined, the DOD's Directive 3000.09, AI ethical principles and responsible AI S&I pathway provide general guidance for the responsible procurement of military AI capabilities. How this guidance can be operationalized in the context of compressed procurement timelines, like in the case of the Replicator initiative or the more recent push to 'accelerate America's military AI dominance', remains unclear.[54] The tension between acquisition speed and thorough legal, safety and ethical review remains unresolved in public documentation.

### *The United Kingdom*

Like the USA, the UK has positioned AI and autonomy as enablers of its future defence posture, reflecting an assessment that the use of AI capabilities is no longer a theoretical concern but rather an operational reality.[55] The British Ministry of Defence (MOD) 2025 Strategic Defence Review commits to doubling investment in autonomous systems, establishing a Defence Uncrewed Systems Centre by February 2026, and creating a new 'digital targeting web' by 2027 that will leverage AI to compress the sensor-to-shooter cycle from hours to minutes.[56] The UK has also publicly committed to pursuing the adoption of AI capabilities in a responsible way. The June 2022 Defence Artificial

[48] Kahn, L., 'Scaling the future: How Replicator aims to fast-track US defense capabilities', *War on the Rocks*, 20 Sep. 2023.

[49] US DOD, 'Autonomy in Weapon Systems', Directive 3000.09, 25 Jan. 2023.

[50] US DOD, Directive 3000.09 (note 49), p. 4, para. 1.2.b. See also Scharre P., 'Noteworthy: DoD autonomous weapons policy', CNAS Press Note, 6 Feb. 2023.

[51] US DOD, 'DOD adopts ethical principles for artificial intelligence', Press release, 24 Feb. 2020.

[52] US DOD, Responsible AI Working Council, *US Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway* (DOD: Washington, DC, June 2022), p. 36.

[53] Hitchens, T., 'Pentagon's long-awaited "responsible AI" pathway highlights flexibility, "trust" ', *Breaking Defense*, 22 June 2022.

[54] Sayler (note 45); and US Secretary of War (note 3), p. 4.

[55] British Parliament, House of Commons Defence Committee (note 23), p. 1.

[56] British MOD, *Strategic Defence Review—Making Britain Safer: Secure at Home, Strong Abroad*, Policy Paper, 2 June 2025, pp. 20, 21 and 48–50.

Intelligence Strategy committed the MOD to developing and deploying AI-enabled systems in ways that are 'ambitious, safe and responsible' and that uphold 'lawful and ethical AI use in line with [the MOD's] core values'.[57]

To fulfil the ambitions laid out in the 2022 Defence AI strategy and the 2025 Strategic Defence Review, the UK took a series of notable measures. The MOD issued a directive on dependable AI in Defence, which 'mandates the application of ambitious, safe and responsible practices relating to all Defence projects that include [AI]'.[58] In response to this directive, each command and component organization (CO) of the MOD nominated a Responsible AI Senior Officer whose role includes ensuring the command or CO has the right processes and policies to implement the principles set out in the Defence AI strategy.[59]

The MOD also empowered the Integration Design Authority within Strategic Command to monitor programmes for opportunities to 'better harness AI or novel technologies'.[60] It also gave a stronger role to the Defence Science and Technology Laboratory in assessing the viability and risks of technological offers.[61] In November 2025 the Defence AI Centre (established in 2021 on the recommendation of the British Cabinet Office's Integrated Review 2021) also launched an 'AI Model Arena' pilot, developed with British AI company Advai, which provides a standardized platform to evaluate AI models against MOD benchmarks for performance, reliability, robustness and security, potentially supporting more rigorous pre-deployment assessment of AI capabilities.[62]

Regarding procurement, the MOD adopted in 2024 a new Integrated Procurement Model (IPM), which commits to deliver capabilities within a shorter timeframe: maximums of five years for equipment programmes and three years for digital programmes.[63] The compression of the timeframe is to be achieved through a series of institutional changes: Defence-wide portfolio management to break down organizational silos; new checks and balances through expert-informed decision-making at program inception; prioritization of exportability to drive industrial resilience; empowerment of industrial innovation through earlier engagement; and adoption of spiral development as the default approach.[64] The MOD describes a 'spiral development approach' as including 'Delivering a minimum deployable capability quickly, and then iterating it in the light of experience and advances in technology—rather than waiting for a 100% solution that may be too late and out of date.'[65] The IPM does not explicitly articulate how the MOD's commitment to responsible adoption of military AI will be considered in the procurement process. The IPM does include features that could facilitate legal and ethical compliance, though they are not explicitly framed as legal and ethical review mechanisms. For example, the IPM includes 'new checks and balances to challenge assumptions and ensure better, expert-informed, decision making at the start of programmes'.[66]

[57] British MOD, *Defence Artificial Intelligence Strategy* (note 11), pp. 5 and 13.

[58] British MOD, 'Dependable artificial intelligence (AI) in Defence—part 1: Directive', JSP 936 V1.1, Nov. 2024, p. v, para. 1.

[59] British MOD, 'Laying the groundwork—Responsible AI Senior Officers' Report 2025', 3 Oct. 2025, p. 4.

