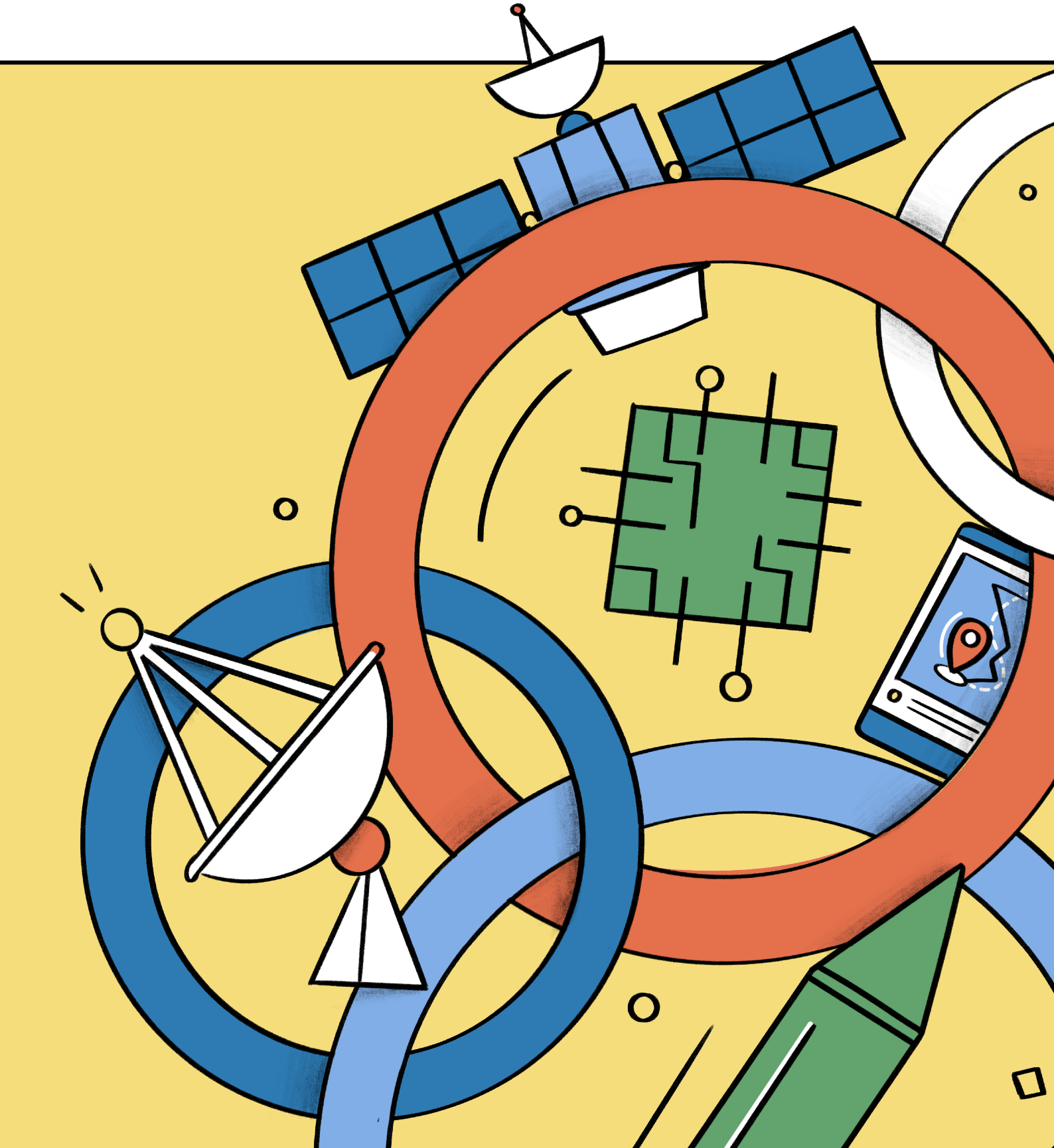
WHEN ALGORITHMS GO TO WAR

Tech giants, the arms industry and the weaponisation of AI

June 2026



About this report

In this report, we examine the rapid militarisation of data-intensive technologies and the deepening of convergence between tech giants and arms producers. Amid booming military budgets and unprecedented investment in artificial intelligence, we document how some of the world's largest technology companies have become key suppliers to the military, while traditional arms producers race to build increasingly autonomous weapons - two once-distinct sectors that are now fusing.

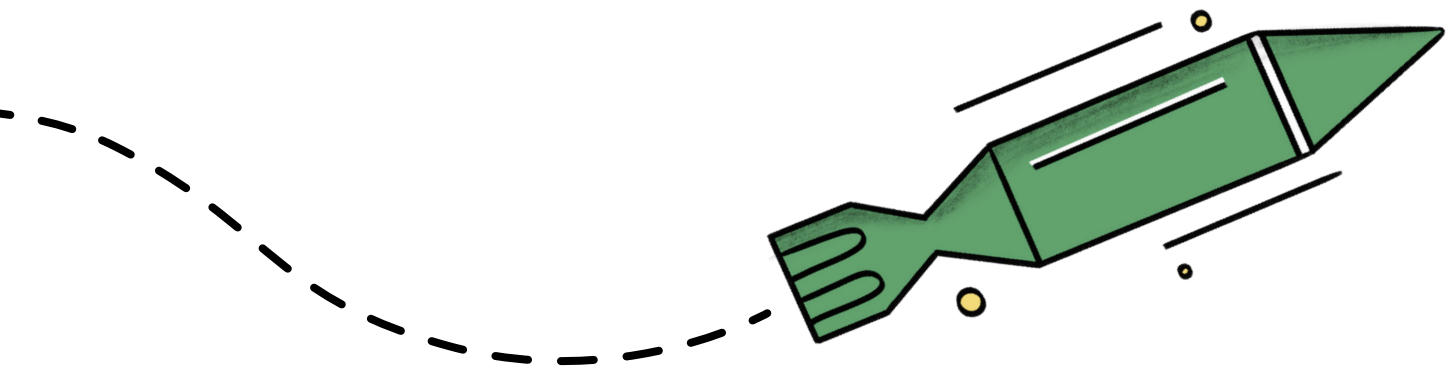
Through an overview of military contracts, we examine some of the companies driving this shift: the computing-hardware producers whose chips and networks underpin modern warfare (AMD, Cisco, IBM and Nvidia); the tech giants supplying cloud services, software and generative AI (Alphabet, Amazon, Meta, Microsoft, Oracle and SpaceX); the venture-backed "neo-primes" Anduril and Palantir, built expressly for defence (even if the latter has today several contracts outside the military sphere); and the world's five largest arms producers (BAE Systems, General Dynamics, Lockheed Martin, Northrop Grumman and RTX). We also look briefly at China, the only other state with comparable capacity. The selection is deliberately weighted towards the biggest players and is, by design, not exhaustive.

Across these profiles, we trace a set of shared concerns: the spread of AI decision-support systems that compress the kill chain and weaken meaningful human control; the erosion of companies' own ethical commitments; and a dangerous concentration of power in a handful of firms with unusually close ties to government. We argue that these developments are outpacing the rules meant to govern them, and make the case - to states and companies alike - for binding international rules, grounded in international humanitarian law and international human rights law, covering AI in the military domain, and corporate accountability.

This report was written by Frank Slijper in collaboration with Dr Ilia Siatitsa and Ioannis Kouvakas. Thanks also to Magnus van Loosdrecht, Roos Boer and Thomas van Gool. Cover and report by Ann Macleod.

DISCLAIMERS

PAX and Privacy International observe the greatest possible care in using information and drafting publications, but cannot guarantee that this report is complete and assumes no responsibility for errors in the sources used. The report is provided for informational purposes and is not to be read as providing endorsements, representations or warranties of any kind whatsoever. Nothing in this report should be seen as investment advice. Opinions and information provided are made as of early May 2026 and are subject to change without notice. PAX and Privacy International will not accept any liability for damage arising from the use of this publication.



CONTENTS

Executive Summary

Data-intensive technologies are increasingly important in the development of new weapons and in warfare, as seen in every recent conflict involving major military powers. This latest military revolution is built on everything from advanced microchips, data centres and cloud services to AI-generated targets and autonomous drones. We witness this on an almost daily basis, from Ukraine to across the Southwest Asia and North Africa (commonly referred to as Middle East).

Amid booming military budgets and unprecedented investment in AI, the global tech and arms industries are being reshaped. Tech giants have become key suppliers to the military, while traditional arms producers race to build increasingly autonomous weapons.

A central concern highlighted throughout this report is the massive concentration of power with a few American technology companies - which also own the main social media platforms - controlled by the world's wealthiest individuals, who are themselves unusually close to the centre of US political and military power. At the same time, as democracy and the rule of law risk being compromised, this is a potentially dangerous combination.

These trends are not new, but the current acceleration of technological change, combined with rising geopolitical tension and conflict, demands a far more urgent response from the international community than we have seen until now, in order to ensure that long established legal principles are safeguarded and the use of these new technologies are bound by international human rights and international humanitarian law.

What this report covers

Through an overview of military contracts, in this report, we survey how some of the world's largest technology companies are becoming more militarised, and how civilian and military technology are becoming ever more intertwined. We examine the role of tech giants by focusing especially on ten of the largest US companies that cover the whole hardware-and-software range and how these technologies are being adopted by the military. We also highlight the activities of two so-called neo primes and the world's five biggest arms-producing companies.

The companies and deals examined are the largest in their sector. This makes the report heavily US-focused, and by design, not exhaustive with developments included until early May 2026. Focusing on the wide range of well established and emerging military and tech companies, including in countries such as Israel and Ukraine, would require a separate study. China is the only other country with the capacity to build large-scale AI infrastructure and models. Although reliable information on its military programmes is scarce, we briefly look into this as well.

We distinguish four main categories of companies:

- **Computing hardware producers**: AMD, Cisco, IBM and Nvidia
- **Tech giants** (infrastructure, software and programming): Alphabet, Amazon, Meta, Microsoft, Oracle and SpaceX
- **Military-tech neo primes**: Anduril and Palantir
- **Prime arms producers** with increasingly autonomous weapons: BAE Systems, General Dynamics, Lockheed Martin, Northrop Grumman and RTX

Computing hardware producers

The most controversial activities of the hardware companies concern their cooperation with the US nuclear weapons programme (AMD), given the catastrophic and unacceptable humanitarian consequences of such weapons, and with the Israeli military (IBM, Nvidia) in the context of its atrocities in Gaza. AMD chips have also been found in Russian weapons used in the full-scale invasion of Ukraine. Nvidia is not only the world's most valuable company, but it also has the widest range of military contracts in this category. Its chips have long been used in weapon systems, from F-22 fighter jets to the newest drones - including those used by Russia to attack Ukraine. Nvidia is the largest tech employer in Israel and works with Israel's largest arms producer Elbit. Palantir, Lockheed Martin and Northrop Grumman are other key business partners.

Tech giants

Among the Tech giants, Alphabet, Amazon, Microsoft and Oracle won the Pentagon's USD 9 billion Joint Warfighting Cloud Capability contract in 2022. The same year, the National Security Agency (NSA) awarded Amazon a cloud computing contract codenamed "Wild and Stormy", worth up to USD 10 billion. Two years earlier, Alphabet, Amazon, IBM, Microsoft and Oracle won a contract to supply cloud services to the US intelligence community; reportedly worth "tens of billions" USD over fifteen years. These are the largest such tech contracts to date.

All the featured tech giants are now heavily invested in generative AI, either by developing their own models or through major stakes in OpenAI and Anthropic. The 2025 GenAI.mil contracts for Alphabet, OpenAI and SpaceX are far smaller but may grow significantly as part of the aggressive US AI Strategy and a projected military budget rising from USD 1,000 billion to 1,500 billion. Anthropic was initially part of the deal but was dropped and labelled a 'supply-chain risk' by the Pentagon after it insisted that its products would not be used for internal surveillance or lethal autonomous weapons. Even so, the use of generative AI in US offensive military operations in Venezuela and Iran, particularly Anthropic's Claude, has been reported in recent months.

Meta joined the military circuit only recently but has quickly embraced cooperation with some the most controversial players in the world of weaponised AI, including Scale AI, Anduril and Palantir; Microsoft too cooperates with Anduril and Palantir.

Alphabet, Amazon, Microsoft and Oracle have long and extensive relations with the Israeli army, which deepened further after the start of the ongoing genocide in Gaza in October 2023. Amazon and Google for example provide extensive cloud services to the Israeli government and the IDF, under the USD 1.2 billion Project Nimbus. Microsoft for its part is said to have a "footprint in all major military infrastructures" in Israel.

Neo primes

The relatively new players Anduril and Palantir have become emblematic of a US drive towards increasingly automated warfare with few constraints; their AI-enabled Maven Smart System is one of the flagship examples. Both work closely together and have successfully challenged the position of legacy arms-industry players. Anduril is rapidly expanding the range of weapons it offers, including advanced autonomous technologies such as loitering munitions and collaborative combat aircraft (CCA).

Prime arms producers

The world's largest arms producers are also capitalising on both high military demand and the rapid development of small drones, loitering munitions and other autonomous systems. Lockheed Martin, for example, recently tested AI-enhanced targeting in flight by an F-35 fighter jet under its Project Overwatch. The company says that it marked the first time a tactical AI model suggested a combat target to a fighter pilot independently. RTX's CGU-53 StormBreaker "smart weapon" is delivered from fighter jets such as the F-35 and can "autonomously detect and define targets".

Northrop Grumman calls its Lumberjack one-way attack drone fully autonomous, though it can also be flown with man-in-the-loop control, "depending on what the customer wants". It can fly several hundred miles or loiter for hours and strike multiple targets on a single sortie. In March 2026 BAE Systems announced a "strategic" collaboration with Scale AI to accelerate the development and fielding of advanced AI in support of the US Department of War's "high-stakes mission environments and operational platforms". At the same time BAE Systems says that the future of drones lies in their ability to operate independently, "whilst still maintaining meaningful and context-appropriate human decision-making".

Ethical policies

In light of emerging concerns about the military use of AI, the tech and arms companies have –sometimes after pressure by their employees– published guidelines to govern the use of their products, often including human rights elements or "responsible" AI. How far these policies are reflected in practice is frequently open to question, and they can easily be reversed or withdrawn at will as we have seen. They are therefore no substitute for international standards.

These policies do matter as reference to the 'values' that companies claim to represent and as such provide a benchmark against which to hold them to account. An analysis of these documents provides a mixed picture with only a handful of companies adopting policies limiting their capacity to pursue military contracts on ethical grounds, although none of these companies have demonstrated their compliance with the UN Principles on Business and Human Rights.

Despite the controversial uses mentioned, AMD has one of the most advanced ethical business policies of all computing hardware producers. Among the tech giants, Microsoft's policies appear the best formulated and have been tested in 2025 when abuse was flagged over Israel's use of its Azure cloud in the context of Gaza. Meta and Alphabet have recently rewritten their military policies to expand the scope of their military work, while Amazon, Oracle and Palantir have long considered military contracts as a duty rather than a risk. Anthropic has tried to curtail some military uses of Claude, but its policies still leave ample room for other controversial and potentially unlawful military uses.

Among arms producers, Northrop Grumman stands out that it will forgo certain arms deals where it has concerns about the potential customer country's use of weapons, even where they would get government permission to export. More typically for the sector, none of the arms companies are known to set any limits on US government contracts for increasingly autonomous weapons. Most other companies profiled have human rights policies that do not meaningfully address harmful uses by customers, or in some cases (SpaceX and Anduril) appear to have no policy at all.

Data protection policies

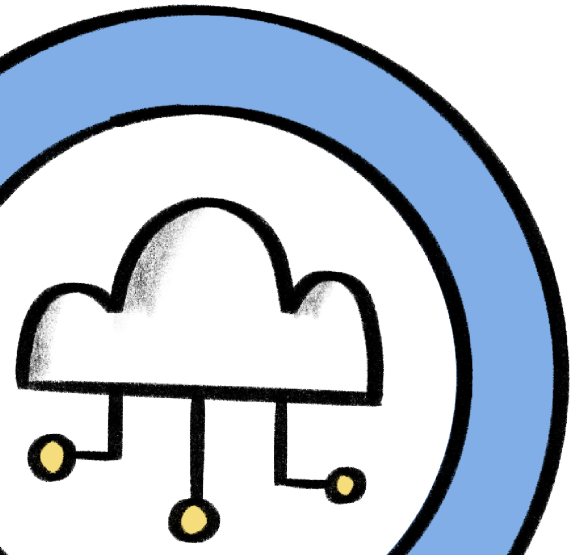
Several of the companies profiled in this report often operate extensive privacy and data-protection frameworks for consumer, civilian and enterprise users. Their policies also show important limits in those frameworks when their infrastructure, models or services are used by military, intelligence or other state customers. In particular, standard consumer privacy policies generally do not govern customer-controlled content processed in cloud environments, public cloud notices often distinguish sharply between provider service data and customer data and open or deployable AI models may be used in military contexts without a dedicated public data-protection framework for affected third parties.

The case for international guidelines

While this report does not review in detail national laws, the overall conclusion based on current practices is that national regulation to prevent or mitigate the human rights risks posed by the use of data intensive technologies in military context is at best ineffective and often absent. As current uses of military AI, both in providing targeting suggestions and in increasingly autonomous weapons, are set to expand and proliferate, new legally binding international rules are more urgent than ever. Such rules should ensure responsible, reliable and accountable use of data-intensive technologies in the military domain, preserve meaningful human control over the use of force and associated operations, and ensure compliance with international humanitarian law and international human rights law.

After more than twelve years of discussion, states have a unique opportunity later in 2026 to decide to open UN negotiations on a treaty on autonomous weapons. Moreover, a separate track of UN General Assembly mandated discussions on the broader issue of 'AI in the military domain' is taking place, with informal exchanges starting in June 2026.

States bear the primary responsibility to create, adapt and enforce international rules for a changing world, but companies have a key role and responsibility too. They need to ensure that their products comply with international norms on business and human rights, including human rights due diligence to ensure their products and services do not contribute to violations.



Recommendations

PAX and Privacy International therefore call on states to:

- without delay begin negotiations with the view to adopt an international treaty on autonomous weapons that should: ban autonomous weapons that do not allow for meaningful human control; ban autonomous weapons that target humans directly; and provide additional rules so that other autonomous weapons will be used with meaningful human control;
- ensure that ongoing international efforts to regulate AI in the military domain explicitly articulate states' obligations to respect and protect privacy and personal data;
- adopt a moratorium on the use of AI systems for the use of force, for example in decision support systems, until necessary international rules and effective safeguards are in place;
- provide transparency on the use of AI and other data-driven technologies in the military domain, including the measures taken to mitigate human rights risks; and
- adopt privacy and data protection legislation, in line with international standards, that protects privacy and personal data in the military domain, setting out clearly what categories of personal data may be processed, on what legal basis, subject to what safeguards, and with what oversight.

We call on companies in the tech and military sectors to:

- stop developing, selling, transferring or servicing autonomous weapon systems that operate without meaningful human control, and stop supplying AI systems for the use of force, until necessary international rules and effective safeguards are in place;
- establish clear public policy committing not to contribute to the development, production or sale of such systems;
- include a clause to their contracts with customers, including government and military agencies, stipulating that their technology may not be used in, or contribute to the development, of such systems;
- carry out effective human rights due diligence to identify, prevent and mitigate the risks of adverse human rights impacts arising from their activities in the military domain;
- demonstrate compliance with international data protection standards, including by adopting data protection policies, clearly setting out what categories of personal data may be processed in military domain context, on what legal basis, subject to what safeguards, and with what oversight; and
- ensure that licences, deployment terms and acceptable-use policies for AI models used by military or government customers include binding minimum data-protection obligations, including in relation to personal data about civilians and other affected third parties.

We call on investors and financial institutions to:

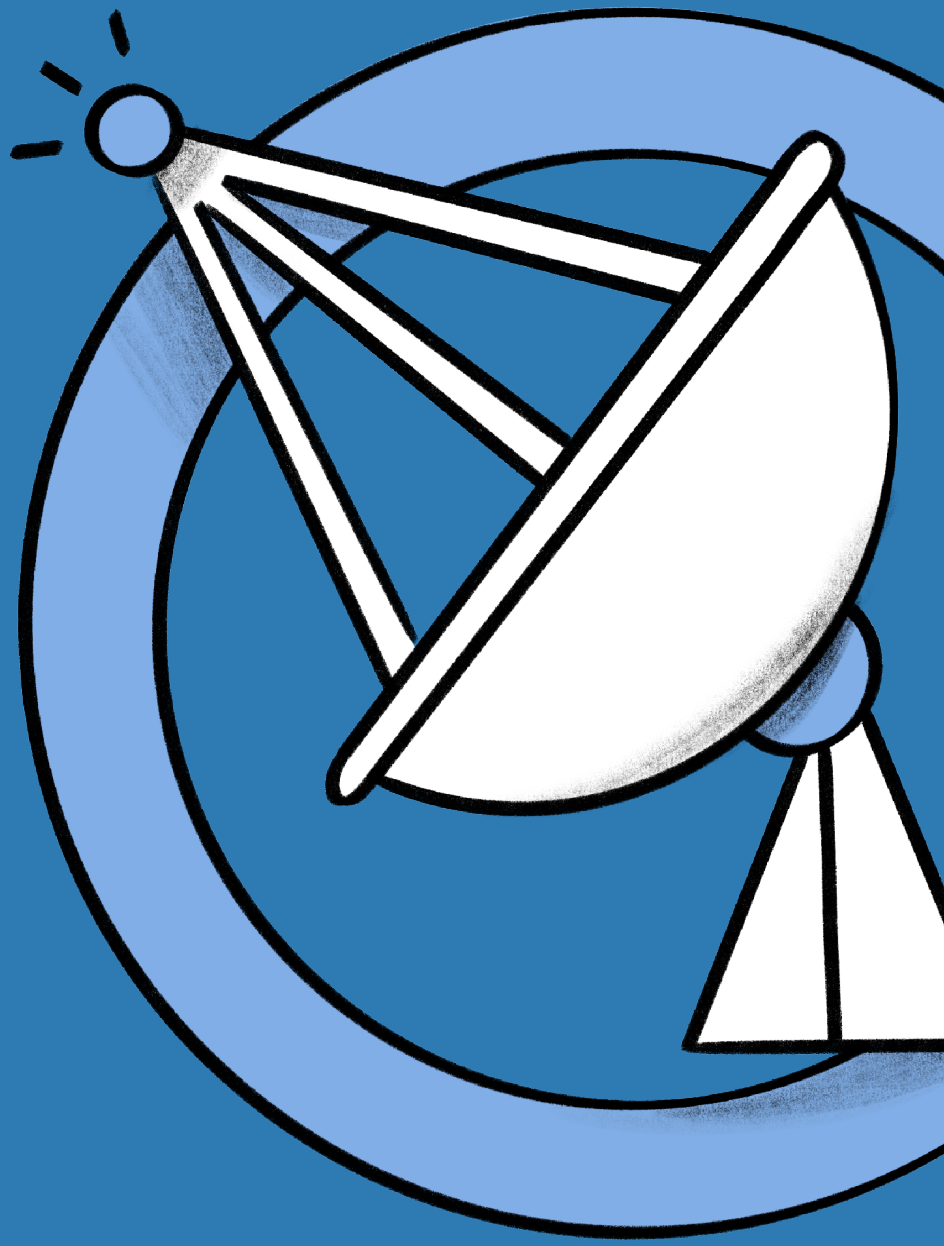
- adopt investment and financing policies on AI in the military domain to address and mitigate human rights risk posed by these technologies; and
- require the companies they invest in or finance to guarantee that their activities do not contribute to the development, sale, or transfer of autonomous weapon systems without meaningful human control, and AI systems for the use of force.

Abbreviations

AI	Artificial Intelligence
AIP	AI Platform (Palantir)
AWS	Amazon Web Services (not: Autonomous Weapon Systems)
CBP	Customs and Border Protection (US)
CCA	Collaborative Combat Aircraft
CCW	Convention on Certain Convential Weapons (UN)
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CTO	Chief Technology Officer
DARPA	Defense Advanced Research Projects Agency (US)
DHS	Department of Homeland Security (US)
DIU	Defense Innovation Unit (US)
DoD	Department of Defense (US – until 2025)
DoE	Department of Energy (US)
DoW	Department of War (US – since 2025)
ESG	Environmental, Social and Governance
EU	European Union
EUR	Euro
GDP	Gross Domestic Product
GenAI	Generative AI
GGE	Group of Governmental Experts
GPU	Graphics Processing Units
IBM	International Business Machines Corporation
ICE	Immigration and Customs Enforcement (US)
ICRC	International Committee of the Red Cross

Abbreviations

ICT	Information and Communication Technology
IDF	Israel Defence Forces
IHL	International Humanitarian Law
IHRL	International Human Rights Law
IVAS	Integrated Visual Augmentation System
JWCC	Joint Warfighting Cloud Capability
LAWS	Lethal Autonomous Weapon Systems
LLM	Large Language Model
MoD	Ministry of Defence
MSS	Maven Smart System
NATO	North Atlantic Treaty Organisation
NNSA	National Nuclear Security Administration
OECD	Organisation for Economic Cooperation and Development
PLA	People's Liberation Army (China)
R&D	Research and development
S&P	Standard & Poor's
SIPRI	Stockholm International Peace Research Institute
SWANA	Southwest Asia and North Africa (Middle East)
UAS	Uncrewed Aerial System
UAV	Uncrewed Aerial Vehicle
UCAV	Uncrewed Combat Aerial Vehicle
UK	United Kingdom
UN	United Nations
UNGP	UN Guiding Principles on business and human rights
US	United States



Chapter 01

Setting the scene: how tech went to war

1. Setting the scene: how tech went to war

1.1 Commercial and military applications of ICTs

In 1966 the Pentagon's Advanced Research Projects Agency (ARPA, now DARPA) established the ARPANET, which laid the foundation of our current internet, and by extension the information revolution. Three years later, it awarded a contract to build Interface Message Processors (IMPs, the equivalent of today's routers) for ARPANET to Bolt Beranek & Newman (BBN), a tech company set up in 1948 by two MIT professors.[1] By the mid-1960s BBN had gained a reputation as "the third university" in Cambridge (after Harvard and MIT), with a focus on information systems for hospitals. Since the late 1960s DARPA has become one of its key customers, including recent contracts to develop the DARPA Quantum Network and the Boomerang shooter detection system.[2] In 2009 Raytheon (now RTX, the world's second[3] biggest arms producer) bought BBN for some USD 350 million.[4] Today's core activities are still in the area of data technologies, command-and-control, situational awareness, sensing, cyber and speech recognition.

The example illustrates how tech companies have always been involved in military activities – some from the start, some later, some only marginally, others substantially. Thus, most legacy (Cold War-era) tech companies have been involved in military activities for much of their existence.[5] DARPA and its equivalents in Europe have been key incubators of emerging (information) technologies[6] (and even more so in state-led economies such as China and the Soviet Union). Whether at IBM, Intel, Oracle, Siemens or Philips, their military customers were always very relevant as incubators of new research and development (R&D) with potential spin-off or spill-over effects to their civilian markets.

Only when consumer demand for information technology boomed in the 1990s - when computers became household products (rather than mostly scientific, industrial or military goods), when ARPANET led to the worldwide web and the internet and when soon after mobile telephones became computers themselves – only then did the consumer market become more lucrative to the tech sector than their military customers[7], and R&D was much more civilian than military-oriented, with military technology more and more enabled by spin-ins from the civilian sector (military simulation profiting from the gaming industry; satellite quality improving with sharply increased civilian use in navigation and imagery). Still, military funding remained an important part of the emerging technologies agenda, with as much as 80 per cent of all US AI research funded by the Pentagon in the mid-2000s.[8]

From the late 1990s, the CIA established non-profit entity Peleus, later renamed In-Q-Tel, to capitalise on innovations in the private sector, with a special focus on Silicon Valley. "By channelling funds from the CIA to nascent firms building surveillance, intelligence gathering, data analysis, and cyber-warfare technologies, the agency hoped to get an edge over global rivals by co-opting creative engineers, hackers, scientists, and programmers."[9] In 2005, the CIA transferred USD 37 million seed money into In-Q-Tel; USD 94 million by

2014. Best known example is Keyhole, a San Francisco-based company that developed software to create three-dimensional models of the earth's surface. In-Q-Tel provided funding in 2003, and within months, the US military was using Keyhole to support US troops in Iraq. It was never revealed how much In-Q-Tel invested in Keyhole, but in 2004, Google purchased the start-up and renamed it Google Earth.[10]

Still, throughout much of the first quarter of this century, huge growth of the ICT market (after the infamous dot-com bubble burst in 2000)[11] enabled massive investments largely drawn from private investors, including many of the new tech billionaires. One clear example is the development of advanced large language models (LLMs) and other generative AI technologies that became best-known with the launch of OpenAI's ChatGPT in November 2022, since followed by rivalling apps such as Microsoft's Copilot and the Chinese DeepSeek. As we will see, militaries worldwide have subsequently looked at incorporating these AI advances into warfighting applications.[12]

1.2 The rapid militarisation of tech

As military organisations started prioritising data-intensive technologies, new initiatives were set up to attract the tech sector and start-ups in particular. In the US, the Defense Innovation Unit (DIU), based in Silicon Valley, was founded in 2015 to help the US military make faster use of emerging commercial technologies and to take away perceptions from the business side regarding the slow-moving bureaucracy, also known as the Valley of Death.[13] While shaping a more favourable business environment, many initiatives had limited success at best.[14] With a more long-term view in 2016 the Defense Innovation Board was set up, chaired by former Google CEO and Alphabet board member Eric Schmidt and with current and former executives from Meta and Google, among others, as members.[15] In 2018, the Trump administration requested a steep increase in DIU's budget for fiscal year 2019, from USD 30 million to USD 71 million and up to USD 164 million for 2020.[16]

Much changed with Russia's full-scale invasion of Ukraine in 2022 and subsequent strong increases in military spending, especially in much of the northern hemisphere. Global military expenditure has risen in real terms for eleven consecutive years, reaching USD 2,887 billion in 2025 – a 41 per cent increase between 2016 and 2025.[17] Because of the heavy costs of the war, both Ukraine and Russia entered a war economy mode[18], with an estimated 40 and 7.5 per cent respectively of their GDP spent on the military in 2025.[19]

After the Russian invasion, EU countries also quickly announced sharp increases of their military budgets, which had already significantly grown since 2015. Military spending in Central and Western Europe - *not* including Russia and Ukraine - rose by 14 per cent between 2023 and 2024 and 59 per cent from 2015-2024.[20] While a significant part of the more recent increases has been for military aid to Ukraine, much larger amounts have been committed to expanding existing military power, both personnel and hardware. Unprecedented was Germany's reaction right after the invasion when it announced it would make available an extra-budgetary EUR 100 billion to fund the expansion of its armed forces.[21]

In addition, the EU entered new territory with a range of new programmes aimed at bolstering military spending and military cooperation and supporting its arms industry. The pre-dating European Defence Fund (subsidising R&D programmes) and the European Peace Facility (supporting militaries outside the EU, including with weapons) have since been expanded significantly. In March 2025, the European Commission launched its ReArm Europe Plan (quickly rebranded as Readiness 2030), which "proposes to leverage over EUR 800 billion in military spending". Many may see such steps towards a more military capable and independent EU as positive, not just because of the perceived threat of Russia, but even more so now with growing concerns regarding the US, its decades-long partner, which has now become increasingly unreliable if not outright hostile.[22] However, many questions remain about democratic oversight and economic sustainability, amongst others, of the ReArm Europe Plan.[23]

Even more radical has been NATO's shift in spending targets where, under heavy pressure from the Trump Administration, its members agreed (with some caveats) in 2025 to increase its funding target from 2 to 5 per cent of countries' GDP (Gross Domestic Product) in 2035, of which 3.5 per cent should be dedicated to "core" military requirements and the additional 1.5 per cent to "defence and security related" needs.[24] While the aims are real and many members have already significantly raised spending since 2022 (and before), further increases are likely to meet more pushback, not least because these NATO targets were merely agreed to please Trump[25], rather than being militarily relevant or required. If spending 3.5 per cent of GDP across the 32 members were met, NATO's collective military spending would reach USD 2.4 trillion by 2035: a 63 per cent real terms increase. Challenges ranging from competing spending priorities (health, education, energy transition) to the sustainment of growing deficits in a challenging fiscal climate will grow.[26] That did not stop Trump from announcing a massive USD 1.5 trillion military budget for 2027, up from USD 901 billion set for 2026.[27] In that spending proposal the thus far little-known Defense Autonomous Warfare Group's (DAWG) budget increased from USD 225 million (fiscal 2026) to no less than USD 54.6 billion, likely pointing to the creation of a new military command focused on autonomous warfare.[28]

It is important to note that spending levels of 3.5 per cent GDP or higher have traditionally been rather exceptional and mostly seen in conflict-affected and/or highly authoritarian countries.[29] In the case of the US, it has been built on a decades-old national security strategy aimed at having full-spectrum dominance or superiority, most recently adapted to having "the world's most powerful, lethal, and technologically advanced military to protect our interests, deter wars, and—if necessary—win them quickly and decisively, with the lowest possible casualties to our forces."[30]

Regardless of the exact way forward, with military spending levels expected to continue growing for the next few years, for the first time since the Cold War the armed forces have become a much more attractive customer for companies that traditionally focused mostly on civilian markets. At the same time, the arms industry, besides adapting to unheard-levels of demand for their traditional weaponry, has put more emphasis on expanding its AI/autonomy-related portfolio. As we will see below, any major arms-producing company

today is integrating advanced automation and AI in its weapon systems.

The originally consumer-oriented tech companies that emerged in the 1990s and beyond, such as Alphabet/Google, Amazon, Meta and Microsoft, have become heavily invested in the military domain – partly through offering dedicated military cloud solutions[31], partly through co-operating with arms producers in the integration of their technologies into weapon systems.[32]

Almost forgotten is the time when substantive backlash reined in some of these companies' military ambitions, with Google ending its participation in Project Maven in 2018 as key example.[33] Currently, concerns regarding their involvement in war (including in Gaza) hardly lead to changes in their business strategy, with just a few exceptions, as we will see in the case study on Israel and tech giants. More recently, domestic deployment of surveillance tech by ICE[34] and other US law enforcement agencies has re-ignited discussions in the tech sector about its role in facilitating unlawful arrests, detention and deportation as well as suppression of dissent.[35]

Especially since the start of the second term of the Trump Administration, the biggest players in the sector appear to have fully embraced the military applications of their technologies now that their access to the presidency is closer than ever before and US government has now put AI front and centre of their policies.[36]

While short-lived, Elon Musk's role in the Administration in early 2025 was unprecedented, heading the Department of Government Efficiency (DOGE), which slashed some 29,000 government jobs and abolished USAID. But rather than cutting USD 1 trillion, as promised, it increased government spending.[37] At the same time Musk - the world's wealthiest person - through his company SpaceX, has huge financial interests in US (military) space policy.[38]

Also, the very prominent presence of the chiefs of Apple, Meta, Google, SpaceX and TikTok at Trump's inauguration is testament to how closely politics, media, tech and wealth have become intertwined.[39] For example, the eight richest people on the planet - all men - are connected to the world's biggest tech companies - all prominently featuring in this report because of their military relevance; their combined wealth reached a mind-boggling USD 2,213 billion by the end of April.[40] Moreover, the six richest have controlling stakes in key media companies - from Facebook, Instagram and TikTok to the Washington Post, X and YouTube.

In his outgoing address, President Biden warned that the US was becoming an oligarchy of tech billionaires wielding dangerous levels of power and influence over the nation[41] - in a very similar vein to President Eisenhower's warning about the military-industrial-complex in his 1961 farewell speech.[42]

RANK	NAME	NET WORTH	COMPANY	AGE
1	Elon Musk	$776.8B	Tesla, SpaceX	54
2	Larry Page	$286B	Google	53
3	Jeff Bezos	$270.5B	Amazon	62
4	Sergey Brin	$263.9B	Google	52
5	Mark Zuckerberg	$229.4B	Facebook	41
6	Larry Ellison	$207.3B	Oracle	81
7	Jensen Huang	$180.8B	Nvidia	63
8	Michael Dell	$173.4B	Dell Technologies	61

Forbes, 'The Real-Time Billionaires List', 30 April 2026, https://www. forbes.com/real-time-billionaires/)

While the US has always been leading ICT developments, China is rapidly narrowing the gap (see DeepSeek, TikTok).[43] With a top-down approach as often has been applied in other sectors too, the state "acts as cheerleader, financier, and protector".[44] These changing realities play an important role in US policy, both economic and military: "The United States is in a race to achieve global dominance in artificial intelligence (AI). Whoever has the largest AI ecosystem will set global AI standards and reap broad economic and military benefits".[45]

For a long time, US export policies towards China have been focused on ensuring that China gets as little access to US - and more broadly western - computing technology as possible. This is illustrated by recent interventions targeting Nvidia[46], as well as longstanding pressure on Dutch company ASML to ensure that China will not get access to their most advanced chip-producing machines.[47] The extent to which these efforts have been successful remains to be seen (see also Chapter 8 on China). It is at least illustrative that DeepSeek surprised Silicon Valley in 2025 with "a model that rivals ChatGPT but built with far less money and computing muscle".[48] At the same time, the US still broadly dominates global computing power, with an estimated three-quarters of global GPU (graphics processing units) cluster performance, with China in second place with 15 per cent.[49]

In that context should we read 'America's AI Action Plan', launched in July 2025 and titled "Winning the Race" and opening with these words from president Trump: "Today, a new

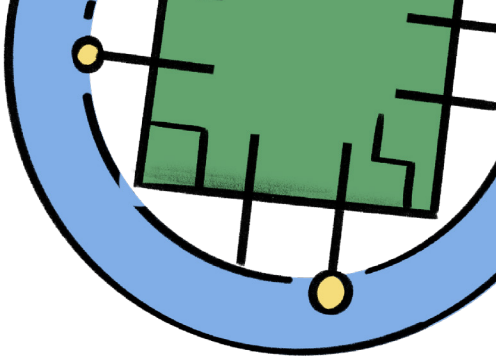
frontier of scientific discovery lies before us, defined by transformative technologies such as artificial intelligence… Breakthroughs in these fields have the potential to reshape the global balance of power, spark entirely new industries, and revolutionize the way we live and work. As our global competitors race to exploit these technologies, it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance. To secure our future, we must harness the full power of American innovation".[50] Or more bluntly, as US vice-president, JD Vance, said: "The AI future will not be won by hand-wringing about safety; it will be won by building".[51]

Running through this report is a single dynamic: a consumer-technology sector being drawn into warfighting just as the arms industry remakes itself around AI and autonomy - a convergence that raises pressing questions for human rights, the laws of war and democratic oversight.

1.3 New battlefield realities

Recent wars show how the militarisation of data-intensive technologies has become visible on the battlefield from Ukraine to Gaza. Just as so-called precision-guided missiles were a leap in military technology when the US attacked Iraq in 1991 after Saddam Hussain's invasion of Kuwait,[52] so to are the increasingly advanced and autonomous first-person-view (FPV) drones deployed by both Russia and Ukraine since 2022.[53] Likewise, Israel's use of algorithms (including so-called decision support systems) in its selection of Palestinian targets during the genocide in Gaza is testament to how quickly advances in AI have been applied to military purposes in ways difficult to imagine just a few years ago. Most recently, US attacks on Venezuela and Iran have shown how target selection and decision-making processes have fundamentally changed with the introduction of large language models (LLMs) and other algorithmic warfare tools, which have enabled the generation of unprecedentedly high numbers of potential targets in ever-shorter periods of time. In turn, Iran has made data centres in neighbouring Gulf states targets of their military actions, referring to the role of such infrastructure in warfare. It shows that "digital infrastructure is not only the backbone of our society, but that it also lies on the frontline of modern conflict".[54]

Fears that these developments spiral out of control and lead to consequences nobody can properly foresee have become very real in a short period of time. General Shanahan, former head of project Maven, who retired from the military in 2020 and is now a fellow at the Centre for a New American Security, a think tank, said the AI race he had helped start kept him up at night. "Governments must set clear boundaries before the technology outruns their control", he said. "There is a risk of an escalatory spiral where we're in danger of fielding untested, unsafe and unproven systems if we're not careful, because we each feel like the other side is hiding something from us".[55]



1.4 Arms control processes

These developments have made longstanding concerns regarding the automation of warfare ever more pressing. Already since 2013, an international group of NGO's, united in the Stop Killer Robots (SKR) coalition[56] has called on the international community to address such concerns by creating new legal frameworks that would ban some autonomous weapon systems (those targeting people and those lacking 'meaningful human control') and ensuring that all others would indeed be controlled meaningfully by humans (soldiers, law enforcement). More recently, concerns about so-called decision support systems have been added to discussions about legal frameworks setting boundaries on the level of human control required in a world where warfare is increasingly dominated by the automation processes that fundamentally change the way wars are being fought. The introduction of new technologies raises questions about international security, proliferation of technology, legality and ethics, and increasingly demands new rules to ensure that decisions over life and death are not taken by algorithms.

As Stop Killer Robots notes:

> "the growing influence of computer processing and algorithmic thinking increasingly shapes our interactions in the world and the outcomes available to us. There are clear threats to peace, justice, dignity, human rights, equality, responsibility and accountability, and respect for law. We are getting closer to machine processes determining whom to kill. […] The quest for greater speed through AI and automation - towards the goal of increasing the tempo of conflict to a point beyond human cognition in the pursuit of a military and strategic edge - is an extremely dangerous one for international peace and security. These risks are further to the impact 'AI in the military domain' is already having on civilian protection. Risks include unwanted escalation, lowered political thresholds to the use of force, and arms race dynamics. […] That AI systems inevitably encode and reproduce the biases of our societies - including racism, sexism and ableism - and that such bias cannot be eliminated, is also well established. The use of such systems to process people in the use of force will inevitably lead to disproportionate - and multiplied - impacts on already marginalised and minoritised people. Integrating automation and AI into decisions and actions in the use of force against people contributes to digital dehumanisation - the process where humans are reduced to data, which is then used to make decisions and/or take actions that negatively affects their lives."[57]

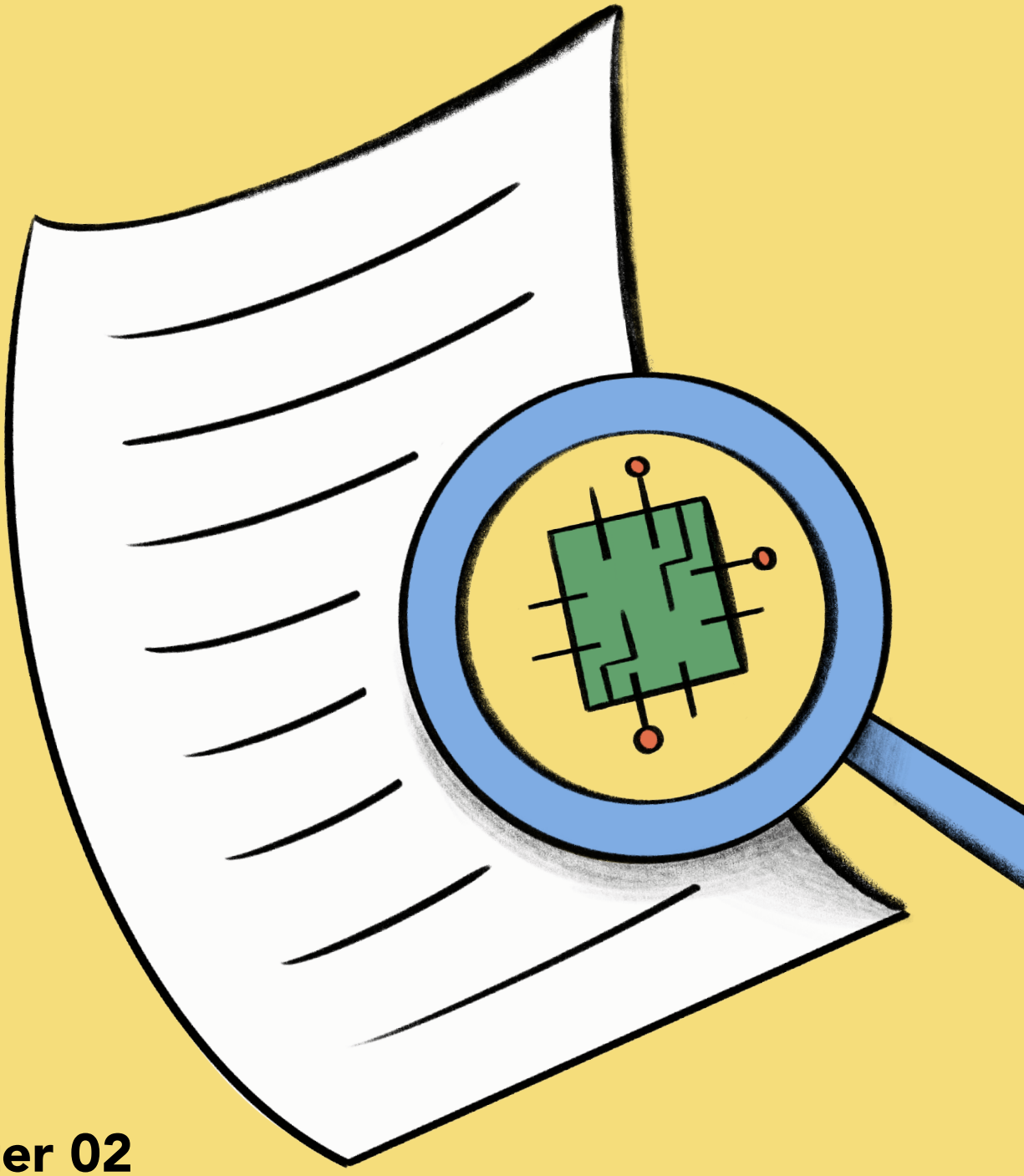
Putting this in a wider context, Jathan Sadowski, a scholar of automation technologies and research fellow at Monash University, sets out how companies are ultimately selling not just software but power. And whether it is Israel and the US today or another government tomorrow, some of these technologies amplify the exercise of power to such an extent that even their use by a country with a spotless human rights record would provide little reassurance. "Give them these technologies and see if they don't get tempted to use them in really evil and awful ways," he said. "These are not technologies that are just neutral intelligence systems, these are technologies that are ultimately about surveillance, analysis, and control."[58]

Many more in the tech sector and academia have long raised concerns about the weaponisation of AI, urging the UN to work towards regulations.[59] In 2018 for example, over 160 AI-related companies and organisations pledged to never develop, produce or use lethal autonomous weapon systems.[60] While the current geopolitical climate has clearly changed, these concerns are still valid and alive, even though some highly influential individuals may have changed their mind.[61]

Finally, the International Committee of the Red Cross, widely recognised as guardian of international humanitarian law, believes that "life-and-death decisions cannot be delegated to sensors and algorithms. States must ensure that the weapons they are developing and investing in comply with international humanitarian law".[62]

Since 2014, the United Nations Convention on Certain Conventional Weapons[63] (CCW) has hosted diplomatic discussions about "possible challenges posed by emerging technologies" in the area of "lethal autonomous weapons systems".[64] Since 2017, through a Group of Governmental Experts (GGE) that meets several days per year in Geneva, states have furthered this discussion with an eye to formulate "a set of elements of an instrument, without prejudging its nature" to set new norms around autonomous weapons.[65] By the end of 2026, States have the opportunity to decide to start working under a negotiating mandate.

In parallel to the discussions within the CCW, autonomous weapons and the use of AI in the military domain have also been discussed in other fora, thereby expanding the discussions also to non-CCW members. At the UN General Assembly in 2025, 156 states voted for a resolution calling on the CCW to complete the set of elements for an instrument being developed "with a view to future negotiations" (with 5 against and 8 abstaining).[66] UN Secretary-General Guterres has repeatedly called these weapons "politically unacceptable and morally repugnant" and has called for a ban on lethal autonomous weapon systems.[67] Meanwhile, in June 2026, for the first time, the UN will host informal discussions, which may eventually also lead to new rules and regulations on the broader theme of AI in the military domain, including for example decision support systems.[68]



Chapter 02

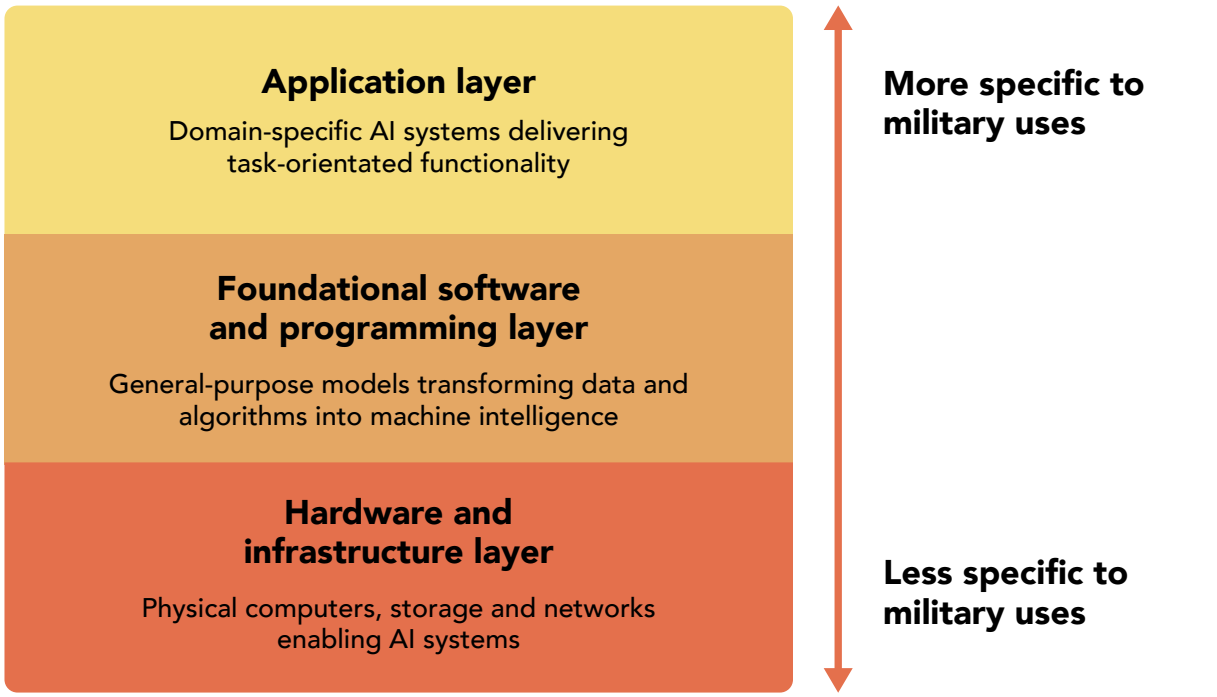
Methodology

2.1 Company selection
2.2 Report outline

2. Methodology

This report has been set up to scope the 'militarisation of tech', which refers to a range of connected processes that have blurred the lines between civilian, security and military uses of 'data-intensive technologies', which is a broader term than AI, as it also includes for example the necessary hardware and infrastructure required, from chips to data centres and the cloud.[69] Weaponisation then refers to the process of adapting or using technologies designed for civilian purposes to cause harm, to damage or disrupt objects or systems in conflict situations.

As SIPRI notes, the industry could be considered in the context of relationships between the products, services and actors involved in developing a military AI system, as they refer to as "the 'stack' - a term drawn from computer science referring to the layered ecosystem of software and hardware that enable applications of AI".[70] SIPRI distinguishes three layers:



Source: Alexander Blanchard, Vincent Boulanin and Laura Bruun, 'Mapping the military AI industry', SIPRI, 23 April 2026, https://www.sipri.org/commentary/topical-backgrounder/2026/mapping-military-ai-industry

Products and services in the lower two layers of the stack are usually general-purpose or dual-use and only become military-specific at the application level. Militaries then usually select and govern parts of a largely shared commercial stack for their specific military purposes. Tech companies can be involved in activities in more than one layer, where indeed the hardware and infrastructure production is less directly military specific than the application of AI in decision support systems. This is also reflected in the (length of the)

profiles of the companies. Arms producing companies involved in producing increasingly autonomous weapons integrate or connect data-intensive technologies to weapon systems; this would only apply to the upper layer.

For this report, we distinguish four main categories of companies:

- **Computing hardware producers**: AMD, Cisco, IBM and Nvidia
- **Tech Giants** (infrastructure, software and programming): Alphabet, Amazon, Meta, Microsoft, Oracle and SpaceX
- **Military-tech neo primes**: Anduril and Palantir
- **Prime arms producers** (with increasingly autonomous weapons): BAE Systems, General Dynamics, Lockheed Martin, Northrop Grumman and RTX

In the next chapters we investigate these largest companies in their category, which all have had significant contracts in the field of data-intensive technologies for military purposes. The tech company profiles outline military uses of their products and services and describe how these can have controversial applications. In the profiles of the five biggest arms-producing companies, we show how their work focuses on developing increasingly autonomous weapons, whether or not in partnership with the tech sector and the neo primes Anduril and Palantir, which themselves, as key amplifiers of AI-enabled warfare, deserve close attention.

2.1 Company selection

The selection of the companies profiled in this report has been made as follows:
For the computing hardware and Tech Giants companies, we selected all companies with a market cap (the total value of a company's outstanding shares of stock) of USD 250 billion or more in the 'Information Technology' and 'Communication Services' sectors plus Amazon (in the Consumer Discretionary sector) of the Standard & Poor (S&P) 500 by 30 December 2025.[71]

Secondly, based on open-source research, out of these companies we selected those with the most relevant military contracts, where relevant should be considered as delivering goods or services for specific military purposes, so that commercial laptop sales would not count as such and 'combat cloud' or military-specific LLMs would. Thus, Apple, Broadcom, Micron and Netflix were then deselected as we could not find (sufficient) military-relevant contracts for them. Not yet listed, but soon to be, is SpaceX, which is expected to go public this summer and has obvious military relevance.[72] This then resulted in the selection of the above-mentioned, all American, tech companies.

We chose to use the US-focused S&P 500 as a benchmark for a number of reasons: in terms of military relevance most public information is available from companies operating from NATO countries, by far most of them US companies. European tech companies simply do not (yet) play a major role, with only Germany's SAP and Dutch ASML passing the USD 250 billion threshold.[73] But SAP's military business is of a very different kind and magnitude compared to the tech giants.

S&P 500 companies in the Information Technology and Communication Services sectors + Amazon by market cap in USD billion (as of 30 December 2025)

Nvidia	4,574	Information Technology
Apple	4,045	Information Technology
Alphabet	3,794	Communication Services
Microsoft	3,620	Information Technology
Amazon	2,841	Consumer Discretionary
Broadcom	1,657	Information Technology
Meta	1,660	Communication Services
Oracle	561	Information Technology
Palantir	438	Information Technology
Netflix	430	Information Technology
AMD	351	Information Technology
Micron	331	Information Technology
Cisco	307	Information Technology
IBM	286	Information Technology

S&P 500 Market Capitalization", 30 December 2025, https://www.slickcharts.com/sp500/marketcap

ASML is Europe's largest tech company and the world's largest producer of advanced lithography equipment - the machines that make chips - and while leading the way in ever more powerful chips has clear security implications, ASML technology itself has no known direct military uses. Not underestimating the relevance of Chinese companies, there is very little concrete information about the extent to which the largest Chinese tech companies are involved in military applications of data-intensive technologies. For illustrative purposes the report has a brief chapter on China and Chinese companies. For the rest of Asia, Taiwan's TSMC is clearly one of the largest tech companies in the world, but mostly producing chips designed by and for other companies, such as Nvidia or AMD. Finally, South Korea's Samsung is probably the only non-American tech company with some military contracts but as it is the exception we did not include it.

Obviously, the high USD 250 billion threshold automatically excludes all start-ups. Especially in Israel and Ukraine there is a host of companies that make products very relevant to the focus of this report. A survey of the highly relevant start-up sector would however have been a study in itself. Significant is also that many tech giants are actively pursuing take-overs of the most promising start-ups, several examples of which we give throughout the report. Bottom line is that the tech companies described in this report lead the way and thus show key developments in the military use of data-intensive technologies by leading military powers, in particular the US and Israel.

For the arms industry, we selected the five largest companies from SIPRI's top 100 list of arms producing companies. Neo primes Anduril and Palantir were then chosen for their very specific role as major military tech start-ups, which have grown the size of the biggest legacy contractors in the military domain, while competing with tech giants. Moreover, there strong political positioning has made them exceptionally relevant. European military-tech start-ups such as German company Helsing would also fall in this category but was not included because of its significantly smaller size.

