sipri

MAPPING THE MILITARY ARTIFICIAL INTELLIGENCE INDUSTRY

Actors, Influence and Policymaking

ALEXANDER BLANCHARD AND LAURA BRUUN

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.

GOVERNING BOARD

Stefan Löfven (Chair)
Dr Zeid Ra'ad Al Hussein
Dr Mohamed Ibn Chambas
Dr Noha El-Mikawy
Jean-Marie Guéhenno
Dr Patricia Lewis
Dr Nathalie Tocci
Dr Jessica Tuchman Mathews
Brian A. Wong

DIRECTOR

Karim Haggag



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

MAPPING THE MILITARY ARTIFICIAL INTELLIGENCE INDUSTRY

Actors, Influence and Policymaking

ALEXANDER BLANCHARD AND LAURA BRUUN

November 2026

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

© SIPRI 2026
DOI: https://doi.org/10.55163/ILNE2191

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, without the prior permission in writing of SIPRI or as expressly permitted by law.

Contents

Acknowledgements iv
Summary v
Abbreviations vi

1. Introduction 1
Scope 2
Methodology and structure 3
Box 1.1. Defining military artificial intelligence and the military artificial intelligence industry 2

2. Mapping actors in the military AI industry 4
What makes a company part of the military AI industry? 4
Who are the actors? 4
Box 2.1. Venture capital firms 10
Figure 2.1. The military AI stack 5
Table 2.1. Business model characteristics of key military AI company types 6

3. Normative positioning and pathways to influence 16
Industry's normative positions around AI in the military domain 16
Pathways to influence 23
Box 3.1. Norms and norm development 18
Box 3.2. Case study: Microsoft's norm entrepreneurship 22
Box 3.3. The military-industrial complex 25
Table 3.1. The military AI industry's pathways to influence 24

4. Managing industry engagement: Mitigating the risks of regulatory capture 31
The context of contemporary international governance 31
Vulnerabilities in the military AI policy process 32
Managing the risks of regulatory capture 34

5. Conclusions 36
Key findings 36
Recommendations 37

About the authors 38

Acknowledgements

SIPRI and the authors express their sincere gratitude to the Ministry of Foreign Affairs of the Netherlands for its generous financial support for this project.

The authors also wish to thank SIPRI colleagues Vincent Boulanin, Netta Goussac, Alina Hueber, Jules Palayer, Elisabeth Sköns and Pieter Wezeman for their invaluable insights and feedback throughout the project. In addition, the authors thank all the experts who in various ways contributed to the research or publication of the report: Ray Acheson, Anke Allenhöfer, Rupert Barrett-Taylor, Renaud Bellais, Ingvild Bode, Jessica Dorsey, Marijn Hoijtink, René Holbach, Martine Jaarsma, Arnav Jagasia, Michael Karimian, Yiokasti Mouraditi, Anna Nadibaidze, Jacob Parakilas, Thomas Plomp, Emma Salisbury, Mark Silverman, Elke Schwarz, Ali Riza Taskale and Joost van Oostenbruggen.

Finally, the authors acknowledge the invaluable editorial work of the SIPRI Editorial Department.

Summary

Rapid advances in artificial intelligence (AI) are changing how states prepare for and conduct war. While these technologies promise military advantages, they also pose serious risks to international peace and security. In the growing international policy efforts to understand and govern military AI, many states agree that industry should have a seat at the table. For this engagement to be effective, policymakers need a working understanding of industry as a policy actor. At a minimum, this means knowing who 'industry' is in this context; what motivates its involvement, including its preferences with respect to policy outcomes; and how it seeks to influence policy discussion. At present, there are few resources to support policymakers in this way.

The military AI industry is not a monolith but a stratified and shifting ecosystem of different actors, products, services and relationships. Actors in the industry can be grouped into four categories according to business model: legacy primes; neo-primes and defence start-ups; big tech; and foundation model providers. No single type of actor spans the whole industry, and each is increasingly dependent on partnerships, consortia and acquisitions, in a way that, in the near term, obscures public understanding of who builds what and for whom, and, in the long term, is likely to drive industry consolidation.

The military AI industry directly and indirectly shapes regulatory and normative outcomes in various ways. Firms bring with them normative positions on how AI should be governed and used in the military domain, shaped by their business model, their relationship to the state and their exposure to public scrutiny. Industry can shape regulatory and normative outcomes through several pathways, which can be gathered into three categories. First is people and places, which includes lobbying at the national and international levels; the movement of personnel between government and industry; and participation in international policy debates. Second is narrative-building, where actors compose 'stories' to frame policy issues and operational and strategic needs. These are reflected in, for example, open letters, manifestos and promotion materials. Third is legal and contractual means, which can allow firms to embed preferences into product terms of use.

States have yet to take a structured approach to industry participation in international policy efforts on military AI, leaving industry actors to shape their own role. This creates a risk of regulatory capture in which the boundary between policy being informed by industry input and policy being shaped in industry's favour becomes difficult to discern. This risk is heightened by the presence of three vulnerabilities in international policy efforts: a poorly defined role for industry; a lack of normative agreement among states; and limited institutional capacity within ministries of foreign affairs and other state bodies to interrogate industry positions.

States should develop criteria for determining which industry actors are relevant to a given aspect of the policy process. Such criteria could include a firm's proximity to use-of-force decisions, its influence over the behaviour of an AI-enabled system and its role in linking other suppliers. States should also take a structured approach to industry engagement in relevant international forums, drawing on frameworks such as the Business Council for Ethics of AI of the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the World Health Organization's Framework of Engagement with Non-state Actors. Finally, states should build the capacity to differentiate technical input from advocacy and to draw on a wider range of expertise than industry alone.

Abbreviations

AI	Artificial intelligence
BDI	Bundesverband der Deutschen Industrie (Federation of German Industries)
BDSV	Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie (Federation of German Security and Defence Industries)
C4ISR	Command, control, communications, computers, intelligence, surveillance and reconnaissance
CEO	Chief executive officer
CTO	Chief technology officer
DOD	Department of Defense (of the United States)
EU	European Union
FENSA	Framework of Engagement with Non-state Actors (of the World Health Organization)
FMP	Foundation model provider
IDF	Israel Defense Forces
LLM	Large language model
MFA	Ministry of foreign affairs
MOD	Ministry of defence
REAIM	Responsible Artificial Intelligence in the Military Domain
R&D	Research and development
TEVV	Test, evaluation, verification and validation
UAS	Uncrewed aerial system
UN	United Nations
WHO	World Health Organization

1. Introduction

Recent advances in artificial intelligence (AI), particularly the emergence of general-purpose foundation models, are changing how states prepare for and conduct war. AI-enabled systems are now used for intelligence analysis, targeting, logistics and planning and have been deployed in active conflicts.[1] While these applications promise some military advantages, they also pose serious risks to international peace and security.[2]

In the growing international policy efforts to understand and govern military applications of AI, many states agree that industry should have a seat at the table.[3] Many of the relevant capabilities are developed—and often fielded—by commercial actors, and the motivation to involve industry in policy efforts flows from a desire by states to take advantage of industry's expertise and to ground governance frameworks in technical realities. For example, the Blueprint for Action outcome document of the 2024 Responsible AI in the Military Domain (REAIM) summit calls on states to invite industry—along with other stakeholders—to help understand and address the risks of military applications of AI and to leverage its benefits.[4] Likewise, the 2026 REAIM outcome document urges states to strengthen links with industry in translating principles of responsible use into practice.[5] Similarly, in 2025 the United Nations secretary-general invited industry to submit views on military AI alongside states and civil society.[6] Some industry actors have already responded to such calls, for example by participating in international conferences and briefing states at the UN Security Council.[7]

While industry involvement can benefit the policy conversation, it also carries risks. For example, engagement may primarily benefit industry actors, with little value returned to the policy process itself. To effectively engage with industry—that is, to enjoy the benefits and avoid the pitfalls of its involvement in these efforts—policymakers need a working understanding of industry as a policy actor. This requires knowing, at minimum, three things: who 'industry' is in this context; what motivates its involvement in this space, including its preferences with respect to policy outcomes; and how industry seeks to influence policy discussion. Presently, there are few resources to support policymakers in this way.[8] This report maps the 'military AI industry' (defined

[1] Mishra, P. et al., 'Code, command, and conflict: Charting the future of military AI', Belfer Center for Science and International Affairs, Nov. 2025; and Bartenstein, B. and Karra, K., 'Inside the US "kill chain" that destroyed an Iranian school', Bloomberg, 18 Sep. 2026.

[2] Blanchard, A. and Bruun, L., *Autonomous Weapon Systems and AI-Enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses* (SIPRI: Stockholm, June 2025); Erskine, T. and Miller, S E., 'AI and the decision to go to war: Future risks and opportunities', *Australian Journal of International Affairs*, vol. 78, no. 2 (Apr. 2024); Chernavskikh, V. and Palayer, J., 'Impact of military artificial intelligence on nuclear escalation risk', SIPRI Insights on Peace and Security no. 2025/06, June 2025; and Couture, N., 'AI's growing role in weapons development raises security concerns', Organization for World Peace, 14 Sep. 2026.

[3] Afina, Y., *The Global Prism of Military AI Governance: Reflections from the 2025 Regional Consultations on Responsible AI in the Military Domain* (UNIDIR: Geneva, 2026), p. 67.

[4] REAIM Summit 2024, 'REAIM Blueprint for Action', Seoul, 10 Sep. 2024.

[5] REAIM Summit 2026, 'REAIM Pathways to Action', A Coruña, 5 Feb. 2026.

[6] United Nations, General Assembly, 'Artificial intelligence in the military domain and its implications for international peace and security', Report of the secretary-general, A/80/78, 5 June 2025.

[7] REAIM Summit 2023, 'Alex Karp's (CEO Palantir Technologies) vision on AI in the military domain', 15 Feb 2023; UK Stop Killer Robots, 'Informal exchanges on artificial intelligence in the military domain and it's [*sic*] implications for international peace and security—Day 1', 16 June 2026; and Nichols, M., Irish, J. and Rozen, C., 'AI leaders to brief UN amid warnings the technology could slip beyond human control', Reuters, 23 Sep. 2026.

[8] E.g. Slijper, F., Siatitsa, I. and Kouvakas, I., *When Algorithms Go To War: Tech Giants, the Arms Industry and the Weaponisation of AI* (PAX and Privacy International: June 2026); Transparency International, *Defence Industry Influence in Germany: Analysing Defence Industry Influence on the German Policy Agenda* (Transparency International: Oct. 2020); Toh, A. and Ayoub, E., *The Business of Military AI* (Brennan Center for Justice at New York University School of Law: New York, Mar. 2026); and Maaser, L. and Verlaan, S., *Big Tech Goes to War: Uncovering the*

Box 1.1. Defining military artificial intelligence and the military artificial intelligence industry

For the purposes of this report, 'artificial intelligence (AI)' is defined as the broad set of techniques, technologies and applications through which computers and robots are enabled to solve complex problems that previously yielded only to human cognition—together with the data collection, processing and storage technologies on which they depend.[a] 'Military AI' is then AI that is employed for military purposes. This is a broad definition, but it reflects the fact that 'AI' itself has a broad meaning and that AI models depend on a wide range of technologies to function.

The 'military AI industry' is broadly defined here as a collective term for entities—whether privately owned corporations, publicly traded corporations or government-owned corporate entities—that provide AI-related products or services, directly or indirectly, to militaries. This includes companies that interface directly with military organizations as well as those providing products and services supporting upstream applications. The military AI industry comprises companies involved in the global 'arms market', here defined as global and domestic sales and purchases of military goods and services, usually between military contractors and governments.

In the international policy debate on military AI, states interchangeably refer to the need to engage 'industry' and 'the private sector'. The more inclusive term 'industry' is preferred in this report since it encompasses both private companies and public–private consortia.

[a] See the detailed definition in Boulanin, V., 'Artificial intelligence: A primer', ed. V. Boulanin, *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. I, *Euro-Atlantic Perspectives* (SIPRI: Stockholm, May 2019).

in box 1.1) by addressing each of these questions in turn. It does so with the aim of not only equipping policymakers to make more effective decisions about the nature of their engagement with industry, but also to help states exercise normative authority over military uses of AI.

Indeed, what is ultimately at stake here is something stressed by states themselves: that decision making about appropriate governance of AI in the military domain should remain the sole prerogative of states.[9] Whether states retain the capacity for independent decision making is not only a question of their nominal control over decision-making processes, but whether their agents (e.g. policymakers) are capable of engaging with industry from a position of informed authority. Failure to do so could mean that the governance of these technologies is ceded—whether by design or default—to the industry actors supplying them.

Scope

This report maps categories of industry actors rather than specific companies. In a rapidly changing military-industrial landscape, a map of categories of actors is less likely to become obsolete than an enumeration of specific actors at a given moment in time. The scope of the mapping is predominantly (but not exclusively) based on the military innovation contexts in the United States and parts of Europe (primarily Western and member states of the North Atlantic Treaty Organization, NATO). This is due primarily to factors of language and information availability. It also reflects the report's focus on private sector involvement in military AI. This focus most readily fits market economies where firms operate independently of the state and the state acts primarily as customer, regulator and funder.

Growing Role of US and European Technology Firms in the Military–Industrial Complex (Rosa-Luxemburg-Stiftung: Berlin, 2022).

[9] United Nations, A/80/78 (note 6), para. 48.

This focus has consequences for how far the findings can be generalized. Significant military AI ecosystems, notably in China and the Russian Federation, are covered only partially. The categories of actors identified here have counterparts in such ecosystems, but the relationships between them and between state and industry may differ substantially and should not be assumed to mirror those described in this report.[10]

Additionally, the preponderance of the US-based firms referenced in this report reflects economic and historic factors. For instance, that the USA has the largest military budget, including for research and development (R&D), and it has a historic propensity to support military innovation, which is an important factor explaining why US companies dominate the military AI industry.[11]

Methodology and structure

Research for this report comprised a literature review of publicly available information in English (academic articles, news articles, company materials, blog posts, podcasts) and direct engagement with subject-matter experts, primarily through 20 expert interviews and participation in events (e.g. policy meetings, dialogues, arms conventions). The semi-structured interviews took place online between March and May 2026 and included experts from academia, states, industry, military organizations, civil society and UN bodies.

This report continues in chapter 2 by mapping the military AI industry. It groups companies into four categories—legacy primes, neo-primes and defence start-ups, big tech, and foundation model providers (FMPs)—and traces the relationships between them. Chapter 3 then surveys the normative positions that industry has taken on military AI governance and maps the pathways through which those positions are translated into practice. The report goes on in chapter 4 to address a key risk posed by industry involvement in policy debate: regulatory capture. It sets out what capture is and the vulnerabilities in policy processes that make capture more likely, before turning to how policymakers might guard against it. Chapter 5 concludes the report with key findings and recommendations for how states can structure industry engagement in international policy efforts on military AI.

[10] Dupont-Sinhsattanak, A., 'Modernizing a giant: Assessing the impact of military–civil fusion on innovation in China's defence-technological industry', *Defence and Peace Economics*, vol. 37, no. 2 (Mar. 2026); George, J., 'China's PLA challenges and competitions', Center for Security and Emerging Technology, 28 Apr. 2026; and Kozyulin V., 'Assessing Russia's national strategy for AI development', eds M. Raska and R. A. Bitzinger, *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories* (Routledge: Abingdon, 2023).

[11] Heidenkamp, H., Louth, J. and Taylor, T., *The Defence Industrial Triptych: Government as a Customer, Sponsor and Regulator of Defence Industry* (Routledge: Abingdon, 2014), chapter 3.

2. Mapping actors in the military AI industry

A core condition for constructive involvement of industry in international policy discussions on AI in the military domain is an appreciation of which actors make up the military AI industry. To support this understanding, this chapter maps key types of company and the products and services that they offer, as well as the relationships these actors have both with each other and with the state.

What makes a company part of the military AI industry?