[60] Cartlidge, J., British Minister for Defence Procurement, 'Oral statement on the new Integrated Procurement Model', Statement to the House of Commons, 28 Feb. 2024.

[61] Cartlidge (note 60).

[62] British MOD, 'Launching the AI Model Arena', Press release, 10 Nov. 2025; and British Cabinet Office, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, Policy Paper, Mar. 2021, p. 73.

[63] Cartlidge (note 60).

[64] Cartlidge (note 60).

[65] Cartlidge (note 60); and British MOD, 'Integrated Procurement Model: Driving pace in the delivery of military capability', Policy paper, 28 Feb. 2024.

[66] British MOD, 'Integrated Procurement Model: Driving pace in the delivery of military capability' (note 65).

### Pathways to accelerated procurement of military AI

Three trends emerge from these cases. First, accelerating military AI procurement may involve a deepening collaboration with suppliers to match capability needs with available products or offers. This reflects a recognition that military AI capabilities increasingly originate in the commercial sector, requiring procurement systems to engage more directly and continuously with industry partners rather than relying solely on traditional specification-driven acquisition. Second, an accelerated procurement process may involve adopting more iterative processes, moving away from linear development cycles towards spiral approaches that allow for rapid fielding of minimum viable capabilities followed by incremental improvement based on operational experience. In some cases, states may even knowingly accept governance trade-offs under acute security or operational pressures. Third, states are tackling the challenge of assurance about the lawfulness, safety and reliability of AI-enabled systems. They are exploring different methods—whether through in-house pre-deployment testing regimes or third-party providers, or by more directly relying on suppliers—to achieve the assurance they need.

A critical policy question in this context is how states can pursue these options for accelerating procurement in a way that still enables them to fulfil their legal obligations and policy commitments around responsible AI in the military domain. This question is the focus of the next chapters. Chapter 3 unpacks the legal and policy demands for responsible AI in the military domain and their implications for the procurement of military AI capabilities. Chapter 4 explores how states can leverage their procurement processes to implement principles around responsible military AI.

# 3. The need for responsibility: legal obligations and policy commitments on AI in the military domain

The procurement of military AI capabilities occurs within an existing legal and policy landscape. Understanding this landscape is essential for understanding responsible procurement of military AI. This chapter examines two governance sources. First, international law, particularly the legal review obligations under Article 36 of the 1977 Protocol Additional to the 1949 Geneva Conventions (API), requires an assessment of whether certain new military capabilities can be used in compliance with applicable international law.[67] Second, national and international policy commitments to responsible military AI establish substantive principles that articulate states' expectations for how military AI should be developed and used.

Taken together, these frameworks converge on core requirements: lawfulness; systematic assessment and mitigation of algorithmic bias; transparent development methodologies with comprehensive documentation; rigorous testing, evaluation, validation and verification (TEVV) throughout system lifecycles; maintenance of human responsibility and control; and explicit, well-defined uses with mechanisms preventing unintended behaviour. This chapter explains how each of these governance sources presents implementation challenges at the procurement stage, but how collectively they point towards several fundamental requirements for responsible procurement of military AI.

Due to diversity in national approaches, this chapter does not specify national legislative frameworks that may nonetheless be relevant to the military procurement process, such as competition, transparency, integrity, industrial security and economic objectives.

## International law relevant to the procurement of military AI

International law contains few obligations directly relevant to military procurement. There are general obligations applicable to any public procurement that entail direct obligations or may indirectly shape military procurements. For example, the 2003 United Nations Convention against Corruption requires states parties to establish 'appropriate systems of procurement, based on transparency, competition and objective criteria in decision-making' for the purposes of preventing corruption.[68] There are also other obligations between states, such as security or alliance agreements, that may impact how a state conducts its military procurements. For example, the 2007 Australia–US Defence Trade Cooperation Treaty establishes an expedited licensing regime that exempts specified defence articles from standard export control requirements.[69] Similar frameworks exist in the 2010 UK–US Defense Trade Cooperation Treaty and the 2021 AUKUS Agreement.[70] But aside from specific prohibitions on the acquisition

[67] Protocol Additional to the 1949 Geneva Conventions, and Relating to the Protection of Victims of International Armed Conflicts (API), opened for signature 12 Dec. 1977, entered into force 7 Dec. 1978.

[68] United Nations Convention against Corruption, opened for signature 31 Oct. 2003, entered into force 14 Dec. 2005, *United Nations Treaty Series*, vol. 2349 (2007), Article 9.

[69] Treaty between the Government of Australia and the Government of The United States of America Concerning Defence Trade Cooperation and Implementing Arrangement, entered into force 5 Sep. 2007, *Australian Treaty Series*, vol. 17 (2013).

[70] Treaty between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America concerning Defense Trade Cooperation, opened for signature June 2007, entered into force 13 Apr. 2012; and Agreement between the Government of Australia, the Government of the United Kingdom of Great Britain and Northern Ireland, and the Government of the United States of America for the Exchange of Naval Nuclear Propulsion Information (AUKUS Agreement), entered into force Sep. 2021.

of certain types of weapons (e.g. biological and chemical weapons, anti-personnel mines and cluster munitions), the key obligation under international law relates to legal reviews—reviewing the legality of a capability prior to its use.