The SIPRI Top 100 arms-producing and military services companies in the world, 2024

Revenue figures are in millions of constant (2024) US dollars and rounded to the nearest $10 milllion

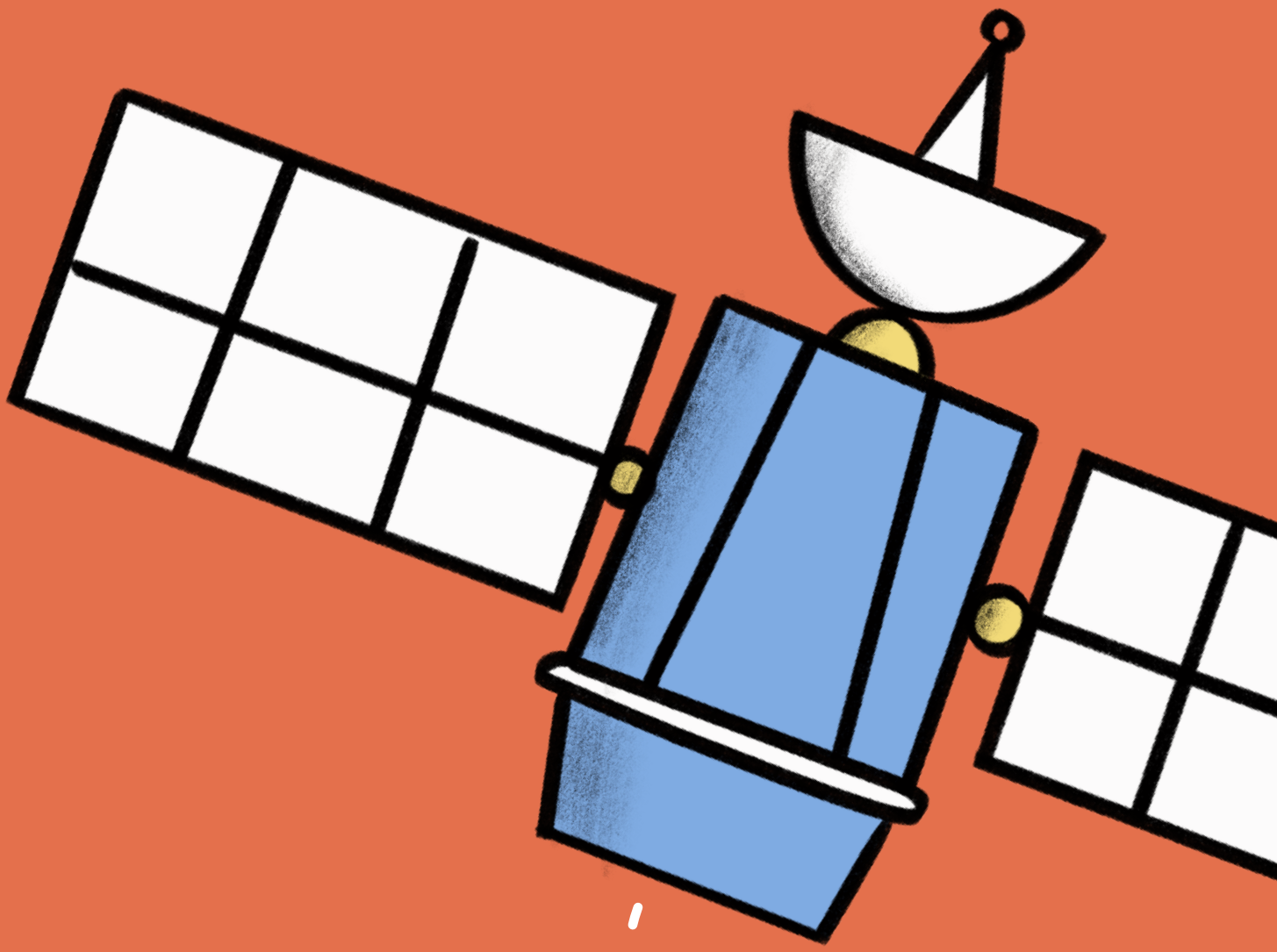
2024	2023	COMPANY	COUNTRY	ARMS REVENUE 2024	ARMS REVENUE 2023	CHANGE IN ARMS REVENUES 2023-24 (%)	TOTAL REVENUES 2024
1	1	Lockheed Martin Corp.	US	64 650	62 630	3.2	71 040
2	2	RTX	US	43 600	41870	4.1	80 740
3	3	Northrop Grumman Corp.	US	37 850	36 630	3.3	41 030
4	6	BAE Systems	UK	33 790	31 600	6.9	35 400
5	5	General Dynamics Corp.	US	33 630	31 100	8.1	47 720
6	4	Boeing	US	30 550	32 030	-4.6	66 520
7	7	Rostec	RUSSIA	27 120	21 450	26	38 890
8	9	AVIC	CHINA	20 320	20 590	-1.3	81 290
9	8	CETC	CHINA	18 920	21 110	120	55 230
10	11	L3Harris Technologies	US	16 210	15 200	6.6	21 330

Source: SIPRI, "The SIPRI Top 100 Arms-Producing And Military Services Companies, 2024", December 2025, https://www.sipri.org/sites/default/files/2025-11/fs_2512_top_100_2024.pdf

This approach clearly is not meant to be comprehensive and the company profiles are not exhaustive. The activities and contracts referred to serve as examples of relevant activities in the context of this report. The report rather aims to highlight significant developments within key companies worldwide taking part in the current militarisation of tech, where we have included developments until early May 2026. Also, it does not label companies as inherently 'bad', nor does it negatively label military uses of data-intensive technologies in general. At the same time, companies are highlighted with a reason, even as differences between them are also clear: there are obvious concerns with how data-intensive military technologies, as well as military applications of originally commercial technologies are now transforming warfare and vice versa. While most of the companies investigated in this report have ethical business policies, it is urgently important that they ensure that these policies are properly reflected in their actual businesses.

2.2 Report outline

The report is set up to look first into the computing hardware producers (Chapter 3), to be followed by Tech Giants (Chapter 4) and a chapter dedicated to Generative AI and LLMs in warfare (Chapter 5). Chapter 6 is a case study into Israel's use of data-intensive technologies, and the role of some of the tech giants. Chapter 7 is dedicated to military-tech neo primes Anduril and Palantir, to be followed by the five biggest arms producing companies (Chapter 8). Chapter 9 looks into developments in China, and Chapter 10 is the concluding chapter with recommendations.



Chapter 03

US computing hardware and infrastructure companies: military applications

3.1 AMD
3.2 Cisco
3.3 IBM
3.4 Nvidia

3. US computing hardware and infrastructure companies: military applications

Military production was long the natural domain of the arms industry, but in the digital era, the tech sector has become increasingly important.[74] In this chapter, we analyse recent developments around data-intensive technologies in the hardware part of the tech sector, where ever-more powerful chips are enabling ever more data-intensive uses required for technological progress in AI. We highlight: what military contracts have tech companies pursued in recent years? How do we see commercial tech being militarised? What are (potentially) problematic uses? What are the companies' ethical policies?

3.1 AMD

Advanced Micro Devices (AMD) was founded in 1969 as a Silicon Valley start-up "creating leading-edge semiconductor products" and has since grown into one of the leading companies in the sector.[75] It is "powering the next generation of supercomputing, high-performance computing, cloud, and AI".[76] Over 2024, AMD reported record revenue of USD 25.8 billion and a net income of USD 1.6 billion.[77] AMD's products find their way into military uses and nuclear weapons in the US, but also in Russian weapons.

Military applications

According to its website, AMD offers "the most dynamic processor technology in the industry"[78], including "defense-grade" integrated circuits "purpose-built" for military applications.[79] In 2023, US authorities increased restrictions for exports of (unspecified) AMD chips to some countries in Southwest Asia and North Africa (often referred to as Middle East). In September 2022, AMD said it had received new license requirements that would halt exports of its MI250 artificial-intelligence chips to China.[80] In the first year of Trump's current presidency new sanction measures have been imposed, of which some were later removed in return for its agreement to pay the US government 15 per cent of Chinese revenues.[81]

Nuclear applications

AMD has a history of collaborating on the US nuclear weapons programme via laboratories that are part of the National Nuclear Security Administration[82] (NNSA, part of the US Department of Energy or DoE), "responsible for enhancing national security through the military application of nuclear science. NNSA maintains and enhances the safety, security, and effectiveness of the U.S. nuclear weapons stockpile".[83]

Most recently, AMD, the DoE, Lawrence Livermore National Laboratory and HPE (Hewlett Packard Enterprise) designed El Capitan, currently the world's most powerful supercomputer at a cost of USD 600 million.[84] According to its designers, El Capitan - built on AMD's Instinct MI300A processing units - is designed for the most demanding HPC and AI/ML workloads[85] and helps the three NNSA weapons labs (Livermore, Los Alamos and Sandia) ensure the safety, security and reliability of the US nuclear stockpile without underground testing.[86]

Global footprint examples

Already in 2022, Reuters reported that AMD and Intel components, among others, had been found in Russian weapons used against Ukraine.[87] Russian customs data shared by Reuters showed that between 2 March and 31 May 2022 there were about 200 shipments of AMD components to Russia. AMD "said they had launched internal investigations after Reuters provided the customs data showing thousands of recent shipments of their products to Russia by third-party sellers".[88]

More recent Ukrainian research on captured or shot-down Russian weapons systems, Sukhoi Su-34 and Su-35S fighter aircraft in particular, has revealed contributions of numerous Western tech companies to those weapons, including goods from AMD, Broadcom and Intel - to name just a few - which "fall under enhanced customer due diligence in accordance with Common High Priority List (CHPL) developed by the United States in coalition with the EU, Japan, and the UK".[89]

In December 2025, American and Ukrainian law firms filed lawsuits against US companies Texas Instruments, AMD, Intel Corporation and Mouser for allegedly exporting "their guidance chips used by Russia to kill innocent civilians in Ukraine". The suits claim the companies "knew or had reason to know" that their components were being used in weapons.[90] A Ukrainian intelligence database with samples of AMD products found in Russian weapons shows 35 examples sourced from missiles, drones and military radios, among others.[91]

Ethical policies

AMD releases an extensive annual corporate responsibility report, where it outlines its commitment "to respecting human rights throughout our company and value chain, from raw minerals sourcing to product use. […] Our approach draws upon internationally recognized human rights standards, including the United Nations Guiding Principles on Business and Human Rights (UNGPs), the Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises and OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk

Areas".[92] Also, in 2023 AMD conducted its first "Human Rights Saliency Assessment", which identified "unintended use of our products" as one of two main assessment results, "similar to those of many technology companies".[93]

It does not, however, elaborate on what these unintended uses involved, but it seems likely that they relate to earlier mentioned uses in Russian weapons. While there is no explicit reference in the report to military use(r)s of its products (let alone its involvement in the US nuclear weapons programme), it seems well aware of potential adverse impacts of diversion of its products. AMD "enhanced downstream due diligence to mitigate adverse impacts to human rights where possible by establishing the AMD Anti-Diversion Committee, increasing distributor audits and strengthening relationships with NGOs."[94] Also, "new product launches, such as for AI products, stakeholder engagement and repeat saliency assessments" may trigger risk assessments.

Two pages in the ESG (Environmental, Social and Governance) report are dedicated to Responsible AI usage. According to the company, AI is a transformative technology that also raises new societal considerations and business risks, and AMD states it is committed to developing and deploying AI responsibly — maximising the benefits while mitigating risks to people, society, the environment and the company.[95]

Finally, "AMD joined the Business Roundtable on AI and Human Rights in 2024 to promote the development of responsible AI, using human rights as its underlying framework. As part of this collaboration, AMD engaged with peer companies to understand the risks due to the rise of generative AI and to mature responsible AI governance models".[96]

> Accountability, explainability, reliability and transparency are among the AMD responsible AI guiding principles – very much in line with requirements often mentioned at UN discussions on autonomous weapons. While avoiding specific mentioning of key concerns of misuse, either in the area of diversion of its products to unintended use(r)s, or via new AI technologies, let alone distinguishing between civil and military uses, AMD's human rights policy is one of the most advanced of the big US companies assessed for this report.

3.2 Cisco

Founded in 1984, Cisco is a US-based company designing internet infrastructure technologies, among others. It was a pioneer in local area network (LAN) technology to connect computers over a router system. The company went public in 1990 and had a market capitalisation of USD 555 billion in March 2000, surpassing Microsoft as the world's most valuable company.[97] Over 2025, Cisco had USD 57.7 billion revenues and USD 10.2 billion net income.[98]

Military applications

Cisco has a long history of supplying its equipment to military[99] and police customers, including to controversial destinations. Cisco's main military customer is the US Department of Defense (DoD).[100] One of its current areas of work is 'Military Installations for the Future', to "establish a reliable, resilient, and agile digital foundation for mission operations and force projection".[101]

Global footprint examples

In 2011, Chinese-origin Falun Gong sued the company, alleging its custom-built "Golden Shield" Internet technology had been used by China to track down devotees of the spiritual movement.[102] A Cisco presentation reviewed by news agency AP said its products could identify over 90 per cent of Falun Gong material on the web, while "other presentations reviewed by AP show that Cisco represented Falun Gong material as a "threat" and built out a national information system to track Falun Gong believers".[103] In 2011, the company's lawyer claimed that Cisco strictly abides by US export controls and doesn't supply any gear to China that is "customized in any way" to facilitate repressive uses".[104] The case is ongoing in 2026, the US Supreme Court agreed to hear an appeal by Cisco in which the tech company and the Trump administration are asking the justices to limit the reach of a federal law that has been used to hold corporations liable for human rights abuses committed abroad.[105]

According to the Wall Street Journal (WSJ) in 2011, Cisco had also been involved in a tender to build a surveillance system in the city of Chongqing, among the largest and most sophisticated video-surveillance projects of its kind at the time in China. Dubbed "Peaceful Chongqing" it would cover a half-million intersections, "over nearly 400 square miles, an area more than 25% larger than New York City".[106] Cisco was brought into the project by Chinese security company Hikvision, the project's main contractor. After the WSJ publication Cisco denied the report: "As a matter of policy, Cisco has not and will not sell video surveillance cameras or video surveillance management software in its public infrastructure projects in China. […] We were offered an opportunity to supply those products in Chongqing and, contrary to the suggestion in the article, declined that opportunity".[107] Contradicting that version is a Cisco news release from two years earlier, when it had signed an agreement with Chongqing municipality "to develop Smart+Connected Communities solutions" – linking those specifically to video surveillance software and cameras.[108]

Cisco has also been working for a few decades in Israel's cybersecurity sector and has "invested in research-and-development centers and acquired more than a dozen Israeli firms".[109]

Ethical policies

Cisco is committed to high standards of product quality and business integrity, and that legal and ethical compliance is everyone's responsibility, expected of both its suppliers and

its employees.[110] All focus appears to be on its suppliers, with a dedicated Cisco Supplier Ethics Policy available in no less than nine languages.[111]

Cisco does not appear to have a human rights policy applicable to its *customers*, while it claims that it "upholds and respects human rights as contained in the United Nations Universal Declaration of Human Rights […] and is committed to the UN Guiding Principles on Business and Human Rights", which do in fact apply to 'downstream' activities.[112]

In December 2024, concerned Cisco employees released an open letter to their bosses, among others saying that: "It goes against Cisco's stated beliefs and publicly available policies to support and enable actors in committing grave human rights violations or engaging partners that commit grave human rights violations. We urge you to reconsider Cisco's (i) engagement in and enablement of Israel's violations of international law and plausible genocide against Palestinians, and (ii) partnership with Bynet Data Communications Ltd., which is involved in the mass surveillance, oppression, and denial of freedom of movement of Palestinians throughout Occupied Palestine. In particular, we implore you to immediately terminate Cisco's 2023 partnership with the Israeli Occupation Forces (IOF) and Bynet Data Communications Ltd. for the provision of Webex".[113]

In March 2025, Cisco announced new "guardrails" restricting internal discussions and debates on the Middle East - and specifically on Palestine. "Some topics are just simply too hard, too painful, too divisive, and they take our focus away from our ability to drive Cisco business, and one example specifically would be the ongoing conflict in the Middle East," a Cisco executive said in a company-wide call. "We have made the decision that this topic cannot be discussed, cannot be debated in company or organization-wide meetings".[114]

3.3 IBM

IBM was founded in 1911. Since the 1990s, it has concentrated on cybersecurity, quantum, software and supercomputers. IBM sold its microcomputer division to Lenovo in 2005. IBM's inventions include the Automated Teller Machine (ATM), the floppy disk and the Deep Blue computer that made headline news defeating then-chess world champion Garry Kasparov. IBM revenues for the twelve months ending 30 September 2025 were USD 65.4 billion; net income amounted to USD 7.9 billion.[115]

Military applications

The Pentagon has long been IBM's most important federal customer.[116] In 2020 IBM, together with Amazon, Google, Microsoft and Oracle, won a contract to supply cloud services to the 17 organisations comprising the US intelligence community. The so-called Commercial Cloud Enterprise (C2E) contract vehicle had an undisclosed value, but documents issued by the CIA in 2019 indicated it could be worth "tens of billions" of dollars over 15 years.[117]

In 2022, Lockheed Martin, the world's largest arms producer, teamed with IBM subsidiary Red Hat "to tackle artificial intelligence and data-sharing challenges" faced by the US military "as it prepares to spread forces over greater distances and equip them with smaller, more mobile gear". According to a Lockheed Martin statement, "Red Hat Device Edge will enable Lockheed Martin to revolutionize artificial intelligence processing for our DOD customers' most challenging missions. […] The ability for small military platforms to handle large AI workloads will increase their capacity in the field, ensuring our military can stay ahead of evolving threats".[118] In 2025 they agreed another contract to work together on accelerating "the development of swarm autonomy technology" for drones.[119]

In 2023, the German Ministry of Defence selected a consortium with Helsing, IBM Deutschland and Rohde & Schwarz to deliver the AI backbone for the Future Combat Air System (FCAS), the long-troubled Franco-German "next-generation" combat aircraft programme. The AI software platform will be developed as part of the national Next Generation Weapon System (NGWS).[120]

Also in 2023, IBM revealed a new prototype neuromorphic microchip design called NorthPole ("modeled loosely on the human brain") which it said could pave the way for much smarter devices that don't rely on the cloud or the internet for their intelligence[121]. It was said to be "more than 20 times as fast as - and roughly 25 times as energy efficient as—any microchip currently on the market when it comes to artificial intelligence tasks"[122]. Possible applications for the new silicon chip include autonomous vehicles and robotics. "That could help soldiers who operate drones, ground robots, or augmented-reality gear against adversaries who can target electronic emissions".[123] IBM has been working on such neuromorphic chips for more than ten years, with at least USD 140 million funding from DARPA's SyNAPSE program.[124]

Illustrative of the close ties with the Pentagon is Radha Plumb, the former Pentagon Chief of Digital and Artificial Intelligence during the Biden administration, who joined IBM in July 2025 to lead its "Next-Generation Transformation Strategy".[125]

In 2025 IBM launched the "IBM Defense Model" developed with military media organisation Janes, "designed to bring trustworthy AI into secure environments where quick, accurate insights can influence real-world outcomes".[126] The platform is trained to understand military terminology, operational tactics, and mission-level strategies. The system is powered by IBM's Granite foundation models and operated through the company's AI studio, watsonx.ai. "Defence organizations need AI they can trust - solutions that deliver accurate insights without compromising security or ethics," said IBM's general manager for US federal technology. It aims to analyse and interpret "verified, up-to-date data, reducing the false or off-target responses common in many large language models".[127]

In 2025 IBM won a GBP 320 million contract from the UK's Defence Equipment Engineering Asset Management Systems (DEEAMS). "The new platform will use artificial intelligence (AI) to help ensure Armed Forces have the right equipment in the right place at the right time".[128] IBM is also leading work on the UK air force NEXUS combat cloud, "a sophisticated digital infrastructure and data platform engineered to deliver Decision Superiority to

warfighters across the air domain".[129]

Also in 2025 IBM, together with ten smaller companies, was also selected by the Defense Advanced Research Projects Agency (DARPA) to participate in the agency's Quantum Benchmarking Initiative (QBI), "which aims to rigorously verify and validate whether any quantum computing approach can achieve utility-scale operation … by the year 2033".[130] The work should help DARPA and the Pentagon "predict if quantum computing will grow from a primarily scientific endeavour to a critical industrial tool" that can be used by or against the US armed forces. Taken together, these contracts show IBM steadily building its cloud, AI, quantum and data-analysis capabilities into US and allied defence programmes.

Global footprint examples

IBM has operated in Israel since 1972. It has a training arrangement for discharged military personnel, especially from the elite Unit 8200 - IDF's Intelligence Corps responsible for clandestine operations, counterintelligence and cyberwarfare, amongst others - to get them to work in the Israeli cyber and high-tech industry.[131] It has two fully owned Israeli subsidiaries, IBM Israel and Red Hat Israel. The latter works extensively with the IDF, providing edge computing and software-based storage data centres to multiple units.[132] IBM has designed and operated "Eitan", the central database of Israel's Population, Immigration, and Borders Authority (PIBA) since 2019.[133] The database's main component is Israel's biometric population registry, which records personal data—including the ethnic and religious identities—of both citizens and non-citizens within Israel and the occupied Palestinian and Syrian territories.[134] Norwegian asset management company Storebrand divested approximately USD 139 million from IBM in March 2024, "based on the impact of its services contributing to enforcing what the United Nations assessed to be a regime of apartheid in the occupied Palestinian territories".[135]

The IDF Operational Cloud was developed in-house by the military's Center of Computing and Information Systems (MAMRAM) using IBM's OpenShift platform. The unit describes the Operational Cloud as "a weapon for all intents and purposes".[136] In December 2023, Red Hat hosted 100 students from the pre-military preparatory of the Israeli military's Computer and Cyber Defense School for a three-day technology hackathon on "Operation Swords of Iron", Israel's genocidal operation against Gaza since October 2023. [137]

In March 2024, IBM Israel hosted a conference for some 100 participants from the Israeli military, the tech industry and other organizations. The conference was held in cooperation with the military ICT and Cyber Defense Directorate and the Cyber Education Center, founded by the Israeli Ministry of Defense. Among the lecturers were the commander of the Israeli Military School of Computer and Cyber Defense and a software engineer at Microsoft.[138]

At least until 2015 IBM, whether or not through local contractors, had business relations with the Chinese military and police.[139] Also, according to The Intercept, the OpenPower Foundation, an American non-profit founded by Google and IBM, has set up a collaboration between IBM, Chinese company Semptian, and US chip manufacturer Xilinx to produce

microprocessors that enable computers to analyse vast amounts of data more efficiently. Shenzhen-based Semptian is using the devices to enhance the capabilities of internet surveillance and censorship technology it provides to human rights-abusing security agencies in China, according to Intercept sources and documents. A company employee said that its technology is being used to covertly monitor the internet activity of 200 million people.[140]

IBM's international sales of "safe city" technology involved the construction of surveillance networks[141] to combat crime in Davao under its then mayor and later Philippines president Rodrigo Duterte, currently on trial at the ICC "for the crime against humanity of murder in the context of the 'war on drugs' campaign".[142] In 2024, IBM was contracted to modernise the Egyptian Air Force's logistics system for USD 39 million until June 2029.[143]

Ethical policies

In 2025, responding to employees' concerns about IBM's ties to the IDF, CEO Arvind Krishna said: "We are a U.S. headquarter company. So, what does the U.S. federal government want to do on international relations? That helps guide a lot of what we do". At the same time Krishna claimed: "We will not work on offensive weapons programs […] Why? I am not taking any kind of moral or ethical judgment. I think that should be on each country who does those. The reason we don't is, we do not have the internal guardrails to decide whether the technology applies in a good way or unethical way for offensive weapons".[144]

As "IBM Human Rights Principles", the company says its corporate responsibility spans environmental and social concerns as well as respect for human rights, informed by the UN Guiding Principles on Business and Human Rights, the ILO Declaration on Fundamental Principles and Rights at Work, and the UN Universal Declaration of Human Rights.[145]

On AI, IBM claims that it "is advancing responsible AI through a multidisciplinary, multidimensional approach that integrates ethics into technology".[146] The IBM Responsible Technology Board's mission is "to provide governance, standards and practical application of principles for how IBM develops and deploys AI and emerging technologies like quantum computing".[147] "Its mission is to promote consistency, champion responsible practices, and advance trustworthy AI for IBM's clients, partners, and the broader global community."[148] It is unclear how these claims relate to some of the more controversial business deals outlined earlier.

3.4 Nvidia

Nvidia - from "invidia", Latin for "envy" - was founded in 1993 and originally focused on making graphics processing units (GPUs) for video gaming, but broadened their use into AI, professional visualisation and supercomputing. In January 2026, NVIDIA held an 85 per cent share of the global GPU market.[149] In 2025, amidst surging global demand for AI data centre hardware, Nvidia became the first company in the world to surpass USD 4 trillion (July) and

then USD 5 trillion (October) in market capitalisation.[150] In 2025 Nvidia had revenues of USD 130.5 billion and a net income of USD 72.9 billion.[151]

Military applications

Nvidia processors have been used in weapons ranging from F-22 fighter jets to US Army tanks for decades.[152] In 2010, a team led by Nvidia was awarded a research grant of USD 25 million by the Defense Advanced Research Projects Agency (DARPA), to address what the agency called a "crisis in computing".[153] The four-year research contract, aimed to develop GPU technologies required to build the new class of exascale supercomputers - 1,000-times more powerful than the fastest supercomputers at that time.

And in 2017, speaking at Nvidia's annual GPU conference, Lt. Gen. Jack Shanahan, the Pentagon's "director for defense for warfighter support", and in charge of Project Maven at the time, declared: "let the machines do what machines do well, and let humans do what only humans can do".[154] "The world has changed, we're in a data-driven environment," he said. "More people are not the answer; better tools are the answer".[155]

Opportunities of Nvidia's AI chips for military applications, in particular increasingly autonomous weapons, have long been recognised. In 2012 Nvidia was awarded a contract worth up to USD 20 million from DARPA "to research embedded processor technologies that could lead to dramatic improvements in the ability of autonomous vehicles to collect and process data from on-board sensors".[156] Journalist David Hambling noted a few years later: "Small UAS [uncrewed aerial systems - FS] are also becoming steadily more independent of both human operators and GPS guidance. Swarming drones are necessarily fairly autonomous, and the latest consumer drones can automatically avoid obstacles, plot routes and follow people or vehicles. These capabilities are largely thanks to the Jetson system-on-a-chip supplied by Nvidia, effectively a miniature supercomputer with deep learning baked in. This technology can be modified to provide target recognition and precise aiming".[157]

Drone producer Skydio for example has long used Nvidia products to foster the capabilities of its drones.[158] Similarly, Belgian startup MAHI, which develops AI automation systems for uncrewed sea-surface vessels, depends on Nvidia GPUs, and calls them the only item they cannot replace by an alternative.[159] Five years later, the same journalist noted that Russian-made Lancet-3 loitering munitions have been found with the Jetson TX2 as well, underscoring the relative ease with which these chips have long been possible to acquire, for example through webshops, even by sanctioned countries.[160] Nvidia Jetsons have also been reportedly found in Russian Albatros M5 drones.[161] In 2021, Nvidia called cooperation with Lockheed Martin, specifically in the area of "AI-guided predictive maintenance" a "success story".[162]

In 2022 Nvidia envisioned a more holistic approach of tackling military challenges, claiming that the Department of Defense should not merely make existing capabilities faster but reinvent itself around data-driven technologies, treating data as a strategic asset that gains value as it is collected and connected.[163]

In 2025, arms company Northrop Grumman announced its adoption of Nvidia RTX PRO Servers "to deploy AI, design and simulation applications across the organization", adding to its existing access to Nvidia's extensive portfolio of (generative) AI software, its platforms and frameworks, including Nvidia Omniverse. "NVIDIA's AI platforms will help us deliver Northrop Grumman's advanced capabilities to our customers faster and with greater effect," said Northrop Grumman.[164] Also in 2025, Nvidia bought Groq, which makes AI hardware and software for applications including military autonomous systems.[165] The USD 20 billion deal is Nvidia's largest to date.[166]

A recent example of Nvidia technology powering advanced weapons is the Switchblade 400 loitering munition produced by American company AV (previously AeroVironment). This latest variant in the Switchblade family is offered to the US Army as part of its Low Altitude Stalking and Strike Ordnance (LASSO) programme. "It has an NVIDIA-based processor that will support automatic target recognition and aided target recognition".[167]

In October 2025, Nvidia announced a collaboration with Palantir "to build a first-of-its-kind integrated technology stack for operational AI — including analytics capabilities, reference workflows, automation features and customizable, specialized AI agents — to accelerate and optimize complex enterprise and government systems".[168] According to Nvidia CEO Huang: "Palantir and NVIDIA share a vision: to put AI into action, turning enterprise data into decision intelligence".[169] Or, as Palantir CEO Alex Karp put it: "Palantir is focused on deploying AI that delivers immediate, asymmetric value to our customers. We are proud to partner with NVIDIA to fuse our AI-driven decision intelligence systems with the world's most advanced AI infrastructure".[170]

Global footprint examples

Nvidia is one of the largest tech employers in Israel since its 2019-20 take-over of local tech company Mellanox for USD 6.9 billion. At the time Nvidia stated that it "intends to continue investing in local excellence and talent in Israel, one of the world's most important technology centers" – in fact its biggest outside the US.[171] In 2024, Nvidia completed its USD 700 million acquisition of Run:ai, an Israeli startup that helps manage and optimize AI hardware infrastructure.[172] In 2025 it announced plans to triple the size of its R&D lab in Beersheba (where arms producers Rafael and Elbit Systems have their R&D sites too) and hire hundreds of additional Israeli staff.[173]

"If you collaborate with these kinds of Israeli companies, you can assume that the knowledge will eventually be used in the war", says Israeli computer scientist Sebastian Ben Daniel.[174] Elbit Systems for example, Israel's largest arms manufacturer, is buying Nvidia products. Elbit is developing an "autonomous" attack drone called Lanius that can operate both alone and in swarms, scan its surroundings and distinguish friend from foe. The drone's AI systems are driven by a Nvidia Jetson TX2 CPU.[175] Elbit also opened a new robotics lab in 2024, partnering with Nvidia and Dell, amongst others.[176] Showing its military relevance, Nati Amsterdam, country director at Nvidia Israel, spoke at the DefenseTech Summit in Tel Aviv in December 2024.[177]

Beyond Israel, back in 2010, China surprised the world by fielding, for the first time, the world's fastest supercomputer. The Tianhe-1A was developed at the National Supercomputing Center of Tianjin, part of the National Defense Science and Technology University, and consisted among others of 7,168 Nvidia Tesla M2050 general purpose GPUs.[178] Again in 2025, DeepSeek was the surprising Chinese rival of ChatGPT and other Western Large Language Models (LLMs). DeepSeek says it uses Nvidia H800 chips, a less powerful chip designed to comply with US export restrictions, but US authorities are investigating whether it may have had access to restricted Nvidia chips through indirect channels.[179]

In September 2025, AP reported that Nvidia staff "collaborated with Chinese police researchers and companies on surveillance technology. Nvidia said in a post dating to 2013 or later that a Chinese police institute used its chips for surveillance technology research. Nvidia said it doesn't currently work with Chinese police but did not address the past".[180]

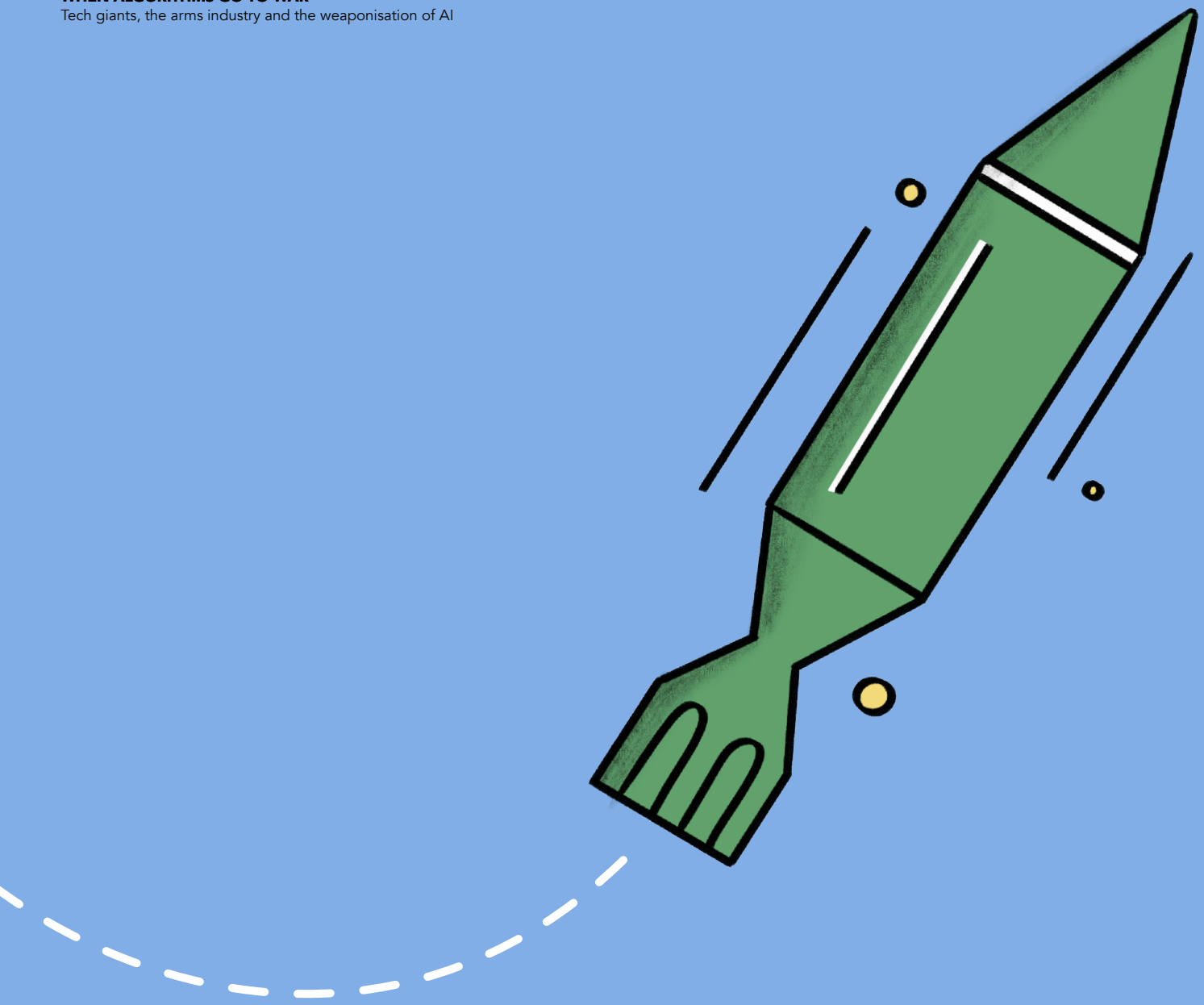
Successive US governments have tried to limit Nvidia's exports, claiming that American technology was feeding China's efforts to develop advanced weapons and surveillance networks that police its citizens.[181] In 2023, US authorities increased restrictions on exports of Nvidia's A100 and H100 chips designed to speed up machine-learning tasks, beyond China, especially to some countries in SWANA.[182] Already in 2022, US officials had informed the company that controls would "address the risk that products may be used in, or diverted to, a 'military end use' or 'military end user' in China".[183]

Under governmental pressure Nvidia has offered a less capable variant of its A100 and H100 chips to China, the A800 and H800.[184] After also those chips came under export control in 2025, president Trump and Nvidia CEO Huang eventually struck a deal that lifted the licencing requirements and made Nvidia return 15 per cent of its Chinese revenues to the US government,[185] or even 25 per cent in the case of the more advanced H200 exports (H200 chips are just one generation from the currently most advanced, the Blackwell chip).[186] New developments in this area will continue to emerge.

Nvidia believes the US sanctions have been useless if not counterproductive: CEO Huang has said that policies meant to prevent China's access to key technologies were "always questionable, and now it's clearly wrong. […] Shielding Chinese chipmakers from U.S. competition only strengthens them abroad and weakens America's position".[187] Remarkably, his colleague at Anthropic (see Chapter 6 on Gen AI), Dario Amodei, strongly disagrees. In January 2026, at the World Economic Forum (WEF), Anthropic boss Amodei criticised the deal to allow H200 chip exports to China, saying it has "incredible national security implications. […] We are many years ahead of China in terms of our ability to make chips. … It would be a big mistake to ship these chips […] I think this is crazy. It's a bit like selling nuclear weapons to North Korea."[188] (see also Chapter 8 on China)

Ethical policies

Similar to many other companies' human rights policies, Nvidia commits to respecting internationally recognised human rights and frames its approach around the UN Guiding Principles on Business and Human Rights and the UN Global Compact. It says it conducts risk-based due diligence across its value chain and has identified five salient risk areas: responsible minerals sourcing; working conditions in the supply chain; a clean, healthy and sustainable environment; responsible product development; and responsible product use.[189] On AI, Nvidia says: "We believe AI should respect privacy and data protection regulations, operate in a secure and safe way, function in a transparent and accountable manner, and avoid unwanted biases and discrimination".[190] Among its guiding principles are privacy, safety and security, transparency and non-discrimination.
Claiming its "AI technologies are leading the charge for global good" is meaningless when Nvidia AI chips dominate the market so strongly, including for uses where civilian harm is likely. Nvidia should elaborate its human rights due diligence and make clear how it ensures that its customers do not use their products in a way that would violate the UN Guiding Principles on Business and Human Rights.



Chapter 04

US tech giants: embracing the military

4. US tech giants: embracing the military

In this chapter we analyse recent developments around data-intensive technologies among the biggest companies in the tech sector. These developments are especially relevant where they may contribute to automated warfare. While certain technologies may well ensure sufficient human control over their use, it is often unclear what this entails and how this is ensured.

Companies working on these technologies need to have clear policies that make explicit how and where they draw the line regarding the military application of their technologies to ensure they do not contribute to violations of international human rights law (IHRL) and international humanitarian law (IHL). What military contracts have tech companies pursued in recent years? How do we see commercial tech being militarised? What are (potentially) problematic uses? What are their ethical policies?

4.1 Alphabet (Google)

Better known through its Google companies, Alphabet was created in 2015 as the parent holding company of Google and its former subsidiaries. It is currently the world's number three company in terms of market cap.[191] It had USD 350 billion in revenues and USD 100 billion net income in 2024.[192] Main business areas include information technology, online advertising, search engine technology, email, cloud computing, software, quantum computing, e-commerce, consumer electronics, and artificial intelligence.[193] Back in 2018 CEO Sundar Pichai said that "We have learned to harness fire for the benefits of humanity, but we had to overcome its downsides too. So my point is, AI is really important, but we have to be concerned about it".[194]

Military applications

Pichai made the above remarks in the context of major backlash due to Google's role in the Pentagon's Project Maven (see also Chapter 6 on Palantir and Anduril), its subsequent withdrawal and the promise to stay away from weapon projects and technologies that may injure people. That obviously did not entail a complete withdrawal from military projects if they wouldn't violate these principles. To better position itself in that market Google hired Josh Marcuse, executive director of the Pentagon's Defense Innovation Board, in 2020, to become Google's "head of strategy and innovation for global public sector".[195] In the CBP border-surveillance tower upgrade in Arizona (see Section 3.3 on IBM), Google plays a critical role by operating a central database for video surveillance data that brings together all those services.

Against this backdrop, Google, together with Amazon, Microsoft and Oracle, won the Pentagon's USD 9 billion Joint Warfighting Cloud Capability (JWCC) contract in 2022.[196]

Storage and processing of information is used "at all classification levels, from headquarters to the tactical edge"; stated capabilities include global accessibility, resilient services, advanced data analytics, fortified security and tactical edge devices.[197] The Pentagon at the time said the technology is expected to support the military in combat.[198] This includes for example warfighting cloud services to US Special Forces.[199] Furthermore, in 2020 Google, together with Amazon, IBM, Microsoft and Oracle, won another contract to supply cloud services to the 17 organisations comprising the US intelligence community–the so-called Commercial Cloud Enterprise (C2E) contract vehicle; for its scale and reported value, see Section 3.3 on IBM.

A Google spokesperson at the time said in a statement: "We remain committed to serving public sector organizations of all sizes, and this award builds on recent federal momentum for Google Cloud with NOAA, the U.S. Department of Energy, Defense Innovation Unit, U.S. Navy, U.S. Patent and Trademark Office, U.S. Small Business Administration, and more."[200]

In late 2025 the Pentagon launched a major push to get military personnel, civilian employees and contractors to use generative AI capabilities through the GenAI.mil website set up by Google Cloud's Gemini for Government. On the occasion, Secretary of War[201] Pete Hegseth said in a social media post: "The future of American warfare is here, and it's spelled AI […] This platform [GenAI.mil] puts the world's most powerful frontier AI models, starting with Google Gemini, directly into the hands of every American warrior".[202] Gemini for Government will use AI processes where autonomous programming makes decisions and takes actions with minimal human involvement and will allow staff to experiment. "There is no prize for second place in the global race for AI dominance," the Under Secretary of Defense for Research and Engineering said in a statement. "We are moving rapidly to deploy powerful AI capabilities like Gemini for Government directly to our workforce"[203] (see also Chapter 5 on GenAI).

Global footprint examples

On Google's partnerships with the Israeli government and military, especially in connection to the ongoing atrocities against Gaza, see Chapter 6. Besides, Google announced in March 2025 that it was paying no less than USD 32 billion - the largest cybersecurity deal in history - for the acquisition of the American-Israeli cloud security company Wiz to join Google Cloud. Its security services would still be available across other cloud platforms, including Amazon Web Services, Microsoft Azure, and Oracle Cloud. The co-founders of Wiz - Yinon Costica, Assaf Rappaport, Ami Luttwak, and Roy Reznik—are all veterans of Unit 8200.[204]

Ethical policies

Google long used "Don't be evil" as their company motto, and it used to be the topline of its Code of Conduct.[205] After withdrawing from Project Maven in 2018, Google published ethical AI principles, which stated that Google will not design or deploy AI in "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people".[206] What that exactly would entail beyond window dressing was

open to debate from the start and concerns were justified with Google's bidding for the JWCC cloud contract a few years later.[207] Previously, in 2018, Google had quit the bidding for JWCC's failed predecessor called JEDI exactly because it "couldn't be sure" the combat cloud would align with the company's AI principles.[208]

But in 2021, these principles proved to be much more flexible, as a Google spokesperson explained they only "apply to custom AI work, not general use of Google Cloud services… It means that our technology can be used fairly broadly by the military".[209] In 2024, protest came from Google's AI division DeepMind where nearly 200 workers signed a letter calling on the tech giant to drop its contracts with military organisations.[210] But in early 2025 – at the beginning of Trump's second term and well into controversy around its ties to Israel's military - Google rewrote its ethical policy, including the remarkable removal of its pledge not to design or deploy AI in weapons or other harmful technologies.[211]

In a blog post co-authored by Google DeepMind CEO and co-founder Demis Hassabis the removal, which was not addressed specifically, was explained as follows:

> "There's a global competition taking place for AI leadership within an increasingly complex geopolitical landscape. We believe democracies should lead in AI development, guided by core values like freedom, equality, and respect for human rights. And we believe that companies, governments, and organizations sharing these values should work together to create AI that protects people, promotes global growth, and supports national security."[212]

Thus, today Google says being "bold" on AI also means being responsible from the start; Google notes it was among the first to publish AI principles, in 2018, has issued an annual transparency report since 2019, and regularly reviews and updates its policies and frameworks.[213] Google also highlights that they "pursue AI responsibly throughout the AI development and deployment lifecycle, from design to testing to deployment to iteration, learning as AI advances and uses evolve". They further list: appropriate human oversight and due diligence, and feedback mechanisms; investing in safety and security research; testing and monitoring for harmful or biased outcomes, as well as "promoting privacy and security, and respecting intellectual property rights".[214]

While much of that appears like language used in UN discussions, including the reference to international law, many questions remain: what is appropriate oversight, how do you implement due diligence, etc. Despite the rhetoric, Google has clearly opened the door to applying its products to military uses, including in warfare. And so the controversy continues, also within Google. In April 2026, more than 600 employees had signed a letter to CEO Pichai demanding that he bar the Pentagon from using Google's artificial intelligence for classified work. "We want to see AI benefit humanity; not to see it being

used in inhumane or extremely harmful ways. This includes lethal autonomous weapons and mass surveillance but extends beyond […] The only way to guarantee that Google does not become associated with such harms is to reject any classified workloads", they wrote.[215]

Data protection policies

Google maintains a layered privacy framework. For consumer and general users, the relevant instrument is the Google Privacy Policy, currently effective 2 April 2026.[216] The policy covers Google services including Search, YouTube, Gmail, Maps, Android, Chrome and products integrated into third-party apps and sites. It describes the information Google collects, the purposes for which it uses that information and the controls available to users.[217] The current policy also states that Google may use information that is publicly available online or from other public sources to help train Google's AI models and build products and features including Google Translate, Gemini Apps and Cloud AI capabilities.[218]

Google's enterprise and government cloud services are addressed through a separate Google Cloud Privacy Notice, currently effective 8 April 2026.[219] That notice applies to Service Data, which is personal information Google collects or generates in the provision, administration and technical support of Google Cloud services. It expressly does not apply to Customer Data or Partner Data, which are governed by the customer's agreements and the relevant Google Cloud Data Processing Addenda.[220] This distinction matters in military and government contexts because data uploaded, stored, analysed or otherwise processed by a government customer inside Google Cloud is not governed by the consumer Privacy Policy and falls outside the scope of the Google Cloud Privacy Notice.

Google has also received authorisations for cloud environments designed for classified US government workloads. In May 2025, Google announced that Google Distributed Cloud and its air-gapped appliance had achieved US Department of Defense Impact Level 6 authorisation, enabling Department of Defense customers to use those environments for Secret classified data and applications.[221]

Based on the above, Google's published privacy notices draw a boundary between Google-controlled service data and customer-controlled content. While this report has documented Google Cloud's availability to defence and government customers, including through the Pentagon's Joint Warfighting Cloud Capability contract and Project Nimbus,[222] where a military or government customer processes personal data through Google Cloud, the public-facing privacy notices reviewed here do not appear to provide affected individuals with a direct account of how that customer uses the data, what military safeguards apply or what practical route of redress exists.

Google states in its enterprise privacy commitments that it does not use customer data to create advertising profiles or improve Google Ads products, and that it does not sell customer data or service data to third parties.[223] For enterprise Workspace customers using Gemini, Google also says customer content is not reviewed by humans or used for Gemini model training outside the customer's domain without permission.[224] Although those are

material safeguards, they are framed around Google's role as cloud provider and the customer's contractual controls, rather than as a dedicated public data-protection policy for military uses of Google infrastructure or for individuals whose data may be processed by state customers.

4.2 Amazon

Founded in 1994 by Jeff Bezos, Amazon originally started as an online marketplace for books, to become today's multinational technology company engaged in e-commerce, multi-media, cloud computing, satellite internet, digital streaming and artificial intelligence, amongst others. Its 2024 revenues amounted to USD 638 billion, with net income of 59 billion.[225]

Military applications

Already in 2018, it was reported that its cloud business, Amazon Web Services or AWS, had generated USD 600 million in classified work with the Central Intelligence Agency (CIA) since 2014.[226] More generally, US military and security services have been long-time customers. "In 2011, AWS GovCloud (US-West) launched, making AWS the first cloud provider to build cloud infrastructure designed to meet U.S. government security and compliance needs. In 2014, AWS launched its first Top Secret Region, AWS Top Secret-East, which was the first air-gapped commercial cloud accredited to support classified workloads". In 2017, "AWS became the first cloud provider accredited to support government workloads across the full range of U.S. government data classifications, including Unclassified, Secret, and Top Secret. In 2021, AWS announced its second Top Secret Region—AWS Top Secret-West".[227]

AWS launched a promotional video in 2018 titled 'Amazon Web Services for the Warfighter',[228] showcasing how its cloud infrastructure supports military operations using real time data, secure communications networks and enhanced levels of situational awareness for troops on the ground. It illustrates how commercial cloud technologies have been irreversibly intertwined with military systems.

In 2020 Amazon, together with Google, IBM, Microsoft and Oracle, won a contract to supply cloud services to the 17 organisations comprising the US intelligence community–the Commercial Cloud Enterprise (C2E) contract vehicle; for its scale and reported value, see under IBM above.[229] "We are honored to continue to support the intelligence community as they expand their transformational use of cloud computing. Together, we're building

innovative solutions across all classification levels that deliver operational excellence and allow for missions to be performed faster and more securely," an AWS spokesperson said at the time.[230]

AWS, together with Google, Microsoft and Oracle, won the Pentagon's USD 9 billion Joint Warfighting Cloud Capability (JWCC) contract in 2022.[231] For the JWCC's stated capabilities and its intended use in combat, see under Section 4.1 on Google above. Also in 2022, the National Security Agency (NSA) re-awarded a once-secret cloud computing contract - codenamed "Wild and Stormy" - worth up to USD 10 billion to AWS after an unsuccessful protest by Microsoft.[232] Then finally in 2022, the AWS *Wickr ATAK Plugin* was launched to improve secure communications. "While ATAK was initially designed for use in combat zones, the technology has been adapted to fit the missions of local, state, and federal agencies".[233] In 2022 ATAK had over 400,000 US DoD operators.

In late 2025, RTX, one of the world's largest arms producers, announced a strategic collaboration with AWS to "integrate mission engineering and data collection capabilities with cloud services to support decision-making [and] operational coordination". The collaboration incorporates advanced AI and ML services from AWS, including Amazon SageMaker and Amazon Bedrock.[234]

AWS subsidiary Rekognition provides computer vision technologies - pre-trained-algorithms and algorithms that a user can train on a custom dataset, including facial recognition. Its customers include law enforcement services including the FBI and the US Immigration and Customs Enforcement (ICE), the agency synonymous with tracking down US residents alleged to be in the country illegally.[235] While it has been demonstrated to military users, it is not known whether and to what extent the US military utilises Rekognition.[236] On Amazon's contracts with the Israeli government and military forces in connection to the ongoing atrocities in Gaza, see Chapter 6.

Ethical policies

Amazon has a rather generally worded Code of Business Conduct and Ethics, which does not refer to military applications of its products and services in particular.[237] AWS is stressing 'responsible AI': Amazon frames its responsible-AI approach as practical and scalable, taking a people-centred approach and applying best practices, built-in safeguards and tooling across the AI lifecycle.[238] It refers to "appropriately obtaining, using, and protecting data," and "preventing harmful system output and misuse."[239] It recently added a "Well-Architected Responsible AI lens".[240]

Founder and largest shareholder Jeff Bezos has always been a supporter of US military uses of its technology. Reacting to Google's decision in 2018 not to bid for the Pentagon's JEDI cloud contract, Bezos, Amazon's chief executive, said: "If big tech companies are going to turn their back on the U.S. Department of Defense, this country is going to be in trouble".[241] A year later he said: "People are entitled to their opinions, but it's the job of a senior leadership team to say no. […] Do you want a strong national defense or don't you? I think

you do … and we have to support that".[242]

Months earlier, workers from Amazon wrote a letter to Bezos stating: "In the face of this immoral US policy, and the US's increasingly inhumane treatment of refugees and immigrants […], we are deeply concerned that Amazon is implicated, providing infrastructure and services", including to Palantir, for use by the Department of Homeland Security (DHS, including ICE).[243] The American Civil Liberties Union (ACLU) called on Amazon to stop providing its facial surveillance technology, Rekognition, to governments and law enforcement.[244] In June 2020, Amazon announced a one-year moratorium on police use of Rekognition, in response to the Black Lives Matter protests. Initially put in place for a year, Amazon extended the moratorium in May 2021 without explanation, but that apparently did not include FBI use.[245]

Today, on its government services webpage AWS states that it remains committed to helping defence and national-security customers mission success. They add: "By removing the undifferentiated heavy lifting of the underlying IT infrastructure, U.S. defense and national security leaders can focus on what's most important—protecting the country and its people".[246] Amazon does not appear to have guardrails in the context of the military uses of its products and services and how these may contribute to human suffering.

Data protection policies

Amazon Web Services uses different privacy and contractual instruments for different categories of data. The AWS Privacy Notice governs personal information AWS collects about AWS website visitors, account holders and customers in the course of providing and administering AWS offerings.[247] The notice states that it does not apply to "the 'content' processed, stored, or hosted by our customers using AWS Offerings in connection with an AWS account".[248]

Customer content is instead addressed through AWS customer contracts, service terms, data-processing terms and security documentation. AWS states that customers maintain control of the content they upload to AWS services and remain responsible for configuring access to AWS services and resources.[249] AWS also describes its cloud-security model as a shared responsibility model: AWS is responsible for security of the cloud, while customers are responsible for security in the cloud, including the way they configure and use services.[250]

AWS offers specialised government and classified cloud environments, including AWS GovCloud and AWS Secret and Top Secret regions for US government customers.[251] If a military or intelligence customer processes personal data inside AWS infrastructure, that customer content is not governed by the AWS Privacy Notice, but by the relevant customer agreement, service terms, data-processing terms, security obligations and the customer's own legal basis for processing. This identifies the limited scope of AWS's public-facing privacy notice when cloud infrastructure is used in a military or intelligence context.
AWS also states that it will not disclose customer content unless required to comply with the law or a valid and binding order of a governmental body, and that it will attempt to redirect

governmental demands to the customer and notify the customer before disclosure where legally permitted.[252] While those might be meaningful commitments for AWS customers, they do not amount to a dedicated public data-protection framework for third parties whose personal data may be processed by a military or intelligence customer using AWS infrastructure.

4.3 Meta

Established in 2004 as Facebook, the American multinational technology company was re-branded Meta in 2022 and operates social media platforms and communication services, including Facebook, Instagram, WhatsApp and Messenger. The company also operates an advertising network for its own sites and third parties, which accounts for almost all its revenue. As of 2022, it was the world's third-largest spender on research and development (after Amazon and Alphabet), with R&D expenses totalling USD 35.3 billion.[253] Meta donated USD 1 million to Trump's inaugural fund for his second term, in a departure from past practice.[254] 2025 total revenues amounted to USD 201 billion and net income USD 60.5 billion.[255]

Military applications

Given the young age of Meta, and its early focus on social media, it has little history in military business; most of it is of very recent date compared to other companies discussed here. Meta's LLM, Llama, used to have a provision in its terms of service that prohibited military uses, but on 4 November 2024, one day before Trump's re-election, the company made a U-turn: "Responsible uses of open source AI models promote global security and help establish the U.S. in the global race for AI leadership".[256] Its announcement indicated collaboration with military contractors including Accenture, Anduril, Booz Allen, Leidos, Lockheed Martin, Palantir, Scale AI and Snowflake, which would "bring Llama to government agencies".

The next day, Scale AI, a machine learning startup focusing on military applications, used similar language to announce: "Defense Llama, the Large Language Model (LLM) built on Meta's Llama 3 that is specifically customized and fine-tuned to support American national security missions. Defense Llama, available exclusively in controlled U.S. government environments within Scale Donovan, empowers our service members and national security professionals to apply the power of generative AI to their unique use cases, such as planning military or intelligence operations and understanding adversary vulnerabilities."[257]
Scale AI furthermore said: "Defense Llama was trained on a vast dataset, including military doctrine, international humanitarian law, and relevant policies designed to align with the Department of Defense (DoD) guidelines for armed conflict as well as the DoD's Ethical Principles for Artificial Intelligence."[258] Experts however pointed out the uselessness, if not irresponsibility, shown by Defense Llama's advertised output.[259]
In a 2023 interview with the Washington Post, co-founder and CEO Alexandr Wang, a vocal proponent of weaponised AI, described himself as a "China-hawk" and said he hoped Scale

AI could "be the company that helps ensure that the United States maintains this leadership position."[260] Scale AI's embrace of military applications and a host of Pentagon contracts have attracted numerous high-end investors, including Peter Thiel's Founders Fund, Nvidia, Amazon and Meta.[261] In a deal that Meta hopes will add muscle to its AI division,[262] it acquired a 49 per cent stake in Scale AI in June 2025 for USD 14.3 billion, bringing in Wang and several other Scale executives to run Meta Superintelligence Labs (MSL).[263] In May 2026, the Pentagon awarded Scale AI a USD 500 million contract to help analyse data and support decision-making, a fivefold increase from the USD 100 million deal the startup signed in September 2025.[264]

Another step is Meta's partnership with controversial military tech company Anduril. In May 2025, Mark Zuckerberg announced that Meta would work with Anduril to "design, build, and field a range of integrated XR [Extended Reality] products that provide warfighters with enhanced perception and enable intuitive control of autonomous platforms on the battlefield."[265] "Meta has spent the last decade building AI and AR to enable the computing platform of the future. We're proud to partner with Anduril to help bring these technologies to the American servicemembers that protect our interests at home and abroad", Zuckerberg said.[266]

Anduril's founder, Palmer Luckey, became known as the inventor of the Oculus Rift VR headset. After Facebook bought Oculus in 2014 for USD 2 billion, Luckey was an employee for some time but in 2017 he was fired after he donated USD 10,000 to a pro-Trump group that paid for a billboard campaign deriding Hillary Clinton as "Too Big to Jail." Zuckerberg recently expressed regret about the firing, according to the New York Review of Books.[267] "I am glad to be working with Meta once again. Of all the areas where dual-use technology can make a difference for America, this is the one I am most excited about. My mission has long been to turn warfighters into technomancers, and the products we are building with Meta do just that", Luckey said.[268] Meta's Llama and Anduril's Lattice AI-driven command and control system are being integrated to enhance IVAS (integrated visual augmentation system) headsets for the US Army. The product family Meta and Anduril are building is called EagleEye.[269]

Ethical policies

Meta's human rights policy is relatively detailed and distinct from most other US companies evaluated here. Meta says all people are equal in dignity and rights,[270] and commits to respecting human rights under the UN Guiding Principles - including in how it builds, tests and deploys AI-enabled products - prioritising the most salient human-rights risks in each context and using due-diligence methods such as human rights impact assessments.[271]

Most of the practical examples in its annual (2024) Human Rights Report relate to online abuse, disinformation and other cybersecurity issues and do not relate to military use per se. Also, an apparent change in dynamics since Trump's election in 2024, and the recent relations with Scale AI ("Data is ultimately the ammunition of AI warfare"[272]) and Anduril (with its Fury autonomous fighter jet[273]), makes one wonder what the future of Meta's military

business will look like.

Data protection policies

Meta's current privacy policy (effective 4 March 2026[274]) covers Meta Products including Facebook, Instagram, Messenger and AI at Meta, and also Meta Quest where a user logs in with a Meta account.[275] It states that Meta collects activity across its products, including content users create, messages users send and receive subject to applicable law, metadata about content and messages, device and network information, information from partners and interactions with AI at Meta.[276]

In November 2024, Meta announced that it was making Llama available to US government agencies and contractors working on national-security applications, as well as named private-sector partners including Accenture Federal Services, Amazon Web Services, Anduril, Booz Allen, IBM, Leidos, Lockheed Martin, Microsoft, Oracle, Palantir, Scale AI and Snowflake.[277] In September 2025, Meta further stated that Llama had been made available for national-security use cases to Five Eyes partners and was being expanded to other US allies and institutions, and that governments can fine-tune Llama models using their own sensitive national-security data, host them in secure environments at various levels of classification and deploy models tailored for field use.[278]

That record points to an important concern. Once Llama is downloaded, hosted, fine-tuned or deployed by a government or military customer or its contractor, Meta's consumer privacy policy does not govern the personal data that those third parties may process in that deployment. Meta's public materials authorise and promote national-security uses of Llama, while no dedicated public data-protection framework, based on the material above, sets out minimum safeguards for personal data processed in those military or national-security deployments.

Meta's Human Rights Policy refers to the UN Guiding Principles on Business and Human Rights and to risk-based human-rights due diligence.[279] While relevant, this is not a substitute for a specific, operational data-protection policy governing military or intelligence uses of Llama by third parties. The resulting accountability concern is significant because the same model family can be deployed outside Meta's consumer-product environment, where the ordinary Meta privacy-policy relationship between platform, user and data subject does not exist.