The military AI industry extends far beyond those companies developing AI models; it encompasses a heterogeneous range of actors supporting a broader AI ecosystem through the provision of various products and services. One way to think about the industry—about the relationships between the products, services and actors supporting the adoption of military AI—is the 'stack', a term drawn from computer science that refers to the layered ecosystem of hardware that enables AI applications (see figure 2.1).[12]

The bottom layer of the stack is hardware and infrastructure. It comprises physical computational resources (e.g. computer chips), storage and networks. Examples include data centres, fibre-optic cables, energy grids and cloud infrastructure. The middle layer is the foundational software and programming layer. This comprises foundational AI models (e.g. large language models, LLMs), coding and training frameworks, and data pipelines that turn data and algorithms into machine intelligence. This layer provides the capabilities from which downstream applications of AI are built. The top layer is the application layer. This is where AI is integrated into domain-specific systems designed to perform tasks for military end users.

Products and services in the first two layers of the stack are usually general-purpose or dual-use (i.e., with both military and civilian applications), and it is at the application level that products and services are chiefly military-specific. Militaries rarely build an entirely separate stack from scratch, particularly because the type of infrastructure required for the most powerful AI models is prohibitively expensive. Instead, they often rely on industry to provide the various technological elements of the stack. In addition, they must commission a range of specialized auxiliary services that support the adoption of AI, including data management and test, evaluation, verification and validation (TEVV) services.[13]

Who are the actors?

The actors comprising the military AI industry can be grouped into four categories: legacy primes; neo-primes and defence start-ups; big tech; and foundation model providers. These categories are organized according to business model, that is, the logic by which a company creates, delivers and captures value (see table 2.1).[14] Grouping firms

[12] Stryker, C., 'What is an AI stack?', IBM, 29 Nov. 2024.

[13] Afina, Y. and Grand-Clément, S., *Bytes and Battles: Inclusion of Data Governance in Responsible Military AI*, Centre for International Governance Innovation (CIGI) Papers no. 308 (CIGI: Waterloo, ON, Oct. 2024); Karner, N. et al., *Growing the UK's AI Assurance Market in Defence and Security* (Alan Turing Institute, Centre for Emerging Technology and Security: London, Jan. 2026); Thales UK, *Evaluating Synthetic Data's Effectiveness: Bridging the Gap Between Synthetic and Real Data and the Feasibility of Achieving High Assurance*, White paper (Thales: Crawley, Mar. 2026); and Advai, 'About', [n.d.].

[14] Teece, D. J., 'Business models, business strategy and innovation', *Long Range Planning*, vol. 43, nos 2–3 (Apr.–June 2010); and Fielt, E., 'Conceptualising business models: Definitions, frameworks and classifications', *Journal of Business Models*, vol. 1 (2013).

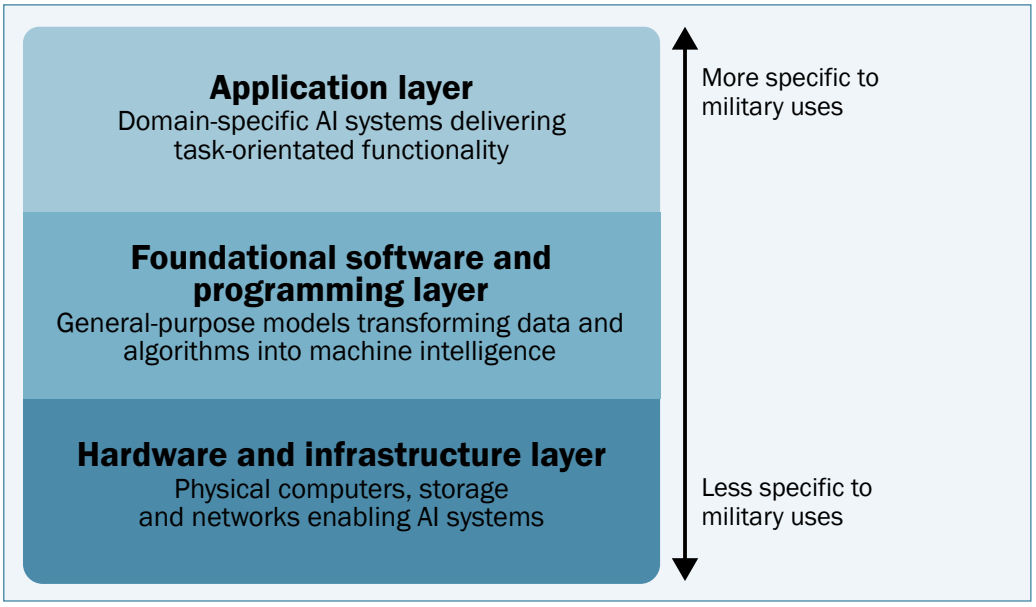


Figure 2.1. The military AI stack

according to business model (rather than, say, business size, location or product) allows commonalities regarding industry behaviours to be identified and explained. Three elements are particularly important for the grouping: (*a*) customer base and revenue model (i.e. to whom an organization sells and how it generates revenue); (*b*) product development logic (i.e. how a company innovates and what it builds); and (*c*) capital structure and risk appetite (i.e. how a company is financed and what time horizons govern its decision-making).[15]

These three elements shape what each type of firm is likely to prioritize. Legacy primes, which sell mainly to governments on long procurement cycles and answer to shareholders, tend to prioritize stable returns, incumbency and consolidation of market position.[16] Neo-primes and defence start-ups, which are often backed by venture capital and are under pressure to demonstrate growth, tend to prioritize a rapid increase in their scale and early contract wins.[17] Big tech firms, for which military sales are a small share of overall revenue, tend to prioritize extending existing infrastructure and platform dominance into new markets. Meanwhile, FMPs, which must bear high costs of computational infrastructure (known as 'compute') and must raise large amounts of capital, tend to prioritize securing market position and increasing their scale ahead of an initial public offering.[18]These different priorities mean that firms respond to different incentives and are therefore exposed to, and likely to care about, different forms of regulation and oversight.

This matters for policymaking because different priorities imply different regulatory interests, and so policy engagement with industry cannot be a one-size-fits-all approach. However, it is important to note that this categorization is a simplification of

[15] Birkinshaw, J. and Asari, S., 'Understanding management models: Going beyond "what" and "why" to "how" work gets done in organizations', eds N. J. Foss and T. Saebi, *Business Model Innovations: The Organisational Dimension* (Oxford University Press: Oxford, 2015); and Teece, D. J., and Linden, G., 'Business models, value capture, and the digital enterprise', *Journal of Organization Design*, vol. 6 (2017).

[16] Carril, R. and Duggan, M., 'The impact of industry consolidation on government procurement: Evidence from Department of Defense contracting', *Journal of Public Economics*, vol. 184 (Apr. 2020); and Dombrowski, P., Gholz, E. and Ross, A. L., 'Selling military transformation: The defense industry and innovation', *Orbis*, vol. 46, no. 3 (summer 2002).

[17] Schwarz, E., 'From blitzkrieg to blitzscaling: Assessing the impact of venture capital dynamics on military norms', *Finance and Society*, Published online 7 Jan. 2025.

[18] Srnicek, N., *Silicon Empires: The Fight for the Future of AI* (Polity: Cambridge, 2025), chapter 2.

Table 2.1. Business model characteristics of key military AI company types

	Customer base and revenue model	Product development logic	Capital structure and risk	Examples
Legacy primes	State as sole customer Cost-plus, multi-year contracts; revenue tied to expenditure duration	Demand-driven: government specification precedes development; complex systems with managed supply chains	Most often publicly listed; government guaranteed income; low financial risk; weak incentives to innovate	Lockheed Martin, Northrop Grumman (both USA), SAAB (Sweden), Israel Aerospace Industries (Israel), BAE System (UK)
Neo-primes and defence start-ups	State as predominant customer, but sometimes legacy primes Recurring revenue via software licensing	Supply-driven: private R&D investment; off-the-shelf, software-first products proactively marketed to militaries	Typically backed by venture capital; 10-year returns horizon; high-risk, high returns; growth through valuation increase	Palantir Technologies, Anduril Industries, Shield Al, Skydio (all USA), Helsing SE (Germany)
Big tech	Customers primarily civilian Militaries as secondary source of revenue from existing commercial products	Civilian-first development; no military-specific R&D but products adapted for military use, particularly at application stage	Large capital reserves, diversified investments; defence revenue a small fraction of income	Microsoft, Google (Alphabet), Amazon (Amazon Web Services), Meta (Facebook), Oracle (all USA)
Foundation model providers	Customers primarily civilian Revenue through pay-per-use model-access fees and enterprise licensing; military contracts as secondary revenue stream	Upstream general-purpose models; fine-tuned for specific applications	Funded by venture capital and big tech; heavy model training costs create pressure to pursue government contracts for additional revenue; some aiming for initial public offering	OpenAl, Anthropic, xAI (all USA), Google DeepMind (UK), Mistral AI (France), DeepSeek (China)

R&D = research and development.

a dynamic and rapidly evolving landscape, and the boundaries between categories are porous. For instance, legacy primes invest in and acquire start-ups; neo-primes partner with legacy primes; some big tech firms develop or hold major stakes in FMPs; and the lines between civil and military markets are increasingly blurred. Many companies therefore straddle two or more categories, and their positions will continue to shift over time (as discussed at the end of this chapter). The categories should therefore be read as analytically useful, rather than precise and mutually exclusive; they are intended to provide a basic structure for making sense of the landscape, rather than a definitive taxonomy.

Legacy primes

Legacy primes are large arms producers that supply a broad range of equipment and services to militaries. These are typically 'big ticket' items, such as combat aircraft, armoured vehicles, air-defence systems and submarines, which usually require these companies to oversee and manage complex supply chains.[19] Legacy primes usually have direct, multi-year contracts with government for military programmes and capabilities.

The legacy primes were all established in the 20th century, mostly in the first half of that century, and typically employ more than 100 000 staff. Based on revenues from sales of arms and military services, the world's largest primes—each with more than $10 billion revenue from military sales annually as of 2024—are Lockheed Martin (headquartered in the United States), RTX (USA, previously Raytheon), Northrop Grumman (USA), BAE Systems (United Kingdom), General Dynamics (USA), Rostec (Russia), Aviation Industry Corporation of China (AVIC, China), China Electronics Technology Group Corporation (CETC, China), China North Industries Corporation (NORINCO, China), Leonardo (Italy) and Thales (France).[20] Some legacy primes are solely engaged in arms production and military services, while others (e.g., Boeing and Airbus) also serve civilian markets. Military sales nonetheless remain central to the business model of all of them.

Military AI-related tools and services. The involvement of many legacy primes in developing the predecessor technologies of contemporary military AI applications—including for maintenance and logistics, for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), and for autonomy in weapon systems—dates back as far as the 1970s and 1980s. Their contribution through large C4ISR and systems-integration programmes pioneered the automated sensing, data fusion and decision support on which current AI applications are built.[21] For example, the Aegis combat system, which was developed by RCA (now part of Lockheed Martin) and fielded from the early 1980s, automates detection, tracking and engagement support for naval air defence.[22] Regarding autonomy in weapon systems, RTX's Phalanx close-in weapon system was first developed in the 1970s and uses rule-based algorithms to identify, track and engage targets.[23] Israel Aerospace Industries' Harpy, a semi-autonomous anti-radar loitering munition under development since the late 1980s, can use AI for target identification.[24] Because of their existing relationships

[19] Klare, M. T., 'Welcome to the new military-industrial complex', *The Nation* (New York), Feb. 2025.

[20] Scarazzato, L. et al., 'The SIPRI Top 100 Arms-producing and Military Services Companies, 2024', SIPRI Fact Sheet, p. 9.

[21] L3Harris 'C4ISR integrated systems', [n.d.]; and 'C4ISR insights: Navigating the future of command, control, communications, intelligence, surveillance, and reconnaissance', Aviation and Defense Market Reports, 22 Apr. 2024.

[22] Lockheed Martin, 'Aegis Combat System', [n.d.]; and Hone, T. C., Smith, D. V. and Easton, R. C. Jr., 'The politics of developing the Aegis Combat System, Pt. 1', Center for International Maritime Security (CIMSEC), 24 Apr. 2023.

[23] RTX, 'Phalanx Weapon System', [n.d.].

[24] Israel Aerospace Industries (IAI), 'Harpy: Anti radiation loitering munition', [n.d.]; 'Israel Aerospace Industries Harpy UAV', Autonomous Weapons Watch, 4 Mar. 2024; and Bode, I. and Watts, T., *Loitering Munitions*

with militaries, legacy primes are positioned at the upper layers of the stack, from where they oversee and manage complex supply chains for integrated systems.

Contemporary AI-related products from legacy primes include crewed and uncrewed aircraft, surface vessels and submarines—some equipped with sensors for intelligence purposes, while others are armed. Examples include the integration of AI in loitering munitions by RTX and the collaborative development of the MQ-28 Ghost Bat uncrewed combat aerial vehicle (UCAV) by Boeing and BAE Systems Australia.[25] Legacy primes also offer AI-supported decision-making tools covering threat detection, cybersecurity, situational awareness and battle management.[26] Many US legacy primes have secured contracts worth over $1 billion to modernize military capabilities and command structures through AI integration, and several (including General Dynamics, Northrop Grumman and RTX) have received contracts from the US Department of Defense (DOD) to develop AI tools for airborne missions and target recognition.[27]

Whilst legacy primes have established programmes for integrating AI into military systems, they have not necessarily spearheaded recent innovation in military applications of the latest AI technologies and techniques.[28] Rather, they primarily keep up with advances in AI by acquiring, subcontracting and partnering with arms industry start-ups with specific competencies in AI (on such partnerships see below).

Business model. States are the foundational customers of legacy primes' military products. This relationship is typically tightly structured through regulatory frameworks related to, for example, procurement and export controls.[29] Traditionally, legacy primes are awarded multi-year contracts and work closely with governments to develop and deliver products based on government specifications and demands. This means that legacy primes usually wait for a formal request before starting to develop a product. However, it is common for legacy primes to work closely with the government in advance of receiving a formal request.

Legacy primes have historically relied on a 'cost-plus' contracting model, which means that the state pays the company the expenses incurred during the process plus an additional profit margin, usually around 5–10 per cent.[30] This business model means that legacy primes can lack incentive to rapidly innovate. However, several legacy primes are increasingly self-funding innovation projects and setting up internal venture capital functions to promote innovation and fund acquisitions of smaller companies.[31]

Neo-primes and defence start-ups

Neo-primes and defence start-ups are companies that enter the arms market from outside the traditional legacy prime contractor base. Their products are diverse, but

and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control (University of Southern Denmark, Center for War Studies: Odense, May 2023).

[25] RTX, 'RTX and Shield AI partner to develop new defense capabilities', Press release, 1 July 2025; and BAE Systems Australia, 'MQ-28 Ghost Bat', [n.d.].

[26] Lockheed Martin, 'CommandIQ: A smarter way to fight', [n.d.]; RTX, 'RTX to optimize cyber vulnerability detection for DARPA', Press release, 5 Aug. 2025; and Easley, M., 'Raytheon ready to add AI-enabled radar warning receiver to fighter jets, other Air Force platforms', DefenseScoop, 24 Feb. 2025.

[27] Northrop Grumman, 'Northrop Grumman secures $1.4 billion in contracts to modernize global air and missile defense', 12 Feb. 2025; and General Dynamics Mission Systems, 'Deep Learning Analytics develops DARPA deep machine learning prototype', 11 May 2016.

[28] Lockheed Martin, 'Artificial intelligence & machine learning', [n.d.]; BAE Systems, 'Digital intelligence', [n.d.]; and Malyasov, D., 'AI startups are reshaping the US defense industrial base', Defence Blog, 25 Aug. 2026.

[29] Heidenkamp et al. (note 11); and Hartley, K., 'The arms industry, procurement and industrial policies', eds T. Sandler and K. Hartley, *Handbook of Defense Economics*, vol. 2 (North-Holland: Amsterdam, 2007).