Legal reviews of military capabilities represent a well-established mechanism within the international law framework governing armed conflict. Article 36 of the API requires states to assess whether weapons, means and methods of warfare under consideration can be used in compliance with applicable international law:[71]

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

Effective legal reviews are important because they can be a potent safeguard against the development and adoption of AI capabilities that are incapable of being used in compliance with international law regulating warfare.[72] These reviews serve both as implementation mechanisms for IHL and as confidence-building measures among states.[73] In multilateral forums such as the UN Convention on Certain Conventional Weapons Group of Governmental Experts on Lethal Autonomous Weapons Systems (CCW GGE on LAWS) and the recent REAIM summits, legal reviews are consistently a critical element of proposed governance frameworks. States, international organizations and civil society actors invoke these mechanisms as essential safeguards against the employment of military AI capabilities that may violate IHL. The emphasis on legal reviews reflects both their formal status as a treaty obligation for many states and their broader usefulness as tools to support legal compliance and responsible behaviour.

The integration of AI into military systems, however, introduces distinctive characteristics that challenge traditional legal review processes and methodologies.[74] Critically, the scope of Article 36 is limited to the review of ‘new’ weapons, means and methods of warfare by high contracting parties. This means not only that a limited number of states are bound to conduct legal reviews, but it also raises interpretative challenges for the review of military AI capabilities. This is because the terms ‘new’ and ‘weapons, means and methods of warfare’ are not defined, raising questions about the circumstances under which a military AI capability meets this material threshold. Unlike traditional military hardware, military AI capabilities are developed iteratively and may be adapted more frequently. This raises the question of when, during the design, development, acquisition and sustainment periods, a specific AI capability is ‘new’. The wide range of applications in which military AI capabilities may be used means that not all such capabilities might be considered weapons, means or methods of warfare. Even where AI capabilities are subject to legal reviews, the iterative and fast-paced approach taken to the acquisition of some AI-enabled military capabilities potentially complicates the linear process of legal reviews within the procurement process.[75] It

[71] International Committee of the Red Cross (ICRC), *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare* (ICRC: Geneva, Jan. 2006).

[72] Goussac, N. and Liivoja, R., ‘Legal review of military artificial intelligence capabilities’, *Articles of War*, 25 Aug. 2025.

[73] On how states are currently practising legal reviews see the Legal Review of Weapons Information Portal; Boulanin, V. and Verbruggen, M., ‘SIPRI compendium on Article 36 reviews’, SIPRI Background Paper, Dec. 2:2017; and ICRC (note 71).

[74] Boulanin, V. and Verbruggen, M., *Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies* (SIPRI: Stockholm, Dec. 2017); Goussac and Liivoja (note 72); and Vestner, T. and Rossi, I., ‘Legal reviews of war algorithms’, *International Law Studies*, vol. 97, no. 509 (2021), p. 512.

[75] Goussac and Liivoja (note 72). For a discussion of how legal reviews are synchronized with procurement processes in select states, see Wolf, R. et al., *Advancing the Legal Review of Autonomous Weapon Systems Report of an Expert Meeting (Sydney, 16–18 April 2024)* (University of Queensland: Brisbane, Sep. 2024), pp. 7–15.

**Table 3.1.** Principles of responsible/ethical military artificial intelligence at the international and national level, ordered from most to least common, 2019–25

| Principle | 2019 France[a] | 2020 USA[b] | 2021 EU[c] | 2022 UK[d] | 2023 Political Declaration[e] | 2024 NATO[f] | 2024 REAIM[g] | 2025 AI Action Summit[h] | 2025 Japan[i] |
|---|---|---|---|---|---|---|---|---|---|
| Reliability, safety and security | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| Traceability, explainability and understanding | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| Responsibility and accountability | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ | – |
| Effects on humans, equitability and bias mitigation | – | ✓ | – | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| Lawfulness | – | – | – | – | ✓ | ✓ | ✓ | ✓ | ✓ |
| Governability | – | ✓ | ✓ | – | ✓ | ✓ | – | – | – |
| Human role | – | – | – | – | ✓ | – | ✓ | – | ✓ |

✓ = principle referenced in the document; – = principle not referenced in the document; EU = European Union; NATO = North Atlantic Treaty Organization; REAIM = Responsible Artificial Intelligence in the Military Domain.

[a] French Ministry of Armaments, *L'Intelligence Artificielle au Service de la Défense* [*Artificial Intelligence in Support of Defence*], Report of the AI Task Force, Sep. 2019.

[b] United States Department of Defense (DOD), 'DOD adopts ethical principles of artificial intelligence', Press release, 24 Feb. 2020.

[c] European Parliament, 'Artificial intelligence: Questions of interpretation and application of international law', Resolution P9_TA(2021)0009, 20 Jan. 2021.

[d] British Ministry of Defence, 'Ambitious, safe, responsible: Our approach to the delivery of AI-enabled capability in Defence', Policy paper, 15 June 2022.

[e] Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, 9 Nov. 2023.

[f] NATO, 'Summary of NATO's revised artificial intelligence (AI) strategy', 10 July 2024.

[g] REAIM Summit, 'Blueprint for Action' 11 Sep. 2024.