4.4 Microsoft

Founded in 1975, Microsoft (or MS) has been at the forefront of developing personal computer software from MS-DOS to Windows and from Office to 365. It acquired Skype in 2011 to be overtaken by Teams as its main videoconferencing tool. Xbox online gaming, Azure cloud services and the LinkedIn social network are also part of Microsoft. In 2019, Microsoft became the third US company to be valued at over USD 1 trillion and co-founder Bill Gates was for much of the 1995-2017 period the world's richest person. Microsoft has long been

criticised for its monopolistic practices. Total revenues in 2025 were USD 281.7 billion with net income USD 101.8 billion, a huge profit margin.[280]

Military applications

> "For more than 40 years, Microsoft has partnered with the Department of Defense, Intelligence Community, and national security agencies to address our nation's most complex challenges", according to the company.[281]

In 2018 Microsoft was awarded a 10-year, USD 22 billion deal[282] to supply its commercially available HoloLens 2 heads-up display for US Army for both training and combat use. However, the device was plagued with problems that ranged from soldiers complaining of cyber sickness symptoms like nausea and visual discomfort to software glitches. In 2025 Anduril took over the programme management to overcome these issues and soon partnered with Meta, while Microsoft is staying on as a cloud provider.[283]

In 2020, Microsoft launched Azure Orbital, the space-connections wing of Microsoft's cloud service Azure. While aimed at the space sector broadly, "it is specifically cultivating ties to the Pentagon and the defense contracting community".[284] One example is Azure Orbital's partnership with Kratos, a company already actively working on military space applications. As part of its bid to build strong ties between Azure and the Department of Defense, Microsoft had specifically hired career professionals in the military and intelligence communities, including Stephen Kitay, former deputy assistant secretary of Defense for space policy, to head Azure's space industry division.[285]

Also in 2020, Microsoft, together with Amazon, Google, IBM and Oracle, won a contract to supply cloud services to the 17 organisations comprising the US intelligence - the Commercial Cloud Enterprise (C2E) contract vehicle; for its scale and reported value, see under Section 3.3 on IBM above. In 2021, Microsoft announced Azure Government Top Secret, a cloud service "that serves the national security mission and empowers leaders across the Intelligence Community (IC), Department of Defense (DoD), and Federal Civilian agencies".[286]

A month earlier Microsoft lost its lucrative – potentially USD 10 billion - but disputed JEDI (Joint Enterprise Defense Infrastructure) cloud contract. The Pentagon cancelled it, partly due to what it called a "shifting technology environment", partly because of delays, extended by legal challenges by Amazon, which lost the competition to Microsoft and claimed the decision had been politically motivated.[287] Thus it was decided to start over and seek multiple vendors. A year later then, Microsoft, together with Alphabet/Google, Amazon and Oracle, won the Pentagon's USD 9 billion Joint Warfighting Cloud Capability (JWCC) contract in 2022.[288] For the JWCC's stated capabilities and its intended use in combat, see under Section 4.1on Google above.

Also in 2022, Microsoft started providing Lockheed Martin with its first classified cloud as part of a three-year deal, making it easier for the world's largest weapons producer to test its military systems and to share information with the Pentagon, its main customer, and user of a similar cloud.[289] Earlier that year the two announced they would cooperate on "5G networking technology for Joint-All Domain Operations (JADO)", using Microsoft 5G and Azure services for Lockheed Martin's Hybrid Base Station, a military-grade "multi-network gateway and cell tower in a box".[290] Late 2025, Microsoft joined Lockheed Martin to develop Sanctum, counter-uncrewed aerial systems (C-UAS) capabilities combining their technologies "to protect lives and defend critical infrastructure".[291]

In 2024, Microsoft announced an expansion of its partnership with the controversial data tech company Palantir to incorporate more cloud-enabled AI and data analytics capabilities in an integrated suite. The partnership will marry large language models created by Microsoft via Azure OpenAI within Palantir's Foundry, Gotham, Apollo and AI Platform products, available on government and classified cloud environments. "Palantir and Microsoft have a long history operating in secure and accredited environments to deliver leading technology for the most critical U.S. Defense and Intelligence missions", according to a Palantir press release.[292] "Bringing Palantir and Microsoft capabilities to our national security apparatus is a step change in how we can support the defense and intelligence communities. […] It's our mission to deliver this software advantage and we're thrilled to be the first industry partner to deploy Microsoft Azure OpenAI Service in classified environments."

Researchers at Microsoft are working on a DARPA-funded project, where they unveiled in 2025 the Majorana 1, "the world's first quantum processor powered by topological qubits […] a transformative leap toward practical quantum computing".[293] Such quantum computer chips could be highly relevant in any future military use, as AI develops further.[294] Also in 2025, the US Air Force announced the launch of an Artificial Intelligence 'Center of Excellence', building on existing partnerships with MIT, Stanford University, and Microsoft.[295]

Also in 2025, Microsoft was awarded a place in a US Army contract, as part of an Anduril-led consortium worth nearly USD 100 million, to "deliver a next-generation command and control (NGC2) prototype" and to "create an ecosystem that can rapidly integrate a range of technologies into a singular architecture so that soldiers can access various kinds of compute, communications and information processing capabilities all at once".[296] Other consortium members include Palantir, Striveworks and Govini.

Global footprint examples

Microsoft has been active in Israel since 1991, developing its largest centre outside the United States. Microsoft has been integrating its systems and civilian tech across the Israeli military since 2003, while acquiring Israeli cybersecurity and surveillance start-ups.[297] The Israeli military have reportedly used Microsoft's HoloLens devices in training.[298] In 2019, Microsoft invested in Israeli facial recognition start-up AnyVision, which reportedly was working

with the army to build a network of smart security cameras using face-scanning technology throughout the West Bank.[299] Also in 2019, the Israeli military announced the introduction of a public facial recognition program, powered by AnyVision, at major checkpoints where Palestinians cross into Israel from the West Bank. Related to the controversy about its relation, Microsoft divested from AnyVision in 2020.[300] Microsoft has a "footprint in all major military infrastructures" in Israel, and sales of the company's cloud and AI services to the Israeli army have skyrocketed since the beginning of its onslaught on Gaza, according to leaked commercial records from Israel's Defense Ministry and files from Microsoft's Israeli subsidiary.[301] See for more details see Chapter 6.

In 2024, Microsoft announced a USD 1.5 billion investment in Abu Dhabi-based AI company G42, with president Smith joining G42's board of directors.[302] Part of the deal, negotiated for a year with both governments, was a provision that G42 would cut links with Chinese companies, as G42 had been subject to congressional scrutiny over its close ties to China.[303] In 2025, the cooperation was further deepened with a USD 15.2 billion Microsoft investment.[304]

Ethical policies

Already in 2018, in response to some employees' demands that Microsoft should not be in the business of warfare[305], Smith wrote that new technologies, including the ability of weapons to act autonomously, raise profoundly important issues; that no military wants to wake to find machines have started a war; and that, rather than withdrawing, the tech sector should engage proactively with governments to ensure AI and other technologies are used responsibly and ethically.[306]

In February 2019, more than 200 Microsoft employees demanded that the firm would cancel its US Army HoloLens contract. In an open letter to Microsoft CEO Satya Nadella, they expressed concern that HoloLens could be "designed to help people kill" by "turning warfare into a simulated video game". The employees added: "we did not sign up to develop weapons, and we demand a say in how our work is used".[307] As Microsoft would not consider cancelling the contract, CEO Nadella said: "we're not going to withhold technology from institutions that we have elected in democracies to protect the freedoms we enjoy".[308]

In December 2019, Microsoft president Brad Smith said: "What I have said repeatedly to our employees is that there are more than a million people in the United States military, and every one of them … has pledged that before the sun sets they will sacrifice their life if that's what they need [to do] to keep us safe […] Of course we will provide all of our technology to them […] How could we possibly not do that?"[309]

In 2020, Microsoft made clear it would "not sell facial-recognition technology to police departments in the United States until we have a national law in place, grounded in human rights, that will govern this technology. […] "The bottom line for us is to protect the human rights of people as this technology is deployed", Microsoft president Smith said.[310]

In September 2025, after major backlash[311] caused by revelations about Microsoft's business with Israel's military, especially in the context of Gaza, and the subsequent termination of certain contracts, Microsoft president Brad Smith wrote: "we do not provide technology to facilitate mass surveillance of civilians. We have applied this principle in every country around the world, and we have insisted on it repeatedly for more than two decades. […] Microsoft's standard terms of service prohibit the use of our technology for mass surveillance of civilians".[312] Also, Smith concluded: "Microsoft will continue to be a company guided by principles and ethics. We will hold every decision, statement, and action to this standard. This is non-negotiable".[313]

But these actions did not come spontaneously and only after thorough journalism that Microsoft could not deny. It remains to be seen to what extent Microsoft's partnerships with companies such as Anduril and Palantir will affect Microsoft's principles, and to what extent they will be contested under an increasingly authoritarian US government.

Technology should serve humanity, Microsoft says in its Global Human Rights Statement, and respecting human rights is a core value inseparable from its mission.[314] Also, Microsoft is committed to helping people use technology "to defend and promote democracy, good governance, and the rule of law"; and "to protect and advance privacy, security, safety, freedoms of opinions, expression, association, peaceful assembly, and other human rights".

To meet its human rights commitment, Microsoft commits to engage with, rather than withdraw from, countries facing serious human-rights challenges. It further commits to operationalise human rights in their business and technologies by: conducting due diligence on the human-rights impact of its technologies, guided by international principles and norms such as the UN Guiding Principles; and applying rights-aware decision-making throughout its products' lifecycles and business relationships.

Microsoft's Responsible AI Principles and Approach state: "We're committed to making sure AI systems are developed responsibly and in ways that warrant people's trust."[315] Microsoft does not explicitly address concerns related to military uses nor the weaponisation of AI. In what however could be meant as reference to that it says in its Responsible AI Transparency Report: "We improved our responsible AI tooling to provide expanded risk measurement and mitigation coverage for modalities beyond text - like images, audio, and video - and additional support for agentic systems, semi-autonomous systems that we anticipate will represent a significant area of AI investment and innovation in 2025 and beyond".[316]

Data protection policies

Although Microsoft has a comparatively developed privacy and data-protection framework, its framework still leaves important limits in the context of military and intelligence use of cloud infrastructure. The Microsoft Privacy Statement, last updated in March 2026, explains the personal data Microsoft processes across consumer and enterprise products and services.[317] For enterprise and developer products, the statement explains that Microsoft

receives, collects and generates data to provide services, improve and secure them, conduct business operations and communicate with customers. It also states that, where there is a conflict between the Privacy Statement and the terms of a customer's agreement for enterprise and developer products, the customer's agreement takes precedent.[318]

For commercial cloud services, Microsoft points customers to the Product Terms and the Products and Services Data Protection Addendum. Microsoft states that it is committed to protecting customer data as set out in those contractual materials, and summarises its commercial-customer privacy approach around customer control, knowledge of data location and use, security of data, and defence from third-party access.[319] Microsoft also publishes government-request transparency reports and states that it will challenge government requests for commercial and public-sector customer data where it can lawfully do so.[320]

Albeit significant, those commitments do not resolve the military-use problem. Microsoft operates cloud environments for classified US national-security missions, including Azure Government Top Secret, which Microsoft announced as generally available in 2021 for US national-security workloads.[321] Data processed in such environments is governed by the relevant customer contracts, security accreditations and public-sector legal frameworks, not by the consumer-facing privacy relationship between Microsoft and individual users. Public privacy materials do not appear to give affected third parties a direct account of how personal data processed by military customers in Azure environments is used, limited, audited or challenged.

The 2025 reporting and Microsoft review concerning Israel's Unit 8200 illustrates the practical significance of that distinction. Microsoft president Brad Smith stated in September 2025 that Microsoft does not provide technology to facilitate mass surveillance of civilians and that Microsoft's standard terms of service prohibit such use.[322] Microsoft also stated that it had ceased and disabled specified subscriptions and services after its review found evidence supporting elements of the reporting about the use of Microsoft cloud storage by the Israeli Ministry of Defense.[323] This episode demonstrates the difficulty of translating contractual prohibitions and privacy principles into effective oversight of how military customers use cloud infrastructure.
Microsoft does not appear, based on the above, to publish a dedicated data-protection policy for military uses of Azure or for the personal data of third parties processed by military customers using Microsoft infrastructure. This points to a lack of specific public standards explaining how those commitments apply when the customer is a military or intelligence actor and the affected individuals are not Microsoft customers.

4.5 Oracle

Oracle Corporation is an American multinational tech company co-founded in 1977 by its current chairman of the board and chief technology officer Larry Ellison, at the time

of writing the world's sixth richest person, with an estimated wealth of more than USD 200 billion.[324] The company sells database software, enterprise applications and cloud infrastructure. While Oracle's cloud revenue is still far behind the top three competitors (Alphabet, Amazon and Microsoft), in 2024 it accounted for 76 per cent of the company's total revenue.[325] Oracle annual revenue for 2025 was USD 57.4 billion; net income was USD 12.4 billion.[326]

Military applications

For decades Oracle has been an important provider of business application software (for example to manage supply chains and equipment) and other data storage services to the US DoD.[327] With government agencies looking to switch to cloud computing in the late 2010s, Oracle's traditional revenue sources were threatened, and it was slow to adapt.

In 2020 Oracle, together with Amazon, Google, IBM and Microsoft, won a contract to supply cloud services to the 17 organisations comprising the US intelligence community - he Commercial Cloud Enterprise (C2E) contract vehicle; for its scale and reported value, see under Section 3.3 on IBM above. In 2020, Oracle also won a deal with the UK MoD's Defence Digital department to implement Oracle Cloud Infrastructure as part of the MODCLOUD multi-hybrid suite of secure services.[328]

In 2021, the US National Security Commission on Artificial Intelligence urged that to get the DoD be made "AI-ready" by 2025 to stay ahead of China. It should boost its artificial intelligence research and development to USD 8 billion a year by 2025, up from about USD 1.5 billion then. One of the Commission's members was Oracle CEO Safra Catz, who said at the launch: "There are very, very bold actions we're asking for. They are asking in many cases for us to break out from our historical siloes and work together. This is pretty much the critical moment for our country".[329]

In July 2021 Oracle won a contract for the US Air Force's Advanced Battle Management System, or ABMS, the service's contribution to Joint All-Domain Command and Control, the Pentagon's effort to connect sensors and shooters across the services and across domains.[330]

Oracle, together with Alphabet, Amazon and Microsoft, won the Pentagon's USD 9 billion Joint Warfighting Cloud Capability (JWCC) contract in 2022.[331] For the JWCC's stated capabilities and its intended use in combat, see Section 4.1 on Google above.

In April 2024, Oracle announced a partnership with the controversial tech company Palantir. "Oracle's AI strategy, including its wide range of partners, provides generative AI services and infrastructure that extend Palantir's AI capabilities to help customers accelerate decision-making. Oracle's long history in defense and intelligence provides a depth of experience and technology critical to the success of high-stakes missions. Together, Oracle and Palantir will bring powerful new capabilities to the defense industry", according to the press release.[332]

Later in 2024, Oracle also teamed with Anduril to combine Anduril's Lattice software platform for command and control (C2), to Oracle Cloud Infrastructure (OCI). "Anduril will also pair its Menace hardware systems with OCI to enhance operations in connected and disconnected mobile command and control environments. Together, Oracle and Anduril will provide secure mission capabilities across the globe from the datacenter to the tactical edge, and at all classification levels", according to Anduril's press release. "Oracle Cloud provides the global infrastructure, price performance, and data sovereignty that mission customers need to deploy scalable, autonomous, and force-multiplying technology to the far edge."[333]

In 2025, Oracle won to provide an "Oracle Cloud Isolated Region that can enhance the command, control, communications, and computers capabilities" of the Singapore Armed Forces (SAF) and "modernise its digital capabilities with increased scalability and performance".[334] That cloud will be disconnected from the internet, providing a secure environment to the MoD and the SAF to "enhance insights and enable faster decision making", according to Oracle.[335] Later that year it launched the Oracle Defense Ecosystem program that it says will help smaller companies more easily sell technology, including artificial intelligence, to the US DoD.[336]

In September 2025, Oracle announced that the NATO Communications and Information Agency (NCIA, NATO's technology and cyber hub) will move its mission-critical workloads to Oracle Cloud Infrastructure (OCI). Delivered in collaboration with "prime contractor Thales, NCIA will move its on-premises workloads to OCI to benefit from OCI's sovereign cloud solutions, high performance, availability, AI innovation, and enterprise-grade security".[337] Oracle's website has plenty more references to its military potential ("Make Every Mission Successful with Oracle").[338] With much detail still lacking regarding the set-up of Donald Trump's Golden Dome missile shield plan, Oracle, for example, offers cloud coverage, mission-ready AI infrastructure, and supporting software.[339]

Global footprint examples

Mostly through Chinese intermediaries, Oracle has been working in China since at least the late 1990s, including on database and cloud services enabling the Chinese surveillance state as well as military entities, The Intercept revealed in 2021.[340] "The fact that an American technology company is marketing capabilities to increase the combat power of Chinese military is definitely poor judgment, especially given how avidly Oracle continues to pursue opportunities to work for the Defense Department," said Elsa Kania, a fellow at the Center for a New American Security and an expert on Chinese military strategy, after

reviewing the relevant documents. "It says something about the pursuit of profits and market share over questions of ethics and due diligence".[341]

In response, Oracle claimed that its practices in China and elsewhere adhere to the law. "We go beyond what one might anticipate from export control regulations, […] we vet

partners, and we have a track record globally of ending partner relationships where there has been some violation in our view".[342] However, export control legislation keeps many tech-related areas uncovered, especially in the area of surveillance technologies, so the law is a rather low barrier here, if the Chinese police and the surveillance state more broadly is not considered problematic.

After more than five years of back and forth related to concerns that TikTok would compromise the privacy of US citizens and national security more broadly, a new law[343] effectively prohibited the app. ByteDance, TikTok's Chinese owner, has meanwhile reached a compromise by setting up a majority American-owned venture, with investors including Oracle, private-equity group Silver Lake and Abu Dhabi's MGX owning 80.1 per cent of the new entity, while ByteDance will own 19.9 per cent.[344] With Oracle's position on Israel (below) it raises "questions about how Oracle might exercise its impending ownership role at TikTok, a platform popular with young adults who are often critical of U.S. support for Israel's war in Gaza and Israel's killing of Palestinian civilians".[345]

Oracle has been one of the firmest defenders of Israel, especially after the 7 October 2023 Hamas attacks, and most outspoken so through Israel-born CEO Safra Catz ("After October 7th, everyone visiting our website was greeted by the Israeli flag, signalling our support for the country and its security forces.") and co-founder and CTO Larry Ellison.[346] The company's branch in Israel employs some 500 staff and plans to open a second data centre. Interviewed by Israeli tech news site Calcalistech, Catz further said: "For employees, it's clear: if you're not for America or Israel, don't work here - this is a free country. Unlike our competitors, we've never had employees sign petitions refusing to work with Israel or the U.S. government". While indeed criticism of Israel or Oracle's position is clearly not accepted by the company, some employees have withstood the pressure and set up a petition in support of Palestine in 2024, rejecting the company's position regarding Israel. "After 8 months of horrific violence which has killed tens of thousands of innocent civilians, we have yet to see the company's leaders express equal concern and empathy towards Palestinian lives". To the contrary: "In response to legitimate concerns, many of us have been referred to internal mental health resources rather than having those concerns addressed appropriately", according to Oracle for Palestine.[347]

Ethical policies

Nevertheless, Oracle says it upholds the highest standards of business ethics and corporate governance, with public reporting on its environmental and social impact.[348] Its "Oracle Policy Positions" document briefly refers to human rights, saying: Oracle universally respects recognised human rights across its operations - addressing issues such as privacy, human trafficking, conflict minerals, labour rights and freedom of expression - works through the Responsible Business Alliance, and condemns any involvement in human rights violations arising from its business.[349] A separate, very brief "Oracle Human Rights Statement" also refers to the UN Guiding Principles on Business and Human Rights but lacks specifics regarding customer due diligence nor the military uses of its technologies and services.[350]

While a dedicated document on responsible AI is hard to find on its corporate website, a Qatari agent's website features what looks like such a policy outline dated July 2025, which highlights a "principle-based governance model" prioritising fairness, accountability, transparency, privacy and safety, operationalised "through policies, internal review boards, and engineering practices that are integrated across Oracle's AI portfolio, including Oracle Cloud Infrastructure (OCI), Oracle Fusion Applications, and Oracle Autonomous Database."[351] It is unclear why something similar appears lacking on Oracle's website.

Data protection policies

Oracle's public privacy framework is divided across several instruments. The General Oracle Privacy Policy addresses personal information Oracle processes in connection with its websites, mobile applications, social-media pages, sales and marketing activities, events and other direct interactions with Oracle.[352] For Oracle cloud, support, consulting and other customer services, the more relevant instrument is the Oracle Services Privacy Policy, supplemented where applicable by Oracle's contractual data-processing terms, including the Data Processing Agreement for Oracle Services.[353]

The Services Privacy Policy distinguishes between Services Personal Information and Systems Operations Data. The former is personal information provided by the customer or residing on Oracle, customer or third-party systems and environments, which Oracle processes on the customer's behalf in order to perform the services. Oracle states that the customer is the controller of that Services Personal Information and that Oracle processes it as specified in the customer's order and documented written instructions.[354] Systems Operations Data covers access, event, diagnostic and other log files, as well as statistical or aggregated information generated by the interaction of users with Oracle systems, tools and networks used to monitor, safeguard and deliver services.[355]

Oracle's Data Processing Agreement for Oracle Services takes the same basic contractual approach. It states that the customer is the controller and Oracle is the processor, and that Oracle will process personal information solely for providing the contracted services. The listed processing activities include hosting and storage, backup and disaster recovery, issue resolution, updates and upgrades, monitoring and testing system use and performance, IT security, support-system maintenance, migration, implementation and configuration.[356]

As set out in this report, Oracle is one of the major cloud providers involved in US defence and intelligence cloud procurement, including the Joint Warfighting Cloud Capability (JWCC) contract, and it has also announced defence and national-security partnerships or offerings involving Oracle Cloud Infrastructure, Palantir, Anduril, NATO and other government customers.[357] Oracle's own JWCC material describes the contract vehicle as enabling the US Department of Defense to purchase commercial cloud services across classification levels, including unclassified environments, Top Secret, Special Compartmented Information and Special Access Program workloads, supporting mission readiness from headquarters to the tactical edge.[358]

Based on the above material, Oracle does not appear to provide a dedicated public data-protection framework explaining how personal data processed by military, intelligence or defence customers inside Oracle Cloud Infrastructure is used by those customers, what safeguards apply to affected third parties or what practical route of redress exists for individuals whose data is processed in those environments.

Oracle also publishes a separate Customer Data Research and Development Privacy Policy for Oracle's AI and machine-learning activities. That policy applies where Oracle has obtained personal information from an Oracle customer and the customer has contractually agreed that Oracle may use such information for AI/ML processing for the purposes specified in the policy. Oracle states that the current lines of business in scope are NetSuite and that the data may include customer data and systems-operations data which may incidentally contain personal information.[359] This allows for the use of customer data for AI/ML development and treats such processing operations as requiring a distinct policy and contractual basis.

4.6 SpaceX

Space Exploration Technologies Corp. or SpaceX is a private American aerospace and AI company headquartered in Starbase, Texas. It was founded in 2002 by Elon Musk, currently the richest person in the world,[360] with a vision of decreasing the costs of space launches. As of 2026, SpaceX is the world's dominant space launch provider through contracts worth billions of dollars a year with NASA and the Pentagon. SpaceX also owns and operates the Starlink satellite internet service, operational since 2019, which has more than 9,000 satellites in orbit and roughly 9 million customers.[361] SpaceX generated reportedly about USD 8 billion in net income on USD 15-16 billion of revenue over 2025 ahead of an expected IPO later in 2026.[362]
Musk founded xAI in 2023 in part to take on OpenAI and other LLM providers. In 2025 xAI acquired Musk-owned social media platform X, previously known as Twitter. In February 2026, he announced the takeover of xAI by SpaceX, the largest merger of all time, combining the two Musk-related companies with an estimated USD 1.25 trillion total market value.[363] A reason for the merger was to better build "orbital data centers", according to Musk.[364] Another reason is to provide more capital to xAI, which makes the Grok chatbot and is racing against rival AI labs. In February 2026 Musk told xAI employees that the company needed a factory on the moon to build A.I. satellites and a massive catapult to launch them into space.[365] In May 2026, a USD 55 billion investment to make AI chips at the company's new semiconductor factory Terafab was revealed.[366]

Military applications

Military use of space is one of the fastest growing areas in the Pentagon budget and the US DoD and the intelligence community are SpaceX's largest customers, including launching classified satellites for the intelligence and military community.[367] Satellites play a major role in US national security, tracking missile launches, monitoring activity on the ground

and providing secure communications. With its much smaller satellites SpaceX broke the oligopoly of legacy military contractors such as Boeing and Lockheed Martin. In 2005 it received its first contract from the US intelligence community.[368] Since then it has rapidly grown to become a leading provider of 'national security' launches.[369]

More recently the Pentagon has done business with SpaceX's Starlink broadband service, including agreements to pay for Ukrainian internet links in the war with Russia, as well as tens of thousands of Starlink terminals. It has provided major promotional benefits to the company, proving the use of the communication system in challenging environments.
In January 2026 Ukraine complained about illicit Russian use of Starlink to coordinate its attacks on Ukraine, as revealed by shot-down Russian BM-35, Shahed and Molniya one-way attack drones or loitering munitions with Starlink receivers, which increased their range of operation as well as their resilience against Ukrainian electronic warfare.[370] Within days, Musk had ensured Russia would no longer be able to use Starlink.[371]

Little-known SpaceX unit Starshield is making low-Earth-orbit (LEO) satellites designed to provide new military space capabilities to US and allied governments. The company entered into USD 1.8 billion classified contract with the U.S. government in 2021.[372] It received another USD 70 million award from the military in 2023 to provide communications services to dozens of Pentagon partners. A space industry analyst sees Starshield as a "logical next step for SpaceX to leverage its mass manufacturing of satellites and terminals" specifically for the military space market. Considering how fast the company builds satellites, he said, "there is an opportunity for DoD to take advantage of a hot manufacturing line to realize meaningful cost savings compared to more traditional bespoke acquisitions."[373]

Ethical policies

While it had a brief 'SpaceX Code of Ethics and Business Conduct' for its suppliers on its website around 2016-18,[374] currently there is no reference to any governance, human rights or responsible AI policy on its website. This may change if the company goes public.

Data protection policies

SpaceX maintains two relevant privacy instruments: a SpaceX website privacy policy and the Starlink Global Privacy Policy, which governs personal data associated with Starlink's satellite-internet service.[375]
The Starlink Global Privacy Policy was revised with an effective date of 15 January 2026. Reuters reported that the revised policy allows Starlink data to be used to train machine-learning or artificial-intelligence models unless the user opts out, and that data may be shared with service providers and third-party collaborators.[376] The current Starlink privacy policy also identifies broad categories of personal information, including contact information, payment information, location information, IP addresses and communication information, including audio, electronic or visual information, files provided by the user and inferences drawn from other personal information.[377] The policy language appears broad enough to permit AI-training uses and certain collaborator sharing including xAI.

Starlink is not merely a consumer internet service. This report documents Starlink's use by the US Department of Defense and by Ukrainian forces, including Pentagon support for Ukrainian internet links and Starlink terminals.[378] To the extent Starlink collects personal information from accounts, devices, communications or operational use in those contexts, the Starlink Global Privacy Policy does not appear to provide a specific carve-out, limitation or protective framework for military customers or users in active conflict zones.

Chapter 05

In focus: Decision-making in warfare: Military applications of GenAI

5.1 OpenAI: Military applications
5.2 Anthropic: Military applications
5.3 US military use of GenAI

Military applications of GenAI

"The future of American warfare is here, and it's spelled AI" said the US Secretary of War Pete Hegseth.[379] Large Language Models or LLMs gained large public use with the release of ChatGPT in November 2022. Relatively simple questions get instant answers, and more elaborate ones produce extensive reports – with all their shortcomings. Soon enough their military relevance was discussed and by now all main players have set up versions specifically tailored to government uses, including for the military. Actual use in US offensive military operations in Venezuela and Iran has since been reported. After ChatGPT was launched in November 2022, the rest of the tech giants rushed to introduce their own GenAI models. Some of the tech giants, such as Googles and Meta, initiatives are discussed in the respective sections in Chapter 4 above. Two further companies deserve mention here, however, as their contributions have been particularly significant in shaping the competitive landscape of generative AI.

5.1. OpenAI: military applications

OpenAI was founded in 2015 as a non-profit, with an initial funding commitment of USD 1 billion from Sam Altman and Elon Musk, among others. The company's stated goal is "to advance digital intelligence in the way that is most likely to benefit humanity as a whole, unconstrained by a need to generate financial return."[380] With getting more billions of dollars in investments from Microsoft, Nvidia and the Japanese SoftBank, however, OpenAI faced increasing corporate pressure to separate business and non-profit operations to attract further investments. In 2019, OpenAI non-profit launched OpenAI LP, a 'capped-profit'[381] company, under the control of the non-profit with its obligation to "humanity as a whole" rather than to shareholders. Among the critics of the change has been co-founder-turned-competitor, Elon Musk, who left OpenAI's board in 2018, sued OpenAI and Microsoft in 2024 and is reportedly seeking damages in the range of USD 79-134 billion from both companies over claims that OpenAI defrauded him by abandoning its nonprofit roots and partnering with the software giant.[382] As part of the litigation OpenAI has filed emails that claim to show Musk himself was pushing for OpenAI to go for-profit while he was still at the company. In 2023, Musk set up his own LLM enterprise: xAI.

Adding to the drama, the nonprofit board fired Sam Altman in November 2023 after concluding that he was "not consistently candid in his communications with the board". Three days later Microsoft hired Altman in response. With nearly all remaining staff threatening to join him, Altman was reinstated and the board replaced. Microsoft, OpenAI's largest external shareholder at an estimated 28 per cent[383], was given a non-voting, observer position on the board. In October 2025, OpenAI announced that its restructure is complete. All but two members of the OpenAI board are shared between the for-profit Public Benefit Corporation and the (non-profit) Foundation. In September 2025, OpenAI signed an unprecedented contract to buy USD 300 billion in computing power from Oracle over five years.[384] OpenAI President Greg Brockman is a top Trump backer with a USD 25 million

donation in September 2025.[385]

Ethical policies

OpenAI prohibits its technology from being used to develop weapons but changed its policies to enable some military uses of its software.[386] It signed a cooperation agreement with weapons start-up Anduril in 2024 to add its AI technology to Anduril's counter-drone products and military software, which raised concerns amongst some OpenAI employees.[387] While OpenAI has said its work with Anduril will be limited to using AI to enhance systems to defend US soldiers from drone attacks, employees asked in internal messages how OpenAI could stop the US military from deploying them in other ways. "We are proud to help keep safe the people who risk their lives to keep our families and our country safe," OpenAI CEO Sam Altman said in a statement.[388]

As already set out in their company profiles, Big Tech competitors Google and Meta have since released their rivalling LLMs, Gemini and Llama respectively, whereas seven former employees of OpenAI set up Anthropic in 2021 to create Claude. xAI is featuring Grok, which quickly became known for sexist, racist and antisemitic answers of the chatbot.[389]

5.2 Anthropic military applications

Anthropic has also collaborated since 2023 with Google and Amazon, which announced a USD 4 billion investment in the start-up.[390] In November 2025, Anthropic, Microsoft and Nvidia announced a USD 45 billion partnership "that ties together Nvidia's next-gen chips and systems, Azure's data-center infrastructure, and Anthropic's Claude models, creating a loop that locks billions in spending - and influence - across all three".[391] Anthropic has committed to purchase USD 30 billion worth of compute on Azure's platform, as Nvidia pledged USD 10 billion and Microsoft USD 5 billion in direct investment in Anthropic. Claude will be trained and deployed on Azure using Nvidia accelerators. Moreover, Nvidia and Anthropic will collaborate on design and engineering, forming a "deep technology partnership". "The agreement places the three companies at the center of the AI race", noted business website Quartz.[392] With its stake in OpenAI, Microsoft now has significant control over both ChatGPT and Claude.

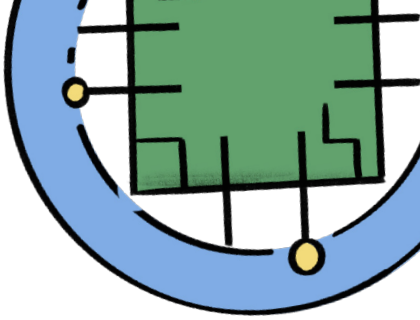
In May 2026, Amodei said that Anthropic could grow 80 times as bigger this year than last year.[393] The huge commitment has clearly elevated the company, which stands out as more conscious and concerned about the risks of AI more generally and military uses in particular, even though it has not excluded military contracts. However, its general positions appear ambiguous and lack clear standards as to what exactly are considered breaches. For example, it is expanding work with Lawrence Livermore National Laboratory (LLNL), one of the United States' premier nuclear weapon research institutions, deploying Claude to its entire laboratory. "LLNL's expansion of Claude access will help bolster research across nuclear deterrence, energy, materials science, and energy security".[394]

Another example is Anthropic's partnership with Palantir announced in November 2024 "to operationalize the use of Claude within Palantir's AI Platform (AIP) […] The partnership facilitates the responsible application of AI, enabling the use of Claude within Palantir's products to support government operations such as processing vast amounts of complex data rapidly, elevating data driven insights, identifying patterns and trends more effectively, streamlining document review and preparation, and helping U.S. officials to make more informed decisions in time-sensitive situations while preserving their decision-making authorities".[395] Aware of both Palantir's (lack of) ethical standards (see Chapter 7 on Palantir) and evidence of US government disdain of international and national law, this sounds less than reassuring, and the company is well-aware of that.

Ethical policies

While it may look sympathetic at first sight, Anthropic's position, read through the writings of its CEO Dario Amodei, in fact sounds naive (or not well thought-through) and neo-colonial at the same time. In 2024, Amodei argued that democratic nations should aim to develop the best AI technology to give them a military and commercial edge over authoritarian countries, which he said would probably use AI to abuse human rights. His "strategy" would aim that "a coalition of democracies seeks to gain a clear advantage (even just a temporary one) on powerful AI by securing its supply chain, scaling quickly, and blocking or delaying adversaries' access to key resources like chips and semiconductor equipment. This coalition would on one hand use AI to achieve robust military superiority (the stick) while at the same time offering to distribute the benefits of powerful AI (the carrot) to a wider and wider group of countries in exchange for supporting the coalition's strategy to promote democracy (this would be a bit analogous to "Atoms for Peace"). […] If we can do all this, we will have a world in which democracies lead on the world stage and have the economic and military strength to avoid being undermined, conquered, or sabotaged by autocracies, and may be able to parlay their AI superiority into a durable advantage."[396]

In a January 2026 essay, Amodei outlines fears about AI's use in both mass surveillance, 'classic' weapons of mass destruction (WMD) (biological and nuclear weapons in particular) and fully autonomous weapons: "A swarm of millions or billions of fully automated armed drones, locally controlled by powerful AI and strategically coordinated across the world by an even more powerful AI, could be an unbeatable army, capable of both defeating any military in the world and suppressing dissent within a country by following around every citizen. […] R&D from powerful AI could make the drones of one country far superior to those of others, speed up their manufacture, make them more resistant to electronic attacks, improve their maneuvering, and so on. […] they are a dangerous weapon to wield: we should worry about them in the hands of autocracies, but also worry that because they are so powerful, with so little accountability, there is a greatly increased risk of democratic governments turning them against their own people to seize power."[397] Below we see how Anthropic's relation with the Pentagon quickly soured.



5.3 US military use of GenAI

As we have seen earlier on, tech companies including Google, Meta, OpenAI and Anthropic have over the past two years changed the terms of their policies to better accommodate cooperation with military customers. They may not have anticipated the force with which the current Trump administration is putting AI and LLMs front and centre - with little eye for accountability and security concerns (privacy, data leakage, bias, inaccuracies etc). The fact is that all major LLM players have now signed contracts with the Pentagon to contribute to its GenAI.mil system.

Already by late 2024, Anthropic, AWS and Palantir had teamed to service military customers, with Claude available for use in Palantir's military-accredited environment, known as Palantir Impact Level 6 (IL6), reserved for systems containing data deemed critical to national security, up to 'secret' level - one step below 'top secret'.

"We're proud to be at the forefront of bringing responsible AI solutions to U.S. classified environments, enhancing analytical capabilities and operational efficiencies in vital government operations," Anthropic's head of sales, Kate Earle Jensen said. "Access to Claude within Palantir on AWS will equip U.S. defense and intelligence organizations with powerful AI tools that can rapidly process and analyze vast amounts of complex data. This will dramatically improve intelligence analysis and enable officials in their decision-making processes, streamline resource intensive tasks and boost operational efficiency across departments."[398]

In July 2025 the Pentagon awarded USD 200 million contracts to OpenAI (ChatGPT), xAI (Grok), Google (Gemini) and Anthropic (Claude) for "frontier AI" projects, "pioneering artificial intelligence projects focused on national security applications".[399] "The adoption of AI is transforming the Department's ability to support our warfighters and maintain strategic advantage over our adversaries," the Pentagon said in a statement. "Leveraging commercially available solutions into an integrated capabilities approach will accelerate the use of advanced AI as part of our Joint mission essential tasks in our warfighting domain as well as intelligence, business, and enterprise information systems."[400]
In its own press release on the contract, Anthropic rephrased its role as "to advance responsible AI in defense operations" and to reassure "At the heart of this work lies our conviction that the most powerful technologies carry the greatest responsibility. We're building AI systems to be reliable, interpretable, and steerable precisely because we recognize that in government contexts, where decisions affect millions and stakes couldn't be higher, these qualities are essential. We believe democracies must work together to ensure AI development strengthens democratic values globally by maintaining technological leadership to protect against authoritarian misuse".[401]

In December 2025, Google Cloud's Gemini for Government was the first AI capability to be launched on GenAI.mil. "The future of American warfare is here, and it's spelled AI,"

Secretary of War Hegseth said in a video. "This platform [GenAI.mil] puts the world's most powerful frontier AI models, starting with Google Gemini, directly into the hands of every American warrior," he said. Users must have a common access card from the department to log onto GenAI.mil; it cannot be accessed by unauthorized personnel.[402]

Late January 2026, US War Secretary Hegseth announced that artificial intelligence chatbot Grok from Elon Musk's xAI (now merging with SpaceX) will join Google's Gemini generative AI engine in operating inside the Pentagon network, as part of big push to feed as much of the military's data as possible into the developing technology. "Very soon we will have the world's leading AI models on every unclassified and classified network throughout our department," Hegseth said in a speech at SpaceX.[403] The announcement came just days after Grok — embedded in the social media network X - drew global outcry for generating highly sexualized deepfake images of people without their consent. Hegseth said he would "make all appropriate data" from the military's IT systems available for "AI exploitation", including from intelligence databases.

Meanwhile, ChatGPT has also been made available "to enhance mission execution and readiness, delivering reliable capabilities to the joint force," according to a DoD press release in February 2026. "Integrating ChatGPT into GenAI.mil marks another critical step in making frontier AI capabilities the standard for daily operations."[404] The Army, Navy, Air Force, Space Force and Marine Corps had already adopted the system as their preferred generative AI platform.[405] At the same time DoD staff have been wondering what the added value of the GenAI hub really is.[406]

Woke AI

Back in January 2026 at SpaceX, Hegseth further elaborated that his vision for military AI systems means that they operate "without ideological constraints that limit lawful military applications" and that the Pentagon's "AI will not be woke"[407], in apparent reference to discussions between the Pentagon and Anthropic over their contractual terms of use. These "dictate that Claude can't be used for any actions related to domestic surveillance". Also "its objection to having its technology used in autonomous lethal operations" caused problems, according to The Wall Street Journal.[408]

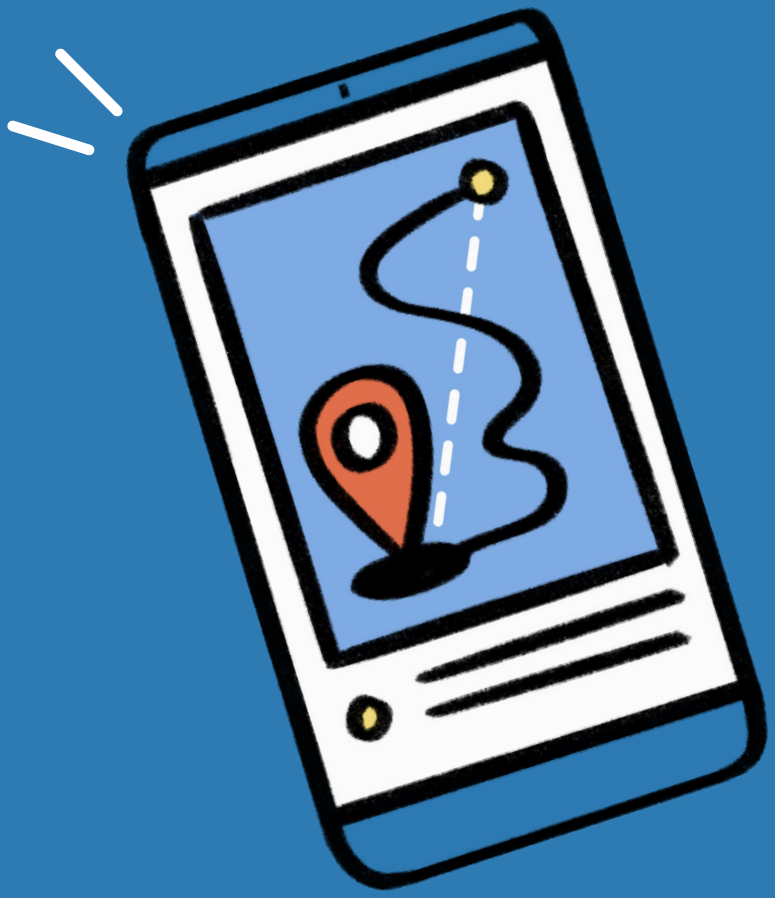
"Anthropic is committed to protecting America's lead in AI and helping the U.S. government counter foreign threats by giving our warfighters access to the most advanced AI capabilities," Anthropic said in response to the controversy. It also said that Claude is used "extensively" for U.S. national security missions.[409]
By mid-February, Hegseth was ready to cut business ties with Anthropic and

designating the AI company a "supply chain risk" - meaning anyone who wants to do business with the US military has to cut ties with the company. "It will be an enormous pain in the ass to disentangle, and we are going to make sure they pay a price for forcing our hand like this", Hegseth said.[410] In March Anthropic was indeed designated a supply chain risk, the first time for an American firm.[411]

The controversy emerged amid reports about the use of Claude, through Palantir tools, including Maven Smart Systems, in the American kidnapping operation of Venezuelan leader Maduro, in January 2026.[412] Such reports also emerged around the US strikes on Iran which started "only hours after Trump directed federal agencies to halt the use of Anthropic's tools".[413] Unclear remains what exactly Claude would have suggested as part of those military operations.

Exemplary for its ambiguous stance regarding autonomous warfare, in January 2026, amidst the clash with the Pentagon, Anthropic reportedly also submitted (but lost) a USD 100 million proposal to the Pentagon to develop voice-controlled autonomous drone swarming technology, using Claude to translate a commander's intent into digital instructions to coordinate a fleet of drones, including "target-related awareness and sharing" and "launch to termination".[414]

In May 2026, the Pentagon announced new deals with SpaceX, OpenAI, Google, Nvidia, Reflection, Microsoft and Amazon to deploy their systems within classified Pentagon networks "to streamline data synthesis, elevate situational understanding and augment decision-making in complex operational environments".[415] "These agreements accelerate the transformation toward establishing the United States military as an AI-first fighting force and will strengthen our warfighters' ability to maintain decision superiority across all domains of warfare," the department said.



Chapter 06

Case study: Israel hosting tech giants

6. Case study: Israel hosting tech giants

6.1 Battlefield tested in the Palestinian laboratory

Back in 2019, Israel's military, the IDF, created the Targets Administrative Division, a unit with hundreds of officers and soldiers using AI to accelerate target generation.[416] In 2021, the Israeli military described its 11-day war on Gaza as the world's first AI war, having relied heavily on machine learning. "For the first time, artificial intelligence was a key component and power multiplier in fighting the enemy," an IDF Intelligence Corps senior officer said. The campaign was a first of its kind, the officer added, deploying new methods and technologies as a force multiplier across the IDF.[417]

What followed offers a most recent—and devastating—example of the consequences of this force multiplication. Late November 2023, after Israel had relentlessly bombed Gaza for almost two months in retaliation for the 7 October attacks by Hamas and other groups, investigative journalists from Israeli media outlets +972 and Local Call revealed AI's pivotal role in the bloodshed. The IDF used an AI target-generating system known as "Habsora" ("The Gospel"), marking buildings and structures that allegedly serve a military function. One former intelligence officer told +972 that this technology enables the Israeli army to essentially operate a "mass assassination factory".[418]

A few months later, further revelations followed. According to six Israeli intelligence officers, the IDF used an AI system nicknamed "Lavender" to generate tens of thousands of "human targets" for assassination on the grounds that they are allegedly part of the armed wings of Hamas or Palestinian Islamic Jihad.[419] These 'outputs' were then fed into an automated tracking system known as "Where's Daddy?", reportedly enabling the army to kill each of them inside their home, along with their whole family and often many neighbours.[420]

These AI-powered decision support systems produced more targets in one day than human personnel can produce in an entire year. With targets generated this fast, authorisation came just as quickly, making human operators nearly redundant. Intelligence officers who spoke to +972 admitted to devoting just 20 seconds to sign off on individual strikes. While not in line with requirements under the laws of war, it was the line Israel had deliberately chosen. "The emphasis is on damage and not on accuracy," said an IDF spokesperson on 9 October 2023.[421] Multiple intelligence sources confirmed to +972 that the number of civilians who may be killed in attacks on private residences is known in advance to Israeli intelligence, and appears clearly in the target file under the category of "collateral damage".[422]

While Lavender and Where's Daddy? may be qualified as AI-powered systems, they are not acting autonomously: a clear chain of command dictates how these technologies are put into action. The abuse of AI may be rooted in military policies and decisions, but it also implicates the civilian technology industry that has offered the technology.

The Israeli private industry flourished since then as well. Since 7 October 2023, more than 130 Israeli startups have reportedly been integrated into Israel's Gaza war effort - around half focused on AI, roughly a quarter on sensor and detection technology such as counter-drone systems, and the rest on navigation and electronic warfare.[423] "The two years of war were beneficial to startups, thanks to the friction on the battlefield".[424] Some USD 100 million was raised by Kela, founded in 2024, which is developing a platform for connecting civilian technologies to military systems. The funding came from funds such as Sequoia, Lux, and IQT - the investment arm of the CIA.[425] Yet the systems at the heart of this targeting did not run on home-grown technology alone; as the following sections show, they rested on the cloud and AI infrastructure of US tech giants.

6.2 Tech giants, the IDF and Project Nimbus

US tech giants have done business with Israel's government for many years. Microsoft's Windows has been its key platform provider, its Azure cloud had been used since at least 2017, and all government employees use Office software.[426] What has evolved is the type of tools and capabilities they provide them and the role they play in conducting military operations.

In 2021 Israel announced that Google and Amazon beat Microsoft and Oracle for its Project Nimbus, a USD 1.2 billion multiyear project to eventually migrate Israel's public information technology to local cloud centres. "The project is intended to provide the government, the defense establishment and others with an all-encompassing cloud solution," according to the Israeli finance ministry which also said that the "cloud services will be hosted by local cloud providers. The data stored on them will remain within Israel's borders under strict data security regulations overseen by the relevant government offices".[427] As part of Nimbus, Israel's largest state-owned arms producers, Israel Aerospace Industries (IAI) and Rafael, are also required to use Amazon and Google for their cloud computing needs.[428]

At the time, Amazon was setting up three server farms in Israel as part of a local partnership with Compass-Azrieli.[429] Google established its Google Cloud Region in Israel in 2022.[430] Documents show that Google was aware it couldn't control what the nation and its military would do with its powerful cloud-computing technology.[431] Worse, multiple reports confirmed that Amazon and Google "agreed to disregard their own terms of service and sidestep legal orders by tipping Israel off if a foreign court demands its data".[432]

While controversial from the start,[433] Nimbus, and the role of foreign tech companies more broadly, has sparked major protests since 7 October 2023. Unlike in 2018 with Project Maven, Google has been much less understanding now. It fired more than 50 workers who, it said, had participated in protests denouncing the company's cloud computing deal with the Israeli government, according to an activist group representing the workers.[434] Chief executive Sundar Pichai told employees in a companywide memo that they should not use the company as a "personal platform" or "fight over disruptive issues or debate politics".[435] It did not, however, take action against colleagues who posted the names and photos of pro-Palestinian workers online, "doxing" them and opening them up to harassment from people on social media.

Google has stated that "the Nimbus contract is for workloads running on our commercial cloud by Israeli government ministries, who agree to comply with our Terms of Service and Acceptable Use Policy. This work is not directed at highly sensitive, classified, or military workloads relevant to weapons or intelligence services. […] Across Google, we've also been clear that we will not design or deploy AI applications as weapons or weapons systems, or for mass surveillance."[436] But that response "does not deny the allegations that its technology enables any form of violence or enables surveillance violating internationally accepted norms," according to a 2024 letter that circulated within DeepMind in May 2024 (see also Section 4.1 on Alphabet's ethical policies).[437] Google's statement on Project Nimbus "is so specifically unspecific that we are all none the wiser on what it actually means," one of the letter's signatories told TIME.[438] Furthermore, the Washington Post revealed how internal documents show that Google has been directly assisting Israel's Defense Ministry and the Israel Defense Forces after 7 October 2023. "The documents, which detail projects inside Google's cloud division, indicate that the Israeli ministry urgently wanted to expand its use of a Google service called Vertex, which clients can use to apply AI algorithms to their own data".[439] In one document a Google employee warned that if the company didn't quickly provide more access, Amazon would.

Both Google and Amazon say they apply the UN Guiding Principles on Business and Human Rights, which seek "to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts." The principles say companies must "identify and assess any actual or potential" rights abuses related to their business. As Matt Mahmoudi, researcher at Amnesty International working on tech issues, said:

> "If tech companies, including Google and Amazon, are engaged in business activities that could impact Palestinians in Gaza, or indeed Palestinians living under apartheid in general, they must abide by their responsibility to carry out heightened human rights due diligence along the entirety of the lifecycle of their products. […] This must include how they plan to prevent, mitigate, and provide redress for possible human rights violation, particularly in light of mandatory relationships with weapons manufacturers, which contribute to risk of genocide."[440]

And contrary to the companies' claims, +972 and Local Call reported that Amazon, Google and Microsoft have been central to Israel's atrocities in Gaza. At the conference 'IT for IDF', near Tel Aviv in July 2024, Col. Racheli Dembinsky, the commander of Israel's Center of Computing and Information Systems Unit, which provides data processing for the whole military, confirmed publicly for the first time that the Israeli army is using cloud storage and artificial intelligence services provided by civilian tech giants in its onslaught on the Gaza Strip. In her lecture slides, the logos of Amazon Web Services (AWS), Google Cloud, and Microsoft Azure appeared twice.[441] She explained how after the start of the ground invasion the IDF internal military systems quickly became overloaded due to the enormous number of soldiers and military personnel who were added to the platform as users. They then decided to "go outside to the civilian world", where cloud services offered by major tech firms allowed the army to purchase unlimited storage and processing servers. But the "most important" advantage that the cloud companies provided was their advanced capabilities in AI. "The crazy wealth of services, big data and AI - we've already reached a point where our systems really need it," she said with a smile. Working with these companies, she added, has granted the military "very significant operational effectiveness" in the Gaza Strip.[442]

According to a former Google employee, who filed a federal complaint, Google allegedly breached its policies barring use of artificial intelligence for weapons or surveillance in 2024 by helping an Israeli military contractor for CloudEx, using an IDF email address, to analyse drone video footage, The Washington Post revealed in February 2026. The request from the IDF email address asked for help making Google's Gemini more reliable at identifying objects. Google responded by making suggestions and doing internal tests. "Many of my projects at Google have gone through their internal AI ethics review process," the former employee wrote to The Post. "That process is robust and as employees we are regularly reminded of how important the company's AI Principles are. But when it came to Israel and Gaza, the opposite was true".[443]

According to multiple intelligence sources of +972 and Local Call, the IDF's cooperation with AWS is particularly close: it provides Israel's Military Intelligence Directorate with a server farm which is used to store masses of intelligence information used by the IDF in the war. "One source who used the cloud-based system during the current war described making "orders from Amazon" for information while carrying out their operational tasks, and working with two screens - one connected to the army's private systems, and the other connected to AWS".[444]

Military sources further emphasised that the scope of intelligence collected from the surveillance of all Palestinian residents of Gaza is so large that it cannot be stored on military servers alone. Much more extensive storage capabilities and processing power were needed to keep billions of audio files (as opposed to just textual information or metadata), which compelled the army to turn to the cloud services offered by tech companies. A military source told +972 and Local Call that most of the new contracts between the military and cloud companies since the war began have been realised through the Nimbus tender.

In parallel, these companies are also earning advertising revenue from the Israeli government, including a June 2025 USD 45 million advertising campaign by Netanyahu's office on Google platforms (YouTube and Display & Video 360) aiming to influence public opinion, for example debunking UN and other reports of starvation in Gaza.[445]

6.3 Mass surveillance

Many of Nimbus' capabilities contribute to Israel's ability to more broadly monitor people and process vast stores of data. "Data collection over the entire Palestinian population was and is an integral part of the occupation," Ori Givati of Breaking the Silence, an anti-occupation advocacy group of Israeli military veterans, told The Intercept back in 2022. "Generally, the different technological developments we are seeing in the Occupied Territories all direct to one central element which is more control."[446]

Similarly, Palestinian Mona Shtaya, at the time digital rights advocate at 7amleh-The Arab Center for Social Media Advancement, said:

> "Living under a surveillance state for years taught us that all the collected information in the Israeli/Palestinian context could be securitized and militarized. […] Image recognition, facial recognition, emotional analysis, among other things will increase the power of the surveillance state to violate Palestinian right to privacy and to serve their main goal, which is to create the panopticon feeling among Palestinians that we are being watched all the time, which would make the Palestinian population control easier."[447]

An online Google presentation of Nimbus indeed refers to the "Faces, facial landmarks, emotions"-detection capabilities of Google's Cloud Vision API, an image analysis toolset, as well as other person/object/pattern recognition and speech/translation tools.[448] A Google worker told The Intercept: "Vision API is a primary concern to me because it's so useful for surveillance," as image analysis would be a natural fit for military and security applications. "Object recognition is useful for targeting, it's useful for data analysis and data labelling. An AI can comb through collected surveillance feeds in a way a human cannot to find specific people and to identify people, with some error, who look like someone. That's why these systems are really dangerous."[449]

Also alarming is the potential surveillance or other militarised applications of AutoML, another Google AI tool offered through Nimbus - training software to recognise patterns in

order to make predictions about future observations. AutoML would allow Israel to leverage Google's computing capacity to train new models with its own government data for virtually any purpose it wishes. "Google's machine learning capabilities along with the Israeli state's surveillance infrastructure poses a real threat to the human rights of Palestinians," said Damini Satija, who leads Amnesty International's Algorithmic Accountability Lab. "The option to use the vast volumes of surveillance data already held by the Israeli government to train the systems only exacerbates these risks."[450]

In 2022, Itai Binyamin, an AI expert who at the time worked with Microsoft Azure, described how it was possible to "deploy [Microsoft's] AI capabilities even on-prem, on your servers, in an environment that is disconnected [from the internet]."[451] In his explanation in the video, Binyamin showed how Microsoft's facial recognition tool could analyse a news video and identify that Hamas leader Ismail Haniyeh appeared in it.

An investigation by the New York Times in March 2024 exposed a "previously undisclosed Israeli facial recognition program" that was started in Gaza late 2023 to conduct mass surveillance, "collecting and cataloguing the faces of Palestinians without their knowledge or consent, according to Israeli intelligence officers, military officials and soldiers".[452] Israel turned to the program "to root out anyone with ties to Hamas or other militant groups. At times, the technology wrongly flagged civilians as wanted Hamas militants, one officer said."