[30] Smith, R. P., *Defence Acquisition and Procurement: How (Not) to Buy Weapons*, Elements in Defence Economics (Cambridge University Press: Cambridge, 2022), chapter 5.

[31] Landor Laursen, K., 'Banks hold back, primes step in: Record investments offer Nordic startups a new route to capital', Defence Nordic, 29 July 2026; and Lockheed Martin, 'Lockheed Martin Ventures: Accelerating t', [n.d.].

they have a shared business model: they are typically venture capital funded and typically develop products on their own initiative with rapid product-iteration cycles. Their products can be loosely clustered into AI-enabled software, data and analytics platforms; autonomous and uncrewed systems; and counter-uncrewed aerial system (counter-UAS, also known as counter-drone) systems and directed-energy systems. Many firms span these product categories.

Most of these companies develop AI-enabled software or embed AI in autonomous hardware. When these firms supply hardware—such as UASs or counter-UAS systems—it tends to be smaller-scale, lower-cost and faster to produce than the large, capital-intensive platforms (e.g. combat aircraft and armoured vehicles) that define the core business of the legacy primes.

US companies in this category include Palantir Technologies, Anduril, Shield AI, Skydio, Epirus, Scale AI and SpaceX. European companies include Helsing (Germany), Stark Defense (Germany), Arondite (UK), Harmattan AI, Comand AI (France), Tekever (UK and Portugal). Most neo-primes and defence start-ups were established from 2016 onwards, with some notable exceptions (e.g. Tekever was founded in 2001, SpaceX in 2002 and Palantir in 2003).

The difference between a neo-prime and a start-up depends on several factors related to company maturity.[32] Defence start-ups are generally early-stage companies that are funded by angel, seed or early venture capital investment and that have yet to achieve sustained revenue. Neo-primes are firms that have grown to a valuation of around $10 billion or more and hold substantial contractual commitments. Thus, while most neo-primes are start-ups, not all start-ups are neo-primes. A growing number of military AI start-ups—predominantly in the USA, but increasingly elsewhere—have attained 'unicorn' status, meaning they are valued at over $1 billion.[33]

Since 2020, states—particularly the USA—have increasingly contracted neo-primes and defence start-ups to deliver both off-the-shelf products and R&D prototypes.[34] Many states view these often smaller, more agile companies as essential to maintaining a technological edge and to reducing dependency on a single provider.[35] These firms are significant for the military AI industry because they are changing how military innovation is funded, developed and procured and they put competitive pressure on the incumbent legacy primes.[36]

Military AI-related tools and services. The neo-primes and defence start-ups that are most directly relevant to military AI are those that provide AI-enabled software or that embed AI in autonomous systems. These are platforms and applications that integrate machine learning and related techniques to process large volumes of data. This could include, for example, fusing feeds from multiple sensors, identifying and classifying objects, or generating recommendations to support command decisions and targeting.

[32] 'Defining a tech scaleup', Startup Genome, [n.d.]; and Coad, A. et al., *Scale-ups and High-Growth Firms* (Springer: Singapore, 2024), chapter 5.

[33] Park, A., 'Thanks to drones, China and Ukraine, a record number of military startups became unicorns in 2025', *Forbes*, Nov. 2025.

[34] McCormick, R., 'Department of Defense other transaction authority trends: A new R&D funding paradigm?', Center for Strategic and International Studies (CSIS), Dec. 2020.

[35] US Department of Defense (DOD), 'Artificial intelligence strategy for the Department of War: Accelerating America's military AI dominance', Memorandum, 9 Jan. 2026; British Ministry of Defence, 'New taskforce to put AI on the UK's frontline', Press release, 10 June 2026; Clapp, S., 'Defence and artificial intelligence', Briefing, European Parliamentary Research Service, Apr. 2025; Finlan, A., 'A fertile soil for AI? Defense AI in Sweden', eds H. Borchert, T. Schütz and J. Verbovszky, *The Very Long Game, Contributions to Security and Defence Studies* (Springer: Cham, 2024); and Sawers, P., 'Software before drones: Dutch defence ministry bets on interoperability', Resilience Media, 3 July 2026.

[36] Klempner, J., Rodriguez, C. and Swartz, D., 'A rising wave of tech disruptors: The future of defense innovation?', McKinsey & Company, 22 Feb. 2024.

Box 2.1. Venture capital firms

Many new entrants to the arms market, especially defence start-ups, are backed by venture capital funds. Key funds, all of which are based in the United States, include Andreesen Horowitz, Founders Fund, 8VC, General Catalyst and 1789 Capital. They provide seed funding to companies such as Palantir, Anduril, Helsing and ShieldAI.

Venture capital is a form of private equity financing for high-risk start-up companies that have a high potential for growth; the aim is to generate large returns when the start-up is sold or listed on a stock exchange.[a] Venture capital has a tendency to operate on short time frames (usually a 10-year window), and it makes returns on growth in the valuation of the start-up and not necessarily on its profit.[b] A valuation reflects expectations about a company's success and is used to get a sense of the value of the company. It is calculated based on different factors, such as market size, sales potential, current sales and management structure.[c]

Historically, venture capital funds avoided the arms market for three main reasons: it was dominated by the legacy primes, leaving little room for new entrants; government acquisition-approval processes were slow and complex; and investments in the arms market were seen as morally problematic by many investors.[d] However, this has recently changed, in both the US and European contexts.[e] In the USA, for example, venture capital investments in the 'national security' sector have reportedly increased by almost 900 per cent in less than a decade.[f]

Many US venture capital funds are explicit about being driven by US national security concerns. For example, Andreeseen Horowitz's American Dynamism Fund invests in companies that support the US national interest and has the tagline 'Security through innovation'.[g] The firm's values are also reflected in the *Techno-optimist Manifesto* written by co-founder Marc Andreessen in 2023, where he celebrates technology innovation while describing the precautionary principle as an 'enemy' of progress.[h] This narrative has been developed by a number of prominent figures associated with neo-primes (see chapter 3).

[a] Schwarz, E., 'From blitzkrieg to blitzscaling: Assessing the impact of venture capital dynamics on military norms', *Finance and Society*, Published online 7 Jan. 2025.

[b] González, R. J., 'How big tech and Silicon Valley are transforming the military-industrial complex', Brown University, Watson Institute for International and Public Affairs, Costs of War Project, 17 Apr. 2024.

[c] Schwarz, E., 'Unicorns for uniforms: On the problematic allure of VC investments in defence', Opinio Juris, 18 Sep. 2024; and Howard, M., 'The rapacious ambivalence of VC investment: Venture capital, value capture, and the valorization of crisis', *Finance and Society*, vol. 10, no. 2 (Aug. 2024).

[d] Metinko, C., 'A16z and Founders Fund lead the way in defense venture capital', Crunchbase News, 20 Aug. 2024; and Schwarz, E., 'Unicorns for uniforms: On the problematic allure of VC investments in defence', Opinio Juris, 18 Sep. 2024.

[e] Bria, F. et al., 'The authoritarian stack: How tech billionaires are building a post-democratic America—and why Europe is next', Nov. 2025; and Sanjuan, S., 'The rise of the defense tech sector in Europe: Market map analysis and VC predictions', GoHub Ventures, 16 Sep. 2025.

[f] Roeder, K., 'The national security startup boom is real—and complicated', Technical.ly, 9 Feb. 2026.

[g] A16Z American Dynamism, 'Supporting the national interest', Andreessen Horowitz, [n.d.]; and A16Z American Dynamism, 'Defense reform: A stronger defense, powered by dynamic tech', Andreessen Horowitz, [n.d.].

[h] Andreessen, M., 'The techno-optimist manifesto', Andreessen Horowitz, 16 Oct. 2023.

Examples include data integration and analysis platforms such as Palantir's Gotham, Anduril's Lattice, Shield AI's Hivemind, Helsing's Altra and Saronic's Echelon.[37] Some, such as Palantir and Anduril, also provide technologies for law enforcement.[38]

[37] Anduril, 'Anduril's Lattice: A trusted dual use platform for public safety and defense', 31 July 2023; Palantir, 'Gotham', [n.d.]; Saronic, 'Echelon', [n.d.]; and Helsing, 'Altra Recce-Strike software platform', [n.d.].

[38] Palantir, 'Introducing Palantir Gotham Europa', [n.d.]; Anduril, 'Anduril and US Customs and Border Protection expand partnership with 200 additional Extended Range Sentry Towers', 12 June 2026; and Privacy International, 'Dual-use tech: The Anduril example', 10 Nov. 2025.

Many of these companies are associated with a 'software-first' approach to the military market: that is, the core product is software, with physical hardware as secondary, usually offered as an add-on or wrapper to make the software operational in the field.[39] However, this is a tendency rather than a rule since some firms in the category are primarily hardware developers.[40]

Due to the iterative product-development model, some systems require continuous updating. Thus, some firms often embed software engineers (sometimes called 'forward-deployed engineers') within armed forces to assist in the real-time operation of these systems.[41]

Business model. Neo-primes and defence start-ups usually flip the traditional business model of legacy primes. Rather than waiting for a ministry of defence (MOD) to issue a specific request prior to developing a product, neo-primes and start-ups tend to invest in their own R&D. This means that they are able to present ready-made, customizable prototypes to customers, which reduces the timeline from product procurement to deployment.[42] These companies are usually backed by venture capital companies (see box 2.1), but many significant neo-primes received initial government funding to get off the ground.

Another component of the business model of neo-primes and defence start-ups is that they typically offer products through a subscription-based model (e.g. cloud services or data collection), rather than allowing militaries to acquire products and intellectual property rights outright. These software products are, in essence, rented capabilities. This matters commercially because software can be updated and scaled at far lower cost than hardware, which generates recurring revenue and higher profit margins.[43]

Some of these companies also use a 'land and expand' tactic as well as vendor lock-in—a situation where a customer becomes heavily dependent on a single provider's products or services. This can be achieved through proprietary data formats, tightly integrated platform ecosystems and continuous software updates that make switching to a competitor technically complex and costly.[44] Over time, militaries that embed these platforms into their command-and-control infrastructure may find themselves dependent on a single vendor for ongoing access, updates and support—this gives that company significant commercial and strategic leverage and also immunizes it against future changes in demand.[45] Vendor lock-in is not itself a novel dynamic and legacy primes have long achieved comparable effects through proprietary architectures. However, neo-primes and start-ups have intensified the practice and have positioned it as a core approach to generating revenue.[46]

[39] Anduril, 'In the 21st century, the Department of Defense must think software-first', 16 Mar. 2021.

[40] Skydio, 'Skydio autonomous drones for DFR, inspection, national security', [n.d.]; and Epirus, 'Epirus—Home of Leonidas, the premier high-power microwave cUAS swarm solution', [n.d.].

[41] Cagan, M., 'Forward deployed engineers', Silicon Valley Product Group, 17 Sep. 2025; and Palantir, 'A day in the life of a Palantir forward deployed software engineer', Palantir Blog, 2 Nov. 2020.

[42] Anduril, 'Mission: Transforming defense capabilities with advanced technology', [n.d.]; and Sari, A. and Evans, G., 'The military use of AI and the law of armed conflict: What role for government and industry?', *Defence Studies*, Published online 10 June 2026, pp. 18–19.

[43] Panter, J., 'A skeptic's view of the hype machine and business model of neo-defense tech', War on the Rocks, 26 Aug. 2025.

[44] Opara-Martins, J., Sahandi, R. and Tian, F., 'Critical review of vendor lock-in and its impact on adoption of cloud computing', Paper presented at the International Conference on Information Society (i-Society 2014), London, 10–12 Nov. 2014.

[45] Barrett-Taylor, R. and Ford, M., 'Eroding sovereignty in the age of "war as a service"', Opinio Juris, 3 Nov. 2025; and Paulus, A., *An Achilles Heel of Today's Armed Forces: Managing Software Supply Chain Risk in the Military Sector*, Stiftung Wissenschaft und Politik (SWP) Research Paper no. 2025/RP 06 (SWP: Berlin, Nov. 2025).

[46] McGinn, J., Aldisert, A. and MacAloney, K., 'Who controls the wrench: The debate over the "right to repair"', Center for Strategic & International Studies (CSIS), 6 Nov. 2025.

Neo-primes and start-ups generate revenue almost exclusively from states, although some also supply their products to legacy primes (e.g. Shield AI licenses its Hivemind software system to several primes, including Airbus and L3Harris).[47]

Big tech

'Big tech' refers to the dominant multinational technology corporations with diversified digital products and services and significant market capitalization.[48] Big tech includes the 'big five' most influential US technology companies—Google (Alphabet), Apple, Meta, Amazon and Microsoft—as well as dot-com boom-era companies such as Salesforce; legacy technology companies such as IBM; and other enterprise software providers such as Oracle. The annual revenues of companies in this category are usually in the range of hundreds of billions of US dollars, and they have hundreds of thousands of employees.

Big tech owns and controls general-purpose digital infrastructure such as cloud platforms and data centres that underpin digital products and services.[49] These companies' core business is selling such digital products and services on a large, but adaptable, scale to consumers, businesses and governments; military and security customers typically account for only a small share of their revenue. Many big tech companies have within the past 5 years or so revised their corporate policies (e.g. acceptable use policies and AI principles) to permit military and national security organizations as end users and military applications as end uses of their products and services.[50]

Military AI-related tools and services. Big tech is increasingly embedded in military infrastructure worldwide, principally through the provision of cloud computing services to support AI applications and related data collection and processing.[51] For example, in 2022 Amazon, Google, Microsoft and Oracle collectively won a $9 billion contract from the US Department of Defense to provide cloud services.[52] In 2025 Google secured a contract worth up to $200 million from the DOD for AI and cloud capabilities, including processing units and agentic AI, and in 2026 it reportedly agreed to make its Gemini models available for classified use.[53] Google and Amazon are partners in Project Nimbus, a $1.2 billion contract for cloud and AI services signed with the Israeli government in 2021 that includes the provision of digital infrastructure to the Israel Defense Forces (IDF).[54] Microsoft has also been linked to cloud services provided to the IDF used for mass surveillance purposes (although it has denied knowing of this use).[55]

Big tech has become embedded in military infrastructure both through deliberate moves into the military domain and also because cloud platforms and data centres

[47] 'Shield AI revenue, valuation & funding', Sacra, [n.d.].

[48] Birch, K. and Bronson, K., 'Big tech', *Science as Culture*, vol. 31, no. 1 (Mar. 2022).

[49] van der Vlist, F., Helmond, A. and Ferrari, F., 'Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence', *Big Data & Society*, vol. 11, no. 1 (Jan.–Mar. 2024).

[50] Manyika, J. and Hassabis, D., 'Responsible AI: Our 2024 report and ongoing work', Google, 4 Feb. 2025.

[51] Javadi, M., 'Infrastructural entanglement and cloud hyperscalers in contemporary warfare: Insights from Ukraine, Israel and Taiwan', *Contemporary Security Policy*, vol. 47, no. 2 (Apr. 2026); and Privacy International, 'Big tech's bind with military and intelligence agencies', 1 Oct. 2025.

[52] Gomes, N. and Stone, M., 'Pentagon splits $9 billion cloud contract among Google, Amazon, Oracle and Microsoft', Reuters, 7 Dec. 2022.

[53] Kelly, J., 'Google Public Sector awarded $200 million contract to accelerate AI and cloud capabilities across Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO)', Google Cloud, 14 July 2025; Albon, C., 'Pentagon taps four commercial tech firms to expand military use of AI', *Defense News*, 15 July 2025; and Mansoor, S., 'Google reportedly signs classified AI deal with US Pentagon', *The Guardian*, 28 Apr. 2026.

[54] Haskins, C., 'The hidden ties between Google and Amazon's Project Nimbus and Israel's military', Wired, 15 July 2024; Abraham, Y., '"No restrictions" and a secret "wink": Inside Israel's deal with Google, Amazon', +972 Magazine, 29 Oct. 2025; and Biddle, S., 'Google Is selling advanced AI to Israel, documents reveal', The Intercept, 24 July 2022.