[h] AI Action Summit, 'Paris declaration on maintaining human control in AI enabled weapon systems', 11 Feb. 2025.

[i] Japanese Ministry of Defense, 'Guideline for responsible AI application in reseasrch and development of AI-equipped defense systems', ver. 1 (provisional translation), June 2025.

also introduces new challenges related to the characteristics of the technology. These challenges are outside the scope of this report but are analysed elsewhere.[76]

## International and national policy commitments

While international law sets binding, albeit limited, obligations, states' policy commitments supplement legal obligations with a more detailed framework for understanding the content of responsible military AI procurement.

The concept of 'responsible' military AI has emerged from recent international policy deliberation. The governments of France, the USA, the UK and Japan, as well as the European Parliament and NATO, have set out the principles that are meant to guide their responsible development and use of military AI. Many more states have endorsed international sets of principles on responsible military AI: the USA-led Political Declaration on Responsible Military Use of AI and Autonomy of 2023, the Netherlands and South Korea–led Blueprint for Action adopted at the REAIM Summit in 2024, and the Paris Declaration on Maintaining Human Control in AI Enabled Weapon Systems adopted at the AI Action Summit held in Paris in February 2025.

These various documents range from high-level political statements and strategic documents to technical guidance. Despite variations in formulation and institutional origin, several core themes demonstrate emerging consensus on fundamental governance requirements (see table 3.1). These shared features are evidence of states' expectations when it comes to the development and use of military AI. The remainder of this section discusses the key principles in turn.

### *Effects on humans, equitability and bias mitigation*

Equitability and bias mitigation appear in nearly every policy framework, requiring deliberate steps to minimize unintended algorithmic bias and ensure equitable outcomes. This includes a proactive requirement for systematic assessment of impacts on humans and mitigation of harmful biases (the documents do not specify the kinds of bias). Though unstated, it seems that this principle demands balancing operational effectiveness with equitability requirements.[77]

Implementation of these principles at the procurement stage would involve scrutinizing the design of AI systems and assessing their technical performance of an AI capability. As discussed in chapter 2, this is a difficult task as machine-learning-based systems are opaque and often require a large dataset, which makes the identification of the harmful bias in the design challenging. Existing methods for testing and evaluating the behaviour and impact of machine-learning-based systems are far from comprehensive while also being resource intensive. This makes it difficult for procurement agencies to test systems across all potential deployment contexts and assess long-term impacts, especially with adaptive learning systems.

### *Traceability, explainability and understanding*

All policy frameworks mandate that relevant personnel possess an adequate understanding of AI capabilities, limitations and outputs. It seems that this requirement encompasses transparent development methodologies, auditable design procedures, comprehensive documentation, and targeted training programmes to mitigate automation bias and enable context-informed operational judgements.

[76] Boulanin and Verbruggen, *Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies* (note 74); Goussac and Liivoja (note 72); and Vestner and Rossi (note 74).

[77] Blanchard, A. and Bruun, L., 'Bias in military artificial intelligence', SIPRI Background Paper, Dec. 2024.

These principles have two facets: personnel competency requirements and system-level operational and data transparency requirements. Implementation of this principle at the procurement stage entails the challenging task of translating these goals into measurable requirements and compliance standards directed both at organizations that develop AI capabilities and at actors that will acquire those capabilities.

#### *Reliability, safety and security*

Reliability, security and safety assurance features prominently across frameworks, requiring rigorous TEVV processes throughout system lifecycles. Frameworks consistently demand implementation of safeguards to detect and mitigate malfunction risks, identify unintended consequences, and enable system disengagement when necessary. For adaptive or self-learning systems, continuous monitoring mechanisms ensure preservation of critical safety parameters—addressing unique challenges posed by systems that evolve post-deployment. At the procurement stage, implementation of these principles raises questions about how to test unpredictable behaviours in complex systems and how to validate performance (particularly in adversarial conditions).

#### *Responsibility and accountability*

Every framework emphasizes that humans must remain responsible for the use of military AI. This includes maintaining human control over the use of force and ensuring appropriate human judgement and oversight, particularly for high-consequence applications such as autonomous weapon systems. States implementing this principle at the procurement stage need to decide and clarify how to allocate responsibility among the various actors involved in the development and use of a military AI capability, and how liability will be managed.[78]

#### *Governability*

Governability features in multiple frameworks, requiring AI systems to have explicit, well-defined uses and mechanisms to fulfil intended functions while avoiding unintended behaviour. Implementation of this principle means suppliers of military AI capabilities need clarity and certainty about what military clients expect from the AI capabilities they procure.

### Implications for the procurement of military AI

Collectively, governance frameworks point towards three fundamental requirements for responsible procurement of military AI.

#### *Interrogate whether and why the military AI capability is needed*

First, states need to interrogate whether and why the military AI capability is needed. The principles of governability and accountability that feature across policy frameworks demand that AI systems have explicit, well-defined uses and that humans remain responsible for their employment. This requires procurement authorities to move beyond traditional capability assessments focused solely on operational effectiveness. Before proceeding with acquisition, states must critically examine the strategic rationale for the capability, whether alternative (non-AI-enabled) approaches could achieve the same objectives, and whether the capability can realistically be employed in compliance with the state’s obligations, policies and resources.