The facial recognition program is run by Israel's military intelligence, including the notorious cyber-intelligence Unit 8200, and relies on technology from Israeli company Corsight and also uses Google Photos. "Combined, the technologies enable Israel to pick faces out of crowds and grainy drone footage".[453] Corsight says that its technology requires less than 50 percent of a face to be visible for accurate recognition and could work with "extreme angles, (even from drones,) darkness, poor quality."[454] By uploading a database of known persons to Google Photos, Israeli officers could use the service's photo search function to identify people. "Google's ability to match faces and identify people even with only a small portion of their face visible was superior to other technology".[455]

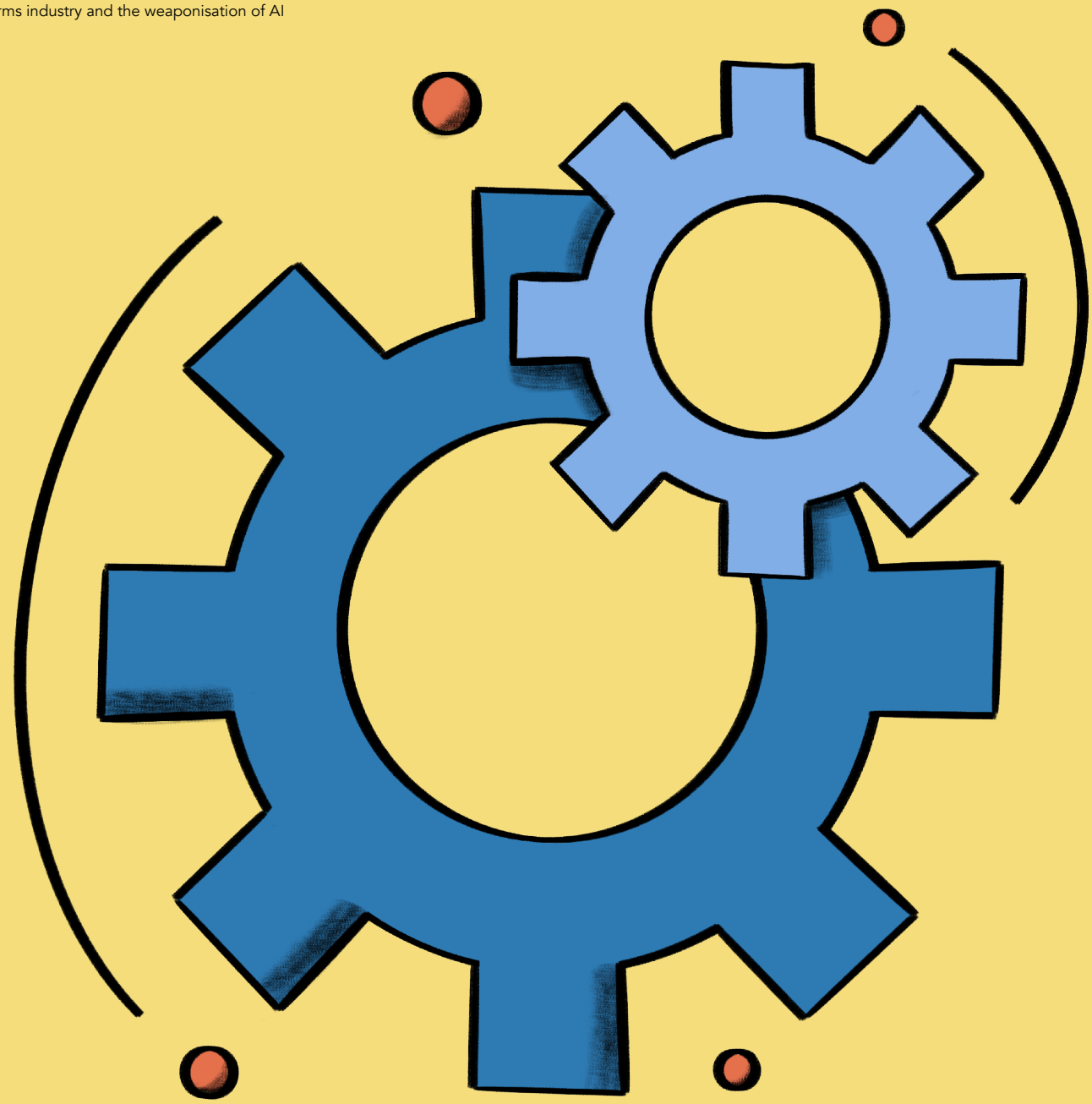
Previously, research from Amnesty International and Breaking the Silence, an Israeli organisation of veteran soldiers aiming to end the occupation, had already revealed details about Israel's extensive surveillance system, including Blue Wolf, an Israeli facial recognition app, used to identify Palestinians, also described as the army's secret "Facebook for Palestinians".[456] Red Wolf is a system of cameras throughout the Occupied Territories to monitor Palestinians. Amnesty calls the surveillance process "automated apartheid".[457] Lastly, White Wolf is a smartphone app used by Jewish settlers in the West Bank to scan and check the identification cards of Palestinians against an Israeli database.[458] These surveillance systems do not stand alone; as the next section shows, they draw on the same commercial cloud and AI services examined here.

6.4 Microsoft

Dozens of units in the Israeli army have purchased services from Microsoft's cloud computing platform, Azure, including the elite intelligence squad, Unit 8200. Other "units revealed to be using services provided by Azure include the Air Force's Ofek Unit, which is responsible for managing large databases of potential targets for lethal airstrikes (known as the "target bank"); the Matspen Unit, which is responsible for the development of operational and combat support systems; the Sapir Unit, which maintains the ICT infrastructure in the Military Intelligence Directorate".[459]

Microsoft has also provided the military with extensive access to OpenAI's GPT-4 language model, the engine behind ChatGPT, thanks to the close partnership between the two companies.[460] Initially, as these reports sparked protests, an internal Microsoft review "did not identify any usage by the IDF that violated the company's terms of service", nor that its "Azure and AI technologies have been used to target or harm people in the conflict in Gaza".[461]

However, further investigations by The Guardian, +972 and Local Call revealed how Microsoft developed a customised version of its cloud platform for Israel's Unit 8200. Unit 8200 "has transferred audio files of millions of calls by Palestinians in the occupied territories onto Microsoft's cloud computing platform, Azure, operationalizing what is likely one of the world's largest and most intrusive collections of surveillance data over a single population group".[462] The system was built to sit on Microsoft's servers behind enhanced layers of security developed by the company's engineers with Unit 8200's instructions. Leaked Microsoft files suggested that a large proportion of the unit's sensitive data were in the company's datacentres in the Netherlands, as was later confirmed by the company.[463] This time, Microsoft launched an external investigation, which eventually concluded that Israel's military use of Azure and AI services had violated its terms of service and therefore had led Microsoft "to cease and disable specified IMOD [Israel Ministry of Defence - FS] subscriptions and their services, including their use of specific cloud storage and AI services and technologies". The message by Microsoft president Brad Smith concluded: "Microsoft will continue to be a company guided by principles and ethics. We will hold every decision, statement, and action to this standard. This is non-negotiable".[464]



Chapter 07

US neo primes: Anduril and Palantir

7. US neo primes: Anduril and Palantir

In this chapter we focus on two companies that have made headlines over the past years for their bold and aggressive way of entering the military market. Palantir and Anduril refer to Tolkien's Lord of the Rings fantasy trilogy. Both were set up with key funding from billionaire conservative libertarian Peter Thiel, the PayPal co-founder, early Facebook investor and initiator of the venture capital Founders Fund. He is also a key adviser to President Trump and is said to have influenced Trump's decision to select J.D. Vance, Thiel's protégé, as his running mate.[465] "Thiel has long expressed a visceral distaste for multiculturalism and progressive politics, and a deep skepticism toward democracy", noted Le Monde.[466]

Palantir and Anduril cooperate and challenge legacy arms companies, especially through their push to "deliver the technological infrastructure, from the edge to the enterprise, that can enable our government and industry partners to transform America's world-leading AI advancements into next-generation military and national security capabilities".[467] Whereas Palantir mostly builds platforms to analyse data, Anduril develops a range of military hardware integrating autonomy and AI. Whereas Palantir has numerous private-sector customers, Anduril fully focuses on the military and law enforcement sector. Where the tech giants discussed in the previous chapters supply general-purpose cloud and AI, Palantir and Anduril are built expressly for war — a new, venture-backed model of defence contractor positioning itself at the centre of US military power.

Besides Project Maven (see box below), the two companies have also teamed up for the US Army's Tactical Intelligence Targeting Access Node (TITAN) program "using artificial intelligence (AI) and machine learning (ML) to enhance the automation of target recognition and geolocation and integrate data from multiple sensors to reduce sensor-to-shooter timelines",[468] building on existing products such as Palantir's AI Platform (AIP) and Anduril's Menace, a "software-defined command and control system".[469] Other subcontractors are Northrop Grumman, L3Harris, Pacific Defense and Sierra Nevada Corporation. Beating rival RTX, in March 2024, Palantir won a USD 178 million contract to build 10 TITAN ground stations, to "connect data-gathering sensors from across multiple domains to shooters in the field to support advanced beyond-line-of-sight targeting".[470] "TITAN provides game changing technologies on how we collect, process and disseminate intelligence across the battlefield, providing us a decisive edge in supporting Multi-Domain Operations", according to the Army's project manager.[471] By 2026, the Army would decide whether TITAN goes into full production. In 2025 Palantir announced that Anduril's Menace had become its preferred hardware solution for Palantir's forward-deployed Edge software.[472]

In December 2024, weeks after Trump's re-election, Anduril and Palantir launched a new consortium "to accelerate AI capabilities for national security", potentially also with others, because "no single company is capable of delivering on the promise of AI for national security. It takes a team of companies that are willing and able to ensure that the U.S. government remains the world leader in fielding advanced technologies that keep our citizens safe".[473]

7.1 Palantir

Founded in 2003, Palantir develops data platforms enabling government agencies and corporations to combine and analyse data from multiple sources. Its flagship product Gotham connects databases to support military and intelligence operations, counterterrorism analysis, law enforcement and enterprise analytics similar to its commercial variant called Foundry. Other products are Apollo and AIP. While the majority of Palantir's revenue comes from the government sector, especially the military, large companies such as BP, Heineken and Stellantis use Palantir software for logistical optimisation and cost savings.

At least until 2020 Palantir never made profits; in fact, it lost as much as around USD 579 million in both 2018 and 2019.[474] In 2020 it commenced trading on the New York Stock Exchange.[475] Palantir has an estimated value of USD 355 billion at the time of writing, making it the 31st biggest company in the world in terms of market capitalisation. That is far higher than Lockheed Martin (USD 144 billion, number 131), the world's biggest weapons producer, or RTX (USD 264 billion, number 54), the arms company with the highest market value.[476] Palantir was worth less than USD 16 billion just in May 2023 and as much as USD 475 billion in November 2025, showing huge growth and volatility at the same time. It reported USD 1.4 billion in revenue in the fourth quarter of 2025, a new record and 70 per cent higher than in the same period a year earlier.[477] It has also become profitable at last, generating a record USD 609 million profit in that same quarter.

While its products are praised for their efficiency in fraud detection and military logistics, critics stress that Palantir's collaboration with ICE and other US law-enforcement agencies contribute to breaches of civil liberties in the hunt for illegal immigrants.[478] Palantir maintains it does not own or store client data, but its role as data processor of sensitive information has led to accusations of data abuse. Palantir says it does not do business with the tobacco industry and in countries that it considers adversarial, namely China and Russia; it also rejected a lucrative deal with the Saudi government because of its human rights record.[479]

Palantir amplifies its users' intentions and biases, helping them make more precise decisions for better or worse, while its polished, warfare-inflected interface can make conclusions feel objective and a person's data feel like their whole life story - a tool, in one former employee's words, that could be very dangerous in the wrong hands.[480]

Not so strange then, that significant UK National Health Service (NHS) contracts for Palantir

have long caused controversy.[481] According to Elke Schwarz, professor of Political Theory at Queen Mary University in London and expert on the ethical implications of AI in war, "European countries and companies that engage with Palantir should be more aware that this company was founded to defend American interests".[482] According to her, the company benefits from as much conflict in the world as possible and is more than ever at the centre of political power.

Military applications

Karp mentioned in a 2019 Washington Post Op-Ed that Palantir "was founded after 9/11 with a commitment to helping those on the front line use data analytics to protect the United States while putting in place privacy protections others thought impossible to achieve."[483] Indeed, early users of Palantir software include the NSA, the FBI and the CIA (an early investor through its In-Q-Tel venture fund) along with other US counterterrorism and military agencies. Its software is reported to have played a role in tracking and killing of al-Qaeda leader Osama bin Laden in 2011.[484] French intelligence turned to Palantir following the November 2015 terror attacks in Paris. Karp claims that Palantir has helped prevent several attacks, including one or two that could have had major consequences. With no lack of modesty he said in 2020: "I believe that Western civilization has rested on our somewhat small shoulders a couple of times in the last 15 years".[485]

During Trump's first term as president, Palantir managed to position itself deep into the Pentagon, with at least three close associates working for the Defense secretary.[486] Karp's senior advisor Jacob Helberg used to be commissioner for the U.S. - China Economic and Security Review Commission, during which he pushed for measures to curb Chinese influence over TikTok.[487] He became Under Secretary of State for Economic Growth, Energy, and the Environment in the second Trump administration.

Palantir became involved in the infamous Project Maven in 2017 and has taken the lead after Google's withdrawal in 2018 until today. In its early years, Maven contracts amounted to an estimated USD 40 million annually. Palantir provides software that can automatically identify buildings, vehicles and people in enormous amounts of video footage captured by US drones (called object detection).[488]

In 2016, Palantir successfully sued the US Army over its procurement strategy for the Distributed Common Ground System (or DCGS-A, for Army), which would favour legacy military contractors – in this case RTX (then Raytheon).[489] It subsequently won the contract, potentially worth more than USD 800 million, in 2019.[490] At the time, it was said it was the first time that the government had tapped a software company, rather than a traditional military contractor, to lead such a large military project.[491] Ever since Palantir has secured countless more multimillion-dollar contracts. DCGS-A lets users gather and analyse information about enemy movements, terrain and weather to create detailed maps and reports in real time. The system is designed to be used by soldiers fighting in remote, harsh environments. Apparently considered successful, Palantir netted an USD 823 million DCGS-A follow-on contract in October 2021.[492]

Late 2019 it won an initial USD 110 million contract, as part of a four-year, USD 440 million program called Vantage, formerly known as Army Leader Dashboard, aimed at piecing together "thousands of complex data sets containing information on U.S. soldiers and the expansive military arsenal that supports them".[493] The contract was extended in 2024 for USD 400 million for a period of four years and could be worth USD 620 million if additional options are exercised.[494] By late 2024 Vantage had over 100,000 users within the US military and growing, according to Palantir.

By 2020 Palantir made clear it wanted to become "the central operating system for all U.S. defense programs".[495] A next step in that mission was the USD 111 million contract won in 2021 "to provide enterprise data management and more to U.S. Special Operations Command".[496] It won at least three more (battlefield) information-management contracts in 2021, including one with BigBear.ai.[497]

In an April 2023 review of Palantir's AI platform AIP, as presented in a promotional video, Vice journalist Matthew Gault describes how an operator uses a chatbot to order drone reconnaissance, generate plans of attack and organise the jamming of enemy communications. "While there is a "human in the loop" in the AIP demo, they seem to do little more than ask the chatbot what to do and then approve its actions." According to the video, users have control over what every LLM and AI in the Palantir-backed system can do. The system keeps a secure digital record of operations, which Palantir says is crucial for managing significant legal, regulatory and ethical risks in sensitive, classified settings. But as Gault points out: "What AIP does not do is walk through how it plans to deal with the various pernicious problems of LLMs and what the consequences might be in a military context. AIP does not appear to offer solutions to those problems beyond "frameworks" and "guardrails" it promises will make the use of military AI "ethical" and "legal.""[498]

In September 2023, the US Army awarded Palantir a three-year contract worth USD 250 million to research and experiment with AI and machine learning.[499] In July 2025, the US Army announced that it was converting all Palantir's 75 separate contracts into one single Enterprise Agreement. "This contract allows the government flexibility to purchase goods and services as needed, resulting in significant cost efficiencies across mission-critical programs. The agreement establishes volume-based discounts for the contract's performance period of up to 10 years. The Army and other Department of Defense agencies have the option to purchase Palantir's commercial products during that period, not to exceed the $10 billion cap. This amount represents the maximum potential value of the contract, not any specific obligations or commitments."[500]

In September 2025, the UK government signed a partnership deal with Palantir, worth up to over USD 2 billion to develop AI-powered capabilities, already tested in Ukraine, "to help accelerate decision making and improve targeting, analysis, intelligence, and military planning".[501] It will also support the development of the so-called 'kill chain', of sensors, command-and-control, and munitions capability.

Cooperation with legacy arms companies

A testament to how Palantir has built its reputation is its more recent close cooperation with the big arms-producing companies it used to denounce for their lack of competitiveness. In 2022, Palantir and Lockheed Martin partnered to develop an "autonomous deployment model" for future combat system software updates, rather than traditional in-port modernisation.[502] As mentioned just above, Northrop Grumman became subcontractor to the Palantir-led TITAN programme.[503] Palantir is a key subcontractor for Northrop's Lumberjack one-way attack drone.[504] More significantly, in September 2025, Boeing and Palantir announced the two companies are working together to integrate AI systems and software across Boeing Defense, Space & Security factories and programs. "This collaboration is a natural fit that brings together two great companies with a common mission: supporting uniformed personnel in protecting freedom around the world", said Boeing boss Steve Parker. In addition, Boeing has tapped Palantir to provide AI expertise and capabilities "on a number of undisclosed classified and proprietary efforts focused on supporting military customers' most sensitive missions".[505]

Global footprint examples

In June 2022, a few months into Russia's full-scale invasion, Palantir visited Ukraine. "„We are at risk of being wiped off the map", president Zelensky told them, „We need your software to prevent that." And Alex Karp said: you can have it."" Ukraine subsequently got access to Palantir's MetaConstellation program, which enables the country to live-stream battlefield scenarios using satellite imagery. That information is merged according to reports with military data from the US and its allies, helping the Ukrainian military better identify targets and enemies, as the Dutch daily NRC recounts.[506] Palantir has now an office in Kyiv and more recently it has partnered with the Ukrainian government-backed military technology cluster, Brave1 to create the Dataroom, a platform where artificial-intelligence models can be tested using data on Russian aerial threats collected by the country's military "with the goal of equipping interceptor drones with AI to enhance their target detection, classification and neutralization capabilities".[507] "In the future, we plan to expand the Dataroom's abilities to other areas related to autonomy and AI – but for now, our focus is on the most urgent task: countering the threats that appear in our skies, Shahed-type drones," according to Mykhailo Fedorov, the Ukrainian Minister of Defence.[508]
The Israeli government has also been a client of Palantir for years and Palantir is "proud to stand alongside Israel. […] There is no multinational company that has expressed such

strong and clear support for Israel," said Ayelet Gilan, general manager of Palantir Israel, in an interview with Forbes.[509] He emphasised that the support to Israel is disconnected from his business considerations. "[After October 7,] demand for our products skyrocketed dramatically. Suddenly all doors opened," the general manager of Palantir Israel, Ayelet Gilan, told Forbes Israel in November. "A rare opportunity for collaborations was created here, and we managed to create relationships that led to joint projects".[510] In January 2024, three months into the genocide in Gaza, Palantir agreed a "strategic partnership" to "harness Palantir's advanced technology in support of war-related missions".[511] The same week Palantir held a board meeting in Tel Aviv "in solidarity with Israel".

A June 2025 report to the UN Human Rights Council by the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, found "reasonable grounds to believe Palantir has provided automatic predictive policing technology, core defence infrastructure for rapid and scaled-up construction and deployment of military software, and its Artificial Intelligence Platform, which allows real-time battlefield data integration for automated decision-making".[512] When a protester accused Alex Karp that „Palantir's technology kills Palestinians", Karp responded, „Mostly terrorists. That's true."[513] „We support Israel as an American ally. For us, nothing has changed since October 7", explained Courtney Bowman, Head of Privacy and Civil Liberties at Palantir in 2025.[514] Palantir has reportedly provided the technological architecture for tracking the delivery and distribution of aid to Gaza at the US-led Civil Military Coordination Center (CMCC) in southern Israel, which was supposed to serve as the so-called Board of Peace's operational headquarters.[515]

Ethical policies

About its responsibility in the use of its products, and if things go 'wrong', Palantir says: "Then we discuss it with the client. Oversight is not our role, but that of the government."[516] Palantir claims to "abide by the law and to build its software in a way that respects privacy and human rights. At the same time, it says it cannot prevent its software from being used in situations where human rights are violated. In theory, Palantir could terminate contracts with clients who misbehave. Bowman calls this „the nuclear option." To his knowledge, Palantir has never used it."[517]

On its website, Palantir outlines "a set of principles that help us ensure we are doing so responsibly" and recognising that its technology "does not exist in vacuum, but rather is inextricably tied to its contexts of application, its operational uses, and the full data operating environment that surrounds the much narrower AI components that tend to dominate the discourse of AI Ethics".[518]

These principles include: systems should embed privacy by design; decisions affecting people's freedom, opportunity and happiness should not be left to computers alone; systems must enable accountability and oversight; and technology is not the answer to every problem. On the latter it elaborates: "Some decisions carry implications that are too complex or significant to be automated or streamlined, even with a human in the loop. We

strive to contextualize major world problems and think critically about whether it's possible to engineer complementary solutions in an ethically responsible way. When the answer is no, we turn the opportunity down."[519] Furthermore, Palantir refers to seven principles guiding its AI ethics, including "Don't solve problems that shouldn't be solved" and "Promote multi-stakeholder engagement".[520]

Palantir acknowledges its corporate responsibility to endeavour to protect human rights. Its global human rights policy "is informed by our 20+ years of experience in complex problem solving around the world" and "based on international human rights laws and guiding principles as defined by the United Nations and other recognized institutions", including the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises.[521] Its policy implementation raises numerous questions, not least regarding its position on Israel and Palestine, and human rights more broadly. Already in 2020, Amnesty International called out Palantir for failing to fulfil its human rights due diligence obligations under international standards.[522] US consultancy firm MSCI rated it 2 out of 10 on "civil liberties" and "human rights concerns" in a November 2025 report.[523]

European investment into Palantir

Apparently attracted by its shareholder value, more than 100 major European banks, asset managers, insurers and pension funds had by the end of 2025 increased the aggregate number of Palantir shares they held by almost 70% compared to the year before, to reach at least USD 27 billion.[524] Some however have started reconsidering their portfolio because of human rights considerations. In October 2025, Norwegian Storebrand Asset Management disclosed that it had excluded Palantir from its investments "due (to) its sales of products and services to Israel for use in occupied Palestinian territories […] including AI-based predictive policing systems" that support Israeli surveillance of Palestinians in the West Bank and Gaza.[525] Storebrand said Palantir had not replied to any of its requests for information. Luxembourg-based asset manager Candiam has also divested from Palantir; Belgian bank KBC did so partially.[526] Most significantly, ABP, the largest Dutch pension fund announced divesting its estimated EUR 825 million in shares after facing sustained criticism regarding its ethical policies.[527]

In focus: Project Maven

A well-known project where Anduril[528] and Palantir cooperate is Project Maven, which in 2018 became the subject of a major controversy, primarily set off by the participation of Google, and the workers there who started protesting the work that was closely linked to assassinating and bombing suspected ISIS terrorists in Iraq and Syria.[529] While Anduril was taking part from the start of the project – also known as the Algorithmic Warfare Cross-Functional Team (AWCFT) – Palantir stepped in after Google left. Maven has long been the Pentagon's most visible AI project.[530]

"Maven is designed to be that pilot project, that pathfinder, that spark that kindles the flame front of artificial intelligence across the rest of the [Defense] Department",[531] according to then US Air Force Lt. Gen. Jack Shanahan in 2017. Maven was a crash programme designed to deliver AI technologies, specifically computer-vision technologies built on deep-learning neural networks, to an active combat theatre within six months from when the project received funding. Spread over three phases, it was meant to first acquire data labelling algorithms, then to acquire the hardware and software necessary to make it happen, to finally put the technology into existing intelligence projects.[532]

The Pentagon established the program as an effort "to accelerate DoD's integration of big data and machine learning. . .[and] to turn the enormous volume of data available to DoD into actionable intelligence and insights at speed".[533] The Bulletin of the Atomic Scientists summarises the problem: "US spy planes and satellites collect more raw data than the Defense Department could analyze even if its whole workforce spent their entire lives on it. Creating algorithms to sort and analyse the images made sense".[534] "Once we show success, people are going to say what else can we apply this to," said Shanahan at the time. "To me that breaks things wide open and we're going to figure out how we really, at scale, bring in some of these capabilities into the department."[535]

Google and Project Maven

The Pentagon had contracted Google for Project Maven in September 2017. According to internal emails from Google executives, the deal was worth at least USD 15 million, with the potential to increase to as much as USD 250 million. At Google there was no lack of ambition, going beyond what was in the Pentagon's initial announcements, such as the suggestion of creating a Google-earth-like spy system giving users the ability to "click on a building and see everything associated with it", including people and vehicles.[536] At the same time Google was aware of a PR problem if the project became publicly known. "WeaponizedAI is probably one of the most sensitized topics of AI — if not THE most. This is red meat to the media to find all ways to damage Google. You

probably heard Elon Musk and his comment about AI causing WW3", wrote the chief scientist for AI at Google Cloud at the time.[537]
When that media storm (and internal opposition[538]) indeed became very strong during the spring of 2018[539], Google rather quickly made a U-turn that June, announcing its AI principles and deciding to stop its involvement after their contract would expire the following year (see section on Alphabet).[540] Karp referred it saying that if the "Google standard takes hold, the single biggest strategic asset America has, which is our ability to produce software platforms, will be taken out of the hands of our war fighters. And that de facto means our adversaries are in a much stronger position".[541]

Apart from Google and Palantir, many other contractors have been or were also involved in Maven, including ECS[542] and Booz Allen Hamilton, with subawards to companies including Microsoft, Clarifai[543], Rebellion Defense, Cubic Corporation and SAP National Security Services.[544] Also Maxar has long been working on Maven, "providing low-latency imagery so that we can run the algorithms against the imagery in a sensor-to-shooter methodology that really resonates with the warfighter".[545]

Within a year after the Pentagon launched Project Maven, the military was using the programme's algorithms to support drone missions against ISIS in Iraq and Syria and a few other countries in the region.[546] By 2022 Maven was also used in the war in Ukraine to improve the AI algorithms, for example to recognise destroyed equipment.[547]
Project Maven evolved from experimental pilot to become the DoD's main AI tool for intelligence and targeting.[548] For its spin-off, the Maven Smart System (MSS), a "data analysis and decision making tool", Palantir was awarded a five-year, USD 480 million contract in May 2024, to expand its user base from a few hundred to tens of thousands of US military users across the globe.[549] Just a year later, the Pentagon further increased its budget on MSS with USD 795 million to nearly USD 1.3 billion through 2029.[550] In 2025, Palantir's Maven Smart System was also adopted by NATO's Allied Command Operations, "marking a significant advancement in the modernization of NATO's warfighting capabilities".[551]

As Shyam Sankar, Palantir's CTO put it: "With Maven, you can perform targeting operations with 20 people that used to take us 2,000 people in Iraq. So that sort of efficiency really drives the ability to hide in a pure conflict. You're much smaller, [there's a] much smaller footprint, less support infrastructure, and [that] drives lethality".[552] In the words of Cameron Stanley, the Department of War's

Chief Digital and Artificial Intelligence Officer, describing use of MSS as simple as: "left click, right click, left click" to target anything or anyone for a military strike.[553]

7.2 Anduril

Anduril Industries was co-founded in 2017 by vocal Trump supporter Palmer Luckey, Trae Stephens (ex-Palantir, Founders Fund partner and currently Anduril's chairman), Matt Grimm, Joe Chen and Brian Schimpf, its current CEO. As outlined earlier under Meta, Luckey is the inventor of the Oculus Rift VR headset and Facebook bought his company for USD 2 billion in 2014. Luckey stayed with Facebook but was fired in 2017, after which he set up Anduril. Luckey said he started Anduril to save US taxpayers hundreds of billions of dollars while making tens of billions of dollars per year.[554]

The company's focus is on military artificial intelligence, autonomous systems and robotics, including uncrewed aerial systems (UAS) as well as counter-UAS, and networked command and control software. More recently it has started working on traditional military products as well, from cruise and hypersonic missiles to rocket motors and spacecraft.[555] Anduril has so far only produced small numbers of weapons for the military and some drone and missile tests that the company conducted in Ukraine in recent years were disappointing, as a New York Times article mentions.[556]

Regardless, it has seen its orderbook expanding rapidly, especially since 2024, and it continues to successfully tap new capital to enable its steep growth curve. After a string of take-overs, including Area-I (loitering munitions), Dive (uncrewed submarines), Copious Imaging (sensors), Blue Force (UAS) and Adranos (rocket motors), it has more than 7,000 employees. Moreover, it has recently opened its USD 1 billion 'Arsenal' hyperscale factory in Ohio, where it may eventually employ another 4,000 workers, starting with roughly 250 by the end of 2026, initially building Fury autonomous combat aircraft (see below).[557] "When we say hyperscale, we mean the ability to produce tens of thousands of a given system," said Chris Brose, Anduril's Chief Strategy Officer.[558]

In March 2026, Anduril had more than USD 6 billion in global contracts with some USD 2 billion in revenue in 2025. It has raised almost USD 7 billion from investors, including from early backers the Founders Fund and Andreessen Horowitz. It is valued at almost USD 31 billion and is considering going public.[559]

In 2018, in an opinion piece in The Washington Post, Luckey and Stephens claimed: "The world is safer and more peaceful with strong U.S. leadership. That requires the U.S. government to maintain its advantage in critical technologies such as AI. But doing so will be difficult if Silicon Valley's rising hostility toward working with Washington continues" -

referring to Google's announcement to discontinue working on Project Maven.[560] They went on writing that tech workers want to build things that help rather than harm, but ostracising the US military would be counter-productive: firms that want to promote peace should stand with America's defence community, not against it.[561]

In another self-promotional opinion piece from 2021, Schimpf put forward Anduril's vision that the traditional arms industry is not innovative enough and too costly: doubling down on existing systems would play into China's hands; that AI is the missing ingredient that can scale today's largely crew-dependent unmanned systems; and that the US could trade its few exquisite platforms for swarms of cheaper autonomous systems - what DARPA calls "mosaic warfare" - operating with far less human oversight.[562] As part of Anduril's production strategy, about 90 per cent of its products use commercially available components and materials to reduce timelines and save on production costs.[563]

Last but not least, using bombastic, scare-mongering language Anduril has set out its view of how the US security policy and with that the US arms industry have failed to stay ahead of the curve in terms of (production) technology - and how Anduril would solve it - in their 2022 "Rebooting the Arsenal of Democracy: Anduril Mission Document".[564] Ignoring the global dominance of both the US military apparatus with its unprecedented budget (higher than the combined spending of the next six countries with the highest military budget: China, Russia, Germany, India, UK and Ukraine[565]) and its arms industry, both in terms of output[566] and export share,[567] Anduril paints a picture of a country overshadowed by its main rival China. Trump's latest budget proposal, increasing Pentagon spending by 50 per cent to USD 1.5 trillion, and the unprecedented focus on autonomous systems, would make you believe that Anduril's message has landed well in Washington.

In focus: Anduril's products

Anduril's legacy product is Lattice, which ingests data from disparate sensors and systems into a single integration layer, where AI and machine learning filter high-value information for users, and now acts as an AI-enabled integration and network layer across many legacy systems, automating hundreds of deployed robotic systems.[568] In 2022, Luckey said: "Lattice is... at the core of everything we do. About two-thirds of our 1,350 are working on software; it's very expensive to develop but once it's developed it's free to keep producing, and in the long run, it's cheaper than hardware […]. Lattice has cost us hundreds of millions of dollars to develop but the US defence primes would have spent billions doing the same".[569]

Lattice, for example, is connected to its Sentry Towers (sold in large quantities to the US Customs and Border Protection), which according to Anduril, "autonomously provides operators with the real-time intelligence they need to detect, identify, and track objects of interest, saving manpower and cost spent on manual surveillance".[570] The company promises that sentry towers can make a virtual wall, tracing people even well beyond the US-Mexican border and up to "100 miles into the US interior and includes highway checkpoints, predator drones, licence plate readers, facial recognition, ground sensors, and mobile surveillance mounted on vehicles, not to mention the digital tracking of

migrants in detention".[571] Anduril has also developed a version to "autonomously identify, classify, detect and track multiple cruise missiles".[572] In 2023, it unveiled its Lattice for Mission Autonomy software, which "serves as a central node for threat identification, electronic signature management, manoeuvring and more". It simplifies the management of potentially hundreds of drones and robots, with fewer people dedicated to oversight, according to CEO Schimpf.[573]

In 2022, Anduril revealed its first loitering munitions, or one-way attack drones, the Altius-600M, originally developed by drone-maker Area-I, which it bought in 2021. "Shot from a tube like a missile, first its wings telescope outwards, then it identifies its target, flying for up to 280 miles. It circles high in the sky, for as long as four hours, and then strikes on the ground. The "M" is for munitions; on impact it explodes in a ball of flames".[574] The Pentagon has bought hundreds of Altius-600Ms as aid to Ukraine. In March 2025, the UK government announced that the UK branch of Anduril would supply Ukraine with some EUR 35 million worth of Altius-600M and Altius-700M loitering munitions.[575] The larger 700M LM variant can carry warheads up to 15 kg. According to the UK MoD, Anduril "continues to invest significantly in the UK with a large footprint across the country and plans to rapidly scale, in line with the government's commitment to keeping the nation safe while providing highly skilled jobs".[576] Taiwan is another Altius-600M customer.[577]

In 2024, Anduril also launched Bolt, a quadcopter drone for surveillance and one-way strike missions (the latter called Bolt-M). The drone can carry a payload of up to three pounds and can shift between warheads intended to strike personnel and equipment, designed in partnership with Kraken Kinetics, based in North Carolina.[578]

Cooperation with companies

Despite criticising their lack of innovative thinking and addiction to traditional big hardware systems, Anduril has apparently realised that it needs those dinosaurs to fuse its software with their hardware capacities. German company Rheinmetall and South Korea's Hanwha, have each partnered with Anduril to develop robotic ground vehicles.[579] With South Korean shipbuilder HD Hyundai Heavy Industries it is teaming to develop and produce crewed and uncrewed platforms. Chief Strategy Officer Brose calls the companies "phenomenally complementary".[580] Saab contracted Anduril to design and build solid rocket motors for its Ground-Launched Small Diameter Bomb, its first major contract in that area.[581]
The UK branch of Anduril works with several companies there, including with GKN on the British Army's combat drone (Project NYX) and has secured contracts with the Royal Marines and Strategic Command.[582] In Japan, Anduril works with Sumisho Aero-Systems to demonstrate its Lattice software to the Japan Maritime Self-Defense Force.[583] Late 2025, Anduril announced a new

cooperation with Boeing to jointly offer a new interceptor missile for the US Army.[584]

Military contracts

In 2021, Anduril won a five-year contract up to USD 99 million to make its counter-drone artificial intelligence technology available across the US military. "This award is precisely the kind of contract vehicle DOD should be issuing to help companies bridge the Valley of Death", Anduril said, referring to difficult access to military customers by start-ups. "This process is repeatable, and it is one the Department should do more".[585] In January 2022, US Special Operations Command picked Anduril to lead its counter-drone systems integration work ("for special operations forces wherever they operate") in a ten-year, USD 1 billion deal.[586]

In March 2022, shortly after acquiring Dive Technologies, Anduril Australia signed a USD 96 million contract with the Australian DoD to co-fund the design, development, and construction of three prototype extra-large autonomous underwater vehicles (XLUUVs), big robotic submarines, within three years.[587] In August 2025 a follow-on order worth about USD 1.1 billion for a "fleet" of these Ghost Shark XLUUVs was signed.[588] Anduril also has a Ghost Shark production facility in Rhode Island. In March 2026 it was selected by the US Navy and the Pentagon's Defense Innovation Unit (DIU) to develop an extra-large unmanned underwater vessel as part of the Combat Autonomous Maritime Platform Project (CAMP).[589]

In April 2024, Anduril's Fury or YFQ-44A, together with General Atomics' Gambit, were selected as two contenders to prototype a new kind of uncrewed, autonomous combat aircraft called Collaborative Combat Aircraft (CCA) for the US Air Force and Navy. Legacy arms producers Boeing, Lockheed Martin and Northrop Grumman lost out.[590] A production decision for up to 100 CCA to be delivered by 2029, is expected in the second half of 2026.[591] CCAs will be highly autonomous, flying with minimal direction from the pilots they accompany, and will be able to carry out missions such as airstrikes, electronic warfare or intelligence gathering.[592] "This is a new age of air power […] There is no operator with a stick and throttle flying the aircraft behind the scenes", said an Anduril director after the first flight test in October 2025.[593]

In October 2024, Anduril won a Pentagon contract worth USD 250 million to counter drone attacks against US forces, buying 500 of its recoverable Roadrunner interceptors as well as its portable Pulsar, which can be integrated with aircraft to jam enemy systems.[594] In December 2024, the Pentagon's Chief Digital and AI Office awarded Anduril a three-year, USD 100 million agreement to scale its "edge data integration services capabilities" for the US military. "The mesh is already operational across multiple services and combatant commands, delivering critical data that enables mission-relevant generative artificial intelligence (AI) solutions specifically tailored to the unique requirements of the warfighter. This agreement will accelerate the expansion of the mesh to increase access to

decentralized, distributed and disconnected systems, and to power new insights and real-time decision making at the edge," Anduril said in a press release.[595]

In March 2025, Anduril won a potential ten-year, USD 642 million contract from the US Navy to install, deliver and sustain Installation-Counter small Unmanned Aircraft Systems (IC-sUAS) at Marine Corps bases worldwide.[596] In July 2025, Anduril was selected by the US Army to lead a consortium with Microsoft, Palantir and others to "deliver a next-generation command and control (NGC2) prototype" and to "create an ecosystem that can rapidly integrate a range of technologies into a singular architecture so that soldiers can access various kinds of compute, communications and information processing capabilities all at once".[597] The contract's value is nearly USD 100 million.

Also in 2025, Anduril took over the lead of the Integrated Visual Augmentation System (IVAS) from Microsoft, which stays on as Azure cloud provider and with Meta joining, as also referred to under Section 4.4 on Microsoft and Section 4.3 on Meta.[598] Relatedly, in September 2025, the US Army awarded a USD 159 million contract to Anduril to develop wearable virtual displays as part of the service's Soldier Borne Mission Command (SBMC) programme. Under the same programme, Palantir-funded start-up Rivet got a USD 195 million contract. SBMC is the follow-on project to IVAS, which is only a headset, while SBMC includes complementary computers and wearables like watches. Anduril has dubbed the new line of mixed-reality heads-up displays EagleEye.[599]

In November 2025, another US Army contract (of undisclosed value) was awarded to Anduril, this time to provide the networking backbone for the counter-UAS element of the service's Integrated Battle Command System (IBCS). The Lattice Mesh networking software will manage sensor data fusion and automated fire-control capabilities, and hasten the UAS kill-chain "from detection to defeat", according to a company statement.[600]

UAE state-owned Edge Group and Anduril announced the Edge-Anduril Production Alliance in November 2025, initially aimed at producing the Omen UAS, of which the UAE ordered 50 systems.[601] "Powered by Anduril's Lattice for Mission Autonomy software, multiple aircraft will co-ordinate flightpaths, share sensor data, and adapt behaviour in real time, enabling new missions that bring the capabilities of much larger systems to smaller, more expeditionary units", according to Anduril.[602] Edge-produced military equipment has been spotted in Sudan's ongoing civil war, adding to evidence of UAE support to the Rapid Support Forces (RSF).[603]

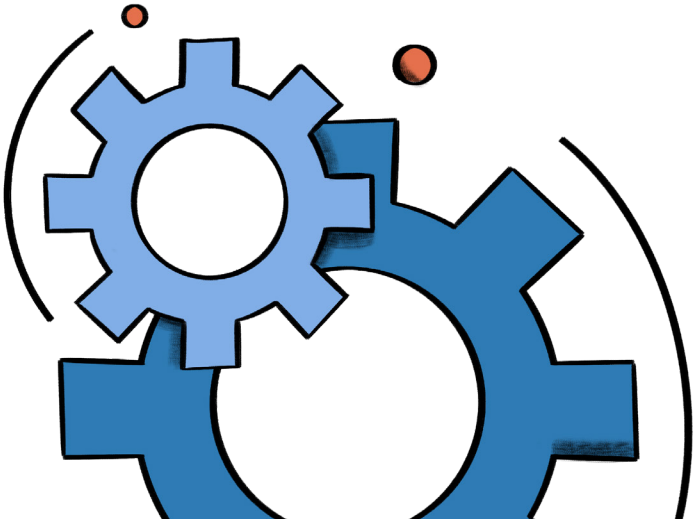
In February 2026, Luckey visited Israel's prime minister Netanyahu, senior military officials and executives at Israeli military and tech companies, including Kela, G2, Axon Vision, Asio Technologies, Smart Shooter and Extend.[604] Asio had already signed an agreement with Anduril to supply components for its drones.[605]

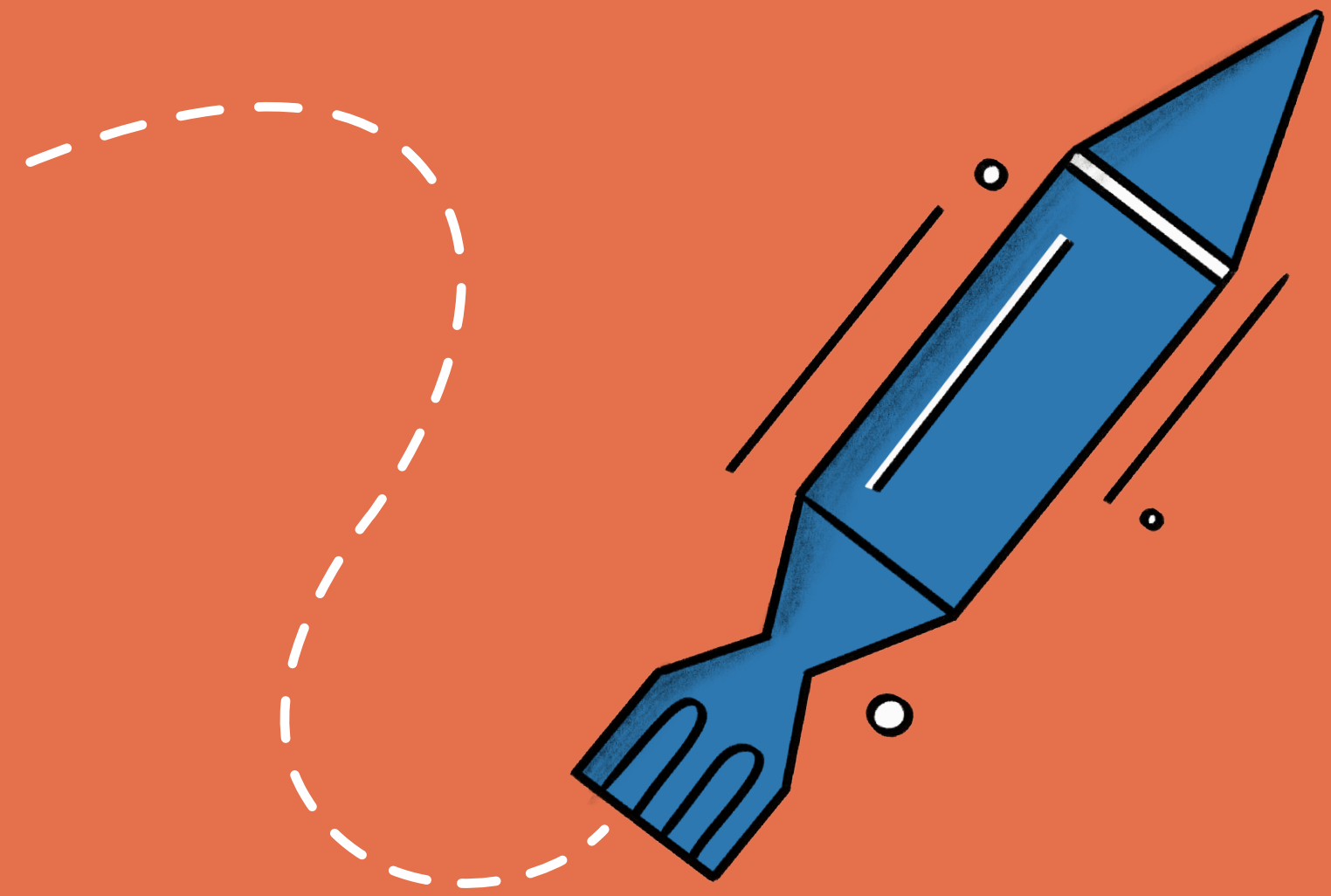
Ethical policies

CEO Schimpf, addressing US Senate in December 2023, wrote:

- "Determining the moral, legal, and ethical standards of AI use on the 21st century battlefield is too important to leave to our adversaries. We must build the critical AI capabilities that our warfighters need for defense and deterrence while simultaneously defining the international rules of the road, which must be grounded in American democratic values.
- Make no mistake: today's most pressing national challenges cannot be solved without AI-enabled systems and autonomy at scale. These systems will help to keep our service members safe and empower them to make better decisions at the speed of modern warfare.
- As you consider future policy frameworks, I would encourage you to consider three main points that will strengthen our national security with AI tools:
- Enable greater adoption of AI-enabled technology and begin fielding it at scale,
- Focus policy making and regulation on how AI-enabled military systems are employed rather than how they are developed, and
- Ensure a wide array of operational end users and defense technology leaders have a seat at the table when shaping policy on the use of AI by the Department of Defense (DoD)."[606]

Apart from the above and similarly phrased quotes by Anduril executives,[607] the company does not appear to have standalone ethical, human rights or responsible AI policy like most other big companies in the tech and arms sectors have.





Chapter 08

Arms industry primes: autonomous weapons and data-intensive technologies

8.1 BAE Systems
8.2 General Dynamics
8.3 Lockheed Martin
8.4 Northrop Grumman

8. Arms industry primes: autonomous weapons and data-intensive technologies

In this chapter we look at the five biggest arms-producing companies in the world - Lockheed Martin, RTX, Northrop Grumman, BAE Systems and General Dynamics - all of which are working on increasingly autonomous weapon systems, such as collaborative combat aircraft (CCA) and loitering munitions or one-way attack drones.[608] These legacy primes have always been in the business of aircraft and munitions, where over time new levels of automation have been introduced, from pilotless flying to increased levels of autonomy in the so-called kill-chain, where attacks can take place with minimal to no involvement of humans. These are often referred to as AI-enabled weapons, aimed at increased precision, speed and scalability.

Over the past fifteen or so years these companies have set up dedicated autonomous weapons divisions, reflecting the importance of this emerging technology. While the difference between propaganda and what these capabilities mean in practice is often unclear, what is clear is that these technologies keep evolving and have been seen used and tested in combat in recent wars.

As we have already seen in previous chapters, arms-producing companies and software companies are rapidly cementing ties through partnerships and common production, starting to fundamentally change the arms industry as we know it by fusing the tech and military sector.[609]

8.1 BAE Systems

BAE Systems is a British multinational aerospace, arms and information security corporation. It is the fourth largest military contractor in the world and the largest outside the US. As of 2025, it operates with 114,400 employees in more than 40 nations.[610] Its 2025 military revenue stood at USD 37.4 billion, with USD 2.7 billion net income.[611] BAE Systems attained 95.4 per cent of its revenue from military activities, according to SIPRI.[612] BAE Systems is involved in the production of most major weapon systems, from warships and artillery to fighter jets, as well as intelligence and cybersecurity services.[613]

Military AI, autonomous weapons contracts

BAE says that as warfare is evolving, drone autonomy is now essential, while still maintaining meaningful, context-appropriate human decision-making; and that this requires advanced AI, resilient navigation and robust decision-making so that drones stay effective in contested environments, whether on surveillance, precision strikes or logistics. They continue: "Autonomous drones are not just about maintaining an edge - they are about redefining how military operations are conducted. Whether it's conducting surveillance, delivering

precision strikes, or supporting logistics in hostile environments, autonomy will help drones remain effective even when manual control is blocked".[614]
While BAE Systems has never been a major drone producer, it has developed several concepts, the best known probably being the Taranis, developed as demonstrator in the 2010s.[615] A more recent development is its "attritable autonomous collaborative platform" known as Concept-2, shown at a Saudi arms fair in 2024.[616]

Since its acquisition of drone company Malloy Aeronautics in 2024, it has taken up work on arming drones, such as the TRV-150 multi-rotor drone to launch BAE's APKWS guided rockets. "Providing medium UAS-delivered air and ground target strike capability will be a force-multiplying game changer and we are excited to play a role in bringing this new capability to our US and allied-nation warfighters", according to the president of SURVICE Engineering, BAE's partner in the project.[617]

Back in 2017, SIPRI labelled another BAE munition, the Dual Mode Brimstone, as "the only guided munition featuring target selection autonomy that is currently operational. It works like a fire-and-forget missile. Once launched, the missile operates in full autonomy; it does not include a human-in-the-loop mode".[618] In December 2025, BAE announced its newest AI-enabled target recognition technology for land vehicles to detect all kinds of ground threats.[619]

In March 2026, it further announced a "strategic" collaboration with Scale AI to speed the development and fielding of advanced AI for the US Department of War, combining BAE's defence-systems expertise with Scale's Data Engine and Generative AI Platform to embed AI in the department's most capable current and future platforms and systems.[620] "Modern warfare is won at the speed of data," said Peder Jungck, Chief Innovation & Strategy Officer for the Intelligence & Security sector at BAE Systems. "By teaming with Scale AI, we are ensuring that the Department of War has access to the world's most advanced AI tools, to create intelligent, adaptive systems that can out-think and out-pace the adversary."[621] This collaboration appears to conflict with ethical positions on AI and autonomy that BAE has taken over the past decade or so, as described below. In 2025, Meta acquired a 49 per cent stake in Scale AI, whose CEO is known as a strong proponent of weaponising AI (more above in Section 4.3 on Meta).

The US branch of BAE Systems has a dedicated 'Intelligent Autonomous Systems R&D' webpage elaborating how "ahead-of-the-curve Autonomy R&D" keeps its customers ahead of their opponents and that its "unparalleled autonomous solutions deliver on land, at sea, in the air, in space, and beyond".[622]

One example of such systems is its "advanced All-Source Track and Identity Fuser (ATIF) technology", a data fusion system designed "to detect, process, and report on adversary combat capabilities across surface, ground, air, missile, maritime, and space domains".[623] According to BAE, ATIF uses AI and "autonomy technology to enable tracking and identification of adversaries and their military or intelligence resources by fusing multiple intelligence […] sources", including radar, image and signal intelligence data. One of

the key benefits mentioned is that ATIF software "improves target identification". ATIF is used under several unspecified programmes for the US DoD, Department of Homeland Security (DHS) and various intelligence agencies. BAE's IntelligenceReveal is another tool to "transform data into digital intelligence", supporting "agencies in the legal acquisition, collation, processing, storage, analysis and sharing of IP Metadata".[624]

Enabled with DARPA funding is the Multi-domain Adaptive Request Service (MARS) software and battle management application developed in 2019-2020 with Carnegie Mellon University, to leverage artificial intelligence (AI) technologies to consolidate and co-ordinate multi-domain combat assets into a single command picture, according to a BAE statement.[625] It is designed to automatically identify all support and sensor assets available to a combat commander, regardless of domain. The software program will also be capable of "rapidly assessing the costs and benefits" tied to the employment of a given asset during the mission planning process through a visual interface on the MARS application.

In the same vein, DARPA awarded BAE an USD 8.3 million contract in 2023 to develop an "advanced autonomy system" to accelerate mission planning at the operational and tactical level to machine speeds. BAE Systems would provide the "machine-learning-backed system" and associated hardware, as well as testing and assessing the machine learning (ML) applications envisaged under DARPA's Strategic Chaos Engine for Planning, Tactics, Experimentation, and Resiliency (SCEPTER) programme.[626] A last example of DARPA funding of BAE work in this area, are the USD 23 million awards for two phases of DARPA's Oversight programme to advance "autonomous satellite tasking" to keep "constant custody" of as many as a thousand ground targets by automatically retasking sensors across government and commercial satellites.[627]

Finally, like Northrop Grumman, the US branch of BAE, also has its in-house foundry providing "high reliability and high-performance microelectronics" to meet demanding mission requirements for military systems, offering technologies with "performance advantages from <1 GHz to >100 GHz that exceed what is available in commercial markets".[628]

Ethical policies

In its 2025 Human Rights Statement, BAE Systems sets out that their "products protect national security and keep critical information and infrastructure secure. Our work is critical to supporting human rights around the globe, providing governments with the ability to protect their people. We understand that some of our stakeholders have views and perceptions of defence companies and human rights, particularly in the area of exports and how our products are used. We engage with organisations who have a focus on business or defence or security issues to understand factors that can impact our business and how we operate".[629]
While not deaf to outside views, BAE does not elaborate in its statement or elsewhere how it views its business in relation to reported human rights abuses. Like most companies in the sector, it goes on to merely stress the role of governments in setting export control

standards, rather than having company standards and due diligence policies regarding its customers, as it has for its suppliers.[630]

Former BAE Systems Chairman Roger Carr called autonomous weapons "very dangerous" and "fundamentally wrong" and made clear that BAE only envisions developing weapons that keep a connection to a human who could authorise and remain responsible for lethal decision-making.[631] And in 2018, BAE Systems stated: "While there are obvious benefits to unmanned systems, our view is that there should always be a 'human in the loop' when it comes to key decisions, including the use of lethal force. We firmly believe that humans must always be in charge when there is a decision such as the use of lethal force".[632]

Answering questions from PAX back in 2019 BAE emphasised also what it considers as the positive side of autonomy: "We believe that the use of autonomous systems does not mean a loss of command or the abdication of responsibility for decisions. Our position is that there are obvious benefits to autonomous and semi-autonomous systems which augment and improve human capabilities. We are developing a range of autonomous systems and future concepts to enable naval, land and air forces to carry out a number of different roles including air surveillance, anti-submarine warfare and better situational awareness to provide greater protection for the armed forces".[633]

Today, BAE calls it "AI with purpose": "We use the best models and approaches so our customers can accelerate their exploitation of AI. Building higher quality efficiencies, faster outcomes, and with responsibility at its core", guided by "foundations" such as: clean, connected and governed data; models that are traceable, monitored and compliant from development to deployment; safe experimentation that does not expose sensitive citizen data; clear, explainable AI that supports rather than replaces decisions; cloud-ready environments from LLMs to real-time analytics; and governance aligned with standards, ethical principles and legislative requirements from day one.[634] While these foundations may sound reassuring, with the fast pace of current developments in the area of military AI and autonomy, especially in the US, also illustrated by recent BAE announcements, such as its collaboration with Scale AI, the big question is how BAE will ensure these foundations comply with ethical and human rights standards.

8.2 General Dynamics

General Dynamics is a US-headquartered company working on shipbuilding, land combat vehicles, weapons systems and munitions. It employs more than 110,000 people worldwide and generated USD 55.25 billion in revenue in 2025, with a USD 4.2 billion net income.[635] It is the world's fifth biggest arms-producing company, according to SIPRI.[636]

Military AI, autonomous weapons contracts

Of the five biggest arms producing companies in the world, General Dynamics is so far least involved in military AI and autonomous weapons. However, its Information Technology arm (GDIT) employs more than a thousand "AI data professionals" and "delivers mission-enabling AI capabilities that streamline processes, advance research, improve decision making, enhance national security, and drive sustainability."[637] As an example, it mentions that for nearly a decade its automation has auto-indexed intelligence repositories - tagging names, locations, currencies and hundreds of other markers analysts would normally miss - and that this data, used by tens of thousands of analysts, can now be fed to the latest LLMs to generate detailed intelligence summaries.[638]

In January 2026, GDIT launched its "Defense Operations Grid Mesh Accelerator (DOGMA) AI solution […]. Integrating advanced AI, machine learning, cloud computing and satellite connectivity capabilities, DOGMA will enable government agencies to rapidly streamline data processing, analysis and decision-making in any operational environment".[639] Moreover, General Dynamics is working on robotic vehicles and autonomous underwater vehicles.[640]

Ethical policies

In its human rights statement, General Dynamics acknowledges "the special responsibility associated with products and services capable of taking human life. Many of our products and services include, or otherwise support, lethal capabilities. This imposes a terrific responsibility on us. To meet this call, we rigorously comply with applicable laws and regulations relating to the export and end use of our products and services".[641] Despite all these seemingly sensible words, the company does not appear to have an independent company position, as it makes clear: "In our complex and international business, some circumstances may be subject to potentially competing imperatives over how and to whom we provide our products and services. Given our role as a core supplier to the United States government and military, we are legally, ethically and morally bound to support the foreign and defense policy of the United States".[642] Worse: "We believe decisions about what types of weapons to buy, where to sell them and how to use them are inherently governmental responsibilities".[643] In conclusion, it looks unlikely that General Dynamics will ever forgo potential arms deals unless forbidden by the US government.

8.3 Lockheed Martin

US company Lockheed Martin has long been the world's biggest arms-producing company.[644] Its revenues over 2025 amounted to USD 75 billion with earnings of USD 5.9 billion. Most of its business comes from the US DoD and other US government agencies. Lockheed Martin has 123,000 employees, twenty per cent of whom are veterans.[645] It has four divisions: Aeronautics; Missiles and Fire Control; Rotary and Mission Systems; and Space. It mentions "aggressively adopting and inserting digital technologies into the

defense enterprise with a standards-based, open architecture approach" as one of its three "lines of effort".[646]

Lockheed Martin has a dedicated Autonomy & Uncrewed Systems webpage where it stresses that "the future of autonomy is human-centered", while at the same time claiming that "we're ushering in a new era of autonomous all-domain mission capability".[647] They explain this ambiguous view by stating that they are "building trust through rigorous validation and verification of our autonomous capabilities to mitigate direct threats to the warfighter – ultimately, increasing mission readiness": mitigating threats to the warfighter, not necessarily to potential civilian casualties. Also, "the deployment of autonomous systems help to maximize the operational effectiveness of a mission while ensuring the safety of the human-in-the-loop across air, land, sea and space." Safety of the human in-the-loop rather than potential civilian casualties. Thirdly, Lockheed mentions "our autonomous solutions leverage artificial intelligence and advanced computing to help operators make more informed decisions" - a claim that again may mean more targets, rather than fewer casualties. Apart from earlier mentioned collaborations with IBM, Meta, Microsoft, Nvidia and Palantir, Lockheed Martin has worked on AI and autonomy in weapons in the following examples.