[55] Davies, H. and Abraham, Y., 'Microsoft blocks Israel's use of its technology in mass surveillance of Palestinians', *The Guardian*, 25 Sep. 2025.

are general-purpose infrastructure shared by civilian and military users, meaning the boundary between the two is becoming increasingly blurred.[56]

Business model. Historically, the core activities of big tech were e-commerce, platform internet services (e.g. Facebook) and online advertising. Cloud computing was originally an offshoot of these services, but it has become increasingly central to these firms since it both offers high profit margins and confers a structural power that comes from occupying a foundational layer of the technological stack.[57] Big tech companies provide raw compute, storage, networking, databases and in some cases the foundation models that power AI applications.

The advent of LLMs has further entrenched the structural position of these firms since training and running the most powerful AI models—including for military purposes—requires specialized infrastructure at a scale that only these companies can provide.[58] In the future, big tech firms are likely to seek to further entrench their position of control of generic AI infrastructure through further investments, partnerships and acquisitions (see below).[59]

Foundation model providers

FMPs develop and maintain large-scale AI models that are capable of complex reasoning, image and text generation, and enabling agentic models.[60] These models provide the 'engine' capable of powering a wide variety of downstream tasks in different domains. FMPs are relatively young; most were founded between 2010 and 2023, with a mixture of funding from venture capital funds, hedge funds and big tech. The more prominent FMPs are Google DeepMind (founded in 2010 in the UK, acquired by Google in 2014), OpenAI (2015, USA), Anthropic (2021, USA), xAI (2023, USA), DeepSeek (2023, China) and Mistral AI (2023, France).

The boundary between FMPs and big tech is perhaps the most porous among the four categories. Some FMPs are owned by big tech firms (e.g. Google DeepMind), others depend heavily on big tech for funding and compute (e.g. OpenAI from Microsoft; Anthropic from both Amazon and Google), and some big tech firms have developed their own foundation models (e.g. Meta). The two categories—big tech and FMPs—are distinguished primarily by their core business (for FMPs, this is the development and provision of foundation models), rather than by clear organizational separation.

Originally, many FMPs were united in their opposition to the military use of their AI models; that stance has shifted since 2024, and they have increasingly made their applications available for military purposes. For example, in January 2024 OpenAI rescinded a ban on its products being used for 'military and warfare purposes', stating that it would permit 'national security use cases that align with our mission'.[61] Anthropic has historically prohibited certain military uses of its technology, although it has become more prominent in the military domain since announcing a partnership with Palantir in

[56] Klonowska, K. and Schmitt, M., 'Iranian attacks on the Amazon data centers: A legal analysis', Just Security, 12 Mar. 2026.

[57] Lehdonvirta, V., *Cloud Empires: How Digital Platforms are Overtaking the State and How We Can Regain Control* (MIT Press: Cambridge, MA, 2022); Miller, R., 'How AWS came to be', TechCrunch, 2 July 2016; and Gurung, D. et al., 'Cloud revolution: Tracing the origins and rise of cloud computing', arXiv:2512.06800, 7 Dec. 2025.

[58] Luitse, D., 'Platform power in AI: The evolution of cloud infrastructures in the political economy of artificial intelligence', *Internet Policy Review*, vol. 13, no. 2 (2024).

[59] Srnicek (note 18), chapter 2.

[60] Jones, E., 'What is a foundation model?', Ada Lovelace Institute, 17 July 2023.

[61] Coldewey, D., 'OpenAI changes policy to allow military applications', TechCrunch, 12 Jan. 2024; and Field, H., 'OpenAI quietly removes ban on military use of its AI tools', CNBC, 16 Jan. 2024.

2024.[62] Indeed, several FMPs have entered partnerships with AI defence start-ups, big tech or legacy primes to supply AI models for military purposes (see below).

Military AI-related tools and services. FMPs typically supply their models to military customers through specially configured government or enterprise variants, often hosted on secure, classified cloud infrastructure.

In the USA, Anthropic launched Claude Gov in 2025, a version of its Claude LLM designed for the US government for classified work and to better handle military-specific tasks, including threat assessment and intelligence analysis.[63] Also in 2025 OpenAI launched ChatGPT Gov, a version of ChatGPT tailored to US government agencies, including within defence and national security, to be deployed together with Microsoft's Azure software.[64] xAI has also launched Grok for Government, described as 'a suite of frontier AI products' made available to US government customers.[65]

The situation is less advanced in Europe, although Mistral AI agreed a deal in 2025 with the French Ministry of Armed Forces to give its personnel access to Mistral's AI technology.[66] Mistral has entered into a strategic partnership on military AI with Helsing and has struck a deal with Faculty, a military-adjacent British firm.[67] The British government has also agreed a memorandum of understanding with OpenAI relating to the military domain.[68]

Business model. The key funding and revenue sources for FMPs are investments through venture capital, hedge funds, strategic investments and partnerships with big tech firms; revenue from commercialization, such as for use of an application programming interface (API, i.e. accessing a model's capabilities); and enterprise licensing (e.g. offering organizations fine-tuning services to create specialized applications).[69] Expanding into military markets provides an opportunity for these firms to tap into national military budgets, which can support the funding of the extremely costly training and running of their foundation models. The weak budget constraints and blurry metrics of success of MODs thus makes the military market highly desirable for FMPs.[70]

Partnerships and acquisitions: Consolidating across the stack

Partnerships are an increasingly important feature of the military AI industry. Partnerships between legacy primes and new actors in the military domain have proliferated (e.g. L3 Harris partnering with ShieldAI, Boeing with Palantir and Lockheed Martin with Google).[71] Neo-primes and start-ups are also partnering with each other (e.g. Palantir and Anduril), with FMPs (e.g. Palantir and Anthropic; Anduril and OpenAI) and

[62] Palantir, 'Anthropic and Palantir partner to bring Claude AI models to AWS for US government intelligence and defense operations', 7 Nov. 2024

[63] Anthropic, 'Claude Gov models for US national security customers', 6 June 2025.

[64] OpenAI, 'Introducing ChatGPT Gov', OpenAI, 28 Jan. 2025.

[65] xAI, 'Announcing xAI for Government', 14 July 2025.

[66] Marchandon, L., 'France's Armed Forces Ministry awards Mistral AI framework agreement', Reuters, 8 Jan. 2026.

[67] Helsing, 'Helsing and Mistral announce strategic partnership in defence AI', Press release, 10 Feb. 2025; and Faculty, 'Faculty announces collaboration with Mistral AI', 29 Nov. 2024.

[68] Memorandum of Understanding between the British government and OpenAI on AI opportunities, 21 July 2025.

[69] Taub, S., 'Anthropic's backers include a who's who of hedge funds', Institutional Investor, 2 June 2026; Taub, S., 'OpenAI backers include hedge fund heavyweights poised for IPO payoff', Institutional Investor, 16 June 2026; 'Anthropic quietly captured over 60% of business AI API spending, leaving OpenAI with roughly 35%', Crypto Briefing, 29 Aug. 2026; and OpenAI, 'Introducing improvements to the fine-tuning API and expanding our custom models program', 4 Apr. 2024.

[70] Srnicek, N., 'How AI companies got caught up in US military efforts', Wired, 14 Jan. 2026; and Burke, H., 'OpenAI is bleeding cash. Its solution? Military contracts', Jacobin, 5 Apr. 2026.

[71] 'Boeing to integrate AI in its defense & space programs through new partnership with Palantir', Simple Flying, 24 Sep. 2025; and Lockheed Martin, 'Lockheed Martin and Google Cloud collaborate to advance generative AI for national security', 27 Mar. 2025.

with big tech (e.g. Anduril and Microsoft).[72] Palantir, Anthropic and Amazon formed a three-way partnership in 2024.[73] Most partnerships remain between US companies, but some now cross borders into Europe and East Asia (e.g. Microsoft with BAE Systems; Anduril with Hyundai).[74] The number of European partnerships is growing (e.g. Saab and Helsing; Helsing and Mistral AI; Leonardo and Faculty AI).[75]

These partnerships illustrate the need for collaboration among industry actors on the development and adoption of AI capabilities for the military domain since no single actor spans the whole stack or holds all the capabilities that the market requires. Legacy primes offer decades-long institutional relationships with MODs, supply-chain accessibility, compliance infrastructure (particularly around export controls) and the capacity for high-volume manufacturing of hardware. Neo-primes and defence start-ups offer software-first novel AI and autonomous capabilities, as well as product development built around rapid iteration, which the R&D cycles of the legacy primes struggle to match. Big tech offers hyperscale compute and infrastructure that dwarfs what any arms company could build alone. FMPs offer frontier models but typically lack the compute infrastructure to run them at scale or the customer access for direct military sales. Partnering lets each actor access what it lacks without the cost and delay of building it in-house.

Acquisitions respond to many of the same technological and structural gaps that partnerships respond to, but they represent a different strategic choice for companies. Acquisition may make more sense than partnering if a company wants to fully control a capability, rather than rely on another company's terms, particularly if that capability becomes a strategic priority. For example, Anduril's 2025–26 acquisitions of the start-ups American Infrared Solutions (which produces infrared sensing hardware components) and ExoAnalytic Solutions (specializing in space domain awareness and missile defence) reflect the same logic as a partnership—filling a capability gap—but also illustrate that Anduril sees this as a long-term strategic priority.[76]

Acquisitions require significant capital, limiting them to well-capitalized actors. Acquisitions lead to the consolidation of the military AI industry, whereas partnerships preserve a multi-actor ecosystem. This matters for understanding the military AI industry landscape since a more consolidated market may mean fewer competing suppliers, greater dependence on a small number of firms and a risk of vendor lock-in. In contrast, a more diverse ecosystem can sustain competitive pressure among suppliers and give states greater leverage over the choice and terms of military AI providers.

[72] Palantir (note 62); Anduril, 'Anduril partners with OpenAI to advance US artificial intelligence leadership and protect US and allied forces', 4 Dec. 2024; and Anduril, 'Anduril and Microsoft partner to advance Integrated Visual Augmentation System (IVAS) program for the US Army', 11 Feb. 2025.

[73] Palantir (note 62).

[74] BAE Systems, 'BAE Systems and Microsoft join forces to equip defence programmes with innovative cloud technology', 14 Apr. 2023; and Anduril, 'HD Hyundai and Anduril Industries announce strategic partnership on maritime systems, autonomy, and mass manufacturing', 13 Apr. 2024.

[75] Saab, 'Saab signs strategic cooperation agreement and makes investment in Helsing', 14 Sep. 2023; Helsing (note 67); and Leonardo, 'Leonardo partners with Faculty AI to accelerate the development of next generation defence technologies', 12 May 2025.

[76] Subin, S., 'Anduril acquires ExoAnalytic Solutions in push for Trump's Golden Dome', CNBC, 11 Mar. 2026; and Anduril, 'Anduril Industries acquires American Infrared Solutions', 20 Oct. 2025.

3. Normative positioning and pathways to influence

Industry engagement in military AI governance is not only a matter of contributing technical expertise. Firms bring with them normative positions on how AI should be governed and used in the military domain. Thus, as states seek to involve industry in policy efforts on AI in the military domain, they must be aware of the normative positions taken by industry actors and of the pathways through which these actors may shape normative development around the use of military AI (see box 3.1 for a description of 'norms'). Recognizing the difficulty of establishing a causal link between industry's normative positioning and actual normative developments around the regulation of AI in the military domain, this chapter maps the normative positions taken by industry actors and examines different ways in which the military AI industry can shape normative developments.[77]

Industry's normative positions around AI in the military domain

This section surveys the positions that legacy primes, neo-primes and defence start-ups, big tech, and FMPs have taken on how AI should be governed and used in the military domain. A 'position' here is a public claim about how military AI should be governed or used that a firm advances in an observable form, such as public statements, corporate AI principles and usage policies, or policy submissions. These claims are often couched in wider strategies of discursive legitimation, such as narratives of storytelling by which an actor stakes out authority on decisions about how AI should be governed and used in the military domain. Industry has clear incentives to engage in normative developments. Shaping the terms of debate and the content, interpretation and application of norms early can reduce future regulatory uncertainty, help with weighing future liability risks, protect market access, and allow firms to influence the standards against which their products and practices will later be judged. Some firms may also have a culture of norm entrepreneurship, seeing defining terms of responsible practice for their sector as an aspect of their corporate identity (see e.g. the Microsoft case study in box 3.2 below).

The following survey is structured by business model (see table 2.1 above), rather than thematically. What a firm claims publicly may differ from what it communicates to governments through procurement negotiations, contract terms, advisory roles and lobbying, which are often confidential. Public and private positions may complement or diverge from one another. Because private engagement is rarely observable, this section draws mainly on public sources and should be read as a partial picture of firms' positioning. The less visible channels are considered in the following section, on pathways to influence.

Legacy primes

Legacy primes' public discursive outputs are overwhelmingly about assurance, testing and evaluation of AI systems for alignment with governmental principles on the military use of AI. For example, Lockheed Martin and Thales have been proactive around issues of TEVV and assurance, and BAE's framing centres on assurance around interoperability.[78]

[77] Čekal, C., 'Advisors or advocates? The European defence industry as a political actor in EU policymaking', *European Security*, Published online 29 Sep. 2026, p. 7; and Dilling, O., 'From compliance to rulemaking: How global corporate norms emerge from interplay with states and stakeholders', *German Law Journal*, vol. 13, no. 5 (May 2012).

[78] Baylor, M., 'No small task: Delivering AI at the speed of relevance in defense', Lockheed Martin, 19 Aug. 2026; Mattioli, J. et al., *End-to-End Trustworthy AI Engineering Lifecycle for Critical Systems* (Thales: Meudon, Jan.

This does not mean an absence of normative positioning. The focus on assurance is itself a kind of normative stance because it turns value-based questions ('Should this system be used in this way?') into a question of technical qualification ('Can this system be shown to perform reliably within its specified envelope?'). Moreover, legacy primes perform normatively weighted work through standards bodies, procurement documentation and trade associations. For example, Thales co-chairs a working group, WG-114, of the European Organisation for Civil Aviation Equipment (EUROCAE) that contributes to defence standardization bodies, while the CEO of Lockheed Martin has highlighted the importance of a standards-based approach for accelerating the adoption of digital technologies like AI.[79] These processes are significant because they are among the means by which states put into practice adopted norms and high-level principles.[80] Firms that contribute to these processes therefore help shape how norms are interpreted and applied in practise.

Legacy primes' lack of direct public intervention on the direction of military AI regulation is in keeping with these companies' tendency to wield influence through lobbying and other means of shaping legislation.[81] This is in turn linked to the historically close relationship that legacy primes have to the state. Given the oligopolistic character of the arms market, legacy primes—as market incumbents—have little need or incentive to engage in public argument on these issues in a way that neo-primes and defence start-ups do (see below). Indeed, relative to the neo-primes and start-ups, the legacy primes' public reticence regarding the normative positions of their respective states might be taken as deference to the state on policy questions, which itself construes the legacy primes as responsible and reliable suppliers.

That said, there are signs that this may be shifting. In September 2026 the CEO of Thales, Patrice Caine, called on governments to create regulatory frameworks for AI, echoing warnings from technology leaders regarding the risks of AI. He argued that 'There are ways and means, on the technical standpoint, to put this type of technology under control, but it's not sufficient', and 'We need frameworks, and this clearly lies, in terms of responsibility, in the hands of governments'.[82] It is possible that Thales's position reflects the fact that the French state owns a significant stake in the company and a concern about competition from privately held foreign companies with no state control.[83]

Neo-primes and defence start-ups

It is neo-primes and unicorn defence start-ups that have developed the most combative framing repertoire. Their public argumentation takes place within a metanarrative of patriotism, strategic competition and geopolitical rivalry, overwhelmingly framed as between the United States and China, with a secondary Russia–West variant.

2026); Thales, 'Thales speeds up its development of AI for defence', Press release, 28 Mar. 2024; and Henstock, D., 'Pioneering AI in defence: Innovation, ethics, and the road ahead', BAE Systems, 28 May 2026.