[78] Bo, M., Bruun, L. and Boulanin, V., *Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS* (SIPRI: Stockholm, Oct. 2022.

### *Maintain or oversee an independent capacity to test supplier claims about the capability*

Second, states must maintain or oversee an independent capacity to test supplier claims about the capability. The principles of explainability, reliability and bias mitigation all require rigorous evaluation of AI system performance, yet military AI capabilities are methodologically difficult and resource-intensive to assess. States cannot simply accept supplier assurances about system reliability, fairness or predictability. Procurement authorities require either internal technical expertise or access to trusted third-party evaluators capable of validating performance claims across potential deployment contexts. This capacity for independent assessment is particularly critical given the iterative nature of AI development and the challenges of testing adaptive or self-learning systems.

### *Ensure clear lines of communication and responsibility with regard to procurement decision-making*

Third, states must ensure clear lines of communication and responsibility regarding procurement decision-making. The accountability principle demands that responsibility be allocated among the various actors involved in the development and use of military AI capabilities. Procurement represents a critical juncture where decisions about supplier selection, contractual requirements and acceptance criteria shape subsequent possibilities for responsible employment. Effective implementation requires multidisciplinary evaluation integrating legal, technical and ethical expertise, as civilian frameworks consistently recommend. It also requires clarity about who bears responsibility for procurement decisions, how information flows between technical evaluators and decision-makers, and how liability will be managed when AI systems produce unintended outcomes.

How these general requirements can be operationalized in practice is the focus of the next chapter.

# 4. Towards responsible procurement of military AI

Chapter 2 identified that states are looking into speeding up military AI procurement in three ways: (*a*) deeper collaboration with suppliers to match capability needs with products; (*b*) the adoption of more iterative acquisition processes; and (*c*) trying different methods to achieve assurance of the lawfulness, safety and reliability of capabilities. Chapter 3 found that legal obligations and policy commitments to responsible AI in the military domain have practical implications for military procurement, suggesting three requirements: (*a*) interrogating whether and why a military AI capability is needed; (*b*) maintaining independent capacity to test supplier claims; and (*c*) ensuring clear lines of communication and responsibility in procurement decision-making. This chapter examines reasons and methods for combining these two dimensions—that is, why and how states' efforts to make military procurement more 'AI-ready' should and can be aligned with their legal obligations and policy commitments to responsible military AI (see figure 4.1).

### A window of opportunity: procurement as a pivotal mechanism to operationalize commitments around responsible military AI

Many modern militaries see a need to adapt their military procurement processes to accelerate the acquisition of AI capabilities and other emerging technologies. There is also an emerging consensus in international policy discussion on responsible AI in the military domain that it is time for states to put the high-level principles they agreed on through the GGE on LAWS and the REAIM process into practice.[79] These concurrent trends represent a window of opportunity: states adapting their procurement processes can, and should, seize the occasion to operationalize their obligations and commitments to responsible military AI.

The procurement stage represents a pivotal intervention point where abstract principles and legal duties can be translated into concrete specifications, supplier obligations and verification mechanisms. Specifically, there are three main reasons why legal obligation and policy principles for responsible military AI can and should be front of mind for military procurement actors as they look into adapting their military procurement processes.

First, design decisions that affect how military AI capability can be used—including whether it can be used responsibly—are often made as part of the procurement process. This includes in-service considerations regarding upgrades, maintenance, technical support and training; and choices regarding interpretability, oversight mechanisms, human–machine interaction, and even TEVV requirements.[80] The legal review obligation under API Article 36 reinforces this point: at the development or acquisition stage, an assessment must already be made as to whether the intended weapon system is prohibited or is capable of being used in compliance with IHL.

Second, suppliers of military AI capabilities need clarity and certainty about what military clients expect from the AI capabilities they procure and from the suppliers themselves. Clear requirements enable suppliers to design systems that meet military

[79] See e.g. Global Commission on Responsible AI in the Military Domain (GC REAIM), *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities and Governance of Artificial Intelligence in the Military Domain* (GC REAIM: The Hague, Sep. 2025); Rosen, B., 'From principles to action: Charting a path for military AI governance', Carnegie Council for Ethics in International Affairs, 12 Sep. 2024; and Sanders, L., Livoja, R. and Assaad, Z., 'REAIM Summit 2024: Slowly but surely towards better governance of military artificial intelligence? From The Hague to Seoul', Australian and New Zealand Society of International Law, 30 Oct. 2024.

[80] Wallin (note 24).