Military AI, autonomous weapons contracts

Lockheed Martin has been working on increasingly autonomous technologies for a while now. For example, in 2014 it received a contract from the US Army Robotics Technology Consortium to conduct "a fully autonomous reconnaissance, surveillance and target acquisition experiment" with uncrewed ground and air vehicles.[648] Also, around 2017, the US Air Force partnered with Lockheed Martin's top-secret Skunk Works laboratory on an experiment called Have Raider, designed to demonstrate the technologies required for an unmanned vehicle to fly with a manned vehicle in the battlespace. "Using an experimental F-16 as a surrogate unmanned aircraft, the demonstration proved the ability to autonomously plan and execute air to-ground strike missions", according to a programme manager at Skunk Works.[649] "We started to marry autonomous vehicle control with autonomous battle management", he said, coining the idea of "dialable autonomy", whereby the level of control can be varied by the operator, from full direct control over flight and other aspects through to a level of autonomy whereby the autonomous system will decide what to do and how to complete a mission and ask the operator if it is cleared to do so.[650]

In 2022 Lockheed Martin announced the USD 100 million self-funded Project Carrera, to develop F-35-controlled small expendable combat drones, "incrementally introducing" human-machine interfaces capable of autonomy and AI.[651] Carrera would inform Lockheed's upcoming submission to the US Air Force's Collaborative Combat Aircraft (CCA) programme, where it was beaten in 2024 by the two winning concepts of General Atomics and Anduril. Currently, Lockheed Martin is pitching its self-funded Vectis CCA to no less than fifteen potential foreign customers.[652]

In 2020, Lockheed Martin was contracted as part of DARPA's Air Combat Evolution (ACE) programme, which aims to use air combat automation as a crucible to give pilots confidence that AI "can handle a high-end fight".[653] In April 2024, DARPA reported that ACE achieved "the first-ever in-air tests of AI algorithms autonomously flying an F-16 against a human-piloted F-16 in within-visual-range combat scenarios".[654]

In November 2024, Lockheed Martin announced its partnering with a consortium led by Iceye, a Finnish earth observation company, to develop AI-powered target recognition technologies to support Finland's F-35 fighter jet programme led by Lockheed Martin. Lockheed Martin will develop AI algorithms using Iceye's synthetic aperture radar (SAR) imagery. SAR satellites generate high-resolution images regardless of weather conditions or time of day. Lockheed Martin has also developed ATR algorithms using Maxar's electro-optical satellite imagery.[655]

In February 2026, Lockheed reported a successful test of its F-35 using AI-enhanced targeting in flight. Dubbed Project Overwatch, it incorporated an AI machine learning model into the plane's information control system. The AI model generated data based on the plane's surroundings and analysed the information to present the pilot with potential targets. It marked the first time a tactical AI model suggested a combat target to a fighter pilot independently, according to the company. Lockheed Martin said it would continue to pursue AI-driven decision-making models to allow pilots to identify combat targets faster.[656]

In June 2025 Lockheed Martin launched its AI Fight Club, a digital platform where other companies can test and vet AI products to see which ones are Pentagon-worthy and "to accelerate the testing and operational deployment of artificial intelligence to support warfighters in their missions".[657] "A lot of these small companies […] have great ideas and great AI, but they don't have the capital to support the full test environment and the full environment"; for Lockheed Martin it appears a potentially lucrative way to get connected to the most promising ideas.[658] In February 2026, Lockheed unveiled its Lamprey "multi-mission autonomous undersea vehicle" that can attach itself to ships.[659]

Ethical policies

Lockheed Martin claims to be "committed to responsible business".[660] In that vein, Lockheed Martin believes that "being a responsible corporate citizen includes a commitment to the protection and advancement of human rights" and that "respect for human rights across our business, operations and supply chain is the responsibility of all".[661] It says it is committed "to respecting human rights in support of our customers' missions"",[662] but it is unclear what that means, for example in the case of Israel's use of F-35 jets over Gaza since October 2023, or American F-35s in the 2026 war against Iran. It claims to have pre-contractual procedures to ensure that new contracts meet its standards and values, but it is not clear how this is implemented. Its procedures that evaluate risks "can result in a decision not to bid".[663] However, once the decision to bid is made, Lockheed Martin seems to fully rely on the US government's judgement of arms exports; even when there is clear risk of human rights violations, it does not appear it would take an independent, diverging position.

On AI, its 2024 sustainability impact report states that the company is committed to the ethical use of AI at every level, building transparent, fair and accountable systems aligned with its values as it integrates AI across the business.[664] It claims to have built its own AI factory capability. This enables it to "add additional safeguards to make sure that these systems are ethically deployed and used in a trustworthy manner", according to a Lockheed Martin executive. "It's always striking that balance of 'we want to add value to whatever process that we're doing but we don't want to insert risk'. We want to take risk out of the equation".[665]

8.4 Northrop Grumman

Northrop Grumman is the world's third largest arms-producing company according to SIPRI.[666] The company hosts approximately 95,000 employees, with 7,500 being employed in 2025, and their reported revenue was USD 41.95 billion with a net income of USD 4.18 billion in the full fiscal year of 2025.[667] Apart from earlier mentioned collaborations with Nvidia and Palantir, Northrop Grumman has worked on AI and autonomy in weapons in the following examples.

Military AI, autonomous weapons contracts

"Northrop Grumman is a leader in autonomous systems, helping our customers meet a wide variety of missions", says its dedicated Autonomous Systems webpage featuring several of its weapon systems.[668] While it never reached the serial production stage, some fifteen years ago, Northrop's X-47B Unmanned Combat Air System (UCAS) demonstrator was thought to become a leading example of highly autonomous uncrewed bomber jets. The tailless, stealthy X-47B still features on its website as a legacy example of the promising weapon it once was.[669] But, the MQ-8 Fire Scout is a "combat-proven, autonomous helicopter system providing real-time Intelligence, Surveillance, Reconnaissance and Target-acquisition, laser designation and battle management to tactical users without relying on manned aircraft or space-based assets", according to Northrop.[670]

The MQ-4C Triton uncrewed aircraft, a derivative of the Global Hawk, provides real-time surveillance. "Triton is the only autonomous high altitude, long endurance (HALE) maritime aircraft capable of operating at altitudes above 50,000 ft, for 24-plus hours with a range of 7,400 nautical miles. […] The aircraft can operate collaboratively with crewed platforms across domains through the intelligent and timely exchange of data".[671]

On 9 April 2026, a US Navy Triton crashed close to or over Iran. At the time of writing, it is unclear whether the USD 238 million costing drone came under fire or crashed due to a malfunction.[672] In the hypothetical scenario that the wreckage is recovered by Iran, sensitive equipment could be compromised,

similar to how a Lockheed Martin RQ-170 Sentinel was captured in 2011 and reverse-engineered into the Shahed-171 and 191.[673]

In collaboration with AeroVironment, Northrop Grumman is developing the Jackal, a loitering missile for precision strikes. Shown for the first time in May 2022, its maximum speed is over 600 km/h, it can cover a range of 100 km. The Jackal can be integrated with different warheads. It "operates autonomously and navigates through preset waypoints. It can be re-tasked mid-flight, offering flexibility in mission objectives, and once a target is identified, the Jackal rapidly accelerates for interception", according to Northrop Grumman PR.[674]

In 2025, Northrop revealed the Lumberjack one-way attack UAS, which Northrop calls fully autonomous but can also be used with man-in-the-loop control, "depending on what the customer wants for certain mission requirements".[675] It can fly several hundred miles or loiter for hours, and strike multiple targets on a single sortie. In March 2026, Northrop demonstrated the Lumberjack during a US Army exercise, showing "Full Autonomous Mission Control" through the Army's Maven Smart System (supplied by Palantir), as well as "Adaptive Targeting with AI Assistance" through Palantir's integrated automated target detection tools (the so-called Agentic Effects Agent) "to quickly adjust to dynamic battlefield scenarios under human supervision".[676]

In September 2025, Northrop announced its three US-based, government-certified semiconductor factories are now taking orders from other aerospace and arms companies, as part of a Pentagon-led push to make the industry less dependent on Asian suppliers.[677] Previously the Northrop-made chips were only available to military programmes Northrop itself was working on. Project Talon and its predecessor Project Lotus are part of Northrop's ongoing CCA efforts, labelled by Aviation Week as its "secret autonomous aircraft".[678]

Another CCA development is its cooperation with Kratos, awarded in early 2026 by the US Marine Corps with a contract valued at USD 231.5 million for 2 years.[679] The programme will combine Northrop Grumman's autonomous system capabilities with Kratos' Valkyrie UAV "to produce a CCA that will operate alongside crewed fighters to provide air dominance in high-threat environments".[680] Under the contract Northrop Grumman will deliver acost-effective mission kit, including sensors and software-defined technologies designed specifically for uncrewed aircraft, and the company's open-architecture autonomy software package called Prism that will manage the aircraft's operations autonomously.

Ethical policies

Northrop Grumman has an elaborate section on their commitment to various human rights and ethics related issues. To begin, they say that they are "committed to maintaining a strong culture with a deep respect for individuals and human rights". In addition to this,

Northrop Grumman CEO Kathy Warden says that "Ethics and integrity are at the center of everything we do at Northrop Grumman. Our reputation is founded on our adherence to the highest ethical standards. We understand it isn't just about what we do, but how we do it".[681]

Northrop summarises its human rights policy as being "deeply committed to human rights, embedding dignity, respect, and equality across its culture, operations, supply chain, and community interactions, guided by global human rights principles. […] Northrop Grumman enforces comprehensive policies and continuous training to uphold human rights throughout its business practices and global partnerships".[682] This includes "additional training to our Business Conduct Officers who are positioned globally and may be called upon to identify and address human rights related concerns".
Furthermore, Northrop mentions that although governments have the primary duty to protect human rights, companies share a responsibility to support them - through their culture, their treatment of employees and stakeholders, how they run their operations and trade, and their contributions to communities - guided by the UN Guiding Principles on Business and Human Rights, adopted in 2011.[683] In its 2023 human rights policy report it further elaborates: "We believe our programs are important to the safety and security of our country and those of our allies. We regularly evaluate our portfolio and, from time to time, we may determine that certain opportunities present undue risks to the Company or others, including risks related to human rights concerns, and elect to exit or not pursue certain business in light of such risks."[684]

Further reaching than most other companies in this sector, Northrop Grumman also says: "We are mindful of how our products might be used over time and potential unintended uses. We have robust processes and procedures in place to help ensure we do not do business in countries, or sell products or provide services to customers, not properly approved by the United States government. These processes also are designed to prevent potential diversion of our products to unintended third parties or for unintended purposes. In addition, the company has procedures in place to engage in due diligence, to assess and potentially to mitigate risks – including to human rights or, more broadly, the reputation of the company – before undertaking certain business opportunities, even if they are or would be approved by the United States government. Where the risks of pursuing such a business opportunity are unacceptable, we will decline the opportunity regardless of whether it is legally permissible" (emphasis added).[685] While still laudable, the latter seems more applicable to certain types of weapons it excludes[686] than certain customers, for which the US government's judgement appears to weigh heaviest.

Finally, on responsible AI policies, Northrop says it is "committed to delivering artificial intelligence (AI) technology to our customers in a safe, effective and responsible way. AI presents us with an opportunity to harness advanced technologies to enhance performance for next-generation mission solutions. We are working with government and trade organizations, as well as industry and academic partners, to build policies for implementing responsible AI and to refine our approach to AI development, testing and operations. This will allow us to continue to meet the standards and expectations set by our values and our customers".[687] Unfortunately, this is too vague to be meaningful as to what it considers acceptable or not, for example in terms of the human role in the use of force.

8.5 RTX

RTX, formerly Raytheon Technologies, is the world's second largest arms producing company. It has 185,000 employees and reported USD 88.6 billion in sales over 2025 with a net income of USD 6.7 billion.[688] Its product range includes aircraft parts, drones, missiles, air defence systems and satellites. RTX has stated that its teams use artificial intelligence and machine learning as tools to improve the design, development and testing of its products, to make them "smarter, easier to use and more capable than ever, with enhanced safety".[689] For example, its command-and-control systems use "artificial intelligence to fuse large, disparate data sources into cohesive, actionable insight for decision-makers". Apart from earlier mentioned collaborations with Amazon, RTX has worked on AI and autonomy in weapons in the following examples.

Military AI, autonomous weapons contracts

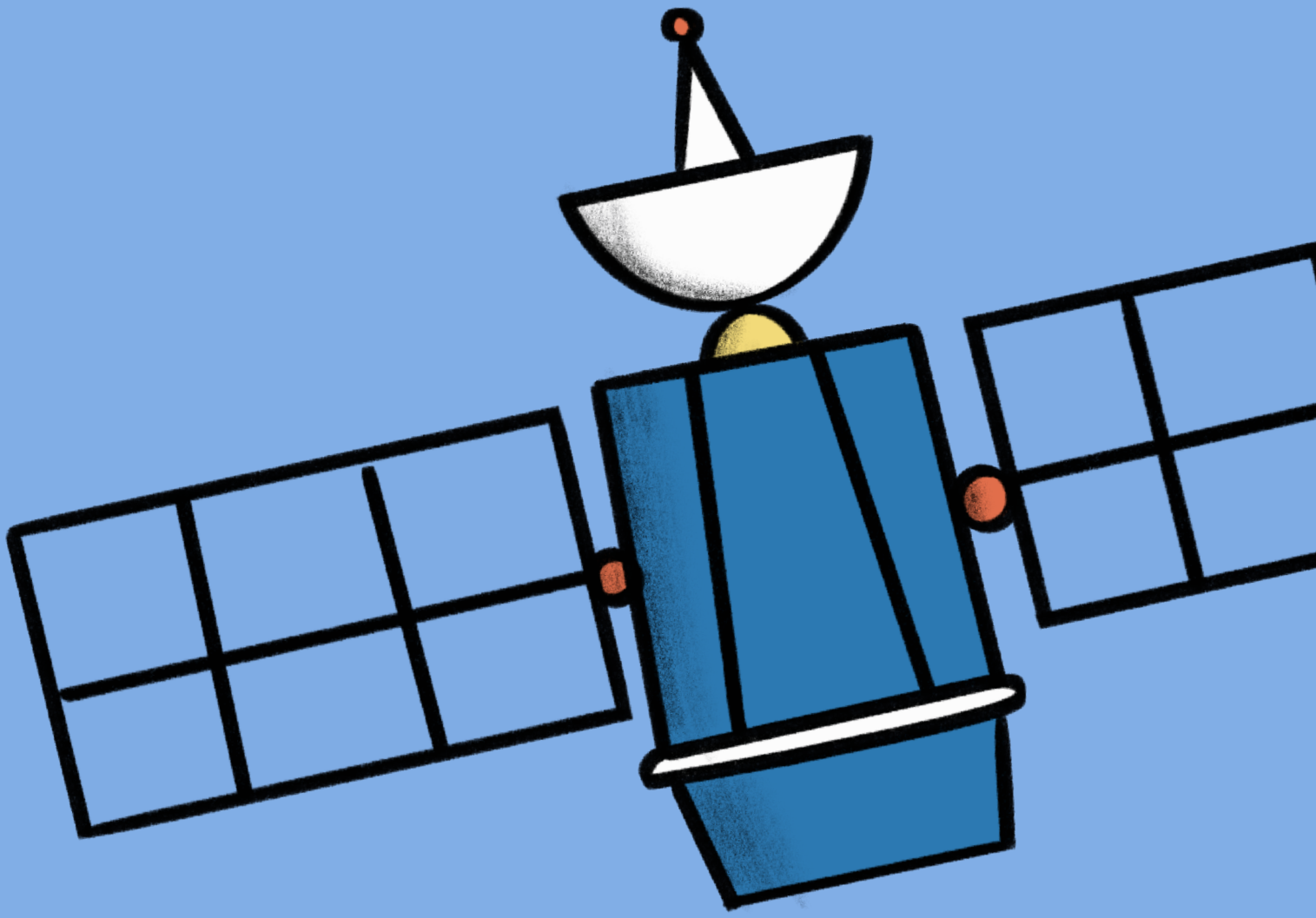
RTX's CGU-53 StormBreaker 'smart weapon' is delivered from fighter jets such as the F-35 and can "autonomously detect and define targets", including in low-visibility conditions such as bad weather or dust.[690] It has been ordered by the US and Norwegian air forces.

The "combat-proven" Coyote is RTX's expendable one-way attack drone that can be fired from the ground, air or sea, and is available in a counter-UAV version or as "launched effects" version, the latter performing target acquisition or delivering precision strikes.[691] Coyotes can be flown individually or networked autonomously in swarms. It is in use with US armed forces.
RTX supplies the "mission autonomy software suite" for the General Atomics YFQ-42 Collaborative Combat Aircraft (CCA) built for the US Air Force. The software packages use "AI-assisted algorithms to enable a set of behaviors during a mission, such as orchestrating a defensive combat air patrol or an offensive sweep for enemy fighters".[692]

Ethical policies

RTX describes its mission as solving "our customers' most complex problems and realize our vision for a safer, more connected world" and it aspires to be a responsible company, innovating new technologies to positively impact the world around us.[693]

More than most of its peers, RTX addresses concerns with the use of its weapons in its human rights policy: "RTX plays an important role in support of the national security interests of the United States and its allies. We recognize that the human rights issues associated with our defense products and services are a dynamic and complex subject. As a result, we monitor and evaluate our impact on human rights through due diligence and other measures and take actions designed to mitigate any adverse impacts".[694] It is unclear though what this entails in practice, for example whether well-documented reports of civilian harm caused by its weapons in Yemen had any effect regarding its sales to either Saudi Arabia or the UAE, which led the aerial bombing campaign at the time.[695] Across all five primes the pattern is consistent: each is pushing deeper into AI-enabled and increasingly autonomous weapons while, on human rights, deferring almost entirely to the judgement of the US government rather than setting independent limits of its own - even as a serious challenger, China, gains ground, as the next chapter shows.



Chapter 09

Meanwhile in China

9.1 Foreign export controls
9.2 Tech developments

9. Meanwhile in China

While American companies dominate both the tech and the weapons sector, China is the runner-up in both sectors, step by step narrowing the tech gap between the two largest economies in the world. The surprisingly advanced state of China's DeepSeek LLM as launched in 2025 is only one such example. Mass use of biometric technologies, such as iris scans, is another.

China's main tech companies, such as Alibaba, Baidu, Bytedance, Tencent and Zhipu AI, have the potential to become as big and powerful as their US peers, but are restrained by a lack of access to superfast semiconductors - partly because of Western export controls, partly because domestic production is still lagging substantially. However, Huawei has said it will need less than two years to produce chips similar to Nvidia's current versions. Nvidia's chips are produced at Taiwan Semiconductor Manufacturing Company, not only the world's biggest chip producer, but also the producer of the majority of the most advanced chips.[696] China's long-standing aim is to make every part of the semiconductor supply chain itself by 2030.

Over the past two years, the Pentagon has designated Alibaba, Baidu, and Tencent as a "military-civil fusion contributor to the Chinese defense industrial base". It alleges that they are affiliated with companies or institutes working with China's armed forces, the People's Liberation Army (PLA), which is strongly denied by all three companies.[697]

Looking at the source of knowledge – research - the situation appears most radically changed: China is leading research in nearly 90 per cent of the crucial technologies that "significantly enhance, or pose risks to, a country's national interests", according to a technology tracker run by the Australian Strategic Policy Institute (ASPI) think tank.[698] Some 25 years ago the US led more than 90 per cent of the assessed technologies, whereas China led less than 5 per cent. In terms of computing power however, China is still far behind the US.[699]

At the same time, much detail is lacking on the exact status of Chinese developments around military AI and autonomous weapons and what little information is known often lacks broader context.[700] For example it is often not clear to what extent technologies are developed or used for military purposes. This is to a large extent related to China's tech policy where civilian innovation should also serve military purposes: the so-called Military-Civil Fusion, overseen by the Central Commission for Military-Civil Fusion Development and considered the primary pathway for achieving what is called "intelligentised warfare".[701] Besides strong emphasis on advances in AI and semiconductor technology, China's strategic control over so-called rare earth minerals, required for renewable energy equipment, microelectronics and military goods, can also be seen as part of this tech race.

9.1 Foreign export controls

Reversely, US export control policies try to keep most advanced dual-use technology away from China. Increasingly, also less advanced versions of for example chips or chip production machines fall under export control measures and US allies have been put under pressure to follow suit. Only ten years ago, there were much closer ties between Silicon Valley and China, both in terms of investment and research, which made advanced technology much more easily accessible to China.[702] Many of those links have been scaled back since, most clearly seen in the purge of Huawei, key to China's computing ambitions, from many Western markets.[703]

The US Entity List bars American companies from supplying those on the list without government permits.[704] On the list are many major Chinese AI and tech companies, including: Huawei, Zhipu AI (large language models), Biren Technology (AI chips), Inspur and Sugon (servers and supercomputers), DJI (drones) as well as these surveillance/recognition technologies companies: Hikvision, SenseTime, Megvii, Cloudwalk, Yitu Technology and Leon Technology.[705]

With regards to the arms trade, US and EU embargoes dating back to at least the 1989 Tiananmen Square massacre have also made western weapons a no-go for China. This has pushed them to develop their own military and dual-use industries since at least the 1990s, through licensed production of Russian equipment,[706] espionage and reverse-engineering,[707] and simply heavily investing in its indigenous, often state-owned, industry.[708]

One area where China appears to make unexpected progress is in chip production equipment. With increased obstacles, pulled up under US pressure, to access advanced machines from Dutch company ASML – notably their Extreme Ultraviolet or EUV lithography machines – China has gone on a quest to master the technology itself. Reverse engineering and the recruitment of former employees of Dutch company ASML have been key to a secret project that, according to a Reuters report, would make China "capable of producing the cutting-edge semiconductor chips that power artificial intelligence, smartphones and weapons central to Western military dominance".[709] During 2025 China would have tested a prototype, and in five years it could be ready to produce advanced chips. Chinese electronics giant Huawei plays a key role coordinating a web of companies and state research institutes across the country involving thousands of engineers, according to the report. "Recruits included Lin Nan, ASML's former head of light source technology, whose team at the Chinese Academy of Sciences' Shanghai Institute of Optics has filed eight patents on EUV light sources in 18 months, according to patent filings".[710]

DeepSeek

In February 2025, arms company Norinco unveiled its P60 military vehicle capable of autonomously conducting combat-support operations at 50 kilometres per hour. According to another Reuters report, "It was powered by DeepSeek, the company whose artificial intelligence model is the pride of China's tech sector".[711] DeepSeek's popularity with the PLA reflects China's pursuit of what it calls "algorithmic sovereignty" - reducing dependence on Western technology while strengthening control over critical digital infrastructure. Researchers at Landship Information Technology, a Chinese company that integrates AI systems into military vehicles, including Norinco's, have said that they build their technology on Huawei chips to rapidly identify targets from satellite imagery, while coordinating with radars and aircraft to execute operations.[712] Another example mentioned by Reuters is about Xi'an Technological University research, according to which a DeepSeek-powered system was able to assess 10,000 battlefield scenarios - each with different variables, terrain, and force deployments - in 48 seconds, which would normally have taken military planners 48 hours.

9.2 Tech developments

Analysis by the Center for Security and Emerging Technology[713] of recent AI-related contracts published by the PLA, shows that most are awarded to traditional arms-producing companies and research institutes with close ties to the PLA, rather than the tech sector.[714] Most contracts were won by China Electronics Technology Group Corporation (CETC), China Aerospace Science and Technology Corporation (CASC) and China North Industries Group Corporation (NORINCO), all among the world's twenty largest arms-producing companies, according to SIPRI.[715] The Chinese Academy of Sciences (CAS) was the most successful of all entities with 92 out of 2,857 AI-related awards over 2023-4. CETC was second with 90, followed by CASC (47) and NORINCO (46). The main so-called non-traditional vendor was iFlytek, best known for its speech recognition technology, with 20 military-AI contracts. Others include PIESAT (AI-enabled geospatial data for live location mapping – 18 contracts) and JOUAV (drones and AI software to fuse data from thermal sensors – 12 contracts).[716]

Autonomous weapon technology

In the area of weapons technology, China is also closely following US developments. Several types of advanced-looking uncrewed air systems, including Collaborative Combat Aircraft (CCA) featured in the Victory Day military parade in September 2025.[717] The Feihong FH-97A 'loyal wingman' prototype, developed by CASC subsidiary Aerospace Times Feihong Technology, is designed for "confrontational, high-intensity and long-lasting combat". It was shown at the 2024 Zhuhai air show.[718]

Also showcased there, was Norinco's Intelligent Precision Strike System, used by the PLA to build a "network information system" that uses AI, cloud computing, and big-data techniques to fuse data from operational units and create "dynamic kill networks".[719] Norinco's AI-Enabled Synthetic Brigade combines armoured vehicles, swarming drones, loitering munitions and electronic warfare tools.

U-Tenet has developed military-focused AI models and systems that support strategic decision-making and autonomous operations, such as a cloud-based "decision-making brain" for operational planning and intelligence analysis; a real-time intelligence repository that integrates multi-source data for situational awareness; and an integrated battlefield-intelligence system.[720] Taken together, it seems that China is closing the gap rather than leading: ahead in research output and racing to localise chipmaking under its military-civil fusion strategy, yet still held back by limited access to the most advanced semiconductors and computing power — the very constraint that Western export controls are designed to preserve.

Loitering munitions

China has also developed a wide range of loitering munitions, often considered precursors of autonomous weapons, depending on their characteristics, such as the type of target it is used for and the level of human intervention required. One of the most prominent loitering munitions is CASC's 'Rainbow' CH-901, which can be launched from ground and air systems and can be used for both reconnaissance and attack missions. Future versions aim to have swarming capabilities.[721] CASC is also developing the AR-XX loitering munition, designed to conduct various missions, including "precision strikes against time-sensitive targets".[722] The company has claimed the munition can conduct missions independently or in collaboration with other weapons and equipment in an integrated system. CETC has developed a vehicle-launched drone swarm system that can carry 48 loitering munitions.[723]

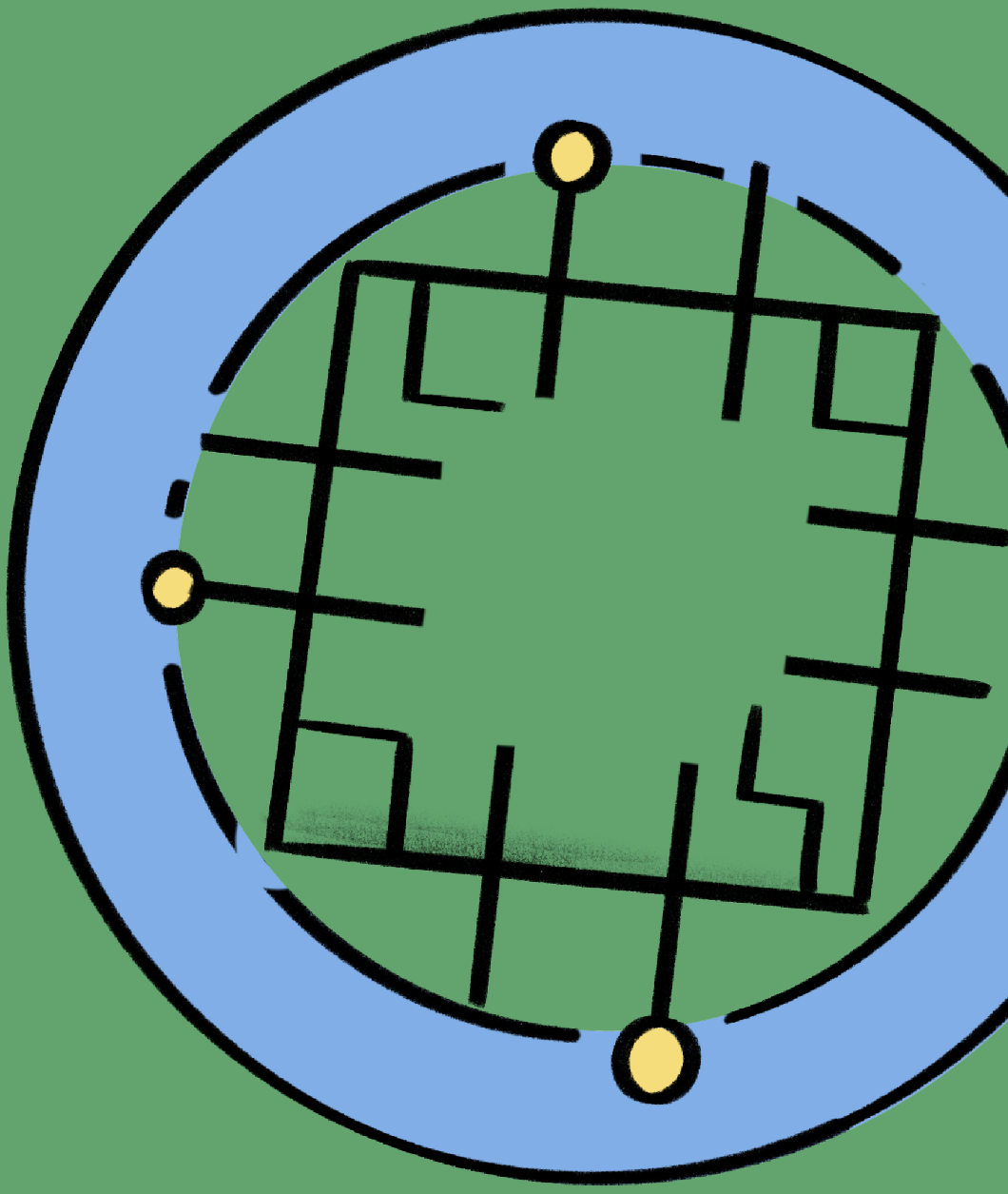
US business contributions

Over the years, numerous reports have revealed close links between US tech companies and the Chinese government, as already mentioned under some of the individual company profiles. In September 2025, Associated Press (AP) for example revealed how "American tech companies to a large degree designed and built China's surveillance state, playing a far greater role in enabling human rights abuses than previously known, an Associated

Press investigation found. They sold billions of dollars of technology to the Chinese police, government and surveillance companies, despite repeated warnings from the U.S. Congress and in the media that such tools were being used to quash dissent, persecute religious sects and target minorities".[724] American companies Cisco, Dell, HP, IBM, Intel, Microsoft, Motorola, Nvidia and Oracle stand out. Asian companies Hitachi, Samsung and Toshiba contributed as well according to the AP investigation. Reuters reported last year that despite the tendency to move to domestic processors, Nvidia hardware is frequently cited in military-affiliated academic research. It identified 35 applications referencing use of Nvidia's A100 chips. Nvidia has played down its role, saying that China "has more than enough domestic chips for all of its military applications".[725]

Global footprint examples

In April 2026, US officials accused Semiconductor Manufacturing International Corporation (SMIC), China's largest chipmaker, of sending chipmaking tools to Iran's military, roughly a year ago and "we have no reason to believe that any of this has stopped," one of the officials said.[726] SMIC has been sanctioned by the US government over alleged ties to the Chinese military, something SMIC denies. Chinese CCTV manufacturers, such as Hikvision and Tiandy, have been sanctioned by the US and the EU in part because of their business links with Iran in the context of the detention and execution of Iranian protesters in recent years.[727]



Chapter 10

In control of our future: regulating autonomous weapons and AI in warfare

10. In control of our future: regulating autonomous weapons and AI in warfare

As this report has shown, the militarisation of data-intensive technologies accelerated and broadened at an unprecedented pace over the last five years. Advances in computing power, (generative) AI, and the cloud have enabled highly automated decision-making processes, sharply compressing the time taken to select targets and, with it, the space for meaningful human control over the use of force. The technologies that increasingly shape modern warfare are no longer the preserve of the traditional arms industry: they are designed, owned and operated by the same companies that dominate civilian computing, and the civilian-military divide has all but disappeared.

The clearest illustration came from Israel's war on Gaza. Reporting examined in this report describes how, since October 2023, AI-powered decision-support systems were used to generate tens of thousands of Palestinian targets – more in a single day than human analysts could produce in a year. Rapid target generation led to rapid authorisation, with commanders reportedly given only seconds to approve strikes. Human operators were left to rubber-stamp an automated kill chain – the textbook definition of automation bias. Greater speed means less time for verification, and therefore greater risk of breaching requirements of distinction, proportionality and precaution under international humanitarian law, as well as a heightened risk of escalation. What also became clear was the role of some of the world's largest technology companies in building and sustaining the digital infrastructure on which such operations depend.

This is not confined to one conflict. The reported use of Palantir's Maven Smart System, drawing on Anthropic's Claude, in US operations against Venezuela and Iran shows how commercial AI has been folded into the use of force – with little or no transparency or accountability. At the same time, the wars in Ukraine and the Middle East (SWANA region) have driven rapid advances in autonomous weapons: drone technologies have visibly changed warfare, leading to spiralling developments in drone and counter-drone technologies. miniaturisation, mass deployment and ever greater autonomy now characterise a spiralling cycle of drone and counter- drone development, and increasingly autonomous functions are being embedded across the products of every major arms producer.

While this report mostly investigated the role of the world's largest arms-producers and tech giants, another feature emerges from Ukraine: how quickly these technologies adapt and proliferate, thanks to highly delegated and flexible procurement programmes fed by fast-established companies able to mass-produce drones in timeframes until recently unheard of among the weapons industry's primes.

Running through all of this is a second, quieter front: as tech and defence industries fuse, each is borrowing the other's weakest feature rather than its strongest. On the civilian side, the even limited safeguards built around data-intensive technology (including, data protection standards, transparency duties and voluntary "responsible AI" commitments) give way

to national-security exemptions and quietly withdrawn ethics policies, so protections designed for civilians disappear. On the military side, procurement grows faster and more permissive, borrowing tech giants agile, lightly overseen acquisition and set aside the slower legal review and accountability traditionally applied to weapons. The result is: military secrecy flows into civilian governance, commercial speed into military governance, and transparency. Oversight and our rights are squeezed from both directions.

These developments risk spiralling further out of control in a context of increased authoritarianism, record military spending, and growing disregard of international norms. Norms which, however, unevenly applied since they were established in the first half of the twentieth century, were established to protect civilians and to put limits on how wars are fought. At the same time, power is concentrating. A handful of companies and individuals control computing capacity, the main digital platforms and much of the media, and their links to government and the military are closer than ever. This establishes a new version of the military-industrial complex.

And yet this future is not inevitable.

At international level there are opportunities to address some of the concerns identified in this report. Beyond the human rights mechanisms to hold states and companies accountable that can and should consider the implication of data driven technologies in military context, there are specific initiatives to develop new international standards. In particular, states and other stakeholders have been discussing the need to limit and regulate lethal autonomous weapons systems since 2014, and it appears to be moving closer to the negotiation of a new treaty.

Also, in June 2026, for the first time, the UN will host talks that may eventually lead to broadly accepted rules and regulations on AI in the military domain, including decision-support systems. These processes are frustratingly slow, and some states will always try to slow them down or even torpedo them. However, a large majority of states has made clear that they want guardrails for these technologies. Over more than a decade, the ICRC, think tanks, civil society organisations and states have already provided ample guidance with their research and recommendations. What is now required is the political will to translate it into robust legal frameworks that can protect humankind from further digital dehumanisation.

10.1 Key findings

Drawing together the evidence across the company profiles and the wider analysis, the report points to ten key findings:

1. The tech and arms sectors are fusing into a new military-industrial complex. Computing-hardware makers, tech giants, generative-AI labs, the "neo-primes", such as Palantir and Anduril, and the legacy arms primes are now bound together by cloud contracts, chip supply chains, and close

partnerships. Commercial computing power, the cloud and off-the-shelf AI are becoming core military infrastructure, and the distinction between civilian and military technology is fading away.

2. Companies have abandoned their own ethical and legal red lines. Within a few years Google removed its pledge not to design AI for weapons, Meta and OpenAI reversed bans on military use, and Anthropic - despite its safety branding – deployed Claude across a US nuclear-weapons laboratory and into Palantir's military environment. Where corporate human rights policies exist, they tend to govern suppliers rather than customers or end-use. Many of the companies examined above ultimately defer to the home government's judgement to make decisions on deployment and exports. This creates a due diligence gap where it matters the most.

3. Increasingly autonomous weapons are proliferating and being battle-tested. Every major arms-producer is embedding autonomy and AI in its weapons – from 'smart' missiles to increasingly autonomous drones, while loitering munitions, drone swarms and collaborative combat aircraft feature on all sides, including in China. Ukraine has shown how quickly such systems proliferate through agile mass-production procurement.

4. AI decision-support systems are squashing the kill chain and turn meaningful human control impossible. In Gaza, AI-driven target generation outpaced any capacity for genuine human review. The same pattern is emerging in reported US operations against Venezuela and Iran. More speed means less verification, raising the risk of violating international humanitarian law and international human rights law.

5. The same technologies drive mass surveillance and the erosion of privacy, in war and as part of the surveillance state. Biometric registries of population, facial-recognition deployments, the normalisation of surveillance states and the domestic use of surveillance tools by immigration and law-enforcement agencies all show that privacy is not a side-issue to these discussions. Data gathered from civilians is increasingly turned into a means of profiling and targeting them.

6. Civilian digital infrastructure has become both weapon and target. Multi-billion-dollar military cloud contracts, satellite-internet constellations and near-ubiquitous AI chips have made commercial infrastructure indispensable to warfare. In turn, that infrastructure - including data centres - has itself become a military target, placing civilian systems and the people who depend on them on the front line of modern conflict.

7. Export controls barely apply to the recipients of these technologies or parts of them and leave surveillance technology largely unregulated. Western chips

continue to be found in weapons of their declared enemies; restricted chip-making technology is being reverse-engineered; and surveillance exports fall largely outside existing control regimes.

8. Power and accountability are dangerously concentrated. A small number of US companies and billionaires control computing power, the main digital platforms and much of the media, and their links to government and the military are closer than ever.

9. An "AI-arms race" is eroding accountability, oversight and rights protections. AI dominance is often described as an existential race, amid record military spending and rising authoritarianism. National security is used to push aside the safeguards meant to constrain these technologies. Commercial actors operate with even less transparency and almost no accountability.

10. None of this is inevitable, and the tools to regulate it already exist. States, companies and international institutions can act now to bring the militarisation of data-intensive technologies within the bounds of international human rights law (IHRL) and international humanitarian law (IHL). Technology should be used to empower people, not to reduce us to data points or targets.

10.2 Recommendations

PAX and Privacy International therefore call on states to:

- without delay begin negotiations with the view to adopt an international treaty on autonomous weapons that should: ban autonomous weapons that do not allow for meaningful human control; ban autonomous weapons that target humans directly; and provide additional rules so that other autonomous weapons will be used with meaningful human control;
- ensure that ongoing international efforts to regulate AI in the military domain explicitly articulate states' obligations to respect and protect privacy and personal data;
- adopt a moratorium on the use of AI systems for the use of force, for example in decision support systems, until necessary international rules and effective safeguards are in place;
- provide transparency on the use of AI and other data-driven technologies in the military domain, including the measures taken to mitigate human rights risks;
- adopt privacy and data protection legislation, in line with international

standards, that protects privacy and personal data in the military domain, setting out clearly what categories of personal data may be processed, on what legal basis, subject to what safeguards, and with what oversight.

We call on companies in the tech and military sectors to:

- stop developing, selling, transferring or servicing autonomous weapon systems that operate without meaningful human control, and stop supplying AI systems for the use of force, until necessary international rules and effective safeguards are in place;
- establish clear public policy committing not to contribute to the development, production or sale of such systems;
- include a clause to their contracts with customers, including government and military agencies, stipulating that their technology may not be used in, or contribute to the development, of such systems;
- carry out effective human rights due diligence to identify, prevent and mitigate the risks of adverse human rights impacts arising from their activities in the military domain
- demonstrate compliance with international data protection standards, including by adopting data protection policies, clearly setting out what categories of personal data may be processed in military domain context, on what legal basis, subject to what safeguards, and with what oversight; and
- ensure that licences, deployment terms and acceptable-use policies for AI models used by military or government customers include binding minimum data-protection obligations, including in relation to personal data about civilians and other affected third parties.
- adopt investment and financing policies on AI in the military domain to address and mitigate human rights risk posed by these technologies; and
- require the companies they invest in or finance to guarantee that their activities do not contribute to the development, sale, or transfer of autonomous weapon systems without meaningful human control, and AI systems for the use of force.

Endnotes

1 Wikipedia, 'RTX BBN Technologies', https://en.wikipedia.org/wiki/RTX_BBN_Technologies
2 RTX, 'Who We Are', https://www.rtx.com/who-we-are/we-are-rtx/transformative-technologies/bbn and https://milcom-security.com/wp-content/uploads/BoomerangGeneral-102010-5.pdf
Among many remarkable company facts, bbn.com is the second oldest currently registered domain name on the Internet (www.bbn.com) and Ray Tomlinson of BBN is widely credited as having invented the first person-to-person network email in 1971 and the use of the @ sign in an email address.
3 Stockholm International Peace Research Institute (SIPRI), 'The SIPRI Top 100 Arms Producing and Military Services Companies in the World', 2024, https://www.sipri.org/visualizations/2025/sipri-top-100-arms-producing-and-military-services-companies-world-2024
4 Raytheon RTX, 'Raytheon Completes Acquisition of BBN Technologies', 26 October 2009, https://raytheon.mediaroom.com/index.php?s=43&item=1424
5 See also: Thomas Heinrich, 'Cold War Armory: Military Contracting in Silicon Valley', Enterprise & Society, June 2002, pp. 247-284, Cambridge University Press https://www.jstor.org/stable/23699688
6 See for example Mustafa Ali Sezal & Francesco Giumelli (2022) Technology transfer and defence sector dynamics: the case of the Netherlands, European Security, 31:4, 558-575, https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2028277; and David Edgerton, 'The Relationship between Military and Civil Technology: A Historical Perspective', in: Philip Gummett, Judith Reppy (eds), 'The Relations between Defence and Civil Technologies', NATO Science Series D, 1988 https://link.springer.com/chapter/10.1007/978-94-015-7803-5_7
7 Jill Aitoro, 'Opinion: Clash of cultures? Maybe. But Google's also ditching Maven because its employees owned the message', Defense News, 6 June 2018, https://www.defensenews.com/opinion/2018/06/06/no-surprise-google-bids-maven-farewell/
8 P.W. Singer, 'Wired for War – the robotics revolution and conflict in the 21st century', Penguin Press, New York, 2009, p.78.
9 Roberto J. Gonzalez, 'Militarizing Big Tech: The rise of Silicon Valley's Digital Defense Industry', Transnational Institute, 7 February 2023, https://www.tni.org/en/article/militarising-big-tech
10 Roberto J. Gonzalez, 'Militarizing Big Tech: The rise of Silicon Valley's Digital Defense Industry', Transnational Institute, 7 February 2023, https://www.tni.org/en/article/militarising-big-tech
11 "Between March 2000 and October 2002, the Nasdaq fell from 5,048 to 1,139, erasing nearly all of its gains during the dot-com bubble. By the time the index bottomed out in October 2002, most publicly traded dot-com companies had failed." (Brian Duignan, 'dot-com bubble', Britannica Money (Encyclopedia Brittanica), https://www.britannica.com/money/dot-com-bubble).
12 Tom Simonite, 'Defense Secretary James Mattis Envies Silicon Valley's AI Ascent', Wired Magazine, 11 August 2017, https://www.wired.com/story/james-mattis-artificial-intelligence-diux/ via https://archive.ph/0ttc7
13 See for example: Joe Gould, 'Tech startups still face the Pentagon's 'valley of death'', Defense News, 30 January 2020, https://www.defensenews.com/2020/01/30/tech-startups-still-face-the-pentagons-valley-of-death/; Mike Gruss, 'The Pentagon wants to create a broader network of innovators', C4ISRNet, 13 May 2019, https://www.c4isrnet.com/pentagon/2019/05/13/the-pentagon-wants-to-create-a-broader-network-of-innovators/
14 Jill Aitoro, 'As tech startups catch DoD's eye, big investors are watching', Defense News, 30 January 2020, https://www.defensenews.com/smr/cultural-clash/2020/01/30/as-tech-startups-catch-dods-eye-big-investors-are-watching/

15 Roberto J. Gonzalez, 'Militarizing Big Tech: The rise of Silicon Valley's Digital Defense Industry', Transnational Institute, 7 February 2023, https://www.tni.org/en/article/militarising-big-tech
16 Roberto J. Gonzalez, 'Militarizing Big Tech: The rise of Silicon Valley's Digital Defense Industry', Transnational Institute, 7 February 2023, https://www.tni.org/en/article/militarising-big-tech
17 Xiao Liang, Nan Tian, Diego Lopes Da Silva, Lorenzo Scarazzato, Zubaida Karim and Jade Guiberteau Ricard, 'Trends In World Military Expenditure, 2025', SIPRI Fact Sheet, April 2026, https://www.sipri.org/sites/default/files/2026-04/2604_milex_2025.pdf
18 Catherine Belton and Robyn Dixon, 'Russia's economy keeps driving its war, but it could break in 2026', The Washington Post, 22 December 2025, https://www.washingtonpost.com/world/2025/12/22/russia-war-economy-ukraine/; https://ces.org.ua/en/tracker-economy-during-the-war/ and 'Financing The Russian War Economy', Report by the Stockholm Institute of Transition Economics (SITE) at the Stockholm School of Economics, April 2025, https://www.consilium.europa.eu/media/d4zd40wd/financing-the-russian-war-economy-stockholm-institute-of-transition-economics.pdf
19 Xiao Liang, Nan Tian, Diego Lopes Da Silva, Lorenzo Scarazzato, Zubaida Karim and Jade Guiberteau Ricard, 'Trends In World Military Expenditure, 2025', SIPRI Fact Sheet, April 2026, https://www.sipri.org/sites/default/files/2026-04/2604_milex_2025.pdf
20 Xiao Liang, Nan Tian, Diego Lopes Da Silva, Lorenzo Scarazzato, Zubaida Karim and Jade Guiberteau Ricard, 'Trends In World Military Expenditure, 2024', SIPRI Fact Sheet, April 2025, https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf
21 Sebastian Sprenger, 'Scholz proposes 100 billion euro defense fund, vows to exceed NATO spending goal', 27 February 2022, https://www.defensenews.com/global/europe/2022/02/27/scholz-proposes-100-billion-euro-defense-fund-vows-to-exceed-nato-spending-goal/. See also: Linus Höller, 'New projects bring German 2025 military-equipment spending near $40bn', Defense News, 4 December 2025, https://www.defensenews.com/global/europe/2025/12/04/new-projects-bring-german-2025-military-equipment-spending-near-40bn/
22 See for example: Jacob Grønholt-Pedersen, 'Greenland dismisses US takeover fears amid Trump's remarks', Reuters, 5 January 2026, https://www.reuters.com/world/europe/greenland-says-no-more-fantasies-about-annexation-after-trump-remarks-2026-01-05/; Victor Goury-Laffont, 'Former EU tech czar says US sanctions against him put Brussels on 'dangerous path'', Politico, 30 December 2025, https://www.politico.eu/article/breton-says-us-sanctions-against-him-put-the-eu-on-an-extraordinarily-dangerous-path/; The United States Executive Office of the President, 'National Security Strategy of the United States of America', November 2025, https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf
23 Also see: León Castellanos-Jankiewicz, Alina Carrozzini, Letizia Bozzi; Antonio Guzmán Mutis, 'ReArm Europe and the Rule of Law', European Defence & Security Law & Policy Quarterly, January 2026, https://edseq.lexxion.eu/data/article/20461/pdf/edseq_2026_01-005.pdf
24 Guy Anderson and Andrew MacDonald, 'Reality check - BRIEFING NATO's defence spend commitment', Janes Defence Weekly, 1 October 2025; Dr Nan Tian, Lorenzo Scarazzato and Jade Guiberteau Ricard, 'NATO's new spending target: challenges and risks associated with a political signal', SIPRI, 27 June 2025, https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal
25 Most sadly illustrated by the text message from NATO Secretary-General Mark Rutte on the eve of the NATO summit in The Hague; see for example: Will Weissert, ''Dear Donald.' Trump posts fawning private text from NATO chief on social media', AP, 24 June 2025, https://apnews.com/article/trump-rutte-text-message-nato-signal-6263810ac3ca77a5bf7366499f51c772.
26 William Hartung, 'Trump's $1.5 Trillion Pentagon Budget Will Make US Weaker', Common Dreams, 3 April 2026, https://www.commondreams.org/opinion/1-5-trillion-pentagon-budget
27 Aamer Madhani and Konstantin Toropin, 'Trump proposes massive increase in 2027 defense spending to $1.5T', Defense News, 8 January 2025, https://www.defensenews.com/news/pentagon-congress/2026/01/07/trump-proposes-massive-increase-in-2027-defense-spending-to-15t/
28 Steve Trimble, 'Debrief: Pentagon's Little-Known DAWG Fetches $54.6B In Spending Plan', Aviation Week, 6 April 2026, https://aviationweek.com/defense/budget-policy-operations/debrief-pentagons-little-known-dawg-fetches-546b-spending-plan

29 Out of the top 40 biggest military spenders, in 2015 3.5 per cent or more was spent by eight countries: the US (3.5), Russia (4.9), Saudi Arabia (13), Ukraine (3.8), Israel (5.4), Algeria (5.6), Kuwait (5) and Iraq (5.4). See Xiao Liang, Nan Tian, Diego Lopes Da Silva, Lorenzo Scarazzato, Zubaida Karim and Jade Guiberteau Ricard, 'Trends In World Military Expenditure, 2024', SIPRI Fact Sheet, April 2025, https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf

30 The United States Executive Office of the President, 'National Security Strategy of the United States of America', November 2025, https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

31 For example: Amazon, 'Cloud Computing for U.S. Defense: Securely supporting U.S. Defense mission success', https://aws.amazon.com/federal/defense/; alternatively: Microsoft, 'Azure for US Department of Defense', https://azure.microsoft.com/en-us/explore/global-infrastructure/government/dod/

32 For example: The Verdict News Network - Army Technology, 'Anduril, Meta to develop advanced XR solutions', 30 May 2025, https://www.army-technology.com/news/anduril-meta-xr-battlefield/

33 See for example: Frank Slijper, Alice Beck, Daan Kayser and Maaike Beenes, 'Don't be evil? A survey of the tech sector's stance on lethal autonomous weapons', PAX, August 2019, https://paxforpeace.nl/wp-content/uploads/sites/2/import/import/pax-report-killer-robots-dont-be-evil.pdf; Gerrit de Vynck, 'Some tech leaders fear AI. ScaleAI is selling it to the military', The Washington Post, 22 October 2023, https://www.washingtonpost.com/technology/2023/10/22/scale-ai-us-military/. More about Maven in Chapter 7.

34 Immigration and Customs Enforcement.

35 'Tech demands ICE out of our cities', https://iceout.tech/ and Joseph Menn, 'Tech workers ask their bosses to 'call the White House' over ICE raids', The Washington Post, 20 January 2026, https://www.washingtonpost.com/technology/2026/01/20/tech-ice-letter-protest/

36 Murad Ahmed et al., 'Transcript: Tech in 2025 — Trump and the tech bros', The Financial Times, 21 January 2025, https://www.ft.com/content/fc02cd00-cd70-4be4-8a59-e90b5f75ed09 and David Jeans, 'Silicon Valley Defense Tech Can't Wait For Trump To Get Started', Forbes, 7 November 2024, https://www.forbes.com/sites/davidjeans/2024/11/07/silicon-valley-defense-tech-cant-wait-for-trump-to-get-started/

37 With federal spending actually going up with DOGE: Emily Badger, David A. Fahrenthold, Alicia Parlapiano and Margot Sanger-Katz, 'How Did DOGE Disrupt So Much While Saving So Little?', The New York Times, 23 December 2025, https://www.nytimes.com/2025/12/23/us/politics/doge-musk-trump-analysis.html

38 Joey Roulette, 'Musk-Trump breakup puts $22 billion of SpaceX contracts at risk, jolting US space program', Reuters, 6 June 2025, https://www.reuters.com/business/aerospace-defense/spacex-will-decommission-dragon-spacecraft-musk-says-feud-with-trump-escalates-2025-06-05/

39 Ali Swenson, 'Trump, a populist president, is flanked by tech billionaires at his inauguration', AP, 21 January 2025, https://apnews.com/article/trump-inauguration-tech-billionaires-zuckerberg-musk-wealth-0896bfc3f50d941d62cebc3074267ecd While the focus of this report is on military uses, similar laisser-faire approaches are evident on the commercial side, and where for example EU AI standards have become a target of US trade policy. See for example: Anda Bologa, 'From AI To Digital Tax: Europe and US Clash on Tech', Center for European Policy Analysis, 28 February 2025, https://cepa.org/article/from-ai-to-digital-tax-europe-and-us-clash-on-tech/; Pieter Haeck, 'Europe prepares AI charm offensive as industry trembles from tariff shocks', Politico, 8 April 2025, https://www.politico.eu/article/europe-prepare-ai-charm-offensive-industry-tariff-shock-artificial-intelligence/ and European Commission, 'EU-US trade deal explained', 29 July 2025, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_25_1930/QANDA_25_1930_EN.pdf.

40 According to Forbes, the seven richest persons on earth are: 1. Elon Musk (SpaceX, Tesla), 2. Larry Page (Alphabet), 3. Jeff Bezos (Amazon), 4. Sergey Brin (Alphabet), 5. Mark Zuckerburg (Meta) 6. Larry Ellison (Oracle) and 7. Jensen Huang (Nvidia) (Forbes, 'The Real-Time Billionaires List', 30 April 2026, https://www.forbes.com/real-time-billionaires/). Also see: Eduardo Porter, 'Tech oligarchs reshape humanity while billionaires of old seem quaint', The Guardian, 8 March 2026, https://www.theguardian.com/technology/2026/mar/08/billionaires-tech-oligarchs and Cade Metz, Karen Weise, Nico Grant and Mike Isaac, 'Ego, Fear and Money: How the A.I. Fuse Was Lit', The New York Times, 3 December 2023, https://www.nytimes.com/2023/12/03/technology/ai-openai-musk-page-altman.html

41 Ali Swenson, 'Trump, a populist president, is flanked by tech billionaires at his inauguration', AP, 21 January 2025, https://apnews.com/article/trump-inauguration-tech-billionaires-zuckerberg-musk-wealth-0896bfc3f50d-941d62cebc3074267ecd

42 "[…] we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military industrial complex." See: Dwight D. Eisenhower, 'Dwight D. Eisenhower's farewell address', 17 January 1961, https://avalon.law.yale.edu/20th_century/eisenhower001.asp

43 Skye Jacobs, 'US tech czar warns China is only two years behind in semiconductor and chip design', TechSpot, 21 June 2025, https://www.techspot.com/news/108400-us-tech-czar-warns-china-only-two-years.html; Gabriel Dominguez, 'US lagging behind China in key dual-use technologies, warns US DoD official', Janes Defence Weekly, 31 October 2019.

44 Michael Schuman, 'The Race for Global Domination in AI - The competition between China and the United States is about more than technology.', The Atlantic, 3 January 2026, https://www.theatlantic.com/international/2026/01/china-ai-competition-differences/685389/

45 See for example: current US AI Action Plan: The United States Executive Office of the President, 'Winning the Race: AMERICA'S AI ACTION PLAN JULY 2025', https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
Weeks before its release, in June 2025 at the AI+ Expo in Washington, DC, military leaders, ministers and government agencies gathered to discuss their (overlapping) interests with Silicon Valley tech companies. Whereas the US government wants to maintain dominance over China through AI; tech companies like Microsoft, Meta, and Google hope to recoup their billion-dollar investments in AI through military/security contracts.

46 See for example: Rebecca Szkutak, 'Department of Commerce approves Nvidia H200 chip exports to China', TechCrunch, 8 December 2025, https://techcrunch.com/2025/12/08/department-of-commerce-may-approve-nvidia-h200-chip-exports-to-china/ and Magdalena Petrova and Eamon Javers, 'How $160 million worth of export-controlled Nvidia chips were allegedly smuggled into China', CNBC, 31 December 2025, https://www.cnbc.com/2025/12/31/160-million-export-controlled-nvidia-gpus-allegedly-smuggled-to-china.html

47 See for example Adam Satariano, 'How the Maker of the 'Most Complex Machine Humans Ever Created' Is Navigating Trade Fights', The New York Times, 5 June 2025, https://www.nytimes.com/2025/06/05/technology/asml-chips-tariffs-trade.html

48 Michael Schuman, 'The Race for Global Domination in AI - The competition between China and the United States is about more than technology.', The Atlantic, 3 January 2026, https://www.theatlantic.com/international/2026/01/china-ai-competition-differences/685389/. Also see: https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2025.07.18-letter-to-commerce-h20-chip.pdf

49 Konstantin F. Pilz, Robi Rahman, James Sanders, Luke Emberson, and Lennart Heim, 'The US hosts the majority of GPU cluster performance, followed by China', Epoch AI, 5 June 2025, https://epoch.ai/data-insights/ai-supercomputers-performance-share-by-country

50 The United States Executive Office of the President, 'Winning the Race: AMERICA'S AI ACTION PLAN', July 2025', https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

51 Robert Booth, 'Tech billionaires fly in for Delhi AI expo as Modi jostles to lead in south', The Guardian, 18 February 2026, https://www.theguardian.com/technology/2026/feb/18/delhi-ai-expo-modi-jostles-lead-south

52 Malcolm W. Browne, 'Invention That Shaped the Gulf War: the Laser-Guided Bomb, The New York Times, 26 February 1991, https://www.nytimes.com/1991/02/26/science/invention-that-shaped-the-gulf-war-the-laser-guided-bomb.html

53 See for example: Tania Myronyshena, 'Ukraine builds AI-driven defense ecosystem as over 200 companies develop drone technologies', Kyiv Independent, 19 April 2026, https://kyivindependent.com/ukraine-builds-ai-driven-defense-ecosystem-as-over-200-companies-develop-drone-technologies/; C.J. Chivers, 'In Ukraine, a New Arsenal of Killer A.I. Drones Is Being Born', The New York Times, 31 December 2025, https://www.nytimes.com/2025/12/31/magazine/ukraine-ai-drones-war-russia.html

54 Yasmin Afina and Federico Mantellassi, 'Clouds of war: The implications of targeting data centres', UNIDIR, 23 April 2026, https://unidir.org/clouds-of-war-the-implications-of-targeting-data-centres/. See also: Reeta

Ramanand and Liv McMahon, 'Amazon says drones damaged three facilities in UAE and Bahrain', BBC, 3 March 2026, https://www.bbc.com/news/articles/cgk28nj0lrjo

55 Sheera Frenkel, Paul Mozur and Adam Satariano, 'Mutually Automated Destruction: The Escalating Global A.I. Arms Race', The New York Times, 16 April 2026, https://www.nytimes.com/2026/04/12/technology/china-russia-us-ai-weapons.html.

56 PAX and Privacy International are members of Stop Killer Robots (https://stopkillerrobots.org/a-global-push/member-organisations/).

57 Stop Killer Robots, 'Submission to the United Nations Secretary-General on "Artificial intelligence in the military domain and its implications for international peace and security"', https://docs-library.unoda.org/General_Assembly_First_Committee_-Eightieth_session_(2025)/79-239-SKR-EN.pdf

58 Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

59 'Killer robots: World's top AI and robotics companies urge United Nations to ban lethal autonomous weapons', Future of Life Institute, 20 August 2017, https://futureoflife.org/ai/killer-robots-worlds-top-ai-robotics-companies-urge-united-nations-ban-lethal-autonomous-weapons/

60 Ariel Conn, 'AI Companies, Researchers, Engineers, Scientists, Entrepreneurs, and Others Sign Pledge Promising Not to Develop Lethal Autonomous Weapons', Future of Life Institute, 18 July 2018, https://futureoflife.org/2018/07/18/ai-companies-researchers-engineers-scientists-entrepreneurs-and-others-sign-pledge-promising-not-to-develop-lethal-autonomous-weapons/

61 See for example: Cade Metz, Karen Weise, Nico Grant and Mike Isaac, 'Ego, Fear and Money: How the A.I. Fuse Was Lit', The New York Times, 3 December 2023, https://www.nytimes.com/2023/12/03/technology/ai-openai-musk-page-altman.html.