[79] US House of Representatives, Committee on Armed Services, Subcommittee on Cyber, Information Technologies, and Innovation, 'Industry perspectives on defense innovation and deterrence', Hearing, 20 Sep. 2023, pp. 3–4.

[80] Blanchard, A., Thomas, C. and Taddeo, M., 'Ethical governance of artificial intelligence for defence: Normative tradeoffs for principle to practice guidance', *AI & Society*, vol. 40, no. 1 (Jan. 2025).

[81] Hartung, W. D., 'Military-industrial complex revisited: How weapons makers are shaping US foreign and military policies', eds M. Honey and T. Barry, *Global Focus: US Foreign Policy at the Turn of the Millennium* (St Martin's Press: New York, 2000).

[82] AFP, 'French defence group Thales calls on governments to regulate AI', Digital Journal, 14 Sep. 2026.

[83] Thales, 'Share and shareholding', [n.d.].

Box 3.1. Norms and norm development

At the international level, norms concern the behaviour of states and, in limited cases, non-state actors. They may be recorded in binding agreements that are enforceable through legal mechanisms (treaties); developed through state practice (customary law); established through judicial decisions; or set out in other documents such as codes of conduct, best practice guides or technical standards. In some cases, norms remain unrecorded altogether because they are never formalized.

Norms emerge in various ways: they may evolve spontaneously, including through an actor's indirect influence; they may be consciously promoted as political strategies serving specific interests; they may be deliberately negotiated as mechanisms for conflict management; or they may emerge through some combination of these. Norms often develop across multiple, concurrent processes at different levels, international, regional, national or subnational, and they often only become apparent in retrospect.

Sources: US National Intelligence Council, Strategic Futures Group, 'US-backed international norms increasingly contested', Global Trends, Oct. 2021; Katzenstein, P. J., 'Introduction: Alternative perspectives on national security', ed. P. J. Katzenstein, *The Culture of National Security: Norms and Identity in World Politics* (Columbia University Press: New York, 1996); Bode, I. and Huelss, H., *Autonomous Weapons Systems and International Norms* (McGill-Queens University Press: Montreal, 2022); Finnemore, M. and Sikkink, K., 'International norm dynamics and political change', *International Organization*, vol. 52, no. 4 (autumn 1998); and Sandholtz, W. and Stiles, K., *International Norms and Cycles of Change* (Oxford University Press: New York, 2009), chapter 1.

For US-based neo-primes, the target of their discourse is often the state's own procurement apparatus and the incumbent military-industrial base.[84] Representatives of Palantir and Anduril especially (but not only) argue for 'reforming' and 'rebooting' the US military-industrial base.[85] They argue that procurement bureaucracy is the principal obstacle to security because it lacks market competition. For example, Anduril's senior vice-president of manufacturing has identified 'reforming acquisition processes to break through the bureaucratic barriers that slow innovation' as a key priority for the company. Regulations, he argues, 'impose massive compliance burdens and barriers to entry, while offering no meaningful benefits to government customers responsible for spending taxpayers' dollars wisely'.[86] Such companies also frequently target the legacy primes for their lack of speed and innovation, with the cost-plus model blamed for removing an incentive to be fast and innovative. For example, in June 2026 Palantir's CTO, Shyam Sankar, argued before the US Senate that this model creates rigid, lengthy R&D cycles and called on the DOD to drop its default reliance on cost-plus contracting.[87]

By concentrating their advocacy on national acquisition and procurement processes, neo-primes and unicorn defence start-ups rarely express views on international governance forums. In the rare cases when they address these governance processes, it is usually as part of a broader claim—or suggestion—that advocates of restraint in the development and use of these technologies are either ill-intentioned or naive. For example, Palmer Luckey, a co-founder of Anduril, has spoken of a 'shadow campaign being waged in the United Nations right now by many of our adversaries to trick West-

[84] Goussac, N. and Boulanin, V., *Responsible Procurement of Military Artificial Intelligence* (SIPRI: Stockholm, Feb. 2026), pp. 6–7.

[85] See e.g. Anduril, 'Rebooting the arsenal of democracy', [n.d.]; Anduril, 'Rebuild the arsenal', [n.d.]; Sankar, S., 'The defense reformation', Palantir, 31 Oct. 2024; and Sankar, S. and Hart, M., *Mobilize: How to Reboot the American Industrial Base and Stop World War III* (Bombardier Books: New York, 2026).

[86] 'How Anduril is transforming defense technology', National Association of Manufacturers (NAM), 8 Aug. 2025.

[87] US Senate, Committee on Armed Services, 'Defense innovation and acquisition reform', Hearing, 28 Jan. 2025.

ern countries . . . into not applying AI to weapons and defense'.[88] These ideas, he says, are 'being laundered through mostly European nations that are useful idiots'. Similarly, the argument of Palantir's CEO, Alex Karp, that the 'grim reality' of present geopolitical struggles means that 'adversaries will not pause to indulge in theatrical debates about the merits of developing technologies with critical military and national security applications' can be read as an implicit rebuke to international military AI governance efforts.[89] Indeed, Karp argues that, with respect to LLM development, the USA—and the 'West' more broadly—presently faces 'an arms race of a different kind' and that 'hesitation . . . to move forward with military applications of artificial intelligence will be punished [by adversaries]'.[90] These claims matter beyond the national level because, to the extent that they transcend any single jurisdiction and shape the broader backdrop against which international governance efforts take place, they can also have a normative effect by shaping understandings of how AI should be governed and used in the military domain.[91]

In the European context, neo-primes and defence start-ups, while also needing to disrupt the prime legacy model, have taken a less aggressive disruptor narrative than their US conterparts. For example, the German firm Helsing has positioned itself as Europe's sovereign capability provider, enabling democracies to defend themselves and set their own ethical standards.[92] In doing so, rather than contesting international governance efforts, Helsing emphasizes its alignment with international regulations and the maintenance of human oversight.[93]

As well as a different business model, the neo-primes and defence start-ups have a relationship to the state that differs from that of the legacy primes. While they use many of the same channels as the legacy primes to influence policy and regulation, such as lobbying (see below), they add a layer of public advocacy on top. They do this for two reasons. First, procurement and acquisition policies currently favour the business model of legacy primes due to longer procurement timeframes, among other things. Newer entrants cannot compete with legacy primes within this existing structure and so seek to change the policies through public advocacy. Second, the valuations of the neo-primes and start-ups are narrative dependent. As discussed above, many neo-primes and start-ups are backed by venture capital, and their valuation depends heavily on a forward-looking story about the arms market being reorganized in their favour. Public argumentation helps sustain that narrative.

Big tech

Big tech's normative positioning differs from both that of the legacy primes and that of the neo-primes and start-ups, predominantly because of its mixed customer base. Big tech sells to the public as well as to militaries, with the public generally the larger market. Branding often rests on decades of building consumer trust, which exposes big tech's military work to public, employee and regulatory backlash in ways that the work

[88] Pepperdine University, 'Palmer Luckey, founder of Anduril defense industry disruptor—president speaker series (2024)', YouTube, 4 Oct. 2024, 41:54–43:50. See also MacColl, M., 'Palmer Luckey: Every country needs a "warrior class" excited to enact "violence on others in pursuit of good aims"', TechCrunch, 1 Oct. 2024.

[89] Karp, A., 'Our Oppenheimer moment: The creation of AI weapons', *New York Times*, 25 July 2023.

[90] Karp (note 89). See also Palantir (@PalantirTech), 'The technological republic, in brief', X, 18 Apr. 2026; and Karp, A. C. and Zamiska, N. W., *The Technological Republic: Hard Power, Soft Belief, and the Future of the West* (Crown Currency: New York, 2025).

[91] Nadibaidze, A., 'Startups envisioning algorithmic warfare: The discourses of US tech companies in defense AI', *Global Policy*, vol. 16, no. 3 (June 2025), pp. 490–91.

[92] Helsing, 'Helsing further strengthens European defence capabilities with funding round', Press release, 11 July 2024; and Helsing, 'About Helsing', [n.d.].

[93] E.g. Meaker, M., 'A battlefield AI company says it's one of the good guys', Wired, 28 July 2023; and Höltschi, R., 'German defense startup Helsing is bringing artificial intelligence to the battlefield', NZZ, 17 July 2025.

of the primes and neo-primes may not. Google's early work on the US DOD's Project Maven programme, helping to develop machine learning tools to analyse UAS footage, is a well-known example of this backlash.[94] Google did not renew the contract in 2018 after protests from its employees.[95] Public statements by big tech companies on military AI—whether norm advocacy, published AI principles or acceptable-use limits—can therefore be read partly as management of that exposure. However, to the extent that it is possible to identify positions, there is variation among companies in the sector.

Microsoft, for example, has been vocal in the military AI policy debate. It argues for clear international norms, risk-based regulation, human-centric oversight and industry-led measures such as voluntary codes of conduct.[96] Microsoft's position has been relatively stable since 2018, with its CEO, Brad Smith, stating that the company will supply the military with its products and services while at the same time advocating for responsible governance and ethical guidelines.[97] It has also maintained a red line against using its cloud infrastructure for mass surveillance.[98] In September 2025 Microsoft enforced this limit and disabled cloud storage and AI services supplied to a unit within the IDF on the grounds that it had breached the terms of service (see the case study in box 3.2).

After Microsoft, Google has been most influential in big tech's normative positioning due to the controversy around its involvement with Project Maven and, more recently, its abandonment of the principles initially adopted to address that controversy. In 2025 Google retracted a commitment not to design or deploy AI for technologies likely to cause overall harm; weapons or technologies whose principal purpose is to cause or facilitate injury; surveillance violating internationally accepted norms; and uses contravening international law and human rights.[99] In its place, Google says it will pursue AI 'responsibly' and in line with 'widely accepted principles of international law and human rights'.[100] The CEO of Google DeepMind, Demis Hassabis, has used a justification similar to that of the FMPs (see below) for this normative shift, arguing that democracies should lead AI development guided by human rights.[101] The shift can also be understood against the commercial cost to Google of the original commitment. For example, in October 2018 Google withdrew from bidding on the DOD's Joint Enterprise Defense Infrastructure contract, worth up to $10 billion, stating that it could not be assured the work would align with its AI principles.[102]

Meta has cited the US-led Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy as the source of the standard it expects to be met by military and national security customers in the USA and US allies in their use of its Llama LLM.[103] Other platform providers, such as Amazon Web Services (AWS), are largely reticent about military AI governance. This may be because cloud providers are

[94] Hoijtink, M. and Planqué-van Hardeveld, A., 'Machine learning and the platformization of the military: A study of Google's machine learning platform TensorFlow', *International Political Sociology*, vol. 16, no. 2 (June 2022).

[95] 'Google should not be in business of war, say employees', BBC, 5 Apr. 2018; and Wakabayashi, D. and Shane, S., 'Google will not renew Pentagon contract that upset employees', *New York Times*, 1 June 2018.

[96] United Nations, A/80/78 (note 6), pp. 147–51.

[97] Lerman, R., 'Microsoft president Brad Smith defends company's work with US military, bid for Pentagon contract', *Seattle Times*, 26 Oct. 2018.

[98] Davies, H. and Abraham, Y., 'Microsoft to tighten human rights measures after inquiry into Israel's use of its tech', *The Guardian*, 4 June 2026; and Davis and Abraham (note 55).

[99] Pichai, S., 'AI at Google: Our principles', Google, 7 June 2018.

[100] Google AI, 'Our AI principles', [Feb. 2025].

[101] Manyika, J. and Hassabis, D., 'Responsible AI: Our 2024 report and ongoing work', Google, 4 Feb. 2025.

[102] Nix, N., 'Google drops out of Pentagon's $10 billion cloud competition', Bloomberg, 8 Oct. 2018.

[103] Kaplan, J., 'Strengthening US national security by making Llama available to key allies', Meta, 23 Sep. 2025; and Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, US Department of State, 9 Nov. 2023.

largely positioned as suppliers of a general-purpose infrastructure supporting downstream applications, thereby reducing their apparent proximity to normative debate.

Foundation model providers

The parameters established by FMPs around the appropriate use of their products in military settings have shifted as their business interests have changed. Generally, the positions of FMPs on military use of their products and services have moved towards greater accommodation to military uses, although there are differences. OpenAI removed its prohibition on 'military and warfare' uses of its foundation models shortly before partnering with Anduril in December 2024.[104] Likewise, Google, which sets policy for Google DeepMind, retracted its 2018 weapons commitments in 2025, as noted above. In contrast, Anthropic has never prohibited military uses and has consistently supported lawful national security and foreign intelligence applications of its models.[105]

What distinguishes the FMPs is where and how they place limits around such uses. OpenAI's 2026 'Principles for national security partnerships' states that it does not support the use of its technology in 'systems that remove or limit users' ability to exercise appropriate human judgement over the use of force'.[106] By way of example, it includes 'systems that autonomously identify, select, and engage targets without appropriate levels of human authorization and human-defined operational parameters'. Anthropic maintains red lines against the use of its products for fully autonomous weapon systems and for mass domestic surveillance, although its position on autonomous weapons relates to its estimation of the present reliability of the technology, rather than a principled judgement of appropriateness.[107] In February 2026 Anthropic's refusal to drop these limits from the terms of its agreements with the US DOD led the DOD to designate it as a supply-chain risk.[108] Shortly afterwards, OpenAI agreed a deal with the DOD in which it agreed to the use of its foundation models 'for all lawful purposes, consistent with applicable law, operational requirements, and well-established safety and oversight protocols'.[109]

FMPs justify this shift in their normative stance by employing the same metanarrative as the neo-primes—geopolitical competition—but recasting it as a global contest between democratic and authoritarian uses of AI. For instance, OpenAI's national security principles state that, if democratic countries are denied access to advanced AI while authoritarian states obtain it, then the global balance of power could shift against democratic governance of these technologies.[110] This framing also overlaps with ideas associated with the effective altruism movement, which has influenced the founders and staff of some FMPs, notably Anthropic and, in its early years, OpenAI.[111] Thinking influenced by effective altruism treats advanced AI as a source of potential existential risk, making the question of who controls the most capable AI models central. According to this view, powerful systems are safer in the hands of actors seen as accountable, such as democratic governments and the firms working with them.

[104] Field (note 61).

[105] Anthropic, 'Statement from Dario Amodei on our discussions with the Department of War', 26 Feb. 2026.

[106] OpenAI, 'OpenAI principles for national security partnerships', [July 2026], p. 4.

[107] Hays, K., 'Anthropic boss rejects Pentagon demand to drop AI safeguards', BBC, 27 Feb. 2026.

[108] Capoot, A., 'US Appeals Court upholds Pentagon designation of Anthropic as supply chain risk', CNBC, 25 Sep. 2026; and Dorsey, J. et al., 'The Pentagon/Anthropic clash over military AI guardrails', Opinio Juris, 26 Feb. 2026.

[109] OpenAI, 'Our agreement with the Department of War', 28 Feb. 2026.

[110] Amodei, D., 'The adolescence of technology: Confronting and overcoming the risks of powerful AI', Jan. 2026. See also Amodei, D., 'Our position on open-weights models', Anthropic, 27 July 2026.

[111] Bauer, J., 'What is effective altruism? A philosopher explains', World Economic Forum, 1 Feb. 2023; Berber, J. and Hagey, K., '"Things will never be chill again": The doomers who shaped the AI safety freakout', *Wall Street Journal*, 26 Sep 2026; and 'Effective altruism is the century's biggest idea', *The Economist*, 1 Oct. 2026.

Box 3.2. Case study: Microsoft's norm entrepreneurship

Microsoft has shown a long-standing pattern of digital norm entrepreneurship, particularly around cyber norms, as well as multilateral engagement.