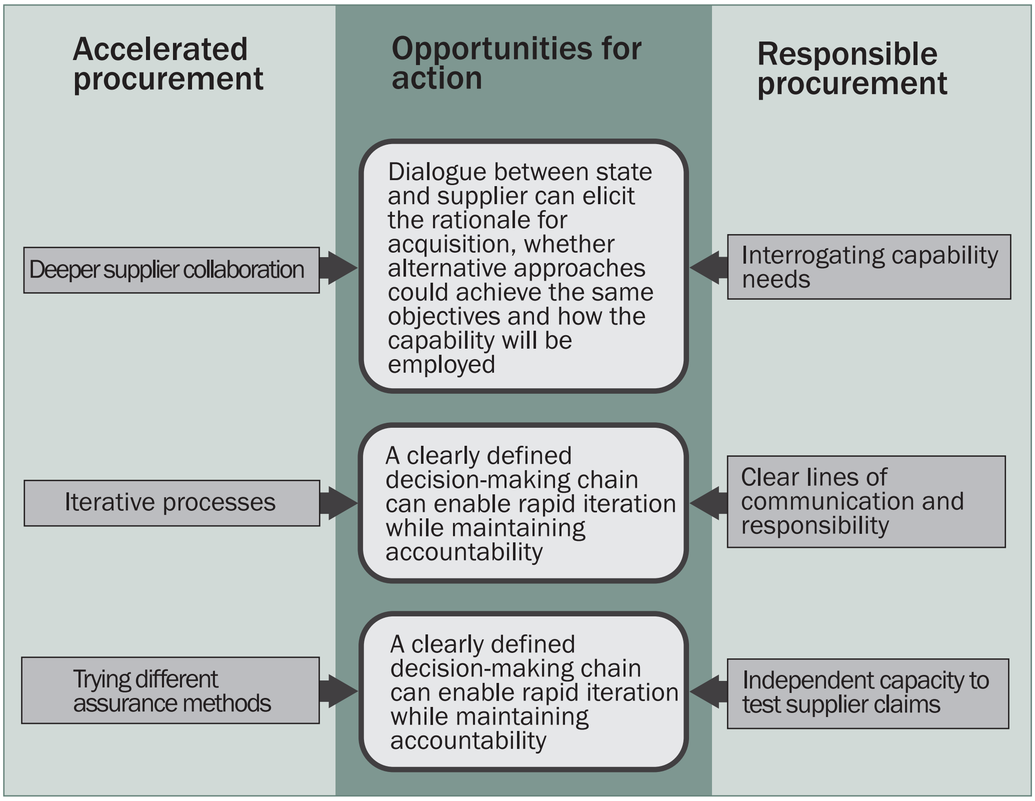
Accelerated procurement
Opportunities for action
Responsible procurement
Deeper supplier collaboration
Dialogue between state and supplier can elicit the rationale for acquisition, whether alternative approaches could achieve the same objectives and how the capability will be employed
Interrogating capability needs
Iterative processes
A clearly defined decision-making chain can enable rapid iteration while maintaining accountability
Clear lines of communication and responsibility
Trying different assurance methods
A clearly defined decision-making chain can enable rapid iteration while maintaining accountability
Independent capacity to test supplier claims

**Figure 4.1.** Opportunities for aligning acceleration of military AI procurement with commitments to responsible military AI

AI = artificial intelligence.

needs, including the appropriate safeguards. Without such clarity, suppliers may struggle to align their products with states' expectations, while militaries risk investing in capabilities that cannot be used in compliance with their legal obligations or policy commitments.

Third, measures critical to implementing principles of responsible military AI may be concurrent with or form part of the procurement process. Several measures that can implement responsible military AI are procurement-adjacent. For example, legal reviews to ascertain whether an AI capability can be used in accordance with the state's international law obligations occur during the procurement process (and should be done as early as possible in the design and development of a military AI capability).[81] Rigorous and independent testing and evaluation of AI capabilities—essential for implementing principles of safety and reliability—are needed at the procurement stage. Information sharing between suppliers and militaries in the design and improvement of AI capabilities is important for implementing principles related to safety and reliability at the procurement stage.

Rather than viewing responsible procurement as an additional burden or trade-off, states can recognize it as the practical mechanism through which their policy commitments and legal obligations are given effect. The next section explores how states could leverage some of their proposed changes around procurement processes to operationalize their commitments around the responsible adoption of military AI.

[81] ICRC (note 71), p. 24.

## Connections between procurement reforms and commitments to responsible AI in the military domain

### *The relationship between supplier collaboration and the interrogation of capability needs*

States are increasingly engaging directly with industry partners rather than relying solely on the traditional method of one-way specification-driven acquisition. Ukraine's Brave1 platform, the US DIUx's engagement with commercial technology providers and the British MOD's IPM all reflect a view by states (and suppliers) that a more dynamic collaboration between military and technology suppliers can help states more easily and quickly leverage innovation from the commercial sector.

This shift towards a more collaborative approach creates an opportunity to operationalize the governance requirement that states critically examine whether and why a military AI capability is needed. When procurement authorities engage with suppliers to match capability needs with available products, they necessarily confront questions about the rationale for acquisition, whether alternative approaches could achieve the same objectives and how the capability will be employed.[82] The dialogue inherent in collaborative procurement can surface these questions in ways that traditional specification-driven models might not.

Realizing this opportunity requires that such engagement be structured to facilitate genuine interrogation of need, not merely the expedited acquisition of available technologies.[83] The risk otherwise is that supplier collaboration becomes a mechanism for the industry to shape military requirements rather than for states to ensure their procurement decisions reflect considered strategic judgement.

### *The relationship between iterative acquisition processes and lines of responsibility and communication*

The case studies in chapter 2 suggest a broad shift away from linear development cycles towards spiral approaches that allow for rapid fielding of minimum viable capabilities followed by incremental improvement. The British MOD's IPM explicitly adopts spiral development as its default approach. These iterative processes demand clear lines of responsibility and communication from senior leaders to operational decision-makers.