62 Mirjana Spoljaric, 'ICRC president: The world cannot afford limitless war', The International Committee of the Red Cross, 21 October 2025, https://www.icrc.org/en/statement/icrc-president-world-cannot-afford-limitless-war. See also ICRC, 'Position Paper', 2025, https://www.icrc.org/sites/default/files/media_file/2025-10/ICRC-Position_Paper-Autonomous_Weapon_Systems_and_IHL-Selected_issues_Oct2025.pdf

63 Officially called: 'the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects' (see: https://treaties.unoda.org/t/ccw).

64 This is the term used by the UN; furthermore, autonomous weapons are also referred to as fully autonomous weapons or killer robots. While they are broadly referring to similar weapons, they can have slightly different meanings with regards to their lethality as well as the level of meaningful human control.

65 United Nations Office for Disarmament Affairs, 'The Convention on Certain Conventional Weapons', United Nations, https://disarmament.unoda.org/en/our-work/conventional-arms/convention-certain-conventional-weapons. As of 2025 there is a "rolling text" that has "consensus on the following formulations for the purpose of advancing its work on a set of elements of an instrument, without prejudging its nature, and other possible measures" – see: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2026)/CCW_GGE_LAWS_Rolling_Text_-_status_18_December_2025.pdf

66 Isabelle Jones, '156 states support UNGA resolution on autonomous weapons', Stop Killer Robots, 6 November 2025, https://www.stopkillerrobots.org/news/156-states-support-unga-resolution/

67 United Nations General Assembly, 'Lethal autonomous weapons systems Report of the Secretary-General', 1 July 2025, https://docs.un.org/en/A/79/88

68 UN Office of Disarmament Affairs (ODA), Informal Exchanges on Artificial Intelligence in the Military Domain and its Implications for International Peace and Security, 15-17 June 2026, Geneva, https://meetings.unoda.org/unoda-stu-meeting/unoda-science-technology-and-international-security-unit-meeting-2026

69 Privacy International, 'What is Militarisation of Tech?', 12 September 2025, https://privacyinternational.org/long-read/5668/what-militarisation-tech

70 Alexander Blanchard, Vincent Boulanin and Laura Bruun, 'Mapping the military AI industry', SIPRI, 23 April 2026, https://www.sipri.org/commentary/topical-backgrounder/2026/mapping-military-ai-industry

71 https://www.sp500live.co/companies as per 30 December 2025
72 Kali Hays, 'Elon Musk's SpaceX set to be worth $1 trillion with planned public listing', BBC, 2 April 2026, https://www.bbc.com/news/articles/c2k35lg92dpo
73 See here for actual market cap values: https://companiesmarketcap.com
74 Privacy International, 'Big Tech's bind with military and intelligence agencies', 1 October 2025, https://www.privacyinternational.org/long-read/5683/big-techs-bind-military-and-intelligence-agencies
75 AMD, 'About Us', https://www.amd.com/en/corporate.html
76 AMD, 'AMD Story: The AMD Brand', https://www.amd.com/en/corporate/amd-story.html
77 Investor Relations Press Release, 'AMD Reports Fourth Quarter and Full Year 2024 Financial Results', AMD, https://ir.amd.com/news-events/press-releases/detail/1236/amd-reports-fourth-quarter-and-full-year-2024-financial-results.
78 AMD, 'AMD Adaptive SoCs and FPGAs', https://www.amd.com/en/products/adaptive-socs-and-fpgas.html
79 So-called adaptive SoCs and FPGAs; see AMD, 'Aerospace and Defense Solutions', https://www.amd.com/en/solutions/aerospace-and-defense.html
80 Stephen Neillis and Max A. Cherney, 'US curbs AI chip exports from Nvidia and AMD to some Middle East countries', Reuters, 31 August 2023, https://www.reuters.com/technology/us-restricts-exports-some-nvidia-chips-middle-east-countries-filing-2023-08-30/
81 Adam Hancock and Peter Hoskins, 'Nvidia and AMD to pay 15% of China chip sales to US', BBC, 12 August 2025, https://www.bbc.com/news/articles/cvgvvnx8y19o
82 Los Alamos, Lawrence Livermore and Sandia National Laboratories; the Kansas City, Pantex and Y-12 plants; tritium operation facilities at the Savannah River Site; the Nevada Test Site – see: USDoE, 'National Nuclear Security Administration (NNSA) Facilities', United States Department of Energy (USDoE), https://www.directives.doe.gov/terms_definitions/national-nuclear-security-administration-nnsa-facilities
83 National Nuclear Security Administration (NNSA), 'About NNSA', United States Department of Energy (USDoE), https://www.energy.gov/nnsa/about-nnsa
84 Keumars Afifi-Sabet, 'World's fastest supercomputer 'El Capitan' goes online — it will be used to secure the US nuclear stockpile and in other classified research', Space.com, 9 February 2025, https://www.space.com/space-exploration/tech/worlds-fastest-supercomputer-el-capitan-goes-online-it-will-be-used-to-secure-the-us-nuclear-stockpile-and-in-other-classified-research
85 The El Capitan exascale supercomputer "can calculate at least one quintillion (1,000,000,000,000,000,000+) double precision (64-bit) operations per second (1 exaflop)"; El Capitan is a collaboration among the three National Nuclear Security Administration (NNSA) labs—Livermore, Los Alamos, and Sandia. NNSA "maintains and enhances the safety, security, and effectiveness of the U.S. nuclear weapons stockpile". See https://asc.llnl.gov/exascale/el-capitan https://www.energy.gov/nnsa/us-nuclear-weapons-stockpile and https://www.energy.gov/nnsa/national-nuclear-security-administration
86 Advanced Systems and Computing (ASC), 'El Capitan: NNSA's first exascale machine', Lawrence Livermore National Laboratory (LLNL), https://asc.llnl.gov/exascale/el-capitan
87 A review by Reuters of Russian customs records identified more than 15,000 shipments of Western electronic components that reached Russia after its Feb. 24 invasion of Ukraine through the end of May. The manufacturers included AMD, Analog Devices, Infineon, Intel and Texas Instruments. The parts included microprocessors, programmable chips, storage devices and other items, according to the Russian customs data - https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-missiles-chips/
88 David Gauthier-Villars, Steve Stecklow, Maurice Tamman, Stephen Grey and Andrew Macaskill, 'As Russian missiles struck Ukraine, Western tech still flowed', Reuters, 8 August 2022, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-missiles-chips/
89 IPHR, 'PARTS OF THE PROBLEM: Tracing Western Tech in Russia's Deadliest Jets', International Partnership for Human Rights (IPHR), 8 July 2025, pp. 58-63, https://nako.org.ua/storage/pdf/2025-07-09--10:52:41-jets-report-2025.pdf
90 Naheed Rajwani-Dharsi and Tasha Tsiaperas, 'Texas Instruments, Intel microchips used in Russian missiles,

lawsuits say', Axios, 11 December 2025, https://www.axios.com/local/dallas/2025/12/11/texas-instruments-intel-lawsuit-russia-weapons-ukraine and Mikal Carter Watts, 'FaceBook Post', Facebook, 10 December 2025, https://www.facebook.com/100005961666747/posts/2762631080612254/

91 War Sanctions, 'Components in the aggressor`s weapon', The Main Intelligence Directorate of the Ministry of Defense of Ukraine (GUR MOU), https://war-sanctions.gur.gov.ua/en/components?f%5Bsearch%5D=&f%5Bcountry_id%5D=&f%5Bmanufacturer_id%5D=32&f%5Btitle_uk%5D=&f%5Bpd%5D=&i%5Bmarking%5D=&page=2&per-page=12, (or via https://war-sanctions.gur.gov.ua/en/components).

92 AMD, '2024-25 CORPORATE RESPONSIBILITY REPORT', p. 14, https://www.amd.com/content/dam/amd/en/documents/corporate/cr/corporate-responsibility-report.pdf#page=86

93 AMD, '2024-25 CORPORATE RESPONSIBILITY REPORT', p. 14, https://www.amd.com/content/dam/amd/en/documents/corporate/cr/corporate-responsibility-report.pdf#page=86

94 AMD, '2024-25 CORPORATE RESPONSIBILITY REPORT', p. 14, https://www.amd.com/content/dam/amd/en/documents/corporate/cr/corporate-responsibility-report.pdf#page=86

95 AMD, '2024-25 CORPORATE RESPONSIBILITY REPORT', p. 15, https://www.amd.com/content/dam/amd/en/documents/corporate/cr/corporate-responsibility-report.pdf#page=86

96 AMD, '2024-25 CORPORATE RESPONSIBILITY REPORT', p. 15, https://www.amd.com/content/dam/amd/en/documents/corporate/cr/corporate-responsibility-report.pdf#page=86

97 CNET Staff, 'Cisco ascends to most valuable company', CNET, 27 March 2000, https://www.cnet.com/tech/mobile/cisco-ascends-to-most-valuable-company/

98 With year ending 31 October 2025. See Macrotrends, 'Cisco Revenue 2012-2026 | CSCO', https://www.macrotrends.net/stocks/charts/CSCO/cisco/revenue and Macrotrends, 'Cisco Net Income 2012-2026 | CSCO', https://www.macrotrends.net/stocks/charts/CSCO/cisco/net-income

99 See for example these news releases: Cisco, 'Cisco Provides Core Network Infrastructure for World's Largest Multinational Military Exercise', 15 May 2006, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2006/m05/cisco-provides-core-network-infrastructure-for-world-s-largest-multinational-military-exercise.html; Cisco, 'Cisco Extends Mobile Networking Portfolio for Military, Public Services and Transportation Personnel Operating on the Go', 23 August 2011, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2011/m08/cisco-extends-mobile-networking-portfolio-for-military-public-services-and-transportation-personnel-operating-on-the-go.html; Cisco, 'Military Installations for the Future', 2023, https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/Federal/DoD_Smart_Base_infographic.pdf; Samuel Pasquier, 'Industries: The new Catalyst ESS9300: Transforming critical military communications through open standards', Cisco, 14 October 2024, https://blogs.cisco.com/industries/the-new-catalyst-ess9300-transforming-critical-military-communications-through-open-standards

100 Cisco, 'Solutions for Federal Government', https://www.cisco.com/site/us/en/solutions/industries/government/us-federal/index.html
"We have a strong commitment to our mission: Protect all that matters for the Department of Defense (DoD)".

101 Cisco, 'Military Installations for the Future', 2023, https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/Federal/DoD_Smart_Base_infographic.pdf

102 AFP, 'Cisco sued for helping China monitor Internet', 23 May 2011, https://www.brecorder.com/news/15085.

103 Mark Sherman, 'Supreme Court will take up Cisco's bid to shut down lawsuit by Falun Gong', AP, 9 January 2026, https://apnews.com/article/china-cisco-falun-gong-surveillance-c336e8ab44d9e1e59c748450a6ddf078

104 As quoted in Lauretta Chao and Don Clark, 'Cisco Poised to Help China Keep an Eye on Its Citizens', The Wall Street Journal, 5 July 2011, http://online.wsj.com/article/SB10001424052702304778304576377141077267316.html

105 Reuters, 'U.S. Supreme Court to hear suit claiming Cisco helped China pursue Falun Gong', 9 January 2026, https://www.cnbc.com/2026/01/09/us-supreme-court-to-hear-suit-claiming-cisco-helped-china-pursue-falun-gong.html

106 Lauretta Chao and Don Clark, 'Cisco Poised to Help China Keep an Eye on Its Citizens', Wall Street Journal, 5 July 2011, http://online.wsj.com/article/SB10001424052702304778304576377141077267316.html

and Amy Lee, 'Cisco Said To Aid China In Installing Massive 'Peaceful Chongqing' Surveillance System', Huffington Post (now HuffPost), 5 July 2011, https://www.huffpost.com/entry/cisco-china-peaceful-chongqing-surveillance_n_890382

107 China Economic Review, 'Cisco denies building video surveillance network in Chongqing', 7 July 2011, https://chinaeconomicreview.com/content-cisco-denies-building-video-surveillance-network-chongqing/

108 Cisco, 'Cisco Signs MoU with Chongqing to Foster Economic, Social and Environmental Sustainability', https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2009/m09/cisco-signs-mou-with-chongqing-to-foster-economic-social-and-environmental-sustainability.html

109 Barbara Opall-Rome, 'Netanyahu, Trump to Talk Joint Cybersecurity Push', Defense News, 31 January 2017, https://www.defensenews.com/2017/01/31/netanyahu-trump-to-talk-joint-cybersecurity-push/

110 Cisco, 'Supplier Code of Ethics', https://www.cisco.com/c/en/us/about/suppliers/policies/code-of-ethics.html

111 Cisco, 'Cisco Supplier Ethics Policy', 2024, https://www.cisco.com/c/dam/en_us/about/ac50/ac142/docs/english-cisco-supplier-ethics-policy.pdf

112 Cisco, 'Cisco Supplier Ethics Policy', 2024, https://www.cisco.com/c/dam/en_us/about/ac50/ac142/docs/english-cisco-supplier-ethics-policy.pdf

113 'An Open Letter from Concerned Cisconians: To Chuck, Fran and Dev', https://bdsmovement.net/sites/default/files/2024-12/Open_Letter_From_Concerned_Cisconians.pdf

114 Archit Mehta, 'Cisco, a Major Contributor to Israel's Military Technology, Fired a Pro-Palestine Employee', Drop Site News, 18 April 2025, https://www.dropsitenews.com/p/cisco-israel-tech-internal-speech-palestine-gaza.

115 Macrotrends, 'IBM Revenue 2012-2025 | IBM', https://www.macrotrends.net/stocks/charts/IBM/ibm/revenue

116 'IBM…is GOVCON seeing a come back for Big Blue?', FedSavvy Strategies, 23 April 2024, https://www.fedsavvystrategies.com/ibm-is-govcon-seeing-a-come-back-for-big-blue/

117 Frank Konkel, 'Pentagon will 'open the door' to more companies for next major cloud contract', Defense One, 25 July 2025, https://www.defenseone.com/defense-systems/2025/07/pentagon-will-open-door-more-companies-next-major-cloud-contract/406994/; Colin Demarest, 'Pentagon inks dozens of cloud contract orders, more in the pipeline', Defense News, 25 March 2025, https://www.defensenews.com/battlefield-tech/it-networks/2024/03/25/pentagon-inks-dozens-of-jwcc-orders-with-more-in-the-pipeline/; Frank Konkel, 'CIA Awards Secret Multibillion-Dollar Cloud Contract', Nextgov/FCW, 20 November 2020, https://www.nextgov.com/modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227; Frank Konkel, 'CIA Awards Secret Multibillion-Dollar Cloud Contract', Nextgov/FCW, 20 November 2020, https://www.nextgov.com/modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227

118 Colin Demarest, 'Lockheed, IBM's Red Hat team up to speed AI development for Pentagon', C4ISRNet, 25 October 2022, https://www.c4isrnet.com/artificial-intelligence/2022/10/25/lockheed-ibms-red-hat-team-up-to-speed-ai-development-for-pentagon/

119 Giulia Bernacchi, 'Lockheed, Red Hat Partner on Drone Swarm Technology', The Defense Post, 30 May 2025, https://thedefensepost.com/2025/05/30/lockheed-red-hat-drone-swarm/

120 Olivia Savage, 'Germany selects consortium to fashion artificial intelligence backbone for FCAS', Janes Defence Weekly 13 September 2023.

121 Mike Murphy, 'A new chip architecture points to faster, more energy-efficient AI', IBM, 19 October 2023, https://research.ibm.com/blog/northpole-ibm-ai-chip and Dharmendra S. Modha et al., 'Neural inference at the frontier of energy, space, and time', Science, 19 October 2023, 382, pp. 329-335, https://www.science.org/doi/full/10.1126/science.adh1174

122 Charles Q. Choi, 'IBM Debuts Brain-Inspired Chip For Speedy, Efficient AI > NorthPole is the top, says its maker', IEEE Spectrum, 23 October 2023, https://spectrum.ieee.org/neuromorphic-computing-ibm-northpole

123 Patrick Tucker, 'Microchip breakthrough may reshape the future of AI', DefenseOne, 19 October 2023, https://www.defenseone.com/technology/2023/10/microchip-breakthrough-may-reshape-future-ai/391351/

124 Patrick Tucker, 'Microchip breakthrough may reshape the future of AI', DefenseOne, 19 October 2023,

https://www.defenseone.com/technology/2023/10/microchip-breakthrough-may-reshape-future-ai/391351/
125 Billy Mitchell, 'Former Pentagon CDAO Radha Plumb takes AI transformation role at IBM', DefenseScoop, 28 July 2025, https://defensescoop.com/2025/07/28/radha-plumb-ibm-cdao-defense-department/
126 IBM, 'IBM Defense Model', https://www.ibm.com/products/watsonx-ai/defense-model; Rojoef Manuel, 'IBM Debuts Military-Grade AI Designed for Secure Defense Ops', 3 November 2025 https://thedefensepost.com/2025/11/03/ai-ibm-secure-defense/
127 Brandi Vincent, 'A first look at IBM's new large language model that's fine-tuned for defense - applications', DefenseScoop, 29 October 2025, https://defensescoop.com/2025/10/29/ibm-new-large-language-model-defense-applications-janes/.
128 MoD and Luke Pollard MP, 'Press Release: Boost to jobs and military capability with new defence equipment system', Government of the United Kingdom (GOV.UK), 2 October 2025, https://www.gov.uk/government/news/boost-to-jobs-and-military-capability-with-new-defence-equipment-system
129 Athena Commercial, 'MOD Projects - Project Nexus', Athena Commercial, https://www.commercial-consulting.co.uk/post/mod-projects---project-nexus
130 Carlo Munoz, 'DARPA selects industry partners for second phase of QBI', Janes Defence Weekly 10 December 2025.
131 Who Profits Research Center, 'IBM', information valid until 23 May 2024, http://www.whoprofits.org/companies/company/7236
132 Who Profits Research Center, 'IBM', information valid until 23 May 2024, http://www.whoprofits.org/companies/company/7236 See also Michael Biesecker et al., 'As Israel uses US-made AI models in war, concerns arise about tech's role in who lives and who dies', AP, 18 February 2025, https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108
133 Population and Immigration Authority, 'IBM has assumed overall responsibility for the Population Authority's systems.', Government of Israel, 2 July 2019, www.gov.il/he/pages/ibm_maintanance_contract_with_piba (in Hebrew).
134 Investigate, 'AMAZON.COM INC: The world's largest online retailer and cloud storage provider. It is the main provider of cloud infrastructure and services for the Israeli government and military, US immigration authorities, and US prisons and police.', The American Friends Service Committee, valid as of 7 August 2024, https://investigate.afsc.org/company/amazon and Who Profits Research Center, 'IBM: A Major Facilitator of Israel's Surveillance and Security Apparatus', December 2021, https://www.whoprofits.org/publications/report/158?ibm-a-major-facilitator-of-israels-surveillance-and-security-apparatus
135 Kamil Zabielski, 'Sustainable Investment Review Q1 2024', Storebrand, 25 April 2024, https://www.storebrand.com/sam/no/asset-management/insights/perspectives/perspectives-folder/sustainable-investment-review-q1-2024 and Andrew Kersley, 'Storebrand divests from IBM over supply of biometrics to Israel', Computer Weekly, 29 May 2024, https://www.computerweekly.com/news/366586713/Storebrand-divests-from-IBM-over-supply-of-biometrics-to-Israel
136 As quoted in Investigate, 'AMAZON.COM INC: The world's largest online retailer and cloud storage provider. It is the main provider of cloud infrastructure and services for the Israeli government and military, US immigration authorities, and US prisons and police.', The American Friends Service Committee, valid as of 7 August 2024, https://investigate.afsc.org/company/amazon
137 Who Profits Research Center, 'IBM', information valid until 23 May 2024, http://www.whoprofits.org/companies/company/7236
138 Who Profits Research Center, 'IBM', information valid until 23 May 2024, http://www.whoprofits.org/companies/company/7236
139 Dake Kang and Yael Grauer, 'Detailed findings from AP investigation into how US tech firms enabled China's digital police state', AP, 9 September 2025, https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-a80904158b771a14d5a734947f28d71b
140 Ryan Gallagher, 'How U.S. Tech Giants Are Helping to Build China's Surveillance State', The Intercept, 11 July 2019, https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian/. Also see: Ryan Gallagher, 'Middle East Dictators Buy Spy Tech From Company Linked to IBM and Google', The Intercept, 12 July

2019, https://theintercept.com/2019/07/12/semptian-surveillance-mena-openpower/
141 Phoebe Magdirila, 'IBM Helps the Biggest City in the Philippines Transform to a Smart City', Tech in Asia, 7 June 2013, https://www.techinasia.com/ibm-helps-philippines-city-transform-into-smart-city and Johanna O. Bajenting, 'A proud Dabawenyo in corporate world', SunStar, 6 September 2015, https://www.sunstar.com.ph/more-articles/a-proud-dabawenyo-in-corporate-world
142 ICC, 'Duterte Case: The Prosecutor vs. Rodrigo Roa Duterte', 2025, https://www.icc-cpi.int/philippines/duterte
143 Awad Mustafa, 'Egypt Air Force modernising its logistics system, contract awarded', Defense and Security Middle East, 13 October 2023, https://www.defsecme.com/defence/air/egypt-air-force-modernising-its-logistics-system-contract-awarded
144 Sam Biddle, 'IBM CEO: We Listen to What Israel and Saudi Arabia Consider "Correct Behavior"', The Intercept, 4 September 2024, https://theintercept.com/2024/09/04/ibm-ceo-israel-saudi-arabia-ethics/
145 IBM, 'Data and policies', https://www.ibm.com/responsibility/data-and-policies and IBM, 'Act on Corporate Due Diligence Obligations in Supply Chains (LkSG)', https://www.ibm.com/legal/lksg
146 IBM, 'IBM Impact', https://www.ibm.com/responsibility
147 IBM, 'Responsible AI', https://www.ibm.com/trust/responsible-ai
148 IBM, 'IBM Responsible Technology Board', https://www.ibm.com/think/author/ibm-responsible-technology-board
149 James Hires, 'Nvidia's 85% GPU Market Share Faces Growing Competition: Is This AI Stock Still a Buy for 2026?', Yahoo! Finance, 25 January 2026, https://finance.yahoo.com/news/nvidias-85-gpu-market-share-210500376.html
150 Niket Nishant and Rashika Singh, 'Nvidia hits $5 trillion valuation as AI boom powers meteoric rise', Reuters, 29 October 2025, https://www.reuters.com/business/nvidia-poised-record-5-trillion-market-valuation-2025-10-29/
151 Macrotrends, 'NVIDIA Net Income 2012-2026 | NVDA', https://www.macrotrends.net/stocks/charts/NVDA/nvidia/net-income
152 Nvidia, 'NVIDIA Receives DARPA Contract Worth up to $20 Million for High-Performance Embedded Processor Research', 12 December 2012, https://nvidianews.nvidia.com/news/nvidia-receives-darpa-contract-worth-up-to-20-million-for-high-performance-embedded-processor-research
153 Nvidia, 'NVIDIA-Led Team Receives $25 Million Contract From DARPA to Develop High-Performance GPU Computing Systems', August 2010, https://nvidianews.nvidia.com/_gallery/download_pdf/5448192cf6091d27350001d9/ and Brooke Crothers, 'DARPA 'exascale' supercomputer in the works', CNET, 9 August 2010, https://www.cnet.com/science/darpa-exascale-supercomputer-in-the-works/
154 Neil Wilson, 'Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven', Utrecht University, Utrecht, 3 August 2020, https://studenttheses.uu.nl/bitstream/handle/20.500.12932/37392/Neil%20Wilson%20MA%20Thesis%20%281%29.pdf
155 Nvidia, 'AI and Machine Learning to Revolutionize U.S. Intelligence Community', GE, 20 December 2017, https://www.govexec.com/sponsors/2017/12/ai-and-machine-learning-revolutionize-us-intelligence-community/144664/ (Nvidia-sponsored article).
156 Ken Brown, 'NVIDIA Receives DARPA Contract Worth up to $20 Million for High-Performance Embedded Processor Research', Nvidia, 12 December 2012, https://nvidianews.nvidia.com/news/nvidia-receives-darpa-contract-worth-up-to-20-million-for-high-performance-embedded-processor-research
157 David Hambling, 'Military Tackles Problem And Potential Of Drones', Aviation Week & Space Technology, 12 April 2018, http://aviationweek.com/defense/military-tackles-problem-and-potential-drones
158 For example: Bill Carey, 'Is There Another Contender For Drone Dominance?', Aviation Week, 21 July 2020, https://aviationweek.com/aerospace/urban-unmanned-aviation/there-another-contender-drone-dominance and Kelvin Wong, 'From SRR to Blue: US seeks to overturn Chinese sUAS dominance', Janes International Defence Review, November 2020.
159 Nicholas Wallace, 'EUR: Defense tech's critical mineral wars', Arsenal, 2 December 2025, https://www.arsenal.eu/p/eur-defense-tech-s-critical-minerals-war

160 David Hambling 'Russia's Automated Killer Drones May Not Be Working As Planned', Forbes, 14 February 2024, https://www.forbes.com/sites/davidhambling/2024/02/14/it-looks-like-russias-automated-killer-drones-did-not-work-as-planned/ and Francis Farrell, 'How Russia's homegrown Lancet drone became so feared in Ukraine', The Kyiv Independent, 8 November 2023, https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine/ and David Hambling, 'Russia Boosts Production And Displays New 'Swarming' Version Of Lancet-3 Kamikaze Drone', Forbes, 18 July 2023, https://www.forbes.com/sites/davidhambling/2023/07/18/russia-boosts-production-and-displays-new-swarming-version-of-lancet-3-kamikaze-drone/
161 Dylan Malyasov, 'NVIDIA technology found in Russian military drones', Defence Blog, 20 May 2024, https://defence-blog.com/nvidia-technology-found-in-russian-military-drones/
162 Nvidia, 'Success Story, Lockheed Martin: Minimizing Downtime and Improving Productivity with AI-guided Predictive Maintenance', https://www.nvidia.com/content/dam/en-zz/Solutions/Data-Center/nvidia-dgx-lockheed-martin-case-study.pdf
163 David Spirk and Anthony Robbins, 'Data-driven Transformation in the Department of Defense', Nvidia, March 2022, https://www.nvidia.com/en-us/on-demand/session/gtcspring22-s42281/
164 Northrop Grumman, 'Northrop Grumman to Accelerate AI Innovation with NVIDIA Tools', 28 August 2025, https://news.northropgrumman.com/artificial-intelligence/northrop-grumman-to-accelerate-ai-innovation-with-nvidia-tools
165 Rudy Ruitenberg, 'Defense tech startups had their best funding year ever in 2025', Defense News, 20 January 2026, https://www.defensenews.com/industry/2026/01/20/defense-tech-startups-had-their-best-funding-year-ever-in-2025/
166 David Faber, 'Nvidia buying AI chip startup Groq's assets for about $20 billion in its largest deal on record', CNBC, 24 December 2025, https://www.cnbc.com/2025/12/24/nvidia-buying-ai-chip-startup-groq-for-about-20-billion-biggest-deal.html.
167 Meredith Roaten, 'AV lines up Switchblade 400 loitering munition for LASSO...', Janes Defence Weekly, 22 October 2025.
168 Shannon McPhee, 'Palantir and NVIDIA Team Up to Operationalize AI — Turning Enterprise Data Into Dynamic Decision Intelligence', Nvidia, 28 October 2025, https://nvidianews.nvidia.com/news/nvidia-palantir-ai-enterprise-data-intelligence
169 Shannon McPhee, 'Palantir and NVIDIA Team Up to Operationalize AI — Turning Enterprise Data Into Dynamic Decision Intelligence', Nvidia, 28 October 2025, https://nvidianews.nvidia.com/news/nvidia-palantir-ai-enterprise-data-intelligence
170 Shannon McPhee, 'Palantir and NVIDIA Team Up to Operationalize AI — Turning Enterprise Data Into Dynamic Decision Intelligence', Nvidia, 28 October 2025, https://nvidianews.nvidia.com/news/nvidia-palantir-ai-enterprise-data-intelligence
171 Robert Sherbin and Stewart Stecker, 'NVIDIA to Acquire Mellanox for $6.9 Billion', Nvidia, 11 March 2019, https://nvidianews.nvidia.com/news/nvidia-to-acquire-mellanox-for-6-9-billion; see also Sharon Wrobel, 'US chipmaker Nvidia scouts for Israeli AI talent, in expansion of R&D hub in south', The Times of Israel, 26 October 2025, https://www.timesofisrael.com/us-chipmaker-nvidia-scouts-for-israeli-ai-talent-in-expansion-of-rd-hub-in-south
172 Kyle Wiggers, 'Nvidia completes acquisition of AI infrastructure startup Run:ai', TechCrunch, 30 December 2024, https://techcrunch.com/2024/12/30/nvidia-completes-acquisition-of-ai-infrastructure-startup-runai/
173 Sharon Wrobel, 'US chipmaker Nvidia scouts for Israeli AI talent, in expansion of R&D hub in south', The Times of Israel, 26 October 2025, https://www.timesofisrael.com/us-chipmaker-nvidia-scouts-for-israeli-ai-talent-in-expansion-of-rd-hub-in-south/
174 Sofyan El Bouchtili, Machteld Veen and Emiel Woutersen, 'Nederlandse technische universiteiten delen hun kennis met Israëlische bedrijven: 'Je kunt ervan uitgaan dat die in de oorlog wordt gebruikt'', Trouw [in Dutch], 30 September 2025, https://www.trouw.nl/buitenland/nederlandse-technische-universiteiten-delen-hun-kennis-met-israelische-bedrijven-je-kunt-ervan-uitgaan-dat-die-in-de-oorlog-wordt-gebruikt~b3f709d8/
175 Can Emir, 'Israel's Elbit Systems unveils its tiny but powerful search and attack drone', Interesting Engineering, 15 November 2022, https://interestingengineering.com/transportation/lanius-search-and-attack-drone

and Jackson Chung, 'Elbit Systems' LANIUS Drone Has NVIDIA AI Computer, Carries Both Lethal and Non-Lethal Payloads', TechEBlog, 20 November 2022, https://www.techeblog.com/elbit-systems-lanius-drone/

176 Elbit Systems, 'Where Robots Go to Play', 28 March 2024, https://www.elbitsystems.com/blog/where-robots-go-to-play

177 Sophia Goodfriend, 'With Gaza war and Trump's return, Silicon Valley embraces a military renaissance', +972 Magazine, 31 December 2024, https://www.972mag.com/gaza-war-trump-silicon-valley-military/

178 Ashlee Vance, 'Chinese Supercomputer Wrests Title From U.S.', 28 October 2010, http://www.nytimes.com/2010/10/28/technology/28compute.html; https://web.archive.org/web/20140302031237/http://pressroom.nvidia.com/easyir/customrel.do See also Rachael King, 'China's Leap in Supercomputer Rankings', Bloomberg, 10 June 2010, https://web.archive.org/web/20101007224921/http://www.msnbc.msn.com/id/39519135/ns/business-bloomberg_businessweek

179 The Soufan Center, 'The Geopolitics of DeepSeek: Narratives, Perception, and the AI Race', 6 February 2025, https://thesoufancenter.org/intelbrief-2025-february-6/

180 Dane Kang and Yael Grauer, 'Detailed findings from AP investigation into how US tech firms enabled China's digital police state', AP, 9 September 2025, https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-a80904158b771a14d5a734947f28d71b

181 Tripp Mickle, 'Detailed findings from AP investigation into how US tech firms enabled China's digital police state', The New York Times, 15 April 2025, https://www.nytimes.com/2025/04/15/technology/nvidia-h20-chip-china-restrictions.html; Ana Swanson and Edward Wong, 'With New Crackdown, Biden Wages Global Campaign on Chinese Technology', The New York Times, 13 October 2022, https://www.nytimes.com/2022/10/13/us/politics/biden-china-technology-semiconductors.html

182 Stephen Nellis and Max A. Cherney, 'US curbs AI chip exports from Nvidia and AMD to some Middle East countries', Reuters, 31 August 2023, https://www.reuters.com/technology/us-restricts-exports-some-nvidia-chips-middle-east-countries-filing-2023-08-30/

183 Stephen Nellis and Max A. Cherney, 'US curbs AI chip exports from Nvidia and AMD to some Middle East countries', Reuters, 31 August 2023, https://www.reuters.com/technology/us-restricts-exports-some-nvidia-chips-middle-east-countries-filing-2023-08-30/

184 Dan Strumpf, Karen Hao and Raffaele Huang, 'Nvidia Offers Alternative Chip for China to Clear U.S. Export Hurdles', The Wall Street Journal, 8 November 2022, https://www.wsj.com/articles/nvidia-offers-alternative-chip-for-china-to-clear-u-s-export-hurdles-11667891718; Catherine 'Nvidia AI Chips: A100 A800 H100 H800 B200', FiberMall, 25 June 2024, https://www.fibermall.com/blog/nvidia-ai-chip.htm

185 Adam Hancock and Peter Hoskins, 'Nvidia and AMD to pay 15% of China chip sales to US', BBC, 12 August 2025, https://www.bbc.com/news/articles/cvgvvnx8y19o

186 Kevin Breuninger, 'Tech Trump greenlights Nvidia H200 AI chip sales to China if U.S. gets 25% cut, says Xi responded positively', CNBC, 8 December 2025, https://www.cnbc.com/2025/12/08/trump-nvidia-h200-sales-china.html; Rebecca Szkutak, 'Department of Commerce approves Nvidia H200 chip exports to China', TechCrunch, 8 December 2025, https://techcrunch.com/2025/12/08/department-of-commerce-may-approve-nvidia-h200-chip-exports-to-china/

187 Tripp Mickle, 'Department of Commerce approves Nvidia H200 chip exports to China', The New York Times, 28 May 2025, https://www.nytimes.com/2025/05/28/technology/nvidia-earnings-ai-chips.html

188 Alex Daniel, 'Anthropic boss says U.S. is courting disaster by selling AI chips to China', Quartz, 20 January 2026, https://qz.com/anthropic-boss-says-us-is-courting-disaster-by-selling-ai-chips-to-china

189 Human Rights Policy, Nvidia, Last updated: 05 February 2026, https://www.nvidia.com/content/dam/en-zz/Solutions/about-us/documents/HumanRightsPolicy.pdf

190 Nvidia, 'Trustworthy AI', https://www.nvidia.com/en-us/ai-trust-center/trustworthy-ai/; also see Nvidia, 'AI for Good', https://www.nvidia.com/en-us/about-nvidia/ai-for-good/

191 After NVIDIA and Apple, as of 5 January 2026 at https://www.financecharts.com/screener/biggest.

192 United States Securities and Exchange Commission, 'Alphabet Inc. Form 10-K Annual Report (Fiscal Year 2025)', https://www.sec.gov/ix?doc=/Archives/edgar/data/1652044/000165204425000014/goog-20241231.htm.

193 Wikipedia, 'Google', https://en.wikipedia.org/wiki/Google
194 Catherine Glifford, 'Google CEO: A.I. is more important than fire or electricity', CNBC, 1 February 2018, https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html
195 See: Patrick Tucker, 'Defense Innovation Board Director Moves to Google', Defense One, 1 May 2020, https://www.defenseone.com/technology/2020/05/defense-innovation-board-director-moves-google/165086/ also see Will Grannis, 'Google Workspace earns DOD IL4 authorization', Google, 21 July 2022, https://workspace.google.com/blog/product-announcements/google-workspace-earns-dod-il4-authorization; Colin Demarest and Davis Winkie, 'US Army rolls out Google collaboration suite to 180,000-plus personnel', C4ISRNET, 13 Janurary 2023, https://www.c4isrnet.com/battlefield-tech/it-networks/2023/01/13/us-army-rolls-out-google-collaboration-suite-to-180000-plus-personnel/
196 Staff Writer with AFP, 'Pentagon Awards $9B in Cloud Computing Deals to Four Firms', The Defense Post, 8 December 2022, https://thedefensepost.com/2022/12/08/pentagon-cloud-computing-deals/; see also Elisha Gamboa and Elizabeth Nguyen, 'Department of the Navy Awards Cloud Computing Task Orders for Google Cloud Platform, Oracle Cloud Infrastructure', United States Navy, 2 December 2025, https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4345891/department-of-the-navy-awards-cloud-computing-task-orders-for-google-cloud-plat/
197 Leigh Palmer, 'Google Distributed Cloud (GDC) & GDC air-gapped appliance achieve DoD Impact Level 6 (IL6) authorization', Google Cloud: Google Public Sector Newsletter, 28 May 2025, https://cloud.google.com/blog/topics/public-sector/google-distributed-cloud-gdc-gdc-air-gapped-appliance-achieve-dod-impact-level-6-il6-authorization; Carley Welch, 'Full house: Google to be final JWCC partner authorized for Secret-level cloud work in 2025', Breaking Defense, 31 October 2024, https://breakingdefense.com/2024/10/full-house-google-to-be-final-jwcc-partner-authorized-for-secret-level-cloud-work-in-2025/ and United States Department of War, 'Department of Defense Announces Joint Warfighting Cloud Capability Procurement', 7 December 2022, https://www.war.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/
198 Daisuke Wakabayashi and Kate Conger, 'Google Wants to Work With the Pentagon Again, Despite Employee Concerns', The New York Times, 3 November 2021, https://www.nytimes.com/2021/11/03/technology/google-pentagon-artificial-intelligence.html
199 Jack Poulson, 'Brief: Google received cloud contract supporting U.S. Special Operations Forces', All-Source Intel (Substack), 18 March 2024, https://jackpoulson.substack.com/p/brief-google-received-cloud-contract
200 Frank Konkel, 'CIA Awards Secret Multibillion-Dollar Cloud Contract', Nextgov/FCW, 20 November 2020, https://www.nextgov.com/modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227/
201 After nearly 70 years, the Department of Defense has restored the name "Department of War "pursuant to Executive Order 14347, signed by President Trump on September 5, 2025. "Department of Defense" remains the statutory name. See: Wikipedia, 'United States Department of War', https://en.wikipedia.org/wiki/United_States_Department_of_War
202 Stephen Losey, 'Pentagon taps Google Gemini, launches new site to boost AI use', Defense News, 9 December 2025, https://www.defensenews.com/pentagon/2025/12/09/pentagon-taps-google-gemini-launches-new-site-to-boost-ai-use/
203 Stephen Losey, 'Pentagon taps Google Gemini, launches new site to boost AI use', Defense News, 9 December 2025, https://www.defensenews.com/pentagon/2025/12/09/pentagon-taps-google-gemini-launches-new-site-to-boost-ai-use/. See also: Brandi Vincent and Drew F. Lawrence, 'The era of GenAI.mil is here. Users have mixed reactions and many questions', Defense Scoop, 18 December 2025, https://defensescoop.com/2025/12/18/genai-mil-users-have-mixed-reactions-and-many-questions/
204 Google, 'Google announces agreement to acquire Wiz', 18 March 2025, https://blog.google/company-news/inside-google/company-announcements/google-agreement-acquire-wiz/; CTech, 'From Unit 8200 to Wiz's $32B exit: The blueprint for Israeli cyber success', 20 March 2025, https://www.calcalistech.com/ctech-news/article/sjltwsk2kg; Mutaza Hussain, 'Google is Acquiring Tech Firm Founded by Ex-Israeli Intelligence

Officers for Record $32 Billion', Drop Site News, 2 April 2025, https://www.dropsitenews.com/p/google-acquisition-tech-wiz-israel-gaza-8200
205 Richard Lawler, 'Alphabet replaces Google's 'Don't be evil' with 'Do the right thing'', Engadget, 3 October 2015, https://www.engadget.com/2015-10-02-alphabet-do-the-right-thing.html; Lucy Hooker and Chris Vallance, 'Concern over Google ending ban on AI weapons', BBC, 5 February 2025, https://www.bbc.com/news/articles/cy081nqx2zjo
206 Google AI, 'Artificial Intelligence at Google Our Principles', via https://web.archive.org/web/20180611130019/https://ai.google/principles/ (first archived version of 11 June 2018).
207 Jennifer Elias, 'Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting', CNBC, 15 November 2021, https://www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html and Daisuke Wakabayashi and Kate Conger, 'Google Wants to Work With the Pentagon Again, Despite Employee Concerns', The New York Times, 3 November 2021, https://www.nytimes.com/2021/11/03/technology/google-pentagon-artificial-intelligence.html
208 Josh Lipton, 'Google won't pursue $10 billion Pentagon cloud contract', CNBC, 8 October 2018, https://www.cnbc.com/video/2018/10/08/google-wont-pursue-pentagon-cloud-contract-10-billion-google-googl-jedi-bid-stock.html
209 Patrick Tucker, 'New Google Division Will Take Aim at Pentagon Battle-Network Contracts', Defense One, 28 June 2022, https://www.defenseone.com/technology/2022/06/new-google-division-will-take-aim-pentagon-battle-network-contracts/368691/
210 Billy Perigo, Exclusive: 'Workers at Google DeepMind Push Company to Drop Military Contracts', TIME Magazine, 19 January 2026, https://time.com/7013685/google-ai-deepmind-military-contracts-israel/
211 AFP, 'Google axes its promise not to use AI for weapons or surveillance just weeks into the Trump presidency', FORTUNE Magazine, 5 February 2025, https://fortune.com/2025/02/05/google-drops-pledge-not-use-ai-weapons-surveillance/ and Lucy Hooker and Chris Vallance, 'Concern over Google ending ban on AI weapons', BBC, 5 February 2025, https://www.bbc.com/news/articles/cy081nqx2zjo
212 James Manylka and Demis Hassabis, 'Responsible AI: Our 2024 report and ongoing work', Google Blog, 4 February 2025, https://blog.google/technology/ai/responsible-ai-2024-report-ongoing-work/
213 James Manylka and Demis Hassabis, 'Responsible AI: Our 2024 report and ongoing work', Google Blog, 4 February 2025, https://blog.google/technology/ai/responsible-ai-2024-report-ongoing-work/; Google Trust and Safety Team, 'Responsible AI Progress Report', February 2025, https://ai.google/static/documents/ai-responsibility-update-published-february-2025.pdf and Google AI, 'Our AI Principles', current April 2026 version, https://ai.google/principles/
214 Google AI, 'Our AI Principles', https://ai.google/principles/
215 Gerrit De Vynck, 'Google workers petition CEO to refuse classified AI work with Pentagon', The Washington Post, 27 April 2026, https://www.washingtonpost.com/technology/2026/04/27/google-employees-letter-ai-pentagon/
216 Google LLC, "Google Privacy Policy", effective 2 April 2026, https://policies.google.com/privacy
217 Google LLC, "Google Privacy Policy", effective 2 April 2026, https://policies.google.com/privacy
218 "publicly available online or from other public sources" may be used "to help train Google's AI models and build products and features like Google Translate, Gemini Apps and Cloud AI capabilities". Google LLC, "Google Privacy Policy", effective 2 April 2026, https://policies.google.com/privacy
219 Google LLC, "Google Cloud Privacy Notice", effective 8 April 2026, https://cloud.google.com/terms/cloud-privacy-notice
220 Google LLC, "Google Cloud Privacy Notice", effective 8 April 2026, https://cloud.google.com/terms/cloud-privacy-notice ; Google Cloud Data Processing Addendum (Customers), https://cloud.google.com/terms/data-processing-addendum
221 Leigh Palmer, "Google Distributed Cloud (GDC) & GDC air-gapped appliance achieve DoD Impact Level 6 (IL6) authorization", Google Cloud, 28 May 2025, https://cloud.google.com/blog/topics/public-sector/google-distributed-cloud-gdc-gdc-air-gapped-appliance-achieve-dod-impact-level-6-il6-authorization
222 See Chapter 4.1 above and Chapter 6, for the JWCC and Project Nimbus discussion.

223 Google Cloud, "Google Cloud Enterprise Privacy Commitments", https://cloud.google.com/privacy
224 Google Workspace, "Generative AI in Google Workspace Privacy Hub", https://support.google.com/a/answer/15706919.
225 Yahoo Finance, 'Amazon.com, Inc. (AMZN)', https://finance.yahoo.com/quote/AMZN/financials/
226 Mark Bergen, 'Inside Google, a Debate Rages: Should It Sell Artificial Intelligence to the Military?', Bloomberg, 14 May 2018, via https://web.archive.org/web/20190410064200/https://www.bloomberg.com/amp/news/articles/2018-05-14/inside-google-a-debate-rages-should-it-sell-artificial-intelligence-to-the-military. See also: https://youtu.be/r8uzR8hgon8
227 Amazon Public Sector Blog Team, 'Amazon to launch second Secret Cloud Region in 2025', Amazon Web Services, 10 June 2025, https://aws.amazon.com/blogs/publicsector/amazon-to-launch-second-secret-cloud-region-in-2025/
228 Amazon Web Services, 'Amazon Web Services for the Warfighter', YouTube, 9 August 2018, https://www.youtube.com/watch?v=HHbBizyTet4
229 See Section 3.3 on IBM above.
230 Frank Konkel, 'CIA Awards Secret Multibillion-Dollar Cloud Contract', Nextgov/FCW, 20 November 2020, https://www.nextgov.com/modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227/
231 AFP, 'Pentagon Awards $9B in Cloud Computing Deals to Four Firms', The Defense Post, 8 December 2022, https://thedefensepost.com/2022/12/08/pentagon-cloud-computing-deals/ See also Elisha Gamboa and Elizabeth Nguyen, 'Department of the Navy Awards Cloud Computing Task Orders for Google Cloud Platform, Oracle Cloud Infrastructure', United States Navy, 2 December 2025, https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4345891/department-of-the-navy-awards-cloud-computing-task-orders-for-google-cloud-plat/
232 Frank Konkel, 'NSA Re-awards Secret $10 Billion Contract to Amazon', Nextgov/FCW, 27 April 2022, https://www.nextgov.com/emerging-tech/2022/04/nsa-re-awards-secret-10-billion-contract-amazon/366184/
233 Anne Grahn and Randy Brumfield, 'AWS launches AWS Wickr ATAK Plugin', AWS Security Blog, Seattle, 15 August 2022, https://aws.amazon.com/blogs/security/aws-launches-aws-wickr-atak-plugin/
"AWS Wickr is an enterprise-grade secure collaboration service that transforms how organizations protect their most critical communications. Designed with specialized capabilities for executives, security teams, field operators, and professionals managing sensitive information, AWS Wickr empowers every team member to communicate confidently through end-to-end encrypted messaging, voice and video calls, file sharing, and screen sharing" https://aws.amazon.com/wickr/
234 Amazon SageMaker helps developers build, train, and deploy ML models at scale. Amazon Bedrock provides access to foundation models through application programming interfaces, enabling organizations to integrate AI capabilities into applications without managing the underlying infrastructure. Giulia Bernacchi, 'Raytheon, Amazon to Collaborate on Cloud-Based Satellite Operations', The Defense Post, 10 December 2025, https://thedefensepost.com/2025/12/10/raytheon-amazon-satellite-operations/
235 Rebecca Heilweil and Madison Alder, 'Justice Department discloses FBI project with Amazon Rekognition tool', FedScoop, 25 January 2025, https://fedscoop.com/doj-fbi-amazon-rekognition-technology-ai-use-case/; Natasha Singer, 'Amazon Faces Investor Pressure Over Facial Recognition', The New York Times, 20 May 2019, https://www.nytimes.com/2019/05/20/technology/amazon-facial-recognition.html
236 AWS Public Sector Blog Team, 'Amazon Rekognition Demo for Defense', Amazon Web Services, 7 August 2017, https://aws.amazon.com/blogs/publicsector/amazon-rekognition-demo-for-defense/
237 Amazon, 'Code of Business Conduct and Ethics', https://ir.aboutamazon.com/corporate-governance/documents-and-charters/code-of-business-conduct-and-ethics/default.aspx
238 AWS, 'Responsible AI: From principles to practice', https://aws.amazon.com/machine-learning/responsible-ai/
239 Amazon Web Services, 'Responsible AI: From principles to practice', https://aws.amazon.com/machine-learning/responsible-ai/
240 Rachna Chadha and Peter Hallinan, 'Announcing the AWS Well-Architected Responsible AI Lens',

Amazon Web Services, 19 November 2025, https://aws.amazon.com/blogs/machine-learning/announcing-the-aws-well-architected-responsible-ai-lens/.

241 Frank Konkel, 'Microsoft, Amazon CEOs Stand By Defense Work After Google Bails on JEDI', Nextgov/FCW, 15 October 2018, https://www.nextgov.com/modernization/2018/10/microsoft-amazon-ceos-standby-defense-work-after-google-bails-jedi/152047/

242 Aaron Gregg, 'Amazon, Microsoft execs call for closer alliance between Pentagon and big tech', The Washington Post, 9 December 2019, https://www.washingtonpost.com/business/2019/12/09/amazon-microsoft-execs-call-closer-alliance-between-pentagon-big-tech/

243 Sean Keene, 'Amazon employees protest sale of face recognition software to police', CNET, 22 June 2018, https://www.cnet.com/news/politics/amazon-employees-want-jeff-bezos-to-stop-selling-facial-recognition-software-to-law-enforcement/; International Committee for Robot Arms Control (ICRAC), 'Open Letter to Amazon against Police and Government use of Rekognition', https://www.icrac.net/open-letter-to-amazon-against-police-and-government-use-of-rekognition/

244 Kaitlin Benz, 'ACLU wants Amazon to stop offering surveillance technology: the message is loud and clear', CNET, 18 June 2018, https://www.cnet.com/news/privacy/aclu-wants-amazon-to-stop-offering-surveillance-technology-rekognition/; Neema Singh Guliani, 'Amazon Met With ICE Officials to Market Its Facial Recognition Product', American Civil Liberties Union (ACLU), 24 October 2018, https://www.aclu.org/news/privacy-technology/amazon-met-ice-officials-market-its-facial

245 See: Amazon, 'We are implementing a one-year moratorium on police use of Rekognition', 10 June 2020, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition; Sebastian Klovig Skelton, 'Amazon defends facial-recognition tech sale to FBI despite moratorium', Computer Weekly, 9 February 2024, https://www.computerweekly.com/news/366569552/Amazon-defends-facial-recognition-tech-sale-to-FBI-despite-moratorium and Matt O'Brien, 'IBM quits facial recognition, joins call for police reforms', AP, 9 June 2020, https://apnews.com/5ee4450df46d2d96bf85d7db683bb0a6

246 Amazon Web Services, 'Amazon to launch second Secret Cloud Region in 2025', 10 June 2025, https://aws.amazon.com/blogs/publicsector/amazon-to-launch-second-secret-cloud-region-in-2025/

247 Amazon Web Services, "AWS Privacy Notice", https://aws.amazon.com/privacy/

248 Amazon Web Services, "AWS Privacy Notice", https://aws.amazon.com/privacy/

249 Amazon Web Services, "Data Privacy FAQ", https://aws.amazon.com/compliance/data-privacy-faq/

250 Amazon Web Services, "AWS Shared Responsibility Model", https://aws.amazon.com/compliance/shared-responsibility-model/

251 Amazon Web Services, "Amazon to launch second Secret Cloud Region in 2025", 10 June 2025, https://aws.amazon.com/blogs/publicsector/amazon-to-launch-second-secret-cloud-region-in-2025/; Amazon Web Services, "AWS Secret-West Region is now available", 22 October 2025, https://aws.amazon.com/about-aws/whats-new/2025/10/aws-secret-west-region-is-now-available/

252 Amazon Web Services, "Data Privacy FAQ", https://aws.amazon.com/compliance/data-privacy-faq/

253 Alex Irwin-Hunt, 'Top 100 global innovation leaders', FDi Intelligence, 20 June 2023, https://www.fdiintelligence.com/content/7d894243-9c09-5a30-960f-7fe3567c3063

254 Reuters, 'Meta taps Republican Joel Kaplan to lead global policy team, replacing Nick Clegg', 2 January 2025, https://www.reuters.com/technology/meta-taps-republican-joel-kaplan-lead-global-policy-team-replacing-nick-clegg-2025-01-02/

255 Meta, 'Meta Reports Fourth Quarter and Full Year 2025 Results', 28 January 2026, https://investor.atmeta.com/investor-news/press-release-details/2026/Meta-Reports-Fourth-Quarter-and-Full-Year-2025-Results/default.aspx

256 Nick Clegg, 'Open Source AI Can Help America Lead in AI and Strengthen Global Security', Meta, 4 November 2024, https://about.fb.com/news/2024/11/open-source-ai-america-global-security/. Nick Clegg left Meta two months later, and just ahead of Trump's inauguration. Previously he was leading the UK's LibDems, including as deputy-PM from 2010-2015. Reuters, 'Meta taps Republican Joel Kaplan to lead global policy team, replacing Nick Clegg', 2 January 2025, https://www.reuters.com/technology/meta-taps-republican-joel-kaplan-lead-global-policy-team-replacing-nick-clegg-2025-01-02/. Also see: Gerrit De Vynck, 'AI companies get

comfortable offering their technology to the military', The Washington Post, 8 November 2024, https://www.washingtonpost.com/technology/2024/11/08/anthropic-meta-pentagon-military-openai/
257 The Scale Team, 'Defense Llama: The LLM Purpose-Built for American National Security', Scale, 4 November 2024, https://scale.com/blog/defense-llama
258 The Scale Team, 'Defense Llama: The LLM Purpose-Built for American National Security', Scale, 4 November 2024, https://scale.com/blog/defense-llama See also, Brandi Vincent, 'Scale AI to set the Pentagon's path for testing and evaluating large language models', Defense Scoop, 20 February 2024, https://defensescoop.com/2024/02/20/scale-ai-pentagon-testing-evaluating-large-language-models/
259 Sam Biddle, 'Meta-Powered Military Chatbot Advertised Giving "Worthless" Advice on Airstrikes', The Intercept, 24 November 2024, https://theintercept.com/2024/11/24/defense-llama-meta-military/
260 Gerrit De Vynck, 'Some tech leaders fear AI. ScaleAI is selling it to the military', The Washington Post, 22 October 2023, https://www.washingtonpost.com/technology/2023/10/22/scale-ai-us-military/
261 Paul Sawers, 'Data-labeling startup Scale AI raises $1B as valuation doubles to $13.8B', Tech Crunch, 21 May 2024, https://techcrunch.com/2024/05/21/data-labeling-startup-scale-ai-raises-1b-as-valuation-doubles-to-13-8b/
262 Mike Isaac and Cade Metz, 'Meta Invests $14.3 Billion in Scale AI to Kick-Start Superintelligence Lab', The New York Times, 12 June 2025, https://www.nytimes.com/2025/06/12/technology/meta-scale-ai.html. An amount equal to about 10 per cent of Meta's revenue in 2024, it is Meta's second-largest deal, after the $19 billion acquisition of the messaging app WhatsApp in 2014
263 Maxwell Zeff and Marina Temkin, 'Cracks are forming in Meta's partnership with Scale AI', Tech Crunch, 29 August 2025, https://techcrunch.com/2025/08/29/cracks-are-forming-in-metas-partnership-with-scale-ai/
264 Alicia Park, 'Pentagon Hands Meta-Backed Scale AI $500 Million Contract, 5 Times Last Year's Deal', Forbes, 6 May 2026, https://www.forbes.com/sites/aliciapark/2026/05/06/pentagon-hands-meta-backed-scale-ai-500-million-contract-5-times-last-years-deal-report-says/
265 Mark O'Connell, 'The War App', The New York Review of Books, 25 September 2025, https://www.nybooks.com/articles/2025/09/25/the-war-app-the-technological-republic-karp-zamiska/
266 Army Technology, 'Anduril, Meta to develop advanced XR solutions', 30 May 2025, https://www.army-technology.com/news/anduril-meta-xr-battlefield/
267 Mark O'Connell, 'The War App', The New York Review of Books, 25 September 2025, https://www.nybooks.com/articles/2025/09/25/the-war-app-the-technological-republic-karp-zamiska/
268 Army Technology, 'Anduril, Meta to develop advanced XR solutions', 30 May 2025, https://www.army-technology.com/news/anduril-meta-xr-battlefield/. Also see: Anduril, 'Anduril and Meta Team Up to Transform XR for the American Military', 29 May 2025, https://www.anduril.com/news/anduril-and-meta-team-up-to-transform-xr-for-the-american-military
269 Whereas the original IVAS has been renamed Soldier-Borne Mission Command (SBMC). Ashley Roque, "I have got this s— figured out': Anduril unveiling EagleEye mixed-reality device at AUSA', Breaking Defense, 13 October 2025, https://breakingdefense.com/2025/10/i-have-got-this-s-figured-out-anduril-unveiling-eagleeye-mixed-reality-device-at-ausa/ Also see: Julie Bort, 'Meta and Anduril work on mixed reality devices for the US military', Tech Crunch, 30 May 2025 via https://www.defensenews.com/pentagon/2025/05/30/meta-and-anduril-work-on-mixed-reality-devices-for-the-us-military/
270 Meta, 'Corporate Human Rights Policy', https://humanrights.fb.com/policy/; also see: Meta, 'Human Rights Report (2024)', https://humanrights.fb.com/annual-human-rights-report/
271 Meta, 'Corporate Human Rights Policy', https://humanrights.fb.com/policy/
272 Gerrit De Vynck, 'Some tech leaders fear AI. ScaleAI is selling it to the military', The Washington Post, 22 October 2023, https://www.washingtonpost.com/technology/2023/10/22/scale-ai-us-military/
273 Anduril, 'Fury Autonomous Air Vehicle', https://www.anduril.com/fury
274 Meta, "Meta Privacy Policy — How Meta collects and uses user data", effective 4 March 2026, https://www.facebook.com/privacy/policy/
275 Meta, "Meta Privacy Policy — How Meta collects and uses user data", effective 4 March 2026, https://www.facebook.com/privacy/policy/

276 Meta, "Meta Privacy Policy — How Meta collects and uses user data", effective 4 March 2026, https://www.facebook.com/privacy/policy/
277 Nick Clegg, "Open Source AI Can Help America Lead in AI and Strengthen Global Security", Meta, 4 November 2024, https://about.fb.com/news/2024/11/open-source-ai-america-global-security/
278 Joel Kaplan, "Strengthening US National Security by Making Llama Available to Key Allies", Meta, 23 September 2025, https://about.fb.com/news/2025/09/strengthening-us-national-security-by-making-llama-available-to-key-allies/
279 Meta, "Human Rights Policy", https://humanrights.fb.com/
280 Microsoft, 'Annual Report 2025', https://www.microsoft.com/investor/reports/ar25/index.html
281 Microsoft, 'Azure Government Top Secret now generally available for US national security missions', 16 August 2021, https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/
282 Todd South, 'Army moves ahead on 'mixed reality' goggle with Microsoft in $21.8 billion contract', Army Times, 31 March 2021, https://www.armytimes.com/news/your-army/2021/03/31/army-moves-ahead-on-mixed-reality-goggle-with-microsoft-in-218-billion-contract/; Todd South, 'New rollout for the Army's $22 billion 'mixed reality' combat goggles', Defense News, 6 October 2022, https://www.defensenews.com/news/your-army/2022/09/27/new-rollout-for-the-armys-22-billion-mixed-reality-combat-goggles/; Anthony Capaccio, 'Microsoft Tweaked $22B Army Goggles Win Praise From Pentagon Buyer', Bloomberg, 5 October 2023, https://www.bloomberg.com/news/articles/2023-10-05/microsoft-tweaked-22b-army-goggles-win-praise-from-pentagon-buyer#xj4y7vzkg; Carlo Munoz, 'Anduril takes over from Microsoft as prime contractor of IVAS programme', Janes Defence Weekly, 26 February 2025; Ashley Roque, 'Anduril gets green light from Army to take over Microsoft's IVAS project: Exec', Breaking Defense, 15 April 2025, https://breakingdefense.com/2025/04/anduril-gets-green-light-from-army-to-take-over-microsofts-ivas-project-exec/
283 Todd South, 'Oculus founder wants to help troops 'surpass the limits of human form', Army Times, 11 February 2025, https://www.armytimes.com/news/your-army/2025/02/11/oculus-founder-wants-to-help-troops-surpass-the-limits-of-human-form/ and Ashley Roque, 'Anduril gets green light from Army to take over Microsoft's IVAS project: Exec', Breaking Defense, 15 April 2025, https://breakingdefense.com/2025/04/anduril-gets-green-light-from-army-to-take-over-microsofts-ivas-project-exec/ and Julie Bort, 'Meta and Anduril work on mixed reality devices for the US military', Tech Crunch, 30 May 2025 via https://www.defensenews.com/pentagon/2025/05/30/meta-and-anduril-work-on-mixed-reality-devices-for-the-us-military/
284 Kelsey Atheron, 'Microsoft Positions Itself To Win Space Data Market With Azure Orbital', Breaking Defense, 28 September 2020, https://breakingdefense.com/2020/09/microsoft-positions-itself-to-win-space-data-market-with-azure-orbital/
285 Kelsey Atheron, 'Microsoft Positions Itself To Win Space Data Market With Azure Orbital', Breaking Defense, 28 September 2020, https://breakingdefense.com/2020/09/microsoft-positions-itself-to-win-space-data-market-with-azure-orbital/
286 Microsoft, 'Azure Government Top Secret now generally available for US national security missions', 16 August 2021, https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/
287 Robert Burns, 'Pentagon cancels disputed JEDI cloud contract with Microsoft', AP, 7 July 2021, https://apnews.com/article/amazoncom-inc-technology-business-government-and-politics-83dae68a0ed4e24246900a1d1d1d00be; see also: Andrew Eversden, 'Latest court ruling leaves future of the Pentagon's JEDI cloud unclear', C4ISRNET, 28 April 2021, https://www.c4isrnet.com/smr/cloud/2021/04/28/latest-court-ruling-leaves-future-of-the-pentagons-jedi-cloud-unclear/ and Andrew Eversden, 'How the DoD's future war-fighting needs are shaping cloud vendors' products', C4ISRNET, 14 April 2021, https://www.c4isrnet.com/smr/cloud/2021/04/14/how-the-dods-future-war-fighting-needs-are-shaping-cloud-vendors-products/
288 AFP, 'Pentagon Awards $9B in Cloud Computing Deals to Four Firms', The Defense Post, 8 December 2022, https://thedefensepost.com/2022/12/08/pentagon-cloud-computing-deals/; see also Elisha Gamboa and Elizabeth Nguyen, 'Department of the Navy Awards Cloud Computing Task Orders for Google Cloud Platform, Oracle Cloud Infrastructure', United States Navy, 2 December 2025, https://www.navy.mil/Press-Office/

News-Stories/display-news/Article/4345891/department-of-the-navy-awards-cloud-computing-task-orders-for-google-cloud-plat/

289 Mike Stone, 'Lockheed gets Microsoft classified cloud to speed work with Pentagon', Reuters, 16 November 2022, https://www.reuters.com/technology/lockheed-gets-microsoft-classified-cloud-speed-work-with-pentagon-2022-11-16/

290 Lockheed Martin, 'Lockheed Martin Collaborates with Microsoft to Advance 5G.MIL® Technologies using Microsoft Azure', 27 February 2022, https://news.lockheedmartin.com/2022-02-27-lockheed-martin-collaborates-microsoft-advance-5G-MIL-technologies-microsoft-azure

291 Inside Unmanned Systems, 'Defending the Skies: Lockheed Martin and Microsoft Collaborate on Next-Gen C-UAS Technologies', 12 December 2025, https://insideunmannedsystems.com/defending-the-skies-lockheed-martin-and-microsoft-collaborate-on-next-gen-c-uas-technologies/

292 Alexandra Kelley, 'Microsoft, Palantir partner to expand AI offerings to defense and intelligence agencies', Nextgov/FCW, 8 August 2024, https://www.nextgov.com/artificial-intelligence/2024/08/microsoft-palantir-partner-expand-ai-offerings-defense-and-intelligence-agencies/398649/

293 Chetan Nayak, 'Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits', Microsoft, 19 February 2025, https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

294 Patrick Tucker, 'Microsoft-DARPA collaboration yields possible quantum chip breakthrough', Defense One, 19 February 2025, https://www.defenseone.com/technology/2025/02/microsoft-darpa-collaboration-yields-possible-quantum-chip-breakthrough/403127/ and Courtney Albon, 'DARPA continues quest to validate quantum computing utility', Defense News, 7 February 2025, https://www.defensenews.com/pentagon/2025/02/07/darpa-continues-quest-to-validate-quantum-computing-utility/

295 Shaun Waterman 'Air Force Launching New Artificial Intelligence 'Center of Excellence'', Air & Space Forces Association, 13 May 2025, https://www.airandspaceforces.com/air-force-launching-new-artificial-intelligence-center-of-excellence/

296 Christine Casimiro 'Anduril Scores Nearly $100M US Army Deal for Next-Gen C2 Prototype', The Defense Post, 21 July 2025, https://thedefensepost.com/2025/07/21/anduril-us-army-ngc2-prototype/ and Jen Judson, 'Anduril wins $100M deal to build US Army's next-gen C2 ecosystem', Defense News, 21 July 2025, https://www.defensenews.com/land/2025/07/21/anduril-wins-100m-deal-to-build-us-armys-next-gen-c2-ecosystem/

297 Takeshi Numoto, 'Microsoft acquires Adallom to advance identity and security in the cloud', Microsoft, 8 September 2015, https://blogs.microsoft.com/blog/2015/09/08/microsoft-acquires-adallom-to-advance-identity-and-security-in-the-cloud/; Michal Braverman-Blumenstyk, 'Microsoft acquires CyberX to accelerate and secure customers' IoT deployments', Microsoft, 22 June 2020, https://blogs.microsoft.com/blog/2020/06/22/microsoft-acquires-cyberx-to-accelerate-and-secure-customers-iot-deployments/ also see: Microsoft, 'Microsoft Israel: Who we are', https://www.microsoftrnd.co.il/whoweare#AboutUs (sources via Francesca Albanese, 'From economy of occupation to economy of genocide', Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, 2 July 2025, https://docs.un.org/en/A/HRC/59/23).