In 2017 the CEO of Microsoft, Brad Smith, proposed a 'digital Geneva Convention' to protect civilians, private companies and critical infrastructure from state-sponsored cyberattacks.[a] This did not materialize, but related initiatives supported by Microsoft include the Paris Call for Trust and Security in Cyberspace (2018) and the Cybersecurity Tech Accord (2018).[b]

Whilst Microsoft's efforts on cybersecurity date to the early 2000s, its digital diplomacy is more recent and represents an attempt to restore trust following Edward Snowden's revelations of Microsoft's complicity in mass domestic and international surveillance by the US National Security Agency (NSA).[c] Its involvement in debates on governance of military artificial intelligence, including a partnership with the United Nations Institute for Disarmament Research (UNIDIR) to promote industry best practice, continues this pattern of norm entrepreneurship. It was the only industry actor to respond to the 2025 call from the UN secretary-general for input on artificial intelligence in the military domain.[d]

[a] Smith, B., 'The need for a digital Geneva Convention', Microsoft, 14 Feb. 2017.

[b] Microsoft, 'Cybersecurity policy and diplomacy', [n.d.].

[c] Ratnesar, R. and Redmond, W., 'How Microsoft's Brad Smith is trying to restore your trust in big tech', *Time*, 12 Dec. 2023; and 'Edward Snowden: Leaks that exposed US spy programme', BBC, 17 Jan. 2014.

[d] United Nations, General Assembly, 'Artificial intelligence in the military domain and its implications for international peace and security', Report of the secretary-general, A/80/78, 5 June 2025, pp. 147–51.

This risk-centred outlook underpins a second shift in framing that is distinctive to the FMPs. Many speak extensively about the risks and dangers of their products, and, whatever the intent, are thereby positioned as uniquely equipped to contain what they have built. Recent security incidents by 'rogue AI' (e.g. OpenAI's 2026 report that agents in its own cybersecurity evaluations breached external systems[112]) reinforce this position in which the firm that built the capability is also the main source of the disclosure, the account of what went wrong and the proposed remedy. In a sense, this becomes the basis of a normative authority: the systems are dangerous, the FMPs understand them best because they built them, so their safeguards matter and their national security work depends on those safeguards holding. The more hazardous the technology, the stronger the claim to authority over its appropriate use.

Overall, the Anthropic–DOD dispute appears to have chastened the FMPs, and some have become more cautious about unilaterally specifying limits on the use of AI in military settings. OpenAI's national security principles, which were published after the Anthropic–DOD dispute, make a point of arguing that authority for determining the purposes and limits of AI ought to belong to accountable, democratic institutions, not a small group of private actors.[113] In the wake of that dispute, OpenAI's CEO, Sam Altman, reportedly stated that the company cannot control how the DOD uses its products and services.[114] The result is a kind of hybrid position, with some substantive limits on the use of AI in military settings having been articulated, but framed as remaining provisional pending democratic resolution on norms.

[112] OpenAI, 'The Hugging Face incident and the road ahead', 16 Aug. 2026.

[113] OpenAI (note 106).

[114] Robins-Early, N. and Montgomery, B., 'Sam Altman admits OpenAI can't control Pentagon's use of AI', *The Guardian*, 4 Mar. 2026.

Pathways to influence

This section outlines how military AI industry actors seek to translate normative preferences into normative outcomes—referred to here as 'pathways to influence'. Some of the pathways are explicit and tangible attempts to have a direct impact on norm development, including at the national level via state legislators and at the international level through multilateral discussion about the governance of military AI. Others, such as narrative framing, are more subtle and indirect. States' ability to understand and identify these actor's strategies is important to ensure an informed engagement with the military AI industry.

For the purposes of this report, pathways to influence are grouped into three strategy types: people and places; narrative-building; and legal and contractual means (see table 3.1). Many of these pathways overlap, and they are not necessarily unique to this domain. An industry actor's capacity to pursue these strategies rests on structural leverage—including technical dependence, capital, market concentration or infrastructural indispensability—that gives firms bargaining power.[115]

People and places

This first pathway is industry access to policymakers and policy spaces, with the aim of influencing, guiding and informing policy processes and outcomes, whether at the national or the international level. This is sometimes referred to as 'positional access', indicating the way in which industry can shape norms and policy outcomes from within the policymaking process itself by virtue of being present where decisions get made.[116] The strategy is evident across all company categories.

It can be seen materializing through revolving door dynamics; lobbying, personal relations and connections (e.g. between CEOs and political figures); and participation in, and contributions to, policy forums. The following provides examples of how companies practice this strategy in these three ways in turn.

Revolving doors. The development and adoption of AI in the military domain takes place in an arena long characterized by back-and-forth movement of personnel between government and industry, known as the 'revolving door'.[117] This movement carries not only technical and institutional expertise in both directions, but also networks and assumptions that can quietly align policy with industry preferences.[118] This dynamic has long been a part of the interrelationship between the legacy primes and the state, and is being increasingly utilized across the military AI industry (see box 3.3).[119] This strategy can shape multilateral talks on military AI governance indirectly when the assumptions and priorities of industry are carried over into national positions.

[115] Reuven, N. and Shamir, E., 'The shift in technological dominance and the adaption of open innovation by the defence sector', *Defense & Security Analysis*, vol. 41, no. 3 (2025).

[116] Berkhout, J. et al., 'From policy access to lobbying influence: Comparing exchange, insider and signalling models', *Journal of European Public Policy*, Published online 16 Oct. 2025; and Woodcock, T., 'Industry development of military AI: Operationalising international humanitarian law across the lifecycle', eds. Z. Assad, J. Dorsey, and N. Reinic, *Safety, Legal and Ethical Implications of Artificial Intelligence in the Military Domain* (Australian Army Research Centre Collected Papers Series, 2026).

[117] Duncan, T. K. and Coyne, C. J., 'The revolving door and the entrenchment of the permanent war economy', *Peace Economics, Peace Science and Public Policy*, vol. 21, no. 3 (Sep. 2015); and Perlo-Freeman, S., *From Revolving Door to Open-Plan Office: The Ever-closer Union between the UK Government and the Arms Industry* (Tufts University, Fletcher School, World Peace Foundation, Somerville, MA, Sep. 2024).

[118] Yates, S. and Cardin-Trudeau, É., 'Lobbying "from within": A new perspective on the revolving door and regulatory capture', *Canadian Public Administration*, vol. 64, no. 2 (June 2021).

[119] Lipton, E., 'New spin on a revolving door: Pentagon officials turned venture capitalists', *New York Times*, 30 Dec. 2023; Mecklin, J., 'The defense revolving-door, Silicon Valley edition', *Bulletin of the Atomic Scientists*, 17 Aug. 2026; and Warren, E., 'Pentagon alchemy: How defense officials pass through the revolving door and peddle brass for gold', US Senate, Apr. 2023.

Table 3.1. The military AI industry's pathways to influence

	Means		
	People and places	*Narrative-building*	*Legal and contractual means*
What	Access to policymakers and policymaking forums	Policy as narrative: industry actors compose 'stories' to frame policy issues and operational and strategic needs	Norms as legal form (rather than policy debate), including encoding preferences in contracts, terms of use and litigation
How	Participation in multi-stakeholder, multilateral forums; embedded in delegations; revolving door dynamics	Manifestos, open letters, op-eds, podcasts; branding, promotion material and visual narratives; typically through vocal CEOs	Contracts with customers and subcontractors; product terms of use; platform governance; procurement processes and lawsuits
Where	International and domestic policy forums and institutions	Digital and public spaces, internationally and domestically	Between company and user; procurement agencies; courts
Who	All types of industry actors, in different direct and indirect ways	Especially neo-primes and defence start-ups	All industry actors, but especially neo-primes, defence start-ups, and foundation model providers

A particularly high-profile example of the movement of personnel from government to the military AI industry was the appointment of Robert Work to an advisory role at the data analytics start-up HawkEye 360 and to the board of directors of Raytheon, both within one year of leaving his role as US deputy defence secretary.[120] He continued to shape AI policy while in these industry roles through senior roles on governmental bodies such as the National Security Commission on AI and non-governmental national security think tanks.[121] This dynamic also extends to FMPs. For example, in 2025 Anthropic established a national security and public sector advisory council, bringing together former senior officials from military and intelligence organizations of the US government and former members of the US Congress to help guide the company's engagement with government.[122] OpenAI has recruited dozens of former military and national security officials into policy and partnership roles (including a former director of the US National Security Agency) since removing its blanket prohibition on military use of its models in early 2024.[123] Former government officials are also moving into venture capital and private equity firms that invest in defence start-ups.[124]

There has also been movement of personnel in the opposite direction, from industry to government. A high-profile example is the appointment in March 2025 of Stephen Feinberg, co-founder of the private equity firm Cerberus Capital Management, as US

[120] RTX, 'Robert O. Work', [n.d.]; and Wilkers, R., 'Hawkeye 360 adds Robert Work, John Mulholland to advisory board', Washington Technology, 17 Apr. 2018.

[121] US National Security Commission on AI (NSCAI), *Final Report* (NSCAI: Washington, DC, 2021); and 'Defense technology task force', Center for a New American Security, [n.d.].

[122] Anthropic, 'Introducing the Anthropic national security and public sector advisory council', Announcement, 27 Aug. 2025.

[123] OpenAI, 'OpenAI appoints retired US Army general Paul M. Nakasone to board of directors', OpenAI, 13 June 2024.

[124] González, R. J., 'How big tech and Silicon Valley are transforming the military-industrial complex', Brown University, Watson Institute for International and Public Affairs, Costs of War Project, 17 Apr. 2024; Lipton (note 119); and Gvaryahu, A., 'These aren't AI firms, they're defense contractors. We can't let them hide behind their models', *The Guardian*, 15 Mar. 2026.

Box 3.3. The military-industrial complex

The term 'military-industrial complex' was popularized by US President Dwight D. Eisenhower in his farewell address of 17 January 1961. Eisenhower pointed to the 'conjunction of an immense military establishment and a large arms industry', warning of the need to 'guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex'.[a]

Eisenhower's concern was ultimately about democratic control. He linked the rise of the military-industrial complex to a technological revolution that also carried the 'danger that public policy could itself become the captive of a scientific-technological elite'. Preserving democratic government, Eisenhower argued, would be a task for future political leaders who would be required to balance these competing forces—the military establishment and a technological elite—with 'the principles of our democratic system'. He also argued that only 'an alert and knowledgeable citizenry' could keep the arms industry aligned with 'peaceful methods and goals'.

Commentators today have raised similar concerns. They note that the growing entanglement between the technology industry and military establishments risks giving private firms a say over policy in a way that democratic processes cannot easily scrutinize.[b]

[a] Eisenhower, D. D., 'Farewell address', US National Archives, 17 Jan. 1961.

[b] Bousquet, A., 'Inverting the triangle of power: The military–industrial complex after Silicon Valley', *Thesis Eleven*, Published online 10 Sep. 2026; Siegel, E., 'Artificial intelligence's hybrid, public–private sense-makers: The geopolitical race case', *Cambridge Forum on Technology and Global Affairs*, vol. 1 (2026) ; Yeung, B., 'The rise of the military-technology complex', *Bulletin of the Atomic Scientists*, 23 July 2026; and King, A., *AI, Automation, and War: The Rise of a Military-Tech Complex* (Princeton University Press: Princeton, NJ, 2025).

deputy defence secretary.[125] Several technology industry executives have also been directly commissioned into the US Army Reserves as part of the Executive Innovation Corps (also known as Detachment 201). The first cohort, joining in June 2025, consisted of Shyam Sankar, Palantir's CTO, Kevin Weil of OpenAI, Andrew Bosworth, CTO of Meta, and Bob McGrew, a former OpenAI executive.[126] The US Army's stated purpose of the initiative is to 'fuse cutting-edge tech expertise with military innovation' by recruiting senior technology executives to serve part-time in the Army Reserve as senior advisors.[127]

There are also early indications of a similar trend emerging in the European context. Gundbert Scherf, the co-founder and co-CEO of Helsing, worked as a special advisor in the German MOD.[128] A number of US companies—including Palantir and Anthropic—have also been active in the United Kingdom in hiring former government officials, ministers and senior military staff.[129]

Executive and legislative lobbying. Industry influence over military AI policy operates predominantly at the national level, where the density of contact between firms and government is greatest and where significant decisions around things like policy and

[125] Roston, A., 'The billionaire hidden behind the curtain inside Trump's Pentagon', *The Guardian*, 18 June 2026; and Roston, A., 'The Hegseth budget: Defense secretary's $1.5tn ask reveals military-industrial chaos', *The Guardian*, 23 July 2026.

[126] US Army Public Affairs, 'Army commissions second cohort of tech executives into Executive Innovation Corps', US Army, 10 June 2026.

[127] US Army Public Affairs, 'Army launches Detachment 201: Executive Innovation Corps to drive tech transformation', US Army, 13 June 2025.

[128] Ross, C. and Kehoe, C., 'The defence industry's revolving door', *Prospect*, 13 Apr. 2026; and 'Dr Gundbert Scherf, co-founder and co-CEO of Helsing, at Unternehmertag!', Unternehmertag, Mar. 2025.

[129] Booth, R., and Milmo, D., 'Architect of UK's AI policy quits after Anthropic conflict of interest concerns', *The Guardian*, 7 Sep. 2026; Whannel, K., 'Ex-Labour deputy leader Tom Watson joins Palantir', BBC, 18 Sep. 2026; and British Advisory Committee on Business Appointments, 'Advice letter: Nick Carter, member of the advisory council, Helsing Gmbh', Decision, 28 Feb. 2024.

procurement are made. This density of contact can provide opportunity for shaping governmental and institutional preferences. As one interviewee put it: 'At the national level, it is really clear in the USA that the tech industry is not just influencing policy; they are actually writing policy. They are so embedded in government that they are making sure that policy aligns with big tech interests.'[130] Recent reports about industry's involvement in national legislations underpin such claims.[131] Some companies, such as Anduril, have also argued that they need to educate national policymakers to help them understand how to regulate military AI.[132]

Agreements between the US DOD and Anthropic, Google, OpenAI and xAI reportedly require each company to provide policy-relevant knowledge alongside their models, including informing DOD strategy on frontier AI.[133] This includes requirements for each company to supply reports on future trends in frontier AI development, risk forecasting and assessments around future threats to the DOD to help it understand the dangers that frontier AI may pose in the future. In this way, these firms help shape the DOD's own strategic assessment of the technology they sell. This route to influence sits alongside conventional lobbying, since the usual target of lobbying—the DOD—in this case is directly asking firms to supply the analysis on which policy is built. It also creates a potential conflict of interest with the companies assessing the risks of their own products.

Spending on corporate lobbying has risen sharply in both the USA and Europe as military and general-purpose AI have become pressing regulatory issues.[134] For instance, Palantir's US lobbying expenditure rose from just over $1 million in 2016 to $5.8 million in 2024, higher than the spend of some legacy primes.[135] Along with Anduril and others, Palantir also supports a trade association, the New American Industrial Alliance (NAIA), which lobbies for the deregulation of company acquisitions in the arms industry.[136] This national-level presence is duplicated, to varying degrees, across the sector: Anduril and Palantir all maintain dedicated Washington-based 'global defence' or government-relations teams; and in the European Union (EU), Helsing is registered in the Transparency Register, which lists representatives trying to influence EU policy and decision-making processes. Helsing also participates in policy activity in Brussels both directly and through national associations also represented there (e.g. the Federation of German Industries, BDI, and the Federation of German Security and Defence Industries, BDSV).[137] Lobbying can also be via access to advisory bodies or commissions, or through close personal relationships between technology leaders and political figures.[138]

[130] Civil society representative, Interview with author, 22 Apr. 2026

[131] Dahlkamp, O., 'Anthropic quietly pitches its own AI safety bill to lawmakers', Politico, 16 Sep. 2026; and Amin, L. and Geoghegan, P., 'Revealed: Palantir led secret review of how the MoD spends billions', Democracy for Sale, Substack, 24, Oct. 2026.

[132] No Priors, 'AI & defense technology with Anduril CEO Brian Schimpf', YouTube, 1 June 2023.

[133] Biddle, S., 'AI giants work hand-in-hand with the Pentagon, contracts reveal', The Intercept, 8 Sep. 2026.