When capabilities are fielded incrementally and improved based on operational experience, the chain of decision-making authority must be sufficiently defined to enable rapid iteration while maintaining accountability. The MOD's establishment of new checks and balances at programme inception, with expert-informed decision-making and Integration Design Authority oversight, provides an example of how iterative acquisition can be structured to clarify lines of responsibility.

The challenge lies in ensuring that acceleration does not erode these accountability mechanisms. Both the USA's and the UK's unresolved tensions between acquisition speed and responsible governance illustrate this risk: without clarity about how responsibility is allocated across compressed timelines, iterative processes might fragment accountability instead of enhancing it.

### *The relationship between assurance and independent testing capacity*

As part of accelerated military AI procurement processes, states are exploring methods of addressing the challenge of achieving assurance about the lawfulness, safety, secur-

[82] Knack, A., Carter R. J. and Babuta, A., *Human–Machine Teaming in Intelligence Analysis: Requirements for Developing Trust in Machine Learning Systems* (Centre for Emerging Technology and Security: London, Dec. 2022), sect. 4.3.

[83] For an example of the content of such engagement see Article 36 Legal's Lawful by Design Initiative.

ity and reliability of AI-enabled systems, whether through in-house pre-deployment testing, third-party assurance providers or contractual requirements on suppliers. The US DOD's responsible AI S&I pathway calls for standard AI contract language addressing independent test and evaluation and performance monitoring. The UK's AI Model Arena provides a standardized platform to evaluate AI models against Defence benchmarks.

But demanding assurances is not the same as independently verifying them. As noted in chapter 3, states cannot simply accept supplier assurances about system reliability, fairness or predictability. States must maintain the capacity to verify that the technology provided meets expectations. To this end, procurement authorities could explore one or both of two options: develop (or maintain) internal relevant technical expertise within the procurement agency or other relevant agency; or rely on trusted third-party evaluators that can audit the supplied capabilities.

# 5. Findings and recommendations

Current trends in military AI procurement reform are neither inherently aligned with nor opposed to responsible military AI requirements. Supplier collaboration, iterative acquisition and demands for assurances each present opportunities to operationalize these requirements, but only if deliberately structured to do so (as described in chapters 2 and 4). While procurement reform remains beholden to a range of factors, including security and economic concerns, treating procurement reform solely as a means of achieving speed risks subordinating responsible governance to actual or perceived urgency, with consequences for legal compliance and the credibility of states' policy commitments (described in chapter 3). This chapter outlines the key findings of this report and makes practical recommendations on how states pursue the responsible procurement of military AI that balances these factors.

## Findings

### *1. States are seeking to accelerate procurement of military AI, including through closer collaboration with industry, more iterative procurement processes and different methods for achieving assurance.*

There are clear factors driving states to reconsider their military procurement frameworks to accelerate military AI procurement, ranging from strategic competition through operational lessons from contemporary conflicts, to technology sector advocacy. A review of selected state practices and consultations with experts indicate that states are considering three general pathways to expedite the acquisition of military AI capabilities: (*a*) deepening collaboration with suppliers to match capability needs with products; (*b*) adopting more iterative acquisition processes; and (*c*) trying different methods to achieve assurance about lawfulness, safety and reliability. Less clear is how states' formal commitments to responsible military AI (where they exist) are being integrated with modified procurement processes and timeframes.

### *2. States' legal obligations and policy commitments to responsible military AI have practical implications for their procurement of military AI.*

International law sets binding, albeit limited, obligations relevant to military procurement, the most direct of which is the obligation to review the legality of new weapons, means and methods of warfare before they are employed (API Article 36). Many states have adopted high-level policy commitments to the responsible development and use of AI in the military domain. These policy principles have direct and very practical implications for the procurement process. Taken together, the legal obligations and the high-level policy principles require procurement authorities to have the ability to (*a*) interrogate whether and why a military AI capability is needed; (*b*) maintain independent capacity to test supplier claims; and (*c*) ensure clear lines of communication and responsibility in procurement decision-making. The challenge is how to find an efficient way to satisfy these requirements and to condense those requirements to avoid redundant administrative burdens.

### *3. States' efforts to modify their procurement processes provide an opportunity to operationalize their high-level obligations and commitments to responsible military AI.*

Rather than viewing responsible procurement as an additional burden, states can recognize it as the practical mechanism through which their policy commitments and legal obligations are given effect.

There are three main reasons for this connection between procurement and responsible military AI. First, design decisions that affect how military AI capabilities can be used (including whether they can be used responsibly) are often made as part of the procurement process. Second, suppliers of military AI capabilities—whether they are established defence industry companies or tech start-ups—need clarity and certainty about what military clients expect from the AI capabilities they procure. Third, measures critical to implementing principles of responsible behaviour may be concurrent with or form part of the procurement process.