298 Joshua Brustein, 'Microsoft Wins $480 Million Army Battlefield Contract', Bloomberg, 28 November 2018, https://www.bloomberg.com/news/articles/2018-11-28/microsoft-wins-480-million-army-battlefield-contract

299 Elizabeth Dwoskin, 'Israel escalates surveillance of Palestinians with facial recognition program in West Bank', The Washinton Post, 8 November 2021, https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

300 'Joint statement by Microsoft & AnyVision', M12, 27 March 2020, https://m12.vc/news/joint-statement-by-microsoft-anyvision/. In 2025 AnyVision was dissolved, having burned though USD 352 million in funding: Sophie Shulman, 'What went wrong at AnyVision? Lessons from a $352M flameout', CTech, 21 January 2025, https://www.calcalistech.com/ctechnews/article/hyvsba3d1l

301 Yuval Abraham, 'Leaked documents expose deep ties between Israeli army and Microsoft', +972 Magazine, 23 January 2025, https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/

302 Microsoft, 'Microsoft invests $1.5 billion in Abu Dhabi's G42 to accelerate AI development and global expansion', 16 April 2024, https://news.microsoft.com/source/2024/04/16/microsoft-invests-1-5-billion-in-abu-

dhabis-g42-to-accelerate-ai-development-and-global-expansion/#1

303 Aaron Gregg and Cat Zakrzewski 'Microsoft invests in Arabic AI firm as U.S. tries to limit China's sway', The Washinton Post, 16 April 2024, https://www.washingtonpost.com/business/2024/04/16/microsoft-g42-artificial-intelligence-cloud/; Trevor Hunnicutt and Alexandra Alper, 'Microsoft-G42 deal positive because it cut Huawei ties, White House official says', Reuters, 24 June 2024, https://www.reuters.com/technology/microsoft-g42-deal-positive-because-it-cut-huawei-ties-white-house-official-says-2024-06-24/

304 Brad Smith, 'Microsoft's $15.2 billion USD investment in the UAE', Microsoft, 3 November 2025, https://blogs.microsoft.com/on-the-issues/2025/11/03/microsofts-15-2-billion-usd-investment-in-the-uae/

305 Employees of Microsoft, 'An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI', Medium, 13 October 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132.

306 Microsoft, 'Technology and the US military', 26 October 2018, https://blogs.microsoft.com/on-the-issues/2018/10/26/technology-and-the-us-military/; Joshua Brustein, 'Technology Microsoft Wins $480 Million Army Battlefield', Bloomberg, 28 November 2018, https://www.bloomberg.com/news/articles/2018-11-28/microsoft-wins-480-million-army-battlefield-contract

307 Colin Lecher, 'Microsoft workers' letter demands company drop Army HoloLens contract', The Verge, 22 February 2019, https://www.theverge.com/2019/2/22/18236116/microsoft-hololens-army-contract-workers-letter

308 Charles Riley and Samuel Burke, 'Microsoft CEO defends US military contract that some employees say crosses a line', CNN, 25 February 2019, https://edition.cnn.com/2019/02/25/tech/augmented-reality-microsoft-us-military via https://www.tni.org/en/article/militarising-big-tech

309 Aaron Gregg, 'Amazon, Microsoft execs call for closer alliance between Pentagon and big tech', The Washinton Post, 9 December 2019, https://www.washingtonpost.com/business/2019/12/09/amazon-microsoft-execs-call-closer-alliance-between-pentagon-big-tech/

310 Jay Greene, 'Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM', The Washington Post, 11 June 2020, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/

311 See for example Andrew Buncombe, 'Microsoft workers occupy HQ in protest against company's ties to Israeli military', The Guardian, 20 August 2025, https://www.theguardian.com/technology/2025/aug/19/microsoft-workers-protest-washington-israel and Tom Warren and Jay Peters, Microsoft employee disrupts 50th anniversary and calls AI boss 'war profiteer'', The Verge, 4 April 2022, https://www.theverge.com/news/643670/microsoft-employee-protest-50th-annivesary-ai

312 https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/ and Harry Davies and Yuval Abraham, 'Revealed: Israel demanded Google and Amazon use secret 'wink' to sidestep legal orders', The Guardian, 29 October 2025, https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code and Yuval Abraham, 'Microsoft revokes cloud services from Israel's Unit 8200', +972 Magazine, 25 September 2025, https://www.972mag.com/microsoft-cloud-israel-8200-expose/

313 Brad Smith, 'Update on ongoing Microsoft review', Microsoft, 25 September 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/ and Microsoft, 'Microsoft statement on the issues relating to technology services in Israel and Gaza', 15 May 2025, https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/

314 Microsoft, 'Microsoft Global Human Rights Statement', https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Global-Human-Rights-Statement-English.pdf

315 Microsoft, 'Microsoft Responsible AI: Principles and approach', https://www.microsoft.com/en-us/ai/principles-and-approach

316 Microsoft, '2025 Responsible AI Transparency Report', https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Responsible-AI-Transparency-Report-2025-vertical.pdf

317 Microsoft, "Microsoft Privacy Statement", last updated March 2026, https://www.microsoft.com/en-gb/privacy/privacystatement; Microsoft, "Change history for Microsoft Privacy Statement", https://www.microsoft.

com/en-us/privacy/updates
318 Microsoft, "Microsoft Privacy Statement", section on Enterprise and Developer Products.
319 Microsoft Learn, "Privacy and data management overview", Microsoft Service Assurance, https://learn.microsoft.com/en-us/compliance/assurance/assurance-privacy; Microsoft, "Products and Services Data Protection Addendum", May 2026.
320 Microsoft Trust Center, "Data protection and privacy", https://www.microsoft.com/en-gb/trust-center/privacy; Microsoft, "Government Requests for Customer Data Report", https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data
321 Microsoft, "Azure Government Top Secret now generally available for US national security missions", 16 August 2021, https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/
322 Brad Smith, "Update on ongoing Microsoft review", Microsoft, 25 September 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/
323 See Section 4.4 above, and the discussion of the Guardian/+972/Local Call reporting and Microsoft's response.
324 https://www.forbes.com/real-time-billionaires/ On 10 September 2025, Ellison was briefly the wealthiest person in the world after an increase in Oracle stock price, with an estimated net worth of US$393 billion (https://en.wikipedia.org/wiki/Larry_Ellison).
325 Sophie Shulman, 'Oracle CEO: "If we continue on our current trajectory, reaching a valuation of a trillion dollars is inevitable"', CTech, 14 November 2024, https://www.calcalistech.com/ctechnews/article/t05ji8sue
326 Macrotrends, 'Oracle Revenue 2012-2026 | ORCL', https://www.macrotrends.net/stocks/charts/ORCL/oracle/revenue
327 Antonie Boessenkool, 'SAP Takes Aim at DoD Work and Rival Oracle', Defense News, 23 February 2009.
328 Gerrard Cowan, 'UK eyes streamlined data in Oracle cloud computing deal', Janes International Defence Review, December 2020.
329 Andrew Eversden, ''Wakeup call': Report calls for massive AI investments to counter China', Defense News, 1 March 2021, https://www.defensenews.com/artificial-intelligence/2021/03/01/wakeup-call-report-calls-for-massive-ai-investments-to-counter-china/
330 Colin Demarest, 'Oracle gets go-ahead to host top secret Air Force data', Defense News, 15 February 2022l, https://www.defensenews.com/battlefield-tech/it-networks/2022/02/15/oracle-gets-go-ahead-to-host-top-secret-air-force-data/
331 AFP, 'Pentagon Awards $9B in Cloud Computing Deals to Four Firms', The Defense Post, 8 December 2022, 'https://thedefensepost.com/2022/12/08/pentagon-cloud-computing-deals/; see also Oracle, 'Oracle Cloud Capabilities for US Defense and Intelligence', https://www.oracle.com/government/govcloud/defense/ and Elisha Gamboa and Elizabeth Nguyen, 'Department of the Navy Awards Cloud Computing Task Orders for Google Cloud Platform, Oracle Cloud Infrastructure', United States Navy, 2 December 2025, https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4345891/department-of-the-navy-awards-cloud-computing-task-orders-for-google-cloud-plat/
332 Oracle and Palantir, 'Oracle and Palantir Join Forces to Deliver Mission Critical AI Solutions to Governments and Businesses', 4 April 2024, https://investors.palantir.com/news-details/2024/Oracle-and-Palantir-Join-Forces-to-Deliver-Mission-Critical-AI-Solutions-to-Governments-and-Businesses/
333 Anduril, 'Anduril & Oracle Partner to Deliver AI-Powered Defense Solutions from the Datacenter to the Tactical Edge', 9 October 2024, https://www.anduril.com/news/anduril-and-oracle-partner-to-deliver-ai-powered-defense-solutions-from-the-datacenter-to-the
334 Oishee Majumdar, "... and selects Oracle's air-gapped hyperscale isolated cloud", Janes Defence Weekly, 2 April 2025.
335 Oishee Majumdar, "... and selects Oracle's air-gapped hyperscale isolated cloud", Janes Defence Weekly, 2 April 2025.
336 Belle Lin, 'Oracle Unveils Initiative to Help Companies Sell Tech to the Pentagon', The Wall Street Journal, 17 June 2025, https://www.wsj.com/articles/oracle-unveils-initiative-to-help-companies-sell-tech-to-the-pen-

tagon-2c2f6b7c and Lauren C. Williams, 'Established defense contractors lend tech startups a helping hand', Defense One, 23 June 2025, https://www.defenseone.com/business/2025/06/established-defense-contractors-lend-tech-startups-helping-hand/406247/

337 James Drake, 'The NATO Communications and Information Agency Selects Oracle Cloud Infrastructure', Oracle, 11 September 2025, https://www.oracle.com/nl/news/announcement/nato-communications-and-information-agency-selects-oci-2025-09-11/

338 Oracle, 'US Defense and Intelligence', https://www.oracle.com/defense-intelligence/; also see: Oracle, 'Oracle for Defense and Intelligence', 2024 https://www.oracle.com/a/ocom/docs/industries/government/defense-accelerate-misson-br.pdf

339 Oracle, 'Imperatives for Building the Digital Shield of America', 2025, https://www.oracle.com/a/ocom/docs/industries/3-imperatives-building-digital-shield.pdf

340 Mara Hvistendahl, 'How Oracle Sells Repression in China', The Intercept, 18 February 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/; Mara Hvistendahl, 'How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"', The Intercept, 22 April 2021, https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/ See also: Dake Kang and Yael Grauer, 'Detailed findings from AP investigation into how US tech firms enabled China's digital police state', AP, 9 September 2025, https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-a80904158b771a14d5a734947f28d71b

341 Mara Hvistendahl, 'How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"', The Intercept, 22 April 2021, https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/

342 Mara Hvistendahl, 'How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"', The Intercept, 22 April 2021, https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/

343 The "Protecting Americans from Foreign Adversary Controlled Applications Act"

344 Sam Levin and Mark Sweney, 'TikTok announces it has finalized deal to establish US entity, sidestepping ban', The Guardian, 23 January 2026, https://www.theguardian.com/us-news/2026/jan/22/tiktok-us-venture-oracle. See also Georgia Gee, 'Poised to Take Over TikTok, Oracle Is Accused of Clamping Down on Pro-Palestine Dissent', The Intercept, 18 February 2025, https://theintercept.com/2025/02/18/oracle-tiktok-israel-palestine-gaza/; Shawn Musgrave, 'To Ban TikTok, Supreme Court Would Rank "National Security" Before First Amendment', The Intercept, 8 January 2025, https://theintercept.com/2025/01/08/tiktok-ban-supreme-court-first-amendment/; The Soufan Center, 'IntelBrief: TikTok's Testimony Troubles', 28 March 2023, https://thesoufancenter.org/intelbrief-2023-march-28/ and Andrew Eversden, 'Is using TikTok a national security risk?', C4ISRNET, 16 December 2019, https://www.fifthdomain.com/congress/capitol-hill/2019/12/16/is-using-tiktok-a-national-security-risk/

345 Eli Clifton, 'Oracle execs: Love Israel or maybe this isn't the job for you', RS, 3 October 2025, https://responsiblestatecraft.org/oracle-tiktok-israel-2674151514/

346 Sophie Shulman, 'Oracle CEO: "If we continue on our current trajectory, reaching a valuation of a trillion dollars is inevitable"', CTech, 14 November 2024, https://www.calcalistech.com/ctechnews/article/t05ji8sue

347 Oracle Employees for Palestine, 'Oracle does not support Palestine', Substack, 14 June 2024, https://oracleforpalestine.substack.com/p/oracle-for-palestine; also see Georgia Gee, 'Oracle allegedly suppresses Pro-Palestinian voices & cuts charity support amid TikTok takeover bid', The Intercept via Business and Human Rights Center, 18 February 2025, https://www.business-humanrights.org/en/latest-news/oracle-allegedly-suppresses-pro-palestinian-voices-cuts-charity-support-amid-tiktok-takeover-bid/

348 Oracle, 'Oracle Environmental and Social Impact Report', https://www.oracle.com/social-impact/

349 Oracle, 'Oracle's Policy Positions', February 2024, https://www.oracle.com/a/ocom/docs/corporate/citizenship/oracle-policy-positions.pdf

350 Oracle, 'Oracle Human Rights Statement', March 2024, https://www.oracle.com/a/ocom/docs/corporate/citizenship/human-rights-statement.pdf

351 Arab Solutions, 'Ethics and Responsible AI Development – Oracle's Approach', 5 July 2025, https://www.arabsolutionsgroup.com/2025/07/05/ethics-and-responsible-ai-development-oracles-approach/; Vibhuti Kadam, 'AI revolution: Oracle's vision for ethical and sustainable AI integration', ET Edge Insights, 1 July 2024, https://etedge-insights.com/technology/artificial-intelligence/ai-revolution-oracles-vision-for-ethical-and-sustainable-ai-in-

tegration/
352 Oracle, "General Oracle Privacy Policy", https://www.oracle.com/uk/legal/privacy/privacy-policy/; Oracle, "Privacy @ Oracle", https://www.oracle.com/legal/privacy/
353 Oracle, "Oracle Services Privacy Policy", https://www.oracle.com/uk/legal/privacy/services-privacy-policy/; Oracle, "Data Processing Agreement for Oracle Services", version 14 August 2025, https://www.oracle.com/contracts/docs/data-processing-agreement-oracle-services-081425.pdf
354 Oracle, "Oracle Services Privacy Policy", sections "Services Personal Information" and "Customer instructions", Oracle, "Oracle Services Privacy Policy", https://www.oracle.com/uk/legal/privacy/services-privacy-policy/; Oracle, "Data Processing Agreement for Oracle Services", version 14 August 2025, https://www.oracle.com/contracts/docs/data-processing-agreement-oracle-services-081425.pdf
355 Oracle, "Oracle Services Privacy Policy", section "Systems Operations Data Processing Terms", Oracle, "Oracle Services Privacy Policy", https://www.oracle.com/uk/legal/privacy/services-privacy-policy/; Oracle, "Data Processing Agreement for Oracle Services", version 14 August 2025, https://www.oracle.com/contracts/docs/data-processing-agreement-oracle-services-081425.pdf
356 Oracle, "Data Processing Agreement for Oracle Services", version 14 August 2025, sections 1 and 2, Oracle, "Oracle Services Privacy Policy", https://www.oracle.com/uk/legal/privacy/services-privacy-policy/; Oracle, "Data Processing Agreement for Oracle Services", version 14 August 2025, https://www.oracle.com/contracts/docs/data-processing-agreement-oracle-services-081425.pdf
357 See Section 4.5 above for the discussion of Oracle's defence, intelligence and government-cloud relationships.
358 Oracle, "Joint Warfighting Cloud Capability (JWCC)", https://www.oracle.com/uk/defense-intelligence/jwcc/
359 Oracle, "Oracle Customer Data Research and Development Privacy Policy", https://www.oracle.com/legal/privacy/customer-data-research-development-privacy-policy/
360 Musk became the first person to achieve a net worth of more than half a trillion (500 billion) dollars in October 2025: Liv McMahon et al., 'Who is Elon Musk and what is his net worth?', BBC, 3 February 2026, https://www.bbc.com/news/articles/c0r1975ded7o
361 Lora Kolodny, ''Muskonomy' shakeup: SpaceX valuation approaches Tesla's after merger with xAI', CNBC, 3 February 2026, https://www.cnbc.com/2026/02/03/muskonomy-shakeup-spacex-valuation-after-xai-merger-nears-tesla.html
362 Echo Wang et al., 'Exclusive: SpaceX generated about $8 billion in profit last year ahead of IPO, sources say', Reuters, 30 January 2026, https://www.reuters.com/business/finance/spacex-generated-about-8-billion-profit-last-year-ahead-ipo-sources-say-2026-01-30/
363 Musk owns an estimated 43 per cent of SpaceX: Lora Kolodny, ''Muskonomy' shakeup: SpaceX valuation approaches Tesla's after merger with xAI', CNBC, 3 February 2026, https://www.cnbc.com/2026/02/03/muskonomy-shakeup-spacex-valuation-after-xai-merger-nears-tesla.html and Samantha Subin, 'Musk's xAI, SpaceX combo is the biggest merger of all time, valued at $1.25 trillion', CNBC, 3 February 2026, https://www.cnbc.com/2026/02/03/musk-xai-spacex-biggest-merger-ever.html Also see Robert Wall, 'SpaceX Buys xAI As Musk Doubles Down On Space-Based AI', Aviation Week, 3 February 2026, https://aviationweek.com/space/satellites/spacex-buys-xai-musk-doubles-down-space-based-ai
364 Samantha Subin, 'Musk's xAI, SpaceX combo is the biggest merger of all time, valued at $1.25 trillion', CNBC, 3 February 2026, https://www.cnbc.com/2026/02/03/musk-xai-spacex-biggest-merger-ever.html
365 Kate Conger and Ryan Mac, 'Elon Musk Wants to Build an A.I. Satellite Factory on the Moon', The New York Times, 10 February 2026, https://www.nytimes.com/2026/02/10/technology/elon-musk-lunar-factory.html
366 Steve Lohr, 'Elon Musk's SpaceX Plans $55 Billion Investment to Make A.I. Chips', The New York Times, 7 May 2026, https://www.nytimes.com/2026/05/07/business/spacex-chips-terafab.html
367 Sandra Erwin, 'With Starshield, SpaceX readies for battle', SpaceNews, 19 January 2023, https://spacenews.com/with-starshield-spacex-readies-for-battle/
368 Andy Pasztor, 'For Rocket Start-Up, Sky's the Limit', The Wall Street Journal, 15 September 2005, https://www.wsj.com/articles/SB112674801818941381 (via: https://archive.ph/1MGwo /).

369 Sandra Erwin, 'With Starshield, SpaceX readies for battle', SpaceNews, 19 January 2023, https://spacenews.com/with-starshield-spacex-readies-for-battle/
370 Zoriana Semenovych and Daria Bevziuk, 'UKR: Ukraine cut off Starlink-aided Russian drones', Arsenal, 12 February 2026, https://www.arsenal.eu/p/ukr-why-ukraine-cut-off-starlink-aided-russian-drones; Tony Osborne, 'Russia Using Starlink-Equipped Attack Drones For Precision Strikes', Aviation Week, 28 January 2026, https://aviationweek.com/defense/budget-policy-operations/russia-using-starlink-equipped-attack-drones-precision-strikes
371 Paul Sonne and Maria Varenikova, 'Musk's Starlink Blocks Russian Troops' Internet Access at Ukraine's Request', The New York Times, 5 February 2026, https://www.nytimes.com/2026/02/05/world/europe/starlink-blocks-russian-troops-access.html and France24 with Reuters, 'SpaceX has stopped Russia's 'unauthorised' use of Starlink against Ukraine, Musk says', 1 February 2026, https://www.france24.com/en/europe/20260201-spacex-stopped-russia-unauthorised-starlink-musk
372 Micah Maidenberg and Drew FitzGerald, 'Musk's SpaceX Forges Tighter Links With U.S. Spy and Military Agencies', The Wall Street Journal, 20 February 2024, via: https://archive.ph/20240322172945/https://www.wsj.com/tech/musks-spacex-forges-tighter-links-with-u-s-spy-and-military-agencies-512399bd
373 Sandra Erwin, 'With Starshield, SpaceX readies for battle', SpaceNews, 19 January 2023, https://spacenews.com/with-starshield-spacex-readies-for-battle/
374 Via SpaceX, 'SpaceX Code of Ethics and Business Conduct', April 2016, https://web.archive.org/web/20170829044849/https://www.spacex.com/sites/spacex/files/supplier_code_of_ethics.pdf
375 Starlink, "Global Privacy Policy", effective 15 January 2026, https://starlink.com/privacy; SpaceX website privacy policy, https://www.spacex.com/assets/media/privacy_policy_spacex.pdf
376 David Jeans and Joey Roulette, "Musk's Starlink updates privacy policy to allow consumer data to train AI", Reuters, 30 January 2026, https://www.reuters.com/legal/litigation/musks-starlink-updates-privacy-policy-allow-consumer-data-train-ai-2026-01-30/
377 Starlink, "Global Privacy Policy", effective 15 January 2026; Reuters, 30 January 2026.
378 See Section 4.6 above.
379 Stephen Losey, 'Pentagon taps Google Gemini, launches new site to boost AI use', Defense News, 9 December 2025, https://www.defensenews.com/pentagon/2025/12/09/pentagon-taps-google-gemini-launches-new-site-to-boost-ai-use/
380 Nikita Ostrovsky, 'A Timeline of the Battle for OpenAI: Musk, Altman, and the For-Profit Shift', TIME Magazine, 27 October 2025, https://time.com/7328674/openai-chatgpt-sam-altman-elon-musk-timeline/
381 Initial investors' returns are capped at 100 times their investment.
382 Robert Burnson, 'Musk Seeks Up to $134 Billion Damages From OpenAI, Microsoft', Bloomberg, 17 January 2026, https://www.bloomberg.com/news/articles/2026-01-17/musk-seeks-up-to-134-billion-damages-from-openai-microsoft and Superior Court of California, 'Musk v Altman OpenAI Complaint, 29 February 2024, https://www.courthousenews.com/wp-content/uploads/2024/02/musk-v-altman-openai-complaint-sf.pdf
383 Irfan Ahmed, 'Who Really Owns OpenAI? The Billion-Dollar Breakdown', Digital Information World, 21 September 2025, https://www.digitalinformationworld.com/2025/09/who-really-owns-openai-billion-dollar.html
384 Berber Jin, 'Oracle, OpenAI Sign $300 Billion Cloud Deal', The Wall Street Journal, 10 September 2025, https://www.wsj.com/business/openai-oracle-sign-300-billion-computing-deal-among-biggest-in-history-ff27c8fe
385 Caroline O'Donovan, Taylor Telford and Jaclyn Peiser, 'Tech leaders' alliance with Trump is tested by a killing in Minneapolis', The Washington Post, 27 January 2026, https://www.washingtonpost.com/technology/2026/01/27/tech-criticism-trump-ice-pretti/
386 Gerrit De Vynck, 'AI companies get comfortable offering their technology to the military', The Washinton Post, 8 November 2024, https://www.washingtonpost.com/technology/2024/11/08/anthropic-meta-pentagon-military-openai/
387 Gerrit De Vynck, 'OpenAI partners with weapons start-up Anduril on military AI', The Washington Post, 4 December 2024, https://www.washingtonpost.com/technology/2024/12/04/openai-anduril-military-ai/; Gerrit De Vynck, 'OpenAI employees question the ethics of military deal with startup Anduril', The Washington Post, 6 De-

cember 2024, https://www.washingtonpost.com/technology/2024/12/06/openai-anduril-employee-military-ai/
388 Gerrit De Vynck, 'OpenAI employees question the ethics of military deal with startup Anduril', The Washington Post, 6 December 2024, https://www.washingtonpost.com/technology/2024/12/06/openai-anduril-employee-military-ai/.https://www.washingtonpost.com/technology/2024/12/06/openai-anduril-employee-military-ai/
389 Courtney Albon, 'Pentagon taps four commercial tech firms to expand military use of AI', Defense News, 15 July 2025, https://www.defensenews.com/pentagon/2025/07/15/pentagon-taps-four-commercial-tech-firms-to-expand-military-use-of-ai/
390 Gerrit De Vynck, 'How Big Tech is co-opting the rising stars of artificial intelligence', The Washington Post, 2 October 2023, https://www.washingtonpost.com/technology/2023/09/30/anthropic-amazon-artificial-intelligence/. Another early investment worth USD 500 million came from the now bankrupt FTX crypto-currency exchange under the leadership of the now imprisoned fraudster Sam Bankman-Fried. Most of that stake was sold in 2024 for USD 884 million, including to a group aligned with Mubadala, a sovereign wealth fund in the United Arab Emirates. (MacKenzie Sigalos, 'FTX estate selling majority stake in AI startup Anthropic for $884 million, with bulk going to UAE', CNBC, 25 March 2024, https://www.cnbc.com/2024/03/25/ftx-estate-sells-majority-stake-in-startup-anthropic-for-884-million.html).
391 Shannon Carroll, 'Nvidia and Microsoft back Anthropic in a $45 billion bid for AI scale', Quartz, 18 November 2025, https://qz.com/nvidia-microsoft-anthropic-partnership-claude-azure; Microsoft, 'Microsoft, NVIDIA and Anthropic announce strategic partnerships', 18 November 2025, https://blogs.microsoft.com/blog/2025/11/18/microsoft-nvidia-and-anthropic-announce-strategic-partnerships/
392 Shannon Carroll, 'Nvidia and Microsoft back Anthropic in a $45 billion bid for AI scale', Quartz, 18 November 2025, https://qz.com/nvidia-microsoft-anthropic-partnership-claude-azure
393 Natallie Rocha, 'Anthropic's C.E.O. Says It Could Grow by 80 Times This Year', The New York Times, 6 May 2026, https://www.nytimes.com/2026/05/06/technology/anthropic-ceo-ai-growth.html
394 Anthropic, 'Lawrence Livermore National Laboratory expands Claude for Enterprise use to empower scientists and researchers', 9 July 2025, https://www.anthropic.com/news/lawrence-livermore-national-laboratory-expands-claude-for-enterprise-to-empower-scientists-and
395 Morgan Gress, 'Anthropic and Palantir Partner to Bring Claude AI Models to AWS for U.S. Government Intelligence and Defense Operations', Business Wire, 7 November 2024, https://www.businesswire.com/news/home/20241107699415/en/Anthropic-and-Palantir-Partner-to-Bring-Claude-AI-Models-to-AWS-for-U.S.-Government-Intelligence-and-Defense-Operations https://techcrunch.com/2024/11/07/anthropic-teams-up-with-palantir-and-aws-to-sell-its-ai-to-defense-customers/; Victor Tangermann, 'The AI Startup Anthropic, Which Is Always Talking About How Ethical It Is, Just Partnered With Palantir', Futurism, 8 November 2024, https://futurism.com/the-byte/ethical-ai-anthropic-palantir
396 Dario Amodei, 'Machines of Loving Grace: How AI Could Transform the World for the Better', October 2024, https://darioamodei.com/essay/machines-of-loving-grace
397 Dario Amodei, 'The Adolescence of Technology: Confronting and Overcoming the Risks of Powerful AI', January 2026, https://www.darioamodei.com/essay/the-adolescence-of-technology
398 Kyle Wiggers, 'Anthropic teams up with Palantir and AWS to sell AI to defense customers', TechCrunch, 7 November 2024, https://techcrunch.com/2024/11/07/anthropic-teams-up-with-palantir-and-aws-to-sell-its-ai-to-defense-customers/
399 Mikayla Easley, 'Pentagon awards mega contracts to Musk-owned company, other firms for new 'frontier AI' projects', DefenseScoop, 14 July 2025, https://defensescoop.com/2025/07/14/pentagon-ai-contracts-musk-xai-google-openai-anthropic-cdao/ also see: Courtney Albon, 'Pentagon taps four commercial tech firms to expand military use of AI', Defense News, 15 July 2025, https://www.defensenews.com/pentagon/2025/07/15/pentagon-taps-four-commercial-tech-firms-to-expand-military-use-of-ai/
400 Mikayla Easley, 'Pentagon awards mega contracts to Musk-owned company, other firms for new 'frontier AI' projects', DefenseScoop, 14 July 2025, https://defensescoop.com/2025/07/14/pentagon-ai-contracts-musk-xai-google-openai-anthropic-cdao/
401 Anthropic, 'Anthropic and the Department of Defense to advance responsible AI in defense operations',

14 July 2024, .
402 Stephen Losey, 'Pentagon taps Google Gemini, launches new site to boost AI use', Defense News, 9 December 2025, https://www.defensenews.com/pentagon/2025/12/09/pentagon-taps-google-gemini-launches-new-site-to-boost-ai-use/
403 Konstantin Totopin and David Klepper, 'Pentagon is embracing Musk's Grok AI chatbot as it draws global outcry', Defense News, 13 January 2026, https://www.defensenews.com/news/pentagon-congress/2026/01/13/pentagon-is-embracing-musks-grok-ai-chatbot-as-it-draws-global-outcry/; also see Jon Harper, 'New Pentagon report on China's military notes Beijing's progress on LLMs', DefenseScoop, 26 December 2025, https://defensescoop.com/2025/12/26/dod-report-china-military-and-security-developments-prc-ai-llm/
404 Jon Harper, 'Pentagon adding ChatGPT to its enterprise generative AI platform', DefenseScoop, 9 February 2026, https://defensescoop.com/2026/02/09/pentagon-adding-chatgpt-to-enterprise-generative-ai-platform/
405 Brandi Vincent, '5 out of 6 military branches have elevated GenAI.mil as their go-to enterprise AI platform', DefenseScoop, 2 February 2026, https://defensescoop.com/2026/02/02/military-branches-genai-mil-enterprise-ai-adoption/
406 Brandi Vincent and Drew F. Lawrence, 'The era of GenAI.mil is here. Users have mixed reactions and many questions', DefenseScoop, 18 December 2025, https://defensescoop.com/2025/12/18/genai-mil-users-have-mixed-reactions-and-many-questions/
407 Konstantin Totopin and David Klepper, 'Pentagon is embracing Musk's Grok AI chatbot as it draws global outcry', Defense News, 13 January 2026, https://www.defensenews.com/news/pentagon-congress/2026/01/13/pentagon-is-embracing-musks-grok-ai-chatbot-as-it-draws-global-outcry/
408 Keach Hagey, Shalini Ramachandran and Amrith Ramkumar, 'Anthropic-Pentagon Clash Over Limits on AI Puts $200 Million Contract at Risk', The Wall Street Journal, 29 January 2026, https://www.wsj.com/tech/ai/anthropic-ai-defense-department-contract-947d5f33. Also see: Reed Albergotti,
'Defense Secretary Pete Hegseth jabs Anthropic over safety policies', Semafor, 16 January 2026, https://www.semafor.com/article/01/16/2026/defense-secretary-pete-hegseth-jabs-anthropic-over-safety-policies
409 Keach Hagey, Shalini Ramachandran and Amrith Ramkumar, 'Anthropic-Pentagon Clash Over Limits on AI Puts $200 Million Contract at Risk', The Wall Street Journal, 29 January 2026, https://www.wsj.com/tech/ai/anthropic-ai-defense-department-contract-947d5f33. Also see: Reed Albergotti,
'Defense Secretary Pete Hegseth jabs Anthropic over safety policies', Semafor, 16 January 2026, https://www.semafor.com/article/01/16/2026/defense-secretary-pete-hegseth-jabs-anthropic-over-safety-policies
410 Dave Lawler, 'Exclusive: Pentagon warns Anthropic will "pay a price" as feud escalates', Axios, 16 February 2026, https://www.axios.com/2026/02/16/anthropic-defense-department-relationship-hegseth
Also see: David Jeans and Mike Stone, 'Palantir faces challenge to remove Anthropic from Pentagon's AI software', Reuters, 4 March 2026, https://www.reuters.com/technology/palantir-faces-challenge-remove-anthropic-pentagons-ai-software-2026-03-04/; Olivia Solon and Amy Thomson, 'Anthropic talks snag on AI surveillance, weapons', Bloomberg, 16 February 2026, via https://www.msn.com/en-us/technology/artificial-intelligence/pentagon-is-close-to-cutting-ties-with-anthropic-report-says/ar-AA1WsFwW
411 Mike Isaac, 'Federal Court Denies Anthropic's Motion to Lift 'Supply Chain Risk' Label', The New York Times, 8 April 2026, https://www.nytimes.com/2026/04/08/technology/anthropic-pentagon-risk-circuit-court.html
412 Amrith Ramkumar, Keach Hagey and Vera Bergengruen, 'Pentagon Used Anthropic's Claude in Maduro Venezuela Raid', The Wall Street Journal, 15 February 2026, https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17
413 Times of India referring to Wall Street Journal reporting on the issue: "AI at war: US strikes Iran with Anthropic's Clause hours after Trump", The Times of India, 2 March 2026, https://timesofindia.indiatimes.com/technology/tech-news/ai-at-war-us-strikes-iran-with-anthropics-claude-hours-after-trump-ban/articleshow/128941828.cms. Also see: Parmy Olson, 'Claude AI Helped US Bomb Iran. But How Exactly?, Bloomberg, 4 March 2026, https://www.bloomberg.com/opinion/articles/2026-03-04/iran-strikes-anthropic-claude-ai-helped-us-attack-but-how-exactly; Ian Duncan, 'Anthropic's AI tool Claude central to U.S. campaign in Iran, amid bitter

feud', The Washington Post, 4 March 2026, https://www.washingtonpost.com/technology/2026/03/04/anthropic-ai-iran-campaign/
414 Katrina Manson, 'Anthropic Made Pitch in Drone Swarm Contest During Pentagon Feud', Bloomberg, 2 March 2026, https://www.bloomberg.com/news/articles/2026-03-02/anthropic-made-pitch-in-drone-swarm-contest-during-pentagon-feud.
415 Tanya Noury, 'Pentagon freezes out Anthropic as it signs deals with AI rivals', Defense News, 1 May 2026, https://www.defensenews.com/news/pentagon-congress/2026/05/01/pentagon-freezes-out-anthropic-as-it-signs-deals-with-ai-rivals/
416 Yuval Abraham, "A mass assassination factory': Inside Israel's calculated bombing of Gaza', +972 Magazine, 30 November 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/
417 Anna Ahronheim, 'Israel's operation against Hamas was the world's first AI war', Jerusalem Post, 27 May 2021, https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371
418 Yuval Abraham, "A mass assassination factory': Inside Israel's calculated bombing of Gaza', +972 Magazine, 30 November 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/
419 Yuval Abraham, "Lavender': The AI machine directing Israel's bombing spree in Gaza', +972 Magazine, 3 April 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/
420 Sophia Goodfriend, 'Why human agency is still central to Israel's AI-powered warfare', +972 Magazine, 25 April 2025, https://www.972mag.com/israel-gaza-lavender-ai-human-agency/
421 Bethan McKernan and Quique Kierszenbaum, 'This article is more than 2 years old 'We're focused on maximum damage': ground offensive into Gaza seems imminent', The Guardian, 10 October 2023, https://www.theguardian.com/world/2023/oct/10/right-now-it-is-one-day-at-a-time-life-on-israels-frontline-with-gaza
422 Yuval Abraham, "A mass assassination factory': Inside Israel's calculated bombing of Gaza', +972 Magazine, 30 November 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/
423 Hanno Hauenstein, 'Germany never stopped arming Israel's genocide', +972 Magazine, 20 January 2026, https://www.972mag.com/germany-israel-weapons-cybersecurity-genocide/
424 (Google-translated:) Dean Shmuel Elmas, 'Record year for Israeli defense tech: $1 billion poured into startups in the field', Globes, 8 December 2025, https://www.globes.co.il/news/article.aspx?did=1001528553
425 (Google-translated:) Dean Shmuel Elmas, 'Record year for Israeli defense tech: $1 billion poured into startups in the field', Globes, 8 December 2025, https://www.globes.co.il/news/article.aspx?did=1001528553
426 Amitai Ziv, 'Dark Clouds: Israel Is Splurging on Microsoft and Regulators Are Concerned', Haaretz, 29 October 2020, https://www.haaretz.com/israel-news/tech-news/2020-10-29/ty-article/.premium/dark-clouds-israels-splurging-on-microsoft-regulators-are-concerned/0000017f-e0b7-d7b2-a77f-e3b7b9430000
427 Amitai Ziv, 'Israel Picks Google, Amazon for Massive Official Cloud; 'Data Will Remain Here'', Haaretz, 21 April 2021, https://www.haaretz.com/israel-news/tech-news/2021-04-21/ty-article/israel-picks-google-amazon-for-official-state-cloud/0000017f-e896-dc91-a17f-fc9fd1ce0000; also see: Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/
428 Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/; Sam Biddle, 'As Israel Bombed Gaza, Amazon Did Business With Its Bomb-Makers', The Intercept, 24 October 2025, https://theintercept.com/2025/10/24/amazon-weapons-gaza-israel-rafael-iai/
429 Amitai Ziv, 'Israel Picks Google, Amazon for Massive Official Cloud; 'Data Will Remain Here'', Haaretz, 21 April 2021, https://www.haaretz.com/israel-news/tech-news/2021-04-21/ty-article/israel-picks-google-amazon-for-official-state-cloud/0000017f-e896-dc91-a17f-fc9fd1ce0000
430 Boaz Maoz, 'The new Google Cloud Region in Israel is now open', Google, 19 October 2022, https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-in-israel-is-now-open
431 Sam Biddle, 'Google Worried It Couldn't Control How Israel Uses Project Nimbus, Files Reveal', The Intercept, 12 May 2025, https://theintercept.com/2025/05/12/google-nimbus-israel-military-ai-human-rights/
432 Yuval Abraham, "No restrictions' and a secret 'wink': Inside Israel's deal with Google, Amazon', +972 Magazine, 29 October 2025, https://www.972mag.com/project-nimbus-contract-google-amazon-israel/; Harry

Davies and Yuval Abraham, 'Revealed: Israel demanded Google and Amazon use secret 'wink' to sidestep legal orders', The Guardian, 29 October 2025, https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code and refuted by Google and Amazon: Mohammed R. Mhawish, 'Watched, Tracked, and Targeted Life in Gaza under Israel's all-encompassing surveillance regime', Intelligencer, 3 December 2025, https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html

433 Hundreds of workers at both companies signing an open letter within months calling to cut ties with the Israeli military: The Guardian, 'We are Google and Amazon workers. We condemn Project Nimbus: Anonymous Google and Amazon workers', 12 October 2021, https://www.theguardian.com/commentisfree/2021/oct/12/google-amazon-workers-condemn-project-nimbus-israeli-military-contract

434 Gerrit De Vynck and Caroline O'Donovan, 'Google fires more workers after CEO says workplace isn't for politics', Washington Post, 22 April 2024, https://www.washingtonpost.com/technology/2024/04/22/google-nimbus-israel-protest-fired-workers/

435 Gerrit De Vynck and Caroline O'Donovan, 'Google fires more workers after CEO says workplace isn't for politics', Washington Post, 22 April 2024, https://www.washingtonpost.com/technology/2024/04/22/google-nimbus-israel-protest-fired-workers/

436 Sam Biddle, 'Israeli Weapons Firms Required to Buy Cloud Services From Google and Amazon', The Intercept, 1 May 2024, https://theintercept.com/2024/05/01/google-amazon-nimbus-israel-weapons-arms-gaza/

437 Billy Perrigo, 'Exclusive: Workers at Google DeepMind Push Company to Drop Military Contracts', TIME Magazine, 19 January 2026, https://time.com/7013685/google-ai-deepmind-military-contracts-israel/

438 Billy Perrigo, 'Exclusive: Workers at Google DeepMind Push Company to Drop Military Contracts', TIME Magazine, 19 January 2026, https://time.com/7013685/google-ai-deepmind-military-contracts-israel/

439 Gerrit De Vynck, 'Google rushed to sell AI tools to Israel's military after Hamas attack', The Washington Post, 21 January 2025, https://www.washingtonpost.com/technology/2025/01/21/google-ai-israel-war-hamas-attack-gaza/

440 Sam Biddle, 'Israeli Weapons Firms Required to Buy Cloud Services From Google and Amazon', The Intercept, 1 May 2024, https://theintercept.com/2024/05/01/google-amazon-nimbus-israel-weapons-arms-gaza/

441 Col. Racheli Dembinsky speaking at a conference titled "IT for IDF", July 2024, https://www.youtube.com/watch?v=qLBDfnZJrC8 The Intercept revealed that Google had planned to sponsor the conference but that its name was erased at the last minute. Moreover, also Nokia, Dell and Canon were present at the conference: Sam Biddle, 'Google Planned to Sponsor IDF Conference That Now Denies Google Was Sponsor', The Intercept, 25 July 2024, https://theintercept.com/2024/07/25/google-it-idf-tech-conference-sponsor/

442 Yuval Abraham, "Order from Amazon': How tech giants are storing mass data for Israel's war', +972 Magazine, 4 August 2024, https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/

443 Google contested the allegations and said it did not violate its AI principles because the account's usage of its AI services was too small to be "meaningful". "The ticket originated from an account with less than a couple hundred dollars of monthly spend on AI products, which makes any meaningful usage of AI impossible." Google's "cloud video intelligence" service says that tracking objects in video is free for the first 1,000 minutes and then costs 15 cents per minute. Gerrit De Vynck, 'Google helped Israeli military contractor with AI, whistleblower alleges', The Washington Post, 1 February 2026, https://www.washingtonpost.com/technology/2026/02/01/google-ai-israel-military/

444 Yuval Abraham, "Order from Amazon': How tech giants are storing mass data for Israel's war', +972 Magazine, 4 August 2024, https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/

445 Jack Poulson and Lee Fang, 'Google's $45 Million Contract With Netanyahu's Office to Spread Israeli Propaganda', Drop Site News, 3 September 2025, https://www.dropsitenews.com/p/google-youtube-netanyahu-israel-propaganda-gaza-famine

446 Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

447 Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

448 See Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July

2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/ and Google, 'Welcome to Cloud OnBoard', https://www.documentcloud.org/documents/22119704-webinar-big-data-ml/ slide 100 and onwards.

449 Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

450 Sam Biddle, 'Documents Reveal Advanced AI Tools Google Is Selling to Israel', The Intercept, 24 July 2022, https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

451 Yuval Abraham, ''Order from Amazon': How tech giants are storing mass data for Israel's war', +972 Magazine, 4 August 2024, https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/

452 Sheera Frenkel, 'Israel Deploys Expansive Facial Recognition Program in Gaza', The New York Times, 27 March 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

453 Sheera Frenkel, 'Israel Deploys Expansive Facial Recognition Program in Gaza', The New York Times, 27 March 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

454 Robert Watts, 'Please join us next week in Farnborough', LinkedIn, https://www.linkedin.com/posts/robert-watts-b661514b_please-join-us-next-week-in-farnborough-on-activity-7171096975189200896-GDHw/

455 Sheera Frenkel, 'Israel Deploys Expansive Facial Recognition Program in Gaza', The New York Times, 27 March 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

456 By Elizabeth Dwoskin, 'Israel escalates surveillance of Palestinians with facial recognition program in West Bank', The Washington Post, November 8, 2021, https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

457 Adam Satariano and Paul Mozur, 'Facial Recognition Powers 'Automated Apartheid' in Israel, Report Says', The New York Times, 1 May 2023, https://www.nytimes.com/2023/05/01/technology/israel-palestine-facial-recognition.html

458 Mustafa Abu Sneineh, 'Meet Blue Wolf, the app Israel uses to spy on Palestinians in the occupied West Bank', Middle East Eye, 9 November 2021, https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians

459 Yuval Abraham, 'Leaked documents expose deep ties between Israeli army and Microsoft', +972 Magazine, 23 January 2025, https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/

460 Yuval Abraham, 'Leaked documents expose deep ties between Israeli army and Microsoft', +972 Magazine, 23 January 2025, https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/

461 Microsoft, 'Microsoft statement on the issues relating to technology services in Israel and Gaza', 15 May 2025, https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/

462 Yuval Abraham, 'Microsoft storing Israeli intelligence trove used to attack Palestinians', +972 Magazine, 6 August 2025, https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/

463 Microsoft, 'Update on ongoing Microsoft review', 25 September 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/; Sheera Frenkel, 'Microsoft Disables Some Services to Israel's Defense Ministry', The New York Times, 25 September 2025, https://www.nytimes.com/2025/09/25/technology/microsoft-israel-defense-ministry.html; Harry Davies and Yuval Abraham, ''A million calls an hour': Israel relying on Microsoft cloud for expansive surveillance of Palestinians', The Guardian, 6 August 2025, https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud and Harry Davies, 'Activists in Netherlands protest on roof of Microsoft site storing Israeli military data', The Guardian, 10 August 2025, https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data

464 Brad Smith, 'Update on ongoing Microsoft review', Microsoft, 25 September 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/; Microsoft, 'Microsoft statement on the issues relating to technology services in Israel and Gaza', 15 May 2025, https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/. Also see: Sheera Frenkel, 'Microsoft Disables Some Services to Israel's Defense Ministry', The New York Times, 25 September 2025, https://www.nytimes.com/2025/09/25/technology/microsoft-israel-defense-ministry.html

465 Stijn Bronzwaer, 'The West is superior and must always win. This is how Palantir views the world', NRC,

10 October 2025, https://www.nrc.nl/nieuws/2025/10/10/the-west-is-superior-and-must-always-win-this-is-how-palantir-views-the-world-a4909001

466 Raphaëlle Bacqué, Damien Leloup and Alexandre Piquard, 'Peter Thiel, the libertarian billionaire waging war on government', Le Monde, 22 July 2025, https://www.lemonde.fr/en/summer-reads/article/2025/07/22/peter-thiel-the-libertarian-billionaire-waging-war-on-government_6743617_183.html

467 Courtney Albon, 'Defense tech firms establish AI-focused consortium', Defense News, 6 December 2024, https://www.defensenews.com/pentagon/2024/12/06/defense-tech-firms-establish-ai-focused-consortium/

468 Brooke Smitherman Schmidt, 'Northrop Grumman Partners to Advance Deep Sensing for the US Army', Northrop Grumman, 7 March 2024, https://news.northropgrumman.com/sensors/northrop-grumman-partners-to-advance-deep-sensing-for-the-us-army

469 Nathan Strout, 'Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up', C4ISRNET, 12 August 2021, https://www.c4isrnet.com/industry/2021/08/12/palantir-with-joint-all-domain-command-and-control-the-pentagon-is-finally-catching-up/; Courtney Albon, 'Defense tech firms establish AI-focused consortium', Defense News, 6 December 2024, https://www.defensenews.com/pentagon/2024/12/06/defense-tech-firms-establish-ai-focused-consortium/and Anduril, 'Army Selects Anduril and Palantir to Deliver TITAN Deep Sensing Capability for Long Range Fires', 7 March 2024, https://www.anduril.com/news/army-selects-anduril-and-palantir-to-deliver-titan, Palantir, 'TITAN (Tactical Intelligence Targeting Access Node)', https://www.palantir.com/assets/xrfr7uokpv1b/7kEyhuSSUmfQtsGfIwIWZ4/01f49e667d8ff762dd22ad729c670294/AUSA_Titan__1_.pdf

470 Courtney Albon and Colin Demarest, 'Army chooses Palantir to build next-generation targeting system', C4ISRNET, 6 March 2024, https://www.c4isrnet.com/artificial-intelligence/2024/03/06/army-chooses-palantir-to-build-next-generation-targeting-system/

471 Courtney Albon and Colin Demarest, 'Army chooses Palantir to build next-generation targeting system', C4ISRNET, 6 March 2024, https://www.c4isrnet.com/artificial-intelligence/2024/03/06/army-chooses-palantir-to-build-next-generation-targeting-system/

472 Mark Pomerleau, 'Anduril's Menace tech now preferred hardware for Palantir's Edge software', DefenseScoop, 7 May 2025, https://defensescoop.com/2025/05/07/anduril-palantir-partnership-menace-edge-software/

473 Anduril, 'Anduril and Palantir to Accelerate AI Capabilities for National Security', 6 December 2024, https://www.anduril.com/article/anduril-and-palantir-to-accelerate-ai-capabilities-for-national-security/

474 Cade Metz, Erin Griffith and Kate Conger ,'What's a Palantir? The Tech Industry's Next Big I.P.O.', The New York Times, 26 August 2020, https://www.nytimes.com/2020/08/26/technology/palantir-ipo.html

475 Palantir, 'Palantir to Commence Trading on NYSE on September 30, 2020', 22 September 2020, https://investors.palantir.com/news-details/2020/Palantir-to-Commence-Trading-on-NYSE-on-September-30-2020/

476 Largest Companies by Marketcap: https://companiesmarketcap.com – as of 3 April 2026; also see Capitol Trades, 'Palantir surpasses Raytheon to become largest U.S. defense contractor', 5 December 2025, https://www.capitoltrades.com/buzz/palantir-surpasses-raytheon-to-become-largest-u-s-defense-contractor-2024-12-05.