[134] Barnes, D. and Wendler, J., 'Defense lobby on Trump's budget', Politico, 6 Apr. 2026; Marshall-Genzer, N. and Soderstrom, E., 'Defense lobbying surges as Trump looks to boost military spending', Marketplace, 15 May 2026; Braun, E. and Coi, G., 'Defense industry spends big on lobbying Brussels', Politico, 5 Mar. 2025; and US Congress, House of Representatives, 'Human Authority over Autonomous Weapons Act of 2026', Bill HR 9729, 119th Congress, 16 July 2026.

[135] Kinder, T. and O'Murchu, C., 'Palantir's "revolving door" with government spurs huge growth', *Financial Times*, 7 Feb. 2025; and Tech Transparency Project, 'Inside Palantir's expanding influence operation', 7 Feb. 2025.

[136] 'NAIA—We back the builders', New American Industrial Alliance, [n.d.].

[137] 'Helsing Group (Helsing) — EU Lobby', GovLens, [n.d.]; 'Helsing', LobbyFacts, 6 Feb. 2026; and BDSV Exhibitions, 'Helsing Germany GmbH', IDEX 2025 Exhibitor Directory, 17–21 Feb. 2025.

[138] Montgomery, B., 'Big tech continues to bend the knee to Trump a year after his inauguration', *The Guardian*, 20 Jan. 2026.

Participation in international policy discussions on AI in the military domain. Industry participation in multilateral initiatives discussing norms related to AI in the military domain is another pathway to influence. As with previous examples, this pathway is not unique to international governance efforts on military AI—industry has, for example, on many occasions been embedded in diplomatic delegations, such as Rolls-Royce (together with select non-governmental organizations) being part of the British delegation during negotiation of the Arms Trade Treaty.[139] However, it is a pathway that has regained relevance in the light of states' desire to involve industry in policy efforts on AI in the military domain.

The REAIM summits serve as good examples because they are explicitly multi-stakeholder meetings.[140] The first REAIM summit, held in The Hague in 2023, featured a 'responsible innovation hub', with exhibiting firms including primes such as Lockheed Martin, Airbus and Thales alongside smaller AI-specialized firms. Alex Karp of Palantir featured as a speaker during the summit.[141] Other examples of industry participation in the international policy efforts include Microsoft's partnership with the UN Institute for Disarmament Research (UNIDIR) to run the Roundtable for AI, Security and Ethics (RAISE) in 2024, and in 2026 with the launch of a project to develop a framework of responsible industry behaviour for AI in the military domain.[142] Industry representatives have also been invited to brief the UN Security Council, with chief executives of OpenAI and Anthropic briefing the council on AI and international security.[143]

Industry representatives interviewed by the authors frequently expressed a sense of obligation for industry to provide technical expertise. For example, some expressed a need to 'educate' policymakers, provide technical and operational clarity, and 'explain' what is practical.[144] One interviewee expressed the view that industry is 'required to give our input so debate can be practical and grounded in realities'.[145] Another industry representative explicitly said that the advantage of taking part in multilateral discussions on military AI is that they can 'shape the conversation'.[146] While there is wide agreement among states about the value of involving industry in policy conversations, they have not taken a structured approach to this involvement; that is, they have not clarified the parameters and expectations around the role of industry in policy conversations. This largely leaves industry actors to take their own initiatives or shape their own role.

In the UN-based conversations on AI in the military domain, there has been less publicly visible involvement from industry. Despite a mandate explicitly open to industry (alongside states, civil society and academia), the UN secretary-general's report on AI in the military domain received only one submission from an industry actor, Microsoft.[147] The overall absence of visible industry engagement in the UN

[139] Duncan, J., 'The UK's role in the UN Arms Trade Treaty', *Civil Service Quarterly*, July 2013.

[140] Lee, H., 'Global summit in Seoul calls for guardrails for military use of AI', *Korea Times*, 9 Sep. 2024.

[141] REAIM Summit 2023 (note 7); and Cantrill, A., 'Palantir CEO says Europe nations need to "get serious" on tech development', Bloomberg, 15 Feb. 2023.

[142] UN Institute for Disarmament Research (UNIDIR), 'RAISE: The Roundtable for AI, Security and Ethics', [n.d.]; and UN Institute for Disarmament Research (UNIDIR), 'Framework of responsible industry behaviour for AI in the military domain', [n.d.]; and UN Institute for Disarmament Research (UNIDIR), 'UNIDIR highlights regional and industry engagement at REAIM 2026', 12 Feb. 2026.

[143] Nichols et al. (note 7).

[144] Industry representative 1, Interview with author, 16 Apr. 2026; Industry representative 2, Interview with author, 16 Apr. 2026; and Industry representative 3, Interview with author, 17 Apr. 2026.

[145] Industry representative 1 (note 144).

[146] Industry representative 2 (note 144).

[147] UN General Assembly Resolution 79/239, 'Artificial intelligence in the military domain and its implications for international peace and security', 24 Dec. 2024, para. 8; and United Nations, A/80/78 (note 6), pp. 147–51.

context, despite the above-mentioned desire of industry actors to be involved in these conversations, may be due to the procedural barriers to industry participation in UN meetings: private companies can only participate in certain UN high-level meetings or special sessions and require special accreditation to do so. In addition, few industry actors have dedicated teams to take part in multilateral initiatives, and they may just view efforts to affect policy outcomes at a national level as a greater priority.

Narrative-building

The second pathway to influence refers to the way that companies, through the creation of narratives, frame the issues associated with the problem of military AI and the associated solutions.[148] This can include defining what software and hardware products are needed to secure victory in military operations.[149] While such narratives are driven by commercial incentives, they can play a role in defining how states (and wider society) understand operational needs in relation to military AI.

The resort to narratives is closely related to the normative positioning taken by industry. It is becoming increasingly prevalent as newer actors aim to reshape market conditions and consumer preferences. This is especially evident for venture capital-backed companies due to their funding logic: for a venture capital firm to profit, a company in which it invests does not necessarily have to generate profit; what matters is that its valuation grows.[150] Since valuations are a reflection of expectations of a company's anticipated success, venture capital-funded companies rely heavily on the ability to sell certain narratives about the future. According to one academic, 'the more influence [venture capital] and major tech firms can wield on [DOD] officials—and convince them of the dangers of a new kind of big-tech, AI-enabled war—the quicker they can get their products into the marketplace'.[151]

There are many ways through which industry undertakes narrative-building. While company websites, promotional material and visual narratives are central avenues, many of the public figures (e.g. CEOs) associated with some of the neo-primes and defence start-ups write open letters, op-eds, books and manifestos and undertake media engagements to present these narratives.[152] Sometimes these are directed at the national security establishment, sometimes to the wider public.

Narrative-building can also take place through funding research bodies. The Palantir Foundation for Defense Policy and International Affairs, launched in 2023, funds academic research, fellowships and conferences on national security.[153] Its inaugural Atlantic & Pacific Forum, held in May 2024 in partnership with *Foreign Policy* magazine, was dedicated specifically to the role of AI in warfare.[154] The foundation publishes its own journal, *The Republic*, carrying company-aligned framing of AI as the 'pivotal technology' in the China–USA competition. Many larger firms also have internal research capacity to produce public policy-related reports.[155]

[148] Riebe, T. et al., 'Envisioning human–machine interaction in future warfare: Defence industry narratives on human control of autonomous weapon systems', *Global Society*, vol. 39, no. 4 (Oct. 2025).

[149] Bienvenue, E. et al., 'Private tech companies, the state, and the new character of war', Carnegie Endowment for International Peace, 1 Dec. 2025.

[150] González (note 124); and Schwarz (note 17).

[151] González (note 124), p. 25.

[152] Marshall, S., 'The military industrial venture capital complex', Policy Paper no. 23-03, Security in Context, 7 Dec. 2023; Younis, Q. et al., Open letter to Lloyd J. Austin III, US secretary of defense, 23 June 2023; Bode, I., Nadibaidze, A. and Qiao-Franco, G., 'Visuals as sources of normative substance in the debate about artificial intelligence in the military domain', *Critical Studies on Security*, vol. 14, no. 3 (2026); Nadibaidze (note 91); and Riebe et al. (note 148).

[153] Palantir Foundation for Defense Policy & International Affairs, 'About', [n.d.].

[154] 'The Atlantic & Pacific Forum: AI and the future of defense', *Foreign Policy*, 16 May 2024.

[155] E.g. Anthropic, 'Research', [n.d.]; and Google Research, 'Responsible AI', [n.d.].

While assessing the influence of the military AI industry on norms related to military applications of AI is difficult, industry-originated language appears in official policy documents. This suggests that industry's role in shaping military AI governance extends beyond formal engagement channels and into the conceptual vocabulary through which such governance and strategy is itself articulated. For example, the UK's 2025 Strategic Defence Review commits to making the British Army '10x more lethal' in part through greater integration of AI—with the '10x' term popularized for the technology sector by Peter Thiel, Palantir's co-founder, and Blake Masters, an American venture capitalist.[156] This may be evidence of a broader osmosis of ideas and assumptions from industry about the governance of military AI.

Legal and contractual means

The third pathway to influence relates to the way that companies can shape standards of appropriateness through legal or contractual means. This includes, for example, contracts (including in relation to off-the-shelf procurement, terms of use and product policies) or lawsuits. In many cases, it may have an impact on norm development at the national level first, and then in subtle ways affect norm developments at the multilateral level. This strategy is evident among all industry actors.

Contracts with states. Contracts are a standard way for states, whether as a customer or regulator, to give effect to national laws and policies across sectors, including competition policy, the protection of classified information, and procurement and probity requirements. They define requirements on both the supplier and the customer and typically include limits on end use and end user. Firms can use the same instruments to impose their own normative limits on military AI use through acceptable-use policies associated with contracts.

For example, Anthropic's contract with the US DOD for the use of its Claude LLM entailed an acceptable-use policy that included limits on the use of Claude for autonomous weapon targeting and domestic surveillance. The DOD later pushed for a broader standard, permitting 'any lawful use'. As noted above, Anthropic's refusal led to the collapse of the relationship.[157] After criticism of the language in its original contract with the DOD, OpenAI published a revised clause stating that its system 'shall not be intentionally used for domestic surveillance of US persons and nationals'.[158] The Anthropic–DOD dispute reflects not just a disagreement about what constitutes 'appropriate use' but also who should decide this—the state or the company supplying the technology.[159]

Examples also extend to the cloud infrastructure that underpins foundation models. The terms of use for Microsoft's Azure prohibit using the service to facilitate mass surveillance.[160] In September 2025 the company publicly invoked this policy for the first time against a government customer, by cutting off services to an Israeli military unit after reports that the unit had used Azure to store surveillance data on Palestinians.[161] The violation was revealed through media reporting, rather than Microsoft's own monitoring.

[156] British Ministry of Defence (MOD), *The Strategic Defence Review 2025—Making Britain Safer: Secure at Home, Strong Abroad* (MOD: London, 2025), p. 6; and Schwarz, E., 'Tech, venture capital and the hype of war', Tech Policy Press, 22 Jan. 2026.

[157] Dorsey et al. (note 108).

[158] OpenAI (note 109), updated 2 Mar.; and Perlo, J., Collier, K. and Ingram, D., 'OpenAI alters deal with Pentagon as critics sound alarm over surveillance', NBC News, 3 Mar. 2026.

[159] Dorsey et al. (note 108).

[160] Smith, B., 'Update on ongoing Microsoft review', Microsoft, 25 Sep. 2025.

[161] Davies, H. and Abraham, Y., '"A million calls an hour": Israel relying on Microsoft cloud for expansive surveillance of Palestinians', *The Guardian*, 6 Aug. 2025

Procurement off-the-shelf. The military AI industry can also shape states' understanding of capability needs through off-the-shelf procurement. As discussed in chapter 2, many companies are moving away from the cost-plus contracting model to pursue a faster, more agile procurement process in which they sell products off-the-shelf directly to states. This is typically possible for companies backed by venture capital funding or their own capital since they need those resources to develop prototypes independently of a state request (and its funding). Anduril, for example, stresses that 'Unlike most defense companies, we don't wait for our customers to tell us what they need. We identify problems, privately fund our R&D and sell finished products off the shelf. Ideas are turned into deployed capabilities in months, not years'.[162]

When states begin to buy finished products instead of specifying requirements in advance, the options on offer begin to shape what states see as operational needs and desirable capabilities.[163] This gives industry a form of 'choice architecture'—this is the way that available options are structured and framed in order to make certain courses of action appear natural or default, while others recede from view.[164] A state, as it considers these capabilities, may be tempted to adjust its procurement processes (e.g. regarding TEVV and legal review) and its concepts of operations to align them with the available capabilities.

Industry influence over capability needs also extends beyond off-the-shelf procurement. Several MODs, before issuing requests or contracts, are proactively seeking input from industry on how to understand and solve operational challenges. For example, the Netherlands has established channels through which companies can submit and develop ideas and technologies directly to the military.[165] This has a potential normative effect because, when industry helps to define and solve operational challenges, the capabilities that states have, or expect to have, can shape their engagement in normative activities, such as their positions on regulation.

Again, while the precise mechanisms of influence remain difficult to trace, it is worth noting that many states are currently adapting their procurement processes to allow for faster and more agile procurement of AI capabilities. This trend reflects the expressed preference of many military AI industry actors.[166]

[162] Anduril (note 42).

[163] Bienvenue et al. (note 149); and Sari and Evans (note 42), pp. 18–19.

[164] Thaler, R. H., and Sunstein, C. R., *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press: New Haven, CT, 2008).

[165] Gould, L., Arentze, L. and Hoijtink, M., 'Assembling the future of warfare: Innovating swarm technology within the Dutch military–industrial–commercial complex', eds T. Sweijs and J. H. Michaels, *Beyond Ukraine: Debating the Future of War* (Oxford University Press: Oxford, 2024).

[166] Goussac and Boulanin (note 84); Nadibaidze, A. and Vanderborght, R., 'Beyond prototypes and products: The influence of defence startups in military AI governance', eds A. Nadibaidze and J. Lingevicius, *Geopolitics of AI Governance: Actors, Norms, and Trends* (University of Southern Denmark, Center for War Studies: Odense, Mar. 2026); Scholar, Interview with author, 23 Mar. 2026; Defence organization representative, Interview with author, 31 Mar. 2026; and Woodcock (note 116).

4. Managing industry engagement: Mitigating the risks of regulatory capture

Industry engagement in international policy processes on military AI governance offers several benefits. Industry representatives can contribute technical expertise, while their exposure to policy discussions can shape industry practice, influencing firms' internal approaches to responsible AI development and use, and encouraging wider adherence to norms across the sector. Industry actors can also bring resources to governance processes, particularly for capacity-building, where the resources of states and international organization may be limited. Engagement can also lend policy processes legitimacy by giving the actors responsible for developing and supporting the deployment of these systems a stake in the norms being developed.

However, industry engagement also carries risks. Engagement may confer implicit endorsement of a specific actor's brand, products or views; a company may use engagement to boost its reputation or for 'ethics-washing'; or engagement may primarily benefit industry actors, with little value returned to the policy process itself. This chapter focuses in particular on the risk of regulatory capture, whereby industry engagement slides into improper or undue influence over policies, norms and standard-setting, leading to suboptimal or detrimental outcomes. The chapter ends by providing some considerations for managing those risks with respect to international policy discussion on military AI.

The context of contemporary international governance

Industry's involvement in shaping military AI governance reflects a broader transformation in the global order whereby states increasingly rely on non-state actors to manage complex regulatory domains. Over the past few decades, there has been a shift from the exercise of authority through formal, state-based institutions to a much more diffuse set of arrangements through which state and non-state actors take on the work of managing global affairs.[167] Central to this trend is the delegation of regulatory functions from states to non-state actors, including private firms.