Though procurement reform is not the only means to give effect to policy commitments to responsible military AI, states adapting their procurement processes can seize this opportunity to implement their commitments to responsible military AI. Collaborative engagement with industry can become a mechanism for interrogating capability needs instead of merely accelerating acquisition. Iterative processes can clarify rather than fragment lines of responsibility if accountability mechanisms are embedded at each decision point. Demands for supplier assurances can strengthen rather than substitute for independent testing capacity if supported by genuine investment in evaluation infrastructure.

## Recommendations

There are three facets to how states can engage in responsible procurement of military AI. The first relates to how they adapt their own procurement processes. The second relates to their relationship with AI capability suppliers. The third relates to how states address military AI procurement together.[84]

### *1. States should adapt their procurement processes to give effect to their high-level obligations and commitments to responsible development and use of military AI.*

The key phases in the procurement process (see chapter 1) offer significant opportunities for embedding responsible AI considerations.

For example, at the requirements specification stage, a military's task is to develop explicit, testable and contractable requirements before issuing tenders or requests for proposals. If principles of responsible behaviour are not considered at this stage, it may be difficult to 'retrofit' measures aimed at implementing them at a later stage. Specifying technical parameters and performance standards at the requirements specification stage can help ensure that 'downstream' procurement actions align with international law and principles of responsible military AI.

Similarly, the contracting stage is a critical opportunity for implementing principles of responsible behaviour because it determines what the supplier must deliver *and prove* (including claims about the results of testing and assurance processes), who is accountable for certain risks and failures, and what obligations and requirements are borne by the parties. The contracting phase also provides an opportunity to support a state's legal review process by flagging requirements for iterative assessment as military AI capabilities evolve and requirements for suppliers sharing documents necessary for robust legal reviews.

An important first step is to ensure that policies, procedures and practices relating to military procurement explicitly refer to any national policies and commitments related to responsible military AI. The specific measures necessary to give effect to high-level legal obligations and policy commitments to responsible military AI are, however,

[84] While the recommendations are addressed to states, further research work would be useful on the role that other actors—such as suppliers or international institutions—play or could play in implementing states' legal obligations and policy commitments related to responsible military AI.

not always straightforward. Interrogating whether and why a military AI capability is needed and assessing supplier claims requires technical literacy. Implementation of principles of responsible military AI at the procurement stage is challenged by the opacity of some AI capabilities, which complicates traditional TEVV processes. Iterative development processes and adaptive systems challenge more static requirements, while commercial sensitivities limit algorithmic transparency. Addressing these challenges demands further work.

### *2. States should develop and publish documents articulating clear expectations for suppliers of military AI capabilities.*

Suppliers of military AI capabilities—whether established defence industry companies or tech start-ups—need clarity and certainty about what military clients expect from the AI capabilities they procure, as design decisions affecting responsible use are often made during the procurement stage. Without such guidance, procurement authorities and suppliers alike face a more complex process of pre-contract evaluation, back-and-forth requests for documentation and uncertainty around requirements.

States should make public their expectations of suppliers, addressing the technical parameters and performance standards necessary to implement principles of equitability and bias mitigation, traceability and explainability, reliability and security, accountability and governability. Such documents should aim to translate abstract principles into concrete specifications regarding acceptable error rates, confidence thresholds, documentation requirements and testing protocols.

Clear articulation of expectations offers potential benefits. It could enable suppliers to design systems that meet responsible military AI requirements from inception rather than requiring costly retrofitting. It could facilitate more efficient procurement processes by reducing ambiguity and iteration. Finally, it could help states find alignment between national procurement processes and policy commitments to responsible military AI and relevant legal obligations.

### *3. States should address the responsible procurement of military AI in international policy discussions.*

At the moment, states that are adapting or considering adapting their procurement processes to facilitate rapid adoption of military AI are independently navigating fundamental questions about how to implement their legal obligations and policy commitments relevant to responsible development and use of military AI, without the benefit of shared learning or common vocabularies. It is not clear exactly how individual states' frameworks align with principles of responsible development and use of military AI.

Deepening international conversations about responsible military AI procurement is a pathway for operationalizing shared or common principles and legal frameworks. By making procurement practices an explicit component of international military AI governance discussions, states can strengthen both national implementation of responsible AI principles and broader international frameworks.

Early opportunities for such conversations exist at the REAIM summits, the ongoing workshops among states supporting the USA-led Political Declaration and the USA-led AI Partnership for Defence, and at the informal exchanges on AI in the military domain slated to take place in Geneva in 2026 pursuant to the resolution adopted by the UN General Assembly First Committee.[85]

[85] US DOD, Chief Digital and Artificial Intelligence Office (CDAO), 'DOD CDAO holds eleventh AI Partnership for Defense', Press release, 13 Aug. 2025; and United Nations, General Assembly, First Committee, 'Artificial intelligence in the military domain and its implications for international peace and security', A/C.1/80/L.46, 15 Oct. 2025, para. 10.

## About the authors

**Netta Goussac** is an Associate Senior Researcher in the Governance of Artificial Intelligence (AI) Programme at SIPRI. Her work focuses on legal frameworks related to the development, acquisition and transfer of weapons.

**Dr Vincent Boulanin** is Senior Researcher and Director of the Governance of AI Programme at SIPRI. He leads SIPRI's research on how to govern the impact of AI on international peace and security.

**STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE**

Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org