This is a rational response to the complexity of contemporary governance challenges faced by states. As challenges relating to such areas as finance, environmental protection and emerging technologies increasingly outstrip the expertise and capacity of state institutions, there has been an increasing need to defer to, or govern specific policy issues jointly with, private actors that possess the requisite technical knowledge or influence over those policy issues. This includes both the inception of regulatory frameworks as well as their implementation. For example, in international responses to carbon emissions, states have delegated the practical work of verification of emissions reduction and trading to private auditors and certification bodies.[168]

There is a risk at the core of this arrangement: regulatory capture, the process by which regulation, in law or in application, is 'consistently or repeatedly directed away from the public interest and toward the interests of the regulated industry'.[169] Since

[167] Bellamy, R. and Palumbo, A., *From Government to Governance* (Routledge: Abingdon, 2017); and Uribe J., 'Governing on par with states: Private power and practices of political normalisation', *Review of International Studies*, vol. 52, no. 1 (Jan. 2026); and World Economic Forum, 'The rise of pragmatic multilateralists in international security cooperation', Briefing paper, Sep 2026.

[168] Partnership for Market Readiness and International Carbon Action Partnership, *Governance of Emissions Trading Systems* (World Bank: Washington, DC, Mar. 2022).

[169] Carpenter, D. and Moss, D. A. (eds), *Preventing Regulatory Capture: Special Interest Influence and How to Limit It* (Cambridge University Press: Cambridge, 2013), p. 13.

technical expertise and normative authority are often intertwined, a structural risk is that the delegation of governance functions to private actors by states inadvertently tips over into the delegation of normative authority. This may mean that, in practice, those who define the technical terms of a problem end up defining its normative resolution as well. This tension surfaced into the open with the dispute between Anthropic and the US Department of Defense in January 2026. The interesting aspect of that dispute is, arguably, besides what the content of the norms ought to be, also the question of who is entitled to determine them.[170]

Against this backdrop, those involved in international policy discussion on military AI face a balancing act. On the one hand, effective international governance of military AI requires drawing on the technical expertise and capacity possessed by industry. On the other hand, this same reliance could inadvertently lead to a situation where industry is ceded undue influence over regulatory outcomes in this space—this could lead to undue influence being ceded to actors whose interests may not align with the public good, with broader foreign policy objectives or with the goals of arms control.[171] The question of this kind of influence is rarely as stark as in the Anthropic–DOD dispute and tends to accumulate by degrees through the pathways described in chapter 3. Revolving doors, lobbying, narrative-setting and the use of contractual leverage may individually each be a defensible method for industry to engage with policy issues; cumulatively, they may direct regulation away from the public interest and towards the preferred policy outcomes of specific industry actors.

In the short term, regulatory capture may entrench a particular understanding of the policy problem itself. This reflects the notion of a 'choice architecture' discussed in chapter 3. Just as industry actors can structure the options available in procurement to make certain courses of action appear default, they can also shape which regulatory questions, options and risk categories appear appropriate. Political processes are as much concerned with managing interpretations of the subject matter and creating visions of the future as they are with clarifying outcomes. Framing narratives that are established early will provide the backdrop against which later governance choices are evaluated.

In the longer-term, regulatory capture may mean the existence of regulatory or governance frameworks that are substantively hollowed out. This may be achieved through narrow definitions of the problem set, adjusting risk thresholds or categories, or through exemption carve-outs. As an example, lobbying by Google and Microsoft reportedly led drafters of the EU Code of Practice on General-Purpose AI to reclassify 'large-scale, illegal discrimination' from a systemic risk requiring mitigation to a lower-tier 'risk for consideration', thereby leaving the provision nominally intact while narrowing its practical force.[172]

Vulnerabilities in the military AI policy process

The normative positioning of industry does not, in and of itself, present a risk of regulatory capture. Rather, risks arise if policy processes entail vulnerabilities that make them susceptible to undue industry influence. Presently, international discussions on military AI have at least three such vulnerabilities: a poorly defined role for industry;

[170] Dorsey, J. et al., '(Ir-)responsible by design? Corporate guardrails and the governance of military AI', Opinio Juris, 2 Mar. 2026; and Rozenshtein, A. Z., 'Congress—not the Pentagon or Anthropic—should set military AI rules', Lawfare, 20 Feb. 2026.

[171] Čekal (note 77).

[172] European Commission, 'The General-purpose AI Code of Practice', 10 July 2025; and Corporate Europe Observatory and LobbyControl, 'Coded for privileged access: How big tech weakens rules on advanced AI', 30 Apr. 2025.

a lack of normative agreement among states; and limited institutional capacity within ministries of foreign affairs (MFAs).

Poorly defined role for industry

In multilateral processes on military AI, there is clarity about why industry involvement is sought, but far less clarity about how industry ought to be involved in these processes. Unlike some other multilateral policy areas where frameworks for engagement with non-state actors exist, no comparable framework exists for military AI.[173]

This absence raises questions about how the relevance of a given industry actor's involvement in a process is to be judged. It is also important because it means that parameters and expectations around industry involvement cannot be set, leaving considerable room for industry actors to shape their own role.

Lack of state-based normative agreement

That states are, on the whole, slow to agree on clear norms on military AI means that industry has greater latitude to fill that vacuum with their own standards and narratives of acceptable use. This is in part a consequence of the fact that technological development in this area outstrips the tempo of policy development. Developing norms requires coordination within government entities (e.g. between MFAs and MODs), the balancing of numerous interests (including economic, security and rights), and state capacity to meaningfully follow the often numerous and complex policy issues on the table.[174]

The consequence is that frames of discussion around expectations of appropriate use and development are initially being set by industry.

Limited institutional capacity

MFAs and other relevant state bodies have limited institutional capacity to critically engage with industry. For example, rotation on relevant portfolios and insufficient investment in technical capacity-building can prevent a full understanding of the relevant technical issues.[175] Meanwhile, the resources available to large technology and defence companies generally dwarf those of government bodies.[176]

The result is a structural disadvantage in states' ability to interrogate or contest industry positions. Compounding this problem is a tendency within policymaking communities to treat private sector technical judgement as inherently authoritative and, by extension, difficult to question. This deference is rooted in long-standing cultural assumptions about the objectivity of engineering, data-based and computational systems, as well as a related tendency to treat political and moral challenges as problems awaiting technical, rather than normative, solutions.[177]

[173] E.g. World Health Organization (WHO), 'Framework of Engagement with Non-state Actors', *Basic Documents*, 49th edn (WHO: Geneva, 2020); and Lily, H. et al., 'Navigating private-sector contractor participation at the International Seabed Authority', U4 Anti-corruption Resource Centre, 30 June 2026.

[174] Government representative, Interview with authors, 29 Apr. 2026.

[175] Dunleavy, P. and Hood, C., 'From old public administration to new public management', *Public Money & Management*, vol. 14, no. 3 (July–Sep. 1994); Rhodes, R. A. W., 'The hollowing out of the state: The changing nature of the public service in Britain', *Political Quarterly*, vol. 65, no. 2 (Apr. 1994); Ylönen, M. and Kuusela, H., 'McKinseyfication of government', eds G. A. Hodge, C. Greve and E. Reeves, *Research Handbook on Privatisation* (Edward Elgar: Cheltenham, 2025); and Hodge, G. and Bowman, D., 'The "consultocracy": The business of reforming government', ed. G. Hodge, *Privatization and Market Development: Global Movements in Public Policy Ideas* (Edward Elgar: Cheltenham, 2006).

[176] Government representative (note 174).

[177] Bloomfield, B. P. and Danieli, A., 'The role of management consultants in the development of information technology: The indissoluble nature of socio-political and technical skills', *Journal of Management Studies*, vol. 32, no. 1 (Jan. 1995); Jasanoff, S., *The Fifth Branch: Science Advisers as Policymakers* (Harvard University Press:

Managing the risks of regulatory capture

States can take targeted steps to manage the risks of industry engagement.

A first step could be for states to develop criteria for identifying which industry actors are relevant to a given process and on what basis they should participate. Such criteria could include the proximity of a firm to use-of-force decisions (e.g. how directly its product or service shapes the identification, selection or engagement of a target). It could also include the degree of influence that a firm has over an AI-enabled system's behaviour (e.g. whether through control of model weights and training data or through interface design). It may also include a firm's functional role in linking other suppliers of products and services (e.g. where a firm acts as a systems integrator bringing together multiple components into a deployable capability). Such criteria, if properly matched to the overall goals of international military AI governance initiatives, could give policymakers a basis for distinguishing substantive technical input from advocacy.

Second, more structured forms of engagement can also help set parameters and expectations around industry engagement. Examples can be drawn from other international initiatives. For instance, the Business Council for Ethics of AI of the UN Educational, Scientific and Cultural Organization (UNESCO) channels company engagement into a defined set of commitments tied to an existing normative instrument—the Recommendation on the Ethics of AI—rather than open-ended consultation.[178] The Global Alliance on AI for Industry and Manufacturing (AIM Global) of the UN Industrial Development Organization (UNIDO) structures input from industry, government and development agencies around specific working groups and thematic tracks, rather than general dialogue.[179] There is also the Framework of Engagement with Non-state Actors (FENSA) of the World Health Organization (WHO), which conditions engagement on due diligence and risk assessment and differentiates the terms of interaction by actor type.[180] These could provide templates to inform how international military AI processes structure industry engagement.

Third, addressing the limited institutional capacity within MFAs and other relevant state bodies requires capacity-building. This could include establishing independent channels for technical advice to complement industry technical input. For example, in the case of chemical weapon governance, a scientific advisory board, consisting of experts from academia, industry and military institutions nominated by states, provides independent technical advice to the secretariat of the Organisation for the Prohibition of Chemical Weapons (OPCW). Noting that the UN has already set up an independent International Scientific Panel on AI, a comparable standing panel specifically focusing on military applications of AI could play a similar role. MFAs could also look at building internal technical capacity themselves to place technical expertise within MFAs and delegations. This could follow the model of the technical cooperation programme of the International Atomic Energy Agency (IAEA).[181]

Finally, as shown in chapter 3, industry acts simultaneously at different levels and through different means to shape policy outcomes. Given this, it will be difficult to manage industry influence on the governance of military AI through arms control instruments or UN-based processes alone. Because industry shapes outcomes simultaneously

Cambridge, MA, 1998); Porter, T. M., *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life* (Princeton University Press: Princeton, NJ, 1995); and Woodcock (note 116).

[178] UN Educational, Scientific and Cultural Organization (UNESCO), 'Recommendation on the ethics of artificial intelligence', adopted 23 Nov. 2021.

[179] UN Industrial Development Organization (UNIDO), 'AIM Global: Global Alliance on AI for Industry and Manufacturing', [n.d.].

[180] World Health Organization (note 173).

[181] International Atomic Energy Agency (IAEA), 'Technical cooperation programme', [n.d.].

through multiple, often informal channels, states require a coherent approach that connects different policy levers—including export control, procurement, competition and foreign policy communities—and that takes account of the broader environment of incentives (e.g. revenue models, investor pressures and competitive positioning) that structure industry behaviour. Voluntary guidelines and normative instruments have a role to play, but addressing regulatory capture is likely to also require that economic levers, such as procurement conditions, are deployed alongside them.

5. Conclusions

Key findings

The military AI industry is not a monolith but a stratified, shifting ecosystem of different actors, products and services, and relationships

Military AI is big business, and many (new and old) firms want a slice of the pie. A range of commercial actors thus shape the development and adoption of military AI today, ranging from century-old legacy primes, via neo-primes and defence start-ups backed by venture capital, to powerful big tech firms and AI companies, some of which until recently had rejected the use of their foundation models for military applications.

No single type of actor spans the whole industry, and each is increasingly dependent on sets of partnerships and consortia and—for those with significant capitalization—acquisitions to facilitate their involvement in the arms market. This increasingly interdependent web of relationships can obfuscate public understanding about who builds what and for whom.

The military AI industry can directly and indirectly shape regulatory and normative outcomes

Industry engagement in military AI governance is not only a matter of contributing technical expertise. Firms bring with them normative positions on how AI should be governed and used in the military domain, and these positions are shaped by their business model, their relationship to the state and their exposure to public scrutiny.

Industry can shape regulatory and normative outcomes through several pathways, which can be gathered into three categories. First are people and places, which include lobbying at the national and international levels; the movement of personnel between government and industry, and participation in international policy debates. Second is narrative-building, where actors compose 'stories' to frame policy issues and operational and strategic needs. These are reflected in, for example, open letters, manifestos and promotion materials. Third is legal and contractual means, which can allow firms to embed preferences into product terms of use. Through these means, unfolding across domestic and international levels, the military AI industry may directly and indirectly affect and shape global norm development around the responsible use of AI in the military domain.

Unstructured industry engagement could allow firms' commercial interests to unduly shape international military AI governance

States have yet to take a structured approach to industry engagement in international policy efforts on military AI, with little attention thus far paid to the parameters and expectations around the role of industry. This has left industry actors to take their own initiatives or shape their own role. This matters because participation in policy initiatives can provide firms with an opportunity to frame issues, set standards and define best practices in ways that advantage certain business models over others, or that help secure outcomes favourable to their commercial interests.

Left unchecked, this dynamic risks tipping into regulatory capture, where the boundary between informing policy and shaping it in one's own favour becomes difficult to discern. This brings risks that states exercise their decision-making prerogative in an environment unduly shaped by the interests of specific industry actors.

Recommendations

States should develop criteria for determining relevant industry actors with which to engage

For industry involvement in policy debates on the governance of AI in the military domain to be effective, it is essential to bring the most relevant actors to the table. The question for policymakers, therefore, goes beyond simply whether or not to engage industry in the debate on governance of military AI, but which industry actors to engage with, recognizing that the military AI industry is not a monolith.

States should thus develop criteria to help identify the most relevant of these actors. These criteria could include the proximity of a firm to use-of-force decisions; the degree of influence that a firm has over an AI-enabled system's behaviour; and a firm's functional role in linking other product and service suppliers. The criteria could give policymakers a basis for distinguishing substantive technical input from advocacy if properly matched to the overall goals of international military AI governance initiatives.

States should take a structured approach to industry engagement in international military AI governance

For states to be able to reap the benefits and avoid the pitfalls of industry involvement in international policymaking, they must take a more structured approach to industry engagement in relevant forums (e.g. the UN and REAIM processes). States should establish dedicated channels for industry outreach, including through industry bodies, and should develop clearer mechanisms and parameters to govern the terms of engagement with industry. States need not start from scratch and can draw on existing international initiatives as templates for this engagement.

At the same time, states should establish parameters that aim to keep this engagement balanced and guarded against regulatory capture. Again, states can draw on a number of existing frameworks as templates for these parameters, including WHO's FENSA. Taken together, these steps would help address policy process vulnerabilities and better position states to enjoy the benefits of industry engagement while mitigating the risks.

States should strengthen their capacity to engage with industry critically and to draw on a wider range of actors for technical expertise

To prevent undue industry influence in global policymaking on AI in the military domain, states need to strengthen internal capacity to engage with industry critically. States cannot realistically match industry's technical expertise, but they must possess a capacity to differentiate technical input from normative or commercial advocacy; to understand where a firm's interests lie; and to ask the right questions of industry claims. Without this, states may defer to industry on matters that are not purely technical, such as what counts as acceptable risk or appropriate human control.

To build this capacity, states should invest in expertise within ministries of defence and foreign affairs that can assess and contextualize industry input, including technical, legal and policy skills. In the pursuit of technical advice and capacity-building on technical matters, states should also draw on actors with less or little commercial stake in shaping state positions (e.g. technical universities, independent research institutes and international organizations). This would give states independent sources against which to test industry positions and reduce reliance on any single group of experts.

About the authors

Dr Alexander Blanchard is the Defence AI Policy Deputy Lead at The Alan Turing Institute, London. Alexander was previously a Senior Researcher in the Governance of Artificial Intelligence (AI) Programme at SIPRI.

Laura Bruun is a Senior Researcher in the SIPRI Governance of AI Programme. Laura's research focuses on the humanitarian and legal implications of the use of AI in the military domain, including autonomous weapon systems and AI-enabled decision support systems.



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

© SIPRI 2026