477 Alex Karp, 'Letter to Shareholders', Palantir, 2 February 2026, https://www.palantir.com/q4-2025-letter/en/

478 See for example Joseph Cox, 'Here is the User Guide for ELITE, the Tool Palantir Made for ICE, 404 Media, 30 January 2026, https://www.404media.co/here-is-the-user-guide-for-elite-the-tool-palantir-made-for-ice/ and for early criticism Sam Biddle and Ryan Devereaux, 'Peter Thiel's Palantir Was Used to Bust Relatives of Migrant Children, New Documents Show', The Intercept, 2 May 2019, https://theintercept.com/2019/05/02/peter-thiels-palantir-was-used-to-bust-hundreds-of-relatives-of-migrant-children-new-documents-show/

479 Michael Steinberger, 'Does Palantir See Too Much?', The New York Times, 21 October 2020, https://www.nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html

480 Caroline Haskins, 'What Does Palantir Actually Do?', WIRED, 11 August 2025, https://www.wired.com/story/palantir-what-the-company-does/

481 See for example: Chris Osuh, 'Palantir's NHS England contract 'opens door to government abuse of power', health bosses told', The Guardian, 12 March 2026, https://www.theguardian.com/technology/2026/

mar/12/palantirs-nhs-england-contract-opens-door-to-government-abuse-of-power-health-bosses-told, Ethan Shone, 'The great Ministry of Defence-to-Palantir pipeline', openDemocracy, 24 January 2026, https://www.opendemocracy.net/en/palantir-ministry-defence-hire-four-officials-2025-record-defence-contract-240-million/, Rowland Manthorpe, 'Coronavirus: NHS unveils 'data platform' to track beds, staff and ventilators', Sky News, 26 March 2020, https://news.sky.com/story/coronavirus-nhs-unveils-data-platform-to-track-beds-staff-and-ventilators-11964216, Good Law Project, 'Stop Palantir in the NHS', https://goodlawproject.org/campaign/stop-palantir-in-the-nhs/, Medact, 'Briefing: Concerns Regarding Palantir Technologies and NHS Data Systems', 12 March 2026, https://www.medact.org/2026/resources/briefings/briefing-palantir-fdp/, Lindsay Clark, 'Manchester hits snooze again on joining Palantir-run NHS data platform', The Register, 20 November 2025, https://www.theregister.com/2025/11/20/manchester_nhs_fdp_deferred and Palantir, 'Palantir for Healthcare (UK)', https://www.palantir.com/uk/healthcare/

482 Stijn Bronzwaer, 'The West is superior and must always win. This is how Palantir views the world', NRC, 10 October 2025, https://www.nrc.nl/nieuws/2025/10/10/the-west-is-superior-and-must-always-win-this-is-how-palantir-views-the-world-a4909001

483 Alex Karp, 'Opinion - I'm a tech CEO, and I don't think tech CEOs should be making policy', The Washington Post, 5 September 2019, https://www.washingtonpost.com/opinions/policy-decisions-should-be-made-by-elected-representatives-not-silicon-valley/2019/09/05/e02a38dc-cf61-11e9-87fa-8501a456c003_story.html

484 Andy Greenberg, 'How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut', Forbes, 14 August 2013, https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/#6590b4f87785; Cade Metz, Erin Griffith and Kate Conger, 'What's a Palantir? The Tech Industry's Next Big I.P.O.', The New York Times, 26 August 2020, https://www.nytimes.com/2020/08/26/technology/palantir-ipo.html.

485 Michael Steinberger, 'Does Palantir See Too Much?', The New York Times, 21 October 2020, https://www.nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html.

486 Jacqueline Klimas and Bryan Bender, 'Palantir goes from Pentagon outsider to Mattis' inner circle', Politico, 11 June 2017, http://www.politico.com/story/2017/06/11/palantir-defense-jim-mattis-inner-circle-239373

487 Sam Biddle, 'Tech Official Pushing TikTok Ban Could Reap Windfall From U.S.–China Cold War', The Intercept, 21 March 2024, https://theintercept.com/2024/03/21/china-tiktok-jacob-helberg-palantir/

488 Cade Metz, Erin Griffith and Kate Conger ,'What's a Palantir? The Tech Industry's Next Big I.P.O.', The New York Times, 26 August 2020, https://www.nytimes.com/2020/08/26/technology/palantir-ipo.html

489 Jen Judson, 'Palantir Takes Fight With Army To Federal Court', Defense News, 1 July 2016, https://www.defensenews.com/home/2016/07/01/palantir-takes-fight-with-army-to-federal-court/

490 Jen Judson, 'US Army extends Palantir's contract for its data-harnessing platform', Defense News, 18 December 2024, https://www.defensenews.com/land/2024/12/18/us-army-extends-palantirs-contract-for-its-data-harnessing-platform/, Reuters, 'Palantir wins combat data system case against U.S. Army - Bloomber', 31 October 2016, https://www.reuters.com/article/technology/palantir-wins-combat-data-system-case-against-us-army-bloomberg-idUSKBN12V248/; Jenna McLaughlin, 'Peter Thiel's CIA-Backed Data Mining Company Wins Court Battle Against the U.S. Army', The Intercept, 31 October 2016, https://theintercept.com/2016/10/31/peter-thiels-cia-backed-data-mining-company-wins-court-battle-against-the-u-s-army/

491 Shane Harris, 'Palantir wins competition to build Army intelligence system', The Washington Post, 26 March 2019, https://www.washingtonpost.com/world/national-security/palantir-wins-competition-to-build-army-intelligence-system/2019/03/26/c6d62bf0-3927-11e9-aaae-69364b2ed137_story.html; Jen Judson, 'Palantir — who successfully sued the Army — has won a major Army contract', Defense News, 29 March 2019, https://www.defensenews.com/land/2019/03/29/palantir-who-successfully-sued-the-army-just-won-a-major-army-contract/

492 Mark Pomerleau, 'Palantir scores US Army contract to build out intelligence data fabric', C4ISRNET, 6 October 2021, https://www.c4isrnet.com/battlefield-tech/2021/10/06/palantir-scores-us-army-contract-to-build-out-intelligence-data-fabric/

493 Aaron Gregg, 'Palantir deepens its Pentagon business with new $110 million Army contract', The Wash-

ington Post, 13 December 2019, https://www.washingtonpost.com/business/2019/12/13/palantir-deepens-its-pentagon-business-with-new-million-army-contract/
494 Jen Judson, 'US Army extends Palantir's contract for its data-harnessing platform', Defense News, 18 December 2018, https://www.defensenews.com/land/2024/12/18/us-army-extends-palantirs-contract-for-its-data-harnessing-platform/
495 Andrew Eversden, 'Palantir wants to be the 'central operating system for all US defense programs'', C4ISRNET, 30 September 2020, https://www.c4isrnet.com/industry/2020/09/30/palantir-wants-to-be-the-central-operating-system-for-all-us-defense-programs/
496 Nathan Strout, 'Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up', C4ISRNET, 12 August 2021, https://www.c4isrnet.com/industry/2021/08/12/palantir-with-joint-all-domain-command-and-control-the-pentagon-is-finally-catching-up/
497 Colin Demarest, 'BigBear.ai delivering US Army digital info system with Palantir's help', Defense News, 30 September 2022, https://www.defensenews.com/industry/2022/09/30/bigbearai-delivering-us-army-digital-info-system-with-palantirs-help/; Colin Demarest, 'Palantir wins contract to help Army quickly process battlefield data', Defense News, 19 October 2022, https://www.defensenews.com/industry/2022/10/19/palantir-wins-contract-to-help-army-quickly-process-battlefield-data/
498 Matthew Gault, 'Palantir Demos AI to Fight Wars But Says It Will Be Totally Ethical Don't Worry About It', VICE News, 26 April 2023, https://www.vice.com/en/article/qjvb4x/palantir-demos-ai-to-fight-wars-but-says-it-will-be-totally-ethical-dont-worry-about-it
499 Colin Demarest, 'Palantir wins $250 million US Army AI research contract', Defense News, 27 September 2023, https://www.defensenews.com/artificial-intelligence/2023/09/27/palantir-wins-250-million-us-army-ai-research-contract/
500 United States Army, 'U.S. Army Awards Enterprise Service Agreement to Enhance Military Readiness and Drive Operational Efficiency', 31 July 2025, https://www.army.mil/article/287506/u_s_army_awards_enterprise_service_agreement_to_enhance_military_readiness_and_drive_operational_efficiency
501 Tamara Rozouvan, 'UK signs GBP1.5 billion deal with Palantir for AI-powered capabilities', Janes Defence Weekly, 1 October 2025.
502 Megan Eckstein, 'Palantir, Lockheed Martin team up to modernize naval combat systems', Defense News, 30 November 2022, https://www.defensenews.com/industry/techwatch/2022/11/30/palantir-lockheed-martin-team-up-to-modernize-naval-combat-systems/
503 Northrop Grumman, 'Northrop Grumman's Lumberjack Advances Battlefield Capabilities', 31 March 2026, https://news.northropgrumman.com/autonomous-systems/northrop-grummans-lumberjack-advances-battlefield-capabilities and Northrop Grumman, 'Northrop Grumman Partners to Advance Deep Sensing for the US Army', 7 March 2024, https://news.northropgrumman.com/sensors/northrop-grumman-partners-to-advance-deep-sensing-for-the-us-army
504 Northrop Grumman, 'Lumberjack™: The Versatile Multi-Target Uncrewed Aircraft System (UAS)', https://www.northropgrumman.com/what-we-do/aircraft/lumberjack
505 Boeing, 'Boeing Defense, Space & Security Partners with Palantir to Accelerate AI Adoption Across Defense, Classified Programs', 23 September 2025, https://investors.boeing.com/investors/news/press-release-details/2025/Boeing-Defense-Space--Security-Partners-with-Palantir-to-Accelerate-AI-Adoption-Across-Defense-Classified-Programs/default.aspx.
506 Stijn Bronzwaer, 'The West is superior and must always win. This is how Palantir views the world', NRC, 10 October 2025, https://www.nrc.nl/nieuws/2025/10/10/the-west-is-superior-and-must-always-win-this-is-how-palantir-views-the-world-a4909001.
507 Elizabeth Gosselin-Malo, 'Ukraine feeds sensitive military data to Palantir AI for training', Defense News, 21 January 2026, https://www.defensenews.com/global/europe/2026/01/21/ukraine-feeds-sensitive-military-data-to-palantir-ai-for-training/.
508 Elizabeth Gosselin-Malo, 'Ukraine feeds sensitive military data to Palantir AI for training', Defense News, 21 January 2026, https://www.defensenews.com/global/europe/2026/01/21/ukraine-feeds-sensitive-military-data-to-palantir-ai-for-training/

509 Itai Zehorai, 'The Data Queen: Meet the Israeli Ambassador of Wall Street's Fastest-Growing Company', Forbes, 9 November 2024, https://forbes.co.il/e/the-data-queen-meet-the-israeli-ambassador-of-wall-streets-fastest-growing-company/
510 Sophia Goodfriend, 'With Gaza war and Trump's return, Silicon Valley embraces a military renaissance', +972 Magazine, 31 December 2024, https://www.972mag.com/gaza-war-trump-silicon-valley-military/
511 Marissa Newman, 'Thiel's Palantir, Israel Agree Strategic Partnership for Battle Tech', Bloomberg, 12 January 2024, https://www.palantir.com/assets/xrfr7uokpv1b/3MuEeA8MLbLDAyxixTsile/9e4a11a7fb058554a8a-1e3cd83e31c09/C134184_finaleprint.pdf
512 United Nations, 'From economy of occupation to economy of genocide Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese', 2 July 2025, https://docs.un.org/en/A/HRC/59/23
513 Youtube (Shorts), ''Our AI kills Palestinians', Palantir CEO Alex Karp on Gaza war', https://www.youtube.com/shorts/0mhNLTy5pbQ
514 Stijn Bronzwaer, 'The West is superior and must always win. This is how Palantir views the world', NRC, 10 October 2025, https://www.nrc.nl/nieuws/2025/10/10/the-west-is-superior-and-must-always-win-this-is-how-palantir-views-the-world-a4909001
515 Jonathan Whittall, 'NEW: Palantir's AI Is Already Playing a Major Role in Tracking Gaza Aid Deliveries', Drop Site News, 26 February 2026, https://www.dropsitenews.com/p/palantir-ai-gaza-humanitarian-aid-cmcc-srs-ngos-banned-israel
516 Stijn Bronzwaer, 'The West is superior and must always win. This is how Palantir views the world', NRC, 10 October 2025, https://www.nrc.nl/nieuws/2025/10/10/the-west-is-superior-and-must-always-win-this-is-how-palantir-views-the-world-a4909001
517 Stijn Bronzwaer, 'The West is superior and must always win. This is how Palantir views the world', NRC, 10 October 2025, https://www.nrc.nl/nieuws/2025/10/10/the-west-is-superior-and-must-always-win-this-is-how-palantir-views-the-world-a4909001
518 Palantir, 'Principles', https://www.palantir.com/pcl/principles/
519 Palantir, 'Principles', https://www.palantir.com/pcl/principles/
520 Palantir, 'Palantir Technologies' Approach to AI Ethics', https://www.palantir.com/pcl/palantir-ai-ethics/
521 Palantir, 'Palantir Human Rights Policy', https://www.palantir.com/assets/xrfr7uokpv1b/29IHCTi-sO8v2pofVMrxtnX/7e91f4f393074f69ae047d01eaebabce/Palantir_Human_Rights_Policy.pdf
522 Amnesty International, 'Failing to do Right: The Urgent Need for Palantir to Respect Human Rights', 2020, https://www.amnestyusa.org/wp-content/uploads/2020/09/Amnest-International-Palantir-Briefing-Report-092520_Final.pdf
523 Sebastiaan Brommersma, Casper Rouffaer and Salsabil Fayed, 'European funders bet big on tech giant Palantir despite concerns over human rights and democracy', Follow the Money, 19 March 2026, https://www.ftm.eu/articles/european-investors-palantir-investment
524 Sebastiaan Brommersma, Casper Rouffaer and Salsabil Fayed, 'European funders bet big on tech giant Palantir despite concerns over human rights and democracy', Follow the Money, 19 March 2026, https://www.ftm.eu/articles/european-investors-palantir-investment
525 Stefania Spezzati and Gwladys Fouche, 'Thiels Palantir Dumped by Norwegian Investor Over Work for Israel', Reuters, 25 October 2024, https://www.reuters.com/technology/thiels-palantir-dumped-by-norwegian-investor-over-work-israel-2024-10-25/
526 Sebastiaan Brommersma, Casper Rouffaer and Salsabil Fayed, 'European funders bet big on tech giant Palantir despite concerns over human rights and democracy', Follow the Money, 19 March 2026, https://www.ftm.eu/articles/european-investors-palantir-investment
527 NL Times, 'Largest Dutch pension fund cuts ties with controversial tech firm Palantir', 2 April 2026, https://nltimes.nl/2026/04/02/largest-dutch-pension-fund-cuts-ties-controversial-tech-firm-palantir and Casper Rouffaer and Sebastiaan Brommersma, 'Pensioenfonds ABP investeert honderden miljoenen in omstreden techbedrijf Palantir', [in Dutch] Follow the Money, 21 January 2026, https://www.ftm.nl/artikelen/abp-investeert-honderden-miljoenen-in-techbedrijf-palantir

528 Lee Fang, 'Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract', The Intercept, 9 March 2019, https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/
529 See for more insights: Katrina Manson, 'Project Maven: A Marine Colonel, His Team, and the Dawn of AI Warfare', W.W. Norton & Company, 2026 and this interview about the book: Justin Hendrix, 'Project Maven and the Age of AI Warfare', Tech Policy, 9 April 2026, https://www.techpolicy.press/project-maven-and-the-age-of-ai-warfare/
530 Colin Demarest, 'Pentagon's Project Maven transition stymied by Congress, official says', Defense News, 26 October 2022, https://www.defensenews.com/artificial-intelligence/2022/10/26/pentagons-project-maven-transition-stymied-by-congress-official-says/.
531 Gregory C. Allen, 'Project Maven brings AI to the fight against ISIS', The Bulletin of the Atomic Scientists, 21 December 2017, https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/.
532 Marcus Weisgerber, 'The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS', Defense One, 14 May 2017, http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/
533 United States Deputy Secretary of Defense, 'Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)', https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf
534 Gregory C. Allen, 'Project Maven brings AI to the fight against ISIS', The Bulletin of the Atomic Scientists, 21 December 2017, https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/
535 Marcus Weisgerber, 'The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS', Defense One, 14 May 2017, http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/
536 Roberto J. Gonzaleaz, 'Militarising Big Tech: The Rise of Silicon Valley's Digital Defence Industry', The Transnational Institute, 7 February 2023, https://www.tni.org/en/article/militarising-big-tech
537 Scott Shane, Cade Metz and Daisuke Wakabayashi, 'How a Pentagon Contract Became an Identity Crisis for Google', The New York Times, 30 May 2018, https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html and Lee Fang, 'Leaked Emails Show Google Expected Lucrative Military Drone AI Work to Grow Exponentially', The Intercept, 31 May 2018, https://theintercept.com/2018/05/31/google-leaked-emails-drone-ai-pentagon-lucrative/
538 Kate Conger and Cade Metz, 'Tech Workers Now Want to Know: What Are We Building This For?', The New York Times, 7 October 2018, https://www.nytimes.com/2018/10/07/technology/tech-workers-ask-censorship-surveillance.html
539 Scott Shane and Daisuke Wakabayashi, 'The Business of War': Google Employees Protest Work for the Pentagon', The New York Times, 4 April 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html
540 Drew Harwell, 'Google bans development of artificial intelligence used in weaponry', The Washington Post, 7 June 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/06/07/google-bans-development-of-artificial-intelligence-used-in-weaponry/
541 Michael Steinberger, 'Does Palantir See Too Much?', The New York Times, 21 October 2020, https://www.nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html
542 Everforth ECS, 'Maintaining Decision Advantage on the Battlefield', https://ecstech.com/solutions/artificial-intelligence/geospatial-intelligence/the-maven-program/
543 Matthew Zeiler, 'Why We're Part of Project Maven', Clarifai, 13 June 2018, https://www.clarifai.com/blog/why-were-part-of-project-maven
544 Roberto J. Gonzalez, 'Militarising Big Tech: The Rise of Silicon Valley's Digital Defence Industry', The Transnational Institute, 7 February 2023, https://www.tni.org/en/article/militarising-big-tech and Roberto J. Gonzalez, 'Militarising Big Tech: The rise of Silicon Valley's digital defence industry', The Transnational Institute, 2023, https://www.tni.org/files/2023-04/Militarising_Big Tech.pdf
545 Colin Demarest and Courtney Albon, 'Q&A: Maxar execs discuss US Army simulation, Project Maven',

C4ISRNET, 5 June 2023, https://www.c4isrnet.com/industry/2023/06/05/qa-maxar-execs-discuss-us-army-simulation-project-maven/

546 Paul McLeary, 'Pentagon's Big AI Program, Maven, Already Hunts Data in Middle East, Africa', Breaking Defense, 1 May 2018, https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/; Aviation Week, 'Sea Launch partners agree they're ready to fly again', 22 June 2000, https://aviationweek.com/aviation-week-space-technology/how-shadowy-project-maven-uses-ai-mine-combat-data

547 Courtney Albon, 'Geospatial-intelligence agency making strides on Project Maven AI', Defense News, 22 May 2023, https://www.defensenews.com/artificial-intelligence/2023/05/22/geospatial-intelligence-agency-making-strides-on-project-maven-ai/

548 Sydney J. Freedberg Jr., ''Success begets challenges': NGA struggles to meet rising demand for Maven AI', Breaking Defense, 3 September 2024, https://breakingdefense.com/2024/09/success-begets-challenges-nga-struggles-to-meet-rising-demand-for-maven-ai/ Meanwhile the Pentagon was controlling more than 685 AI-related projects as of 2021, according to the Government Accountability Office (Colin Demarest, 'Palantir wins $250 million US Army AI research contract', Defense News, 27 September 2023, https://www.defensenews.com/artificial-intelligence/2023/09/27/palantir-wins-250-million-us-army-ai-research-contract/).

549 Courtney Albon, 'Palantir wins contract to expand access to Project Maven AI tools', C4ISRNET, 30 May 2024, https://www.c4isrnet.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/.

550 Sandra Erwin, 'Pentagon boosts budget for Palantir's AI software in major expansion of Project Maven', Space News, 22 May 2025, https://spacenews.com/pentagon-boosts-budget-for-palantirs-ai-software-in-major-expansion-of-project-maven/

551 NATO, 'NATO acquires AI-enabled Warfighting System', 14 April 2025, https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system- and Sydney J. Freedberg Jr., 'NATO picks Palantir's Maven AI for military planning, amid trans-Atlantic tension', Breaking Defense, 14 April 2025, https://breakingdefense.com/2025/04/nato-picks-palantirs-maven-ai-for-military-planning-amid-trans-atlantic-tension/

552 Lauren C. Williams, 'Eighteen ways Palantir wants the Pentagon to change', Defense One, 3 December 2024, https://www.defenseone.com/defense-systems/2024/12/eighteen-ways-palantir-wants-pentagon-change/401400/

553 Terence O'Brien, 'Palantir's Maven Smart System is an AI-powered Kanban board for killing people', The Verge, 14 March 2026, https://www.theverge.com/ai-artificial-intelligence/895030/palantirs-maven-smart-system-is-an-ai-powered-kanban-board-for-killing-people

554 Pat Host, 'Anduril's Luckey seeks to break the Pentagon's cost-plus contracting model', Janes, 6 October 2020, https://www.janes.com/osint-insights/defence-news/andurils-luckey-seeks-to-break-the-pentagons-cost-plus-contracting-model

555 Steve Trimble, 'Anduril Quietly Working On Hypersonic Missiles, Air Vehicles', Aviation Week, 6 April 2026, https://aviationweek.com/defense/missile-defense-weapons/anduril-quietly-working-hypersonic-missiles-air-vehicles, Audrey Decker, 'Anduril touts new, easy-to-build cruise missiles', Defense One, 12 September 2024, https://www.defenseone.com/business/2024/09/anduril-touts-new-easy-build-cruise-missiles/399473/ and Courtney Albon, 'Anduril partners with satellite body supplier for 2025 space mission', Defense News, 1 October 2024, https://www.defensenews.com/space/2024/10/01/anduril-partners-with-satellite-body-supplier-for-2025-space-mission/

556 Sheera Frenkel and Cade Metz, 'The Pentagon's Favorite Tech Guy Is This Hawaiian Shirt-Wearing Founder', The New York Times, 2 March 2026, https://www.nytimes.com/2026/03/02/technology/pentagon-anduril-palmer-luckey.html

557 Steve Trimble, 'Anduril Starts Building CCA Prototypes In Ohio', Aviation Week, 23 March 2026, https://aviationweek.com/defense/aircraft-propulsion/anduril-starts-building-cca-prototypes-ohio, Mike Stone, 'High-speed combat drone production starts at new US Anduril plant in days', Defense News, 20 March 2026, https://www.defensenews.com/unmanned/2026/03/19/high-speed-combat-drone-production-starts-at-new-us-anduril-plant-in-days/, Steve Trimble, 'Anduril Opens Doors Of The Fury's Future Home', Aviation Week, 29 January

2026, https://aviationweek.com/defense/supply-chain/anduril-opens-doors-furys-future-home; Julie Carr Smyth, 'Anduril to build 'Arsenal-1' autonomous weapons plant in central Ohio', Defense News, 16 January 2025, https://www.defensenews.com/industry/2025/01/16/anduril-to-build-arsenal-1-autonomous-weapons-plant-in-central-ohio/ and Anduril, 'Arsenal-1', https://www.anduril.com/arsenal-1

558 Courtney Albon, 'Anduril to open software-based manufacturing hub to scale production', Defense News, 8 August 2024, https://www.defensenews.com/pentagon/2024/08/08/anduril-to-open-software-based-manufacturing-hub-to-scale-production/

559 Sheera Frenkel and Cade Metz, 'The Pentagon's Favorite Tech Guy Is This Hawaiian Shirt-Wearing Founder', The New York Times, 2 March 2026, https://www.nytimes.com/2026/03/02/technology/pentagon-anduril-palmer-luckey.html

560 Palmer Luckey and Trae Stephens, 'Silicon Valley should stop ostracizing the military', The Washington Post, 8 August 2018, https://www.washingtonpost.com/opinions/silicon-valley-should-stop-ostracizing-the-military/2018/08/08/7a7e0658-974f-11e8-80e1-00e80e1fdf43_story.html

561 Jon Harper, 'Trump nominates Anduril executive, former special operations officer to be Army undersecretary', DefenseScoop, 11 March 2025, https://defensescoop.com/2025/03/11/trump-nominates-michael-obadal-army-undersecretary-anduril/ and United States Army, 'Bio: Hon. Michael A. Obadal Under Secretary of the Army', https://api.army.mil/e2/c/downloads/2025/09/22/1618c0bb/michael-obadal-bio.pdf

562 Brian Schimpf, 'Anduril boss: In an era of strategic competition, we need artificially intelligent systems', Defense News, 6 December 2021, https://www.defensenews.com/outlook/2021/12/06/anduril-boss-in-an-era-of-strategic-competition-we-need-artificially-intelligent-systems/

563 Courtney Albon, 'Anduril to open software-based manufacturing hub to scale production', Defense News, 8 August 2024, https://www.defensenews.com/pentagon/2024/08/08/anduril-to-open-software-based-manufacturing-hub-to-scale-production/

564 Anduril, 'Rebooting the Arsenal of Democracy: Anduril Mission Document', 5 June 2022, https://www.anduril.com/news/rebooting-the-arsenal-of-democracy-anduril-mission-document

565 Xiao Liang, Nan Tian, Diego Lopes Da Silva, Lorenzo Scarazzato, Zubaida Karim and Jade Guiberteau Ricard, 'Trends In World Military Expenditure, 2025', SIPRI Fact Sheet, April 2026, https://www.sipri.org/sites/default/files/2026-04/2604_milex_2025.pdf

566 Lorenzo Scarazzato, Nan Tian, Diego Lopes Da Silva, Xiao Liang, Zubaida Karim and Jade Guiberteau Ricard, 'The SIPRI Top 100 Arms Producing and Military Services Companies, 2024', SIPRI Fact Sheet, December 2025, https://www.sipri.org/sites/default/files/2025-11/fs_2512_top_100_2024.pdf; Xiao Liang, Nan Tian, Diego Lopes Da Silva, Lorenzo Scarazzato, Zubaida Karim and Jade Guiberteau Ricard, 'Trends In World Military Expenditure, 2024', SIPRI Fact Sheet, April 2025, https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf

567 Mathew George, Katarina Djokic, Zain Hussain, Pieter D. Wezeman; Siemon T. Wezeman, 'Trends in International Arms Transfers, 2025', SIPRI Fact Sheet, March 2026, https://www.sipri.org/sites/default/files/2026-03/fs_2603_at_2025.pdf

568 Anduril, 'Anduril's Lattice: a trusted dual use — commercial and military — platform for public safety, security, and defense', 31 July 2023, https://www.anduril.com/news/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security; also see Joe Gould, 'McCain's staff director to lead strategy for Silicon Valley tech firm, Anduril', Defense News, 29 November 2019, https://www.defensenews.com/digital-show-dailies/reagan-defense-forum/2018/11/29/mccains-staff-director-to-lead-strategy-for-silicon-valley-tech-firm-anduril/

569 Julian Kerr, 'Interview Palmer Luckey', Janes Defence Weekly, 5 October 2022.

570 Anduril, 'Anduril Deploys 300th Autonomous Surveillance Tower (AST), Advancing Capability for Border Security', 26 September 2024, https://www.anduril.com/news/anduril-deploys-300th-autonomous-surveillance-tower-ast-advancing-capability-for-border-security; see also Sam Biddle, 'Trump's Big Beautiful Gift to Anduril', The Intercept, 9 July 2025, https://theintercept.com/2025/07/09/trump-big-beautiful-bill-anduril/

571 The Guardian, ''Never sleeps, never even blinks': the hi-tech Anduril towers spreading along the US border', 16 September 2022, https://www.theguardian.com/us-news/2022/sep/16/anduril-towers-surveillance-us-mexico-border-migrants
572 Jen Judson, 'Anduril adapts tech to detect cruise missiles in US Air Force demo', Defense News, 16 October 2020, https://www.defensenews.com/digital-show-dailies/ausa/2020/10/16/anduril-adapts-tech-to-detect-cruise-missiles-in-air-force-demo/ and Anduril, 'Anduril at ABMS', 8 September 2020, https://www.anduril.com/news/anduril-at-abms
573 Colin Demarest, 'Anduril unveils software to manage hordes of drones', Defense News, 3 May 2023, https://www.defensenews.com/industry/2023/05/03/anduril-unveils-software-to-manage-hordes-of-drones/
574 Tabby Kinder, 'Oppenheimer in flip flops', The Financial Times, 28 March 2024, https://www.ft.com/content/ce6f96f8-6ab8-4089-b7db-f99db22c2071
575 Peter Felstead, 'UK MoD contracts Anduril to supply £30 million worth of loitering munitions to Ukraine', European Security & Defence, 6. March 2025, https://euro-sd.com/2025/03/major-news/42958/anduril-lms-to-ukraine/
576 Kenneth Niemeyer, 'Anduril is considering a UK factory as Europe beefs up military power', Business Insider, 23 March 2025, https://www.businessinsider.com/anduril-uk-factory-drones-europe-military-power-ukraine-2025-3
577 Anthony Capaccio, 'Taiwan Moves to Buy 1,000 AeroVironment, Anduril Attack Drones', Bloomberg, 28 October 2024, https://www.bloomberg.com/news/articles/2024-10-28/taiwan-moves-to-buy-1-000-aerovironment-anduril-attack-drones
578 Noah Robertson, 'Anduril debuts Bolt, loitering munition on contract with Marine Corps', Defense News, 10 October 2024, https://www.defensenews.com/industry/2024/10/10/anduril-debuts-bolt-loitering-munition-on-contract-with-marine-corps/
579 Jen Judson, 'Rheinmetall, Anduril join forces on optionally manned fighting vehicle', Defense News, 6 September 2022, https://www.defensenews.com/land/2022/09/06/rheinmetall-anduril-join-forces-on-optionally-manned-fighting-vehicle/; Jen Judson, 'Anduril, Hanwha team up to bid for Army's light payload robot', Defense News, 29 February 2024, https://www.defensenews.com/battlefield-tech/2024/02/29/anduril-hanwha-team-up-to-bid-for-armys-light-payload-robot/
580 Megan Eckstein, 'Anduril pairs with Korean shipbuilder to design new unmanned platforms', Defense News, 16 April 2024, https://www.defensenews.com/naval/2024/04/16/anduril-pairs-with-korean-shipbuilder-to-design-new-unmanned-platforms/; see also: Cristina Stassis, 'Anduril, HD Hyundai expand partnership with first autonomous surface vessel in production', Defense News, 20 April 2026, https://www.defensenews.com/industry/techwatch/2026/04/20/anduril-hd-hyundai-expands-partnership-with-first-autonomous-surface-vessel-in-production/
581 Jen Judson, 'Saab taps Anduril to build rocket motors for ground-launched bomb', Defense News, 20 June 2025, https://www.defensenews.com/industry/2025/06/20/saab-taps-anduril-to-build-rocket-motors-for-ground-launched-bomb/
582 Craig Langford, 'Anduril and GKN join forces for British Army combat drone', UK Defense Journal, 9 December 2025, https://ukdefencejournal.org.uk/anduril-and-gkn-join-forces-for-british-army-combat-drone/
583 Carlo Munoz, 'US Army, Anduril reach formal deal on IBCS Maneuver programme', Janes Defence Weekly, 10 December 2025, www.janes.com/defence-intelligence-insights/defence-news/c4isr/us-army-anduril-reach-deal-on-ibcs-maneuver-programme
584 Brian Everstine, 'Anduril, Boeing Team Up For New U.S. Army Interceptor', Aviation Week, 18 December 2025, https://aviationweek.com/defense/missile-defense-weapons/anduril-boeing-team-new-us-army-interceptor
585 Andrew Eversden, 'DIU awards Anduril Industries contract for counter-drone AI technology', C4ISRNET, 27 July 2021, https://www.c4isrnet.com/unmanned/uas/2021/07/27/anduril-industries-awarded-contract-from-diu-for-counter-drone-technology/
586 Jen Judson, 'US Special Operations Command picks Anduril to lead counter-drone integration work in $1B deal', Defense News, 24 January 2022, https://www.defensenews.com/unmanned/2022/01/24/us-special-

operations-command-picks-anduril-to-lead-counter-drone-integration-work-in-1b-deal/
587 Colin Demarest, 'Anduril Industries in talks with Australia on autonomous undersea vehicle', C4ISRNET, 5 May 2022, https://www.c4isrnet.com/unmanned/2022/05/05/anduril-industries-in-talks-with-australia-on-autonomous-undersea-vehicle/; Oishee Majumdar, 'Advancing autonomy - Australia's Ghost Shark XL-AUV programme', Janes Defence Weekly, 17 July 2024.
588 Gordon Arthur, 'Australia orders fleet of large unmanned submarines from Anduril', Defense News, 10 September 2025, https://www.defensenews.com/global/asia-pacific/2025/09/10/australia-orders-fleet-of-large-unmanned-submarines-from-anduril/
589 Zita Ballinger Fletcher, 'US Navy partners with Anduril to develop XL underwater vessel', Defense News, 12 March 2026, https://www.defensenews.com/news/your-military/2026/03/12/us-navy-partners-with-anduril-to-develop-xl-underwater-vessel/
590 Will Knight, 'Anduril Is Building Out the Pentagon's Dream of Deadly Drone Swarms', WIRED Magazine, 28 May 2024, https://www.wired.com/story/anduril-is-building-out-the-pentagons-dream-of-deadly-drone-swarms/
591 Todd South, 'Air Force Revisiting Production Goals for CCA with Eye Toward 'Scale'', Air & Space Forces Magazine, 17 March 2026, https://www.airandspaceforces.com/air-force-revisiting-production-goals-cca-increment-2/
592 Stephen Losey, 'Air Force starts ground testing Anduril collaborative combat aircraft', Defense News, 1 May 2025, https://www.defensenews.com/air/2025/05/01/air-force-starts-ground-testing-anduril-collaborative-combat-aircraft/
593 Stephen Losey, 'Anduril's drone wingman begins flight tests', Defense News, 31 October 2025, https://www.defensenews.com/air/2025/10/31/andurils-drone-wingman-begins-flight-tests/
594 Courtney Albon, 'Anduril lands $250 million Pentagon contract for drone defense system', Defense News, 8 October 2024, https://www.defensenews.com/unmanned/2024/10/08/anduril-lands-250-million-pentagon-contract-for-drone-defense-system/
595 Jon Harper, 'Anduril wins $100M deal from CDAO to scale 'edge data mesh' capabilities', DefenseScoop, 3 December 2024, https://defensescoop.com/2024/12/03/anduril-awarded-100m-deal-cdao-scale-edge-data-mesh-capabilities-ota/.
596 Jane Edwards, 'Anduril Wins $642M Navy Contract for Counter-Drone Tech', GovCon Wire, 10 March 2025, https://www.govconwire.com/articles/anduril-navy-contract-counter-drone-tech
597 Christine Casimiro, 'Anduril Scores Nearly $100M US Army Deal for Next-Gen C2 Prototype', The Defense Post, 21 July 2025, https://thedefensepost.com/2025/07/21/anduril-us-army-ngc2-prototype/ and Jen Judson, 'Anduril wins $100M deal to build US Army's next-gen C2 ecosystem', Defense News, 21 July 2025, https://www.defensenews.com/land/2025/07/21/anduril-wins-100m-deal-to-build-us-armys-next-gen-c2-ecosystem/
598 Patrick Tucker, 'With IVAS takeover, Anduril looks to build out human-machine 'ecosystem'', Defense One, 13 February 2025, https://www.defenseone.com/business/2025/02/ivas-takeover-anduril-looks-build-out-human-machine-ecosystem/403009/ and Ashley Roque, 'Anduril gets green light from Army to take over Microsoft's IVAS project: Exec', Breaking Defense, 15 April 2025, https://breakingdefense.com/2025/04/anduril-gets-green-light-from-army-to-take-over-microsofts-ivas-project-exec/
599 Ashley Roque, ''I have got this s— figured out': Anduril unveiling EagleEye mixed-reality device at AUSA', Breaking Defense, 13 October 2025, https://breakingdefense.com/2025/10/i-have-got-this-s-figured-out-anduril-unveiling-eagleeye-mixed-reality-device-at-ausa/
600 Carlo Munoz, 'US Army, Anduril reach formal deal on IBCS Maneuver programme', Janes Defence Weekly, 10 December 2025, https://www.janes.com/defence-intelligence-insights/defence-news/c4isr/us-army-anduril-reach-deal-on-ibcs-maneuver-programme
601 Steve Trimble, 'Anduril Joins Forces With Edge On New Omen Tailsitter UAS', Aviation Week, 13 November 2025, https://aviationweek.com/defense/aircraft-propulsion/anduril-joins-forces-edge-new-omen-tailsitter-uas
602 Gareth Jennings, 'Edge Group/Anduril Industries JV to offer Omen autonomous VTOL UAV', Janes De-

fence Weekly, 26 November 2025.
603 See for example: Liselotte Mas and Benjamin Roger, 'The UAE reorganizes its arms supply network for Sudanese paramilitaries', Le Monde, 22 March 2026, https://www.lemonde.fr/en/le-monde-africa/article/2026/03/22/the-uae-is-reorganizing-its-arms-supply-network-for-sudanese-paramilitaries_6751682_124.html; Sam Biddle, 'Anduril Partners With UAE Bomb Maker Accused of Arming Sudan's Genocide', The Intercept, 11 December 2025, https://theintercept.com/2025/12/11/anduril-uae-weapons-edge-sudan/; Quentin Peschard, 'European weapons in Sudan (5/5): Europeans still making deals with Emirati firm diverting weapons', France 24, 21 April 2025, https://www.france24.com/en/africa/20250421-investigation-european-weapons-sudan-part-5-igg-edge-france-uae; Mark Townsend, 'Leaked UN experts report raises fresh concerns over UAE's role in Sudan war', The Guardian, 14 April 2025, https://www.theguardian.com/global-development/2025/apr/14/leaked-un-experts-report-raises-fresh-concerns-over-uaes-role-in-sudan-war; Quentin Peschard, 'European weapons in Sudan (2/5): A €50 million Emirati contract', France 24, 18 April 2025, https://www.france24.com/en/africa/20250418-investigation-european-weapons-sudan-part-2-emirati-contract; Amnesty International, 'Sudan: French-manufactured weapons system identified in conflict – new investigation', 14 November 2024, https://www.amnesty.org/en/latest/news/2024/11/sudan-french-manufactured-weapons-system-identified-in-conflict-new-investigation/
604 Sagi Cohen and TheMarker, 'Founder of U.S. Defense Tech Giant Anduril Visits Israel Secretly, Meets Netanyahu', Haaretz, 20 February 2026, https://www.haaretz.com/israel-news/israel-security/2026-02-20/ty-article/.premium/founder-of-u-s-defense-tech-giant-anduril-visits-israel-secretly-meets-netanyahu/0000019c-79d2-dfbe-a39f-79f2553a0000
605 Sophie Shulman, 'Anduril's Palmer Luckey meets 10 Israeli defense startups in secret visit', CTech, 20 February 2026, https://www.calcalistech.com/ctechnews/article/hyoumeid11e
606 Brian Schimpf, 'Anduril CEO Statement for Senate AI Insights Forum', Anduril, 6 December 2023, https://www.anduril.com/news/ai-insight-forum-national-security
607 Camilla Hodgson,. 'Anduril says drone-killer is not first step to autonomous warfare', Financial Times, 22 October 2019, https://www.ft.com/content/7407c504-ee6d-11e9-ad1e-4367d8281195
608 Less apt often called kamikaze or suicide drones – see: Kelsey Atherton, 'It's time to stop using 'kamikaze' to describe the exploding drones in Ukraine', Popular Science, 25 October 2022, https://www.popsci.com/technology/self-detonating-drones-ukraine-russia/
609 Patrick Tucker, 'Are AI defense firms about to eat the Pentagon?', DefenseOne, 15 December 2024, https://www.defenseone.com/technology/2024/12/are-ai-defense-firms-about-eat-pentagon/401673/. See also: Scott Sacknoff, 'With the world on edge, defense stocks soar', Defense News, 8 August 2024, https://www.defensenews.com/opinion/2024/08/08/with-the-world-on-edge-defense-stocks-soar/
610 BAE Systems, 'Annual Report 2025', https://annualreport.baesystems.com/2025. With its US branch employing 41 thousand people and 50 thousand working in the UK (see: BAE Systems, 'Annual Report 2025', https://www.baesystems.com/en/, https://www.baesystems.com/en-uk/uk-businesses and BAE Systems, 'Who We Are', https://www.baesystems.com/en-us/who-we-are).
611 Macrotrends, 'Bae Systems Revenue 2012-2025 | BAESY', https://www.macrotrends.net/stocks/charts/BAESY/bae-systems/revenue
612 SIPRI, "The SIPRI Top 100 Arms-Producing And Military Services Companies, 2024", December 2025, https://www.sipri.org/sites/default/files/2025-11/fs_2512_top_100_2024.pdf
613 BAE Systems, 'All capabilities', https://www.baesystems.com/en-uk/what-we-do/all-capabilities and BAE Systems, 'IntelligenceReveal: IP Metadata Analysis', https://www.baesystems.com/en-uk/product/intelligencereveal-ip-metadata-analysis
614 BAE Systems, 'Autonomy is changing the shape of future warfare', https://www.baesystems.com/en-uk/insight/autonomy-is-changing-the-shape-of-future-warfare
615 BAE Systems, 'Taranis', https://www.baesystems.com/en/product/taranis
616 Tony Osborne, 'BAE Systems Advances Uncrewed Collaborative Platform Design', Aviation Week, 5 February 2024, https://aviationweek.com/defense-space/aircraft-propulsion/bae-systems-advances-uncrewed-collaborative-platform-design; Adam Morrison, 'Uncrewed Air Systems (UAS)', BAE Systems, https://www.baesys-

tems.com/en-uk/product/uncrewed-air-systems
617 Peter Felstead, 'BAE Systems successfully uses TRV-150 multi-rotor UAV to launch APKWS guided rockets', European Security & Defence, 17 July 2025, https://euro-sd.com/2025/07/major-news/45580/trv-150-uav-launches-apkws/; Adam Morrison, 'Major step towards low-cost Uncrewed Air System launched munitions to combat air and ground targets', BAE Systems, 17 July 2025, https://www.baesystems.com/en-uk/article/trv150-trials-with-apkws
618 Vincent Boulanin and Maaike Verbruggen, 'Mapping the development of autonomy in weapon systems', SIPRI, November 2017, p.49.
619 Carley Welch, 'BAE to debut AI-powered target recognition on Bradley, AMPVs at upcoming Army exercises', Breaking Defense, 3 December 2025, https://breakingdefense.com/2025/12/bae-to-debut-ai-powered-target-recognition-on-bradley-vehicles-at-armys-next-tic-exercise/
620 BAE Systems, 'BAE Systems and Scale AI combine forces to bring agentic AI to defense missions and platforms', 26 March 2026, https://www.baesystems.com/en/article/bae-systems-and-scale-ai-combine-forces-to-bring-agentic-ai-to-defense-missions-and-platforms
621 BAE Systems, 'BAE Systems and Scale AI combine forces to bring agentic AI to defense missions and platforms', 26 March 2026, https://www.baesystems.com/en/article/bae-systems-and-scale-ai-combine-forces-to-bring-agentic-ai-to-defense-missions-and-platforms
622 BAE Systems, 'Intelligent Autonomous Systems R&D', https://www.baesystems.com/en-us/product/autonomy-r-d
623 BAE Systems, 'All-Source Track and Identity Fuser (ATIF)', https://www.baesystems.com/en-us/product/all-source-track-and-identity-fuser-atif
624 BAE Systems, 'IntelligenceReveal: IP Metadata Analysis', https://www.baesystems.com/en-uk/product/intelligencereveal-ip-metadata-analysis
625 Carlo Munoz, 'DARPA awards BAE Systems development deal for AI-enhanced battle management tools', Jane's International Defence Review, February 2020.
626 Carlo Munoz, 'DARPA awards BAE Systems development deal for SCEPTER', Janes Defence Weekly, 10 May 2023.
627 Sandra Erwin, 'BAE Systems wins $16 million DARPA award to advance autonomous satellite tasking', Space News, 11 December 2025, https://spacenews.com/bae-systems-wins-16-million-darpa-award-to-advance-autonomous-satellite-tasking/
628 Laura Ferrante, 'MMIC Foundry Services & Products', BAE Systems, https://www.baesystems.com/en-us/product/foundry-services
629 BAE Systems, 'Human Rights Statement 2025', 2025, https://www.baesystems.com/dam/jcr:4a725249-1d17-48ed-8d5a-ba165e85f55b
630 BAE Systems, 'Responsible supply chain', https://www.baesystems.com/en/sustainability/responsible-business/responsible-supply-chain.html
631 Paul Scharre, 'Army of none', Norton, 2018, p.109.
632 'Out of Control: Irresponsible weapons transfers and future weapon systems. Dirty Profits 7', Facing Finance, May 2019, https://www.facing-finance.org/files/2019/05/ff_dp7_ONLINE_v02.pdf
633 BAE Systems email to PAX, 14 October 2019, as quoted in: Frank Slijper, 'Slippery Slope - The arms industry and increasingly autonomous weapons', PAX, November 2019, https://paxforpeace.nl/wp-content/uploads/sites/2/import/import/pax-report-slippery-slope.pdf
634 BAE Systems, 'AI with purpose', https://www.baesystems.com/en-uk/uk-businesses/digital-intelligence/ai-with-purpose
635 Elodie Collins, 'General Dynamics Q4, Full Fiscal 2025 Financial Results Show Revenue, Backlog Growth', GovCon Wire, 20 January 2026, https://www.govconwire.com/articles/general-dynamics-fy-2025-financial-report
636 SIPRI, "The SIPRI Top 100 Arms-Producing And Military Services Companies, 2024", December 2025, https://www.sipri.org/sites/default/files/2025-11/fs_2512_top_100_2024.pdf
637 General Dynamics Information Technology ,'Unleash new possibilities with AI.', https://www.gdit.com/capabilities/technology/technologies/artificial-intelligence/

638 General Dynamics Information Technology, 'Driving Intelligence Analysis through Data Excellence with Automation', https://www.gdit.com/perspectives/case-studies/driving-intelligence-analysis-through-data-excellence-with-ai-automation/.
639 General Dynamics Information Technology, 'GDIT Launches DOGMA AI Solution to Counter Aerial and Emerging Threats and Accelerate Mission Decision Advantage', press release, 19 January 2026, https://www.gdit.com/about-gdit/press-releases/gdit-launches-dogma-ai-solution-to-counter-aerial-and-emerging-threats-and/
640 See for example: Jen Judson, 'General Dynamics unit puts short-range air defense on robotic vehicle', Defense News, 28 March 2023, https://www.defensenews.com/digital-show-dailies/2023/03/28/general-dynamics-unit-puts-short-range-air-defense-on-robotic-vehicle.
641 General Dynamics, 'Responsibility - Our Values Drive And Determine How We Do Business', https://www.gd.com/responsibility and General Dynamics, 'General Dynamics Mission Systems Introduces New Autonomous Unmanned Underwater Vehicle', press release, 11 September 2019, https://www.gd.com/Articles/2019/09/11/general-dynamics-mission-systems-introduces-new-autonomous-unmanned-underwater-vehicle
642 General Dynamics, 'Human Rights - General Dynamics Recognizes The Fundamental Human Dignity Of All People', https://www.gd.com/responsibility/human-rights
643 General Dynamics, 'Responsibility - Our Values Drive And Determine How We Do Business', https://www.gd.com/responsibility
644 At least ever since 2009 until present according to this SIPRI datasheet: https://www.sipri.org/sites/default/files/SIPRI-Top-100-2002-2024%20%282%29.xlsx
645 Lockheed Martin, 'Who we are', https://www.lockheedmartin.com/en-us/who-we-are.html
646 Lockheed Martin, 'Who We Are (Fact Sheet)', https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/lockheed-martin-fact-sheet.pdf
647 Lockheed Martin, 'Autonomy & Uncrewed Systems: The Future of Autonomy is Human-Centered', https://www.lockheedmartin.com/en-us/capabilities/autonomous-unmanned-systems.html
648 John Kent, 'Lockheed Martin Receives Contract For SMSS-KMAX Cooperative Teaming Demo', Lockheed Martin, February 2014, http://www.lockheedmartin.com/us/news/press-releases/2014/february/mfc-021914-lockheed-martin-receives-contract-smss-kmax-cooperative-teaming-demo.html, via: https://web.archive.org/web/20140704022358/http://www.lockheedmartin.com/us/news/press-releases/2014/february/mfc-021914-lockheed-martin-receives-contract-smss-kmax-cooperative-teaming-demo.html
649 Quoted from: Frank Slijper, 'Slippery Slope - The arms industry and increasingly autonomous weapons', PAX, November 2019, https://paxforpeace.nl/wp-content/uploads/sites/2/import/import/pax-report-slippery-slope.pdf. Also see: Lockheed Martin, 'U.S. Air Force, Lockheed Martin Demonstrate Manned/Unmanned Teaming', News Release, 10 April 2017, https://news.lockheedmartin.com/2017-04-10-U-S-Air-Force-Lockheed-Martin-Demonstrate-Manned-Unmanned-Teaming
650 Quoted from Frank Slijper, 'Slippery Slope - The arms industry and increasingly autonomous weapons', PAX, November 2019, https://paxforpeace.nl/wp-content/uploads/sites/2/import/import/pax-report-slippery-slope.pdf; original source: Richard Scott and Huw Williams, 'Bargain hunt: Air forces move to embrace low-cost UCAVs', Jane's International Defence Review, July 2017.
651 Valerie Insinna, 'Lockheed investing $100M into F-35 controlled combat drones under 'Project Carrera'' Breaking Defense, 15 September 2022, https://breakingdefense.com/2022/09/lockheed-investing-100m-into-f-35-controlled-combat-drones-under-project-carrera/
652 Steve Trimble, 'Hanwha Emerges As Re-Engine Option For Lockheed Vectis', Aviation Week, 19 November 2025, https://aviationweek.com/defense/aircraft-propulsion/hanwha-emerges-re-engine-option-lockheed-vectis
653 Graham Warwick, 'DARPA's ACE Wants To Automate Dogfighting To Empower AI', Aviation Week, 10 March 2020, https://aviationweek.com/defense-space/aircraft-propulsion/darpas-ace-wants-automate-dogfighting-empower-ai. Also see: DARPA, 'ACE: Air Combat Evolution', https://www.darpa.mil/research/programs/air-combat-evolution and Lockheed Martin, 'Skunk Works® Keys to Mission-Centered Decision Making', https://www.lockheedmartin.com/en-us/who-we-are/business-areas/aeronautics/skunkworks/skunkworks-ai-autonomy.

html
654 DARPA, 'ACE Program Achieves World First for AI in Aerospace', https://www.darpa.mil/news/2024/ace-ai-aerospace
655 Sandra Erwin, 'Lockheed Martin teams with Iceye to advance AI-enabled targeting', Space News, 20 November 2024, https://spacenews.com/lockheed-martin-teams-with-iceye-to-advance-ai-enabled-targeting/
656 Zita Ballinger Fletcher, 'Lockheed debuts AI on F-35 fighter jet to identify targets', Defense News, 24 February 2026, https://www.defensenews.com/industry/techwatch/2026/02/24/lockheed-debuts-ai-on-f-35-fighter-jet-to-identify-targets/
657 Lockheed Martin, 'Lockheed Martin's AI Fight Club™ Puts AI to the Test for National Security', 3 June 2023, https://news.lockheedmartin.com/2025-06-03-Lockheed-Martins-AI-Fight-Club-TM-Puts-AI-to-the-Test-for-National-Security
658 Lauren C. Williams, 'Established defense contractors lend tech startups a helping hand', DefenseOne, 23 June 2025, https://www.defenseone.com/business/2025/06/established-defense-contractors-lend-tech-start-ups-helping-hand/406247/
659 Zita Ballinger Fletcher, 'Lockheed unveils Lamprey underwater drone that can attach to ships', Defense News, 11 February 2026, https://www.defensenews.com/unmanned/2026/02/10/lockheeds-unveils-lamprey-undersea-drone-that-can-attach-to-ships/
660 Lockheed Martin, 'Who we are', https://www.lockheedmartin.com/en-us/who-we-are.html
661 Lockheed Martin, 'Human Rights', https://sustainability.lockheedmartin.com/sustainability/other-sustainability-topics/human-rights/
662 Lockheed Martin, 'Notice of 2025 Annual Meeting of Stockholders', 27 March 2025, https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/annual-reports/2025-proxy-statement.pdf
663 Lockheed Martin, 'Notice of 2025 Annual Meeting of Stockholders', 27 March 2025, https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/annual-reports/2025-proxy-statement.pdf
664 Lockheed Martin, '2024 Sustainability Performance Report', https://sustainability.lockheedmartin.com/content/dam/lockheed-martin/sustainability/2024-Sustainability-Performance-Report.pdf
665 Jeremiah Cushman, 'Intelligent Implementation', Janes Defence and Intelligence Review, December 2024.
666 SIPRI, "The SIPRI Top 100 Arms-Producing And Military Services Companies, 2024", December 2025, https://www.sipri.org/sites/default/files/2025-11/fs_2512_top_100_2024.pdf
667 US Security and Exchange Commission, 'Northrop Grumman Corporation Form 10-K Annual Report (Fiscal Year 2025)', https://www.sec.gov/ix?doc=/Archives/edgar/data/1133421/000113342126000003/noc-20251231.htm
668 Northrop Grumman, 'Autonomy: Leading Next-generation Integrated Autonomous Solutions', https://www.northropgrumman.com/what-we-do/aircraft/autonomous-systems
669 Northrop Grumman, 'X-47B UCAS', https://www.northropgrumman.com/what-we-do/aircraft/x-47b-ucas
670 Northrop Grumman, 'Fire Scout', https://www.northropgrumman.com/what-we-do/aircraft/fire-scout
671 Northrop Grumman, 'MQ-4C Triton', https://www.northropgrumman.com/what-we-do/aircraft/triton
672 Sakshi Tiwari, 'U.S. Navy Confirms Loss of $240 Million MQ-4C Triton Drone; Classifies it CLASS 'A' Flight Mishap', Eurasian Times, 15 April 2026, https://www.eurasiantimes.com/u-s-navy-confirms-loss-of-240-million-mq-4c-triton-drone-classifies-it-class-a-flight-mishap/
673 Parth Satam, 'Iran's RQ-170 Clone Destroyed in U.S. Strikes, CENTCOM Video Shows', The Aviationist, 4 April 2026, https://theaviationist.com/2026/04/04/irans-rq-170-clone-destroyed-in-us-strikes/
674 David Cenciotti, 'Northrop Grumman Releases New Details And Video Of Its Jackal Loitering Munition', The Aviationist, 15 October 2024, https://theaviationist.com/2024/10/15/northrop-grumman-jackal/. Company video: https://youtu.be/SDgXUO5ybCs
675 Tyler Rogoway, 'Lumberjack Jet-Powered One-Way Attack Munition Can Drop Its Own Precision Bomblets (Updated)', The War Zone, 30 April 2025, https://www.twz.com/air/lumberjack-jet-powered-one-way-attack-munition-can-drop-its-own-precision-bomblets
676 Laura Chon, 'Northrop Grumman's Lumberjack Advances Battlefield Capabilities', Northrop Grumman, 31

March 2026, https://news.northropgrumman.com/autonomous-systems/northrop-grummans-lumberjack-advances-battlefield-capabilities
677 Sydney J. Freedberg Jr., 'Northrop Grumman offers made-in-USA microelectronics to partner firms', 18 September 2025, https://breakingdefense.com/2025/09/northrop-grumman-offers-made-in-usa-microelectronics-to-partner-firms/
678 Steve Trimble, 'Project Lotus, Northrop Grumman's Secret Autonomous Aircraft Revealed', Aviation Week, 27 October 2025, https://aviationweek.com/defense/aircraft-propulsion/project-lotus-northrop-grummans-secret-autonomous-aircraft-revealed and Brian Everstine, 'Northrop Grumman Unveils Project Talon Collaborative Combat Aircraft', Aviation Week, 4 December 2025, https://aviationweek.com/defense/aircraft-propulsion/northrop-grumman-unveils-project-talon-collaborative-combat-aircraft
679 Stephen Losey, 'US Marine Corps taps Northrop, Kratos to build Valkyrie drone wingmen', Defense News, 8 January 2026, https://www.defensenews.com/unmanned/2026/01/08/us-marine-corps-taps-northrop-kratos-to-build-valkyrie-drone-wingmen/
680 Peter Felstead, 'Northrop Grumman to leverage Kratos Valkyrie for USMC's MUX TACAIR CCA programme', European Security & Defence, 8 January 2026, https://euro-sd.com/2026/01/major-news/48394/ng-mux-tacair-cca-programme/
681 Northrop Grumman, 'Corporate Responsibility', https://www.northropgrumman.com/corporate-responsibility/
682 Northrop Grumman, 'Human Rights Policy', https://www.northropgrumman.com/corporate-responsibility/northrop-grumman-human-rights-policy
683 Northrop Grumman, 'Human Rights Policy', https://www.northropgrumman.com/corporate-responsibility/northrop-grumman-human-rights-policy
684 Northrop Grumman, '2023 Human Rights Report', 2023, https://media.northropgrumman.com/c9ccf7df-2c97-4617-97a4-b385001ce549/2023%20Northrop%20Human%20Rights%20Report%20finalrfs_Original%20file.pdf
685 Northrop Grumman, '2023 Human Rights Report', 2023, https://media.northropgrumman.com/c9ccf7df-2c97-4617-97a4-b385001ce549/2023%20Northrop%20Human%20Rights%20Report%20finalrfs_Original%20file.pdf
686 Such as (components of) AP-mines, cluster munitions, biological and chemical weapons, as well as white phosphorous and depleted uranium (but not nuclear weapons).
687 Northrop Grumman, '2023 Human Rights Report', 2023, https://media.northropgrumman.com/c9ccf7df-2c97-4617-97a4-b385001ce549/2023%20Northrop%20Human%20Rights%20Report%20finalrfs_Original%20file.pdf
688 RTX Corporation, 'RTX reports 2025 results and announces 2026 outlook', 27 January 2026, https://www.rtx.com/news/news-center/2026/01/27/rtx-reports-2025-results-and-announces-2026-outlook-
689 RTX Corporations, 'Transformative Technologies', https://www.rtx.com/who-we-are/we-are-rtx/transformative-technologies
690 Courtney Albon, 'Norway to buy Raytheon's Stormbreaker smart bomb for F-35 fleet', Defense News, 20 July 2022, https://www.defensenews.com/air/2022/07/20/norway-announces-plans-to-buy-raytheons-stormbreaker-weapon-for-f-35-fleet/
691 RTX Corporation, 'Coyote LE', https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/coyote-launched-effects
692 Steve Trimble, 'RTX, Shield AI Win Autonomy Roles For U.S. Air Force CCAs', Aviation Week, 23 September 2025, https://aviationweek.com/defense/aircraft-propulsion/rtx-shield-ai-win-autonomy-roles-us-air-force-ccas
693 RTX Corporation, 'Our Responsibility', https://www.rtx.com/our-responsibility/overview
694 RTX Corporation, 'RTX Human Rights Policy', 2025, https://prd-sc102-cdn.rtx.com/-/media/rtx/r/rtx-human-rights-policy.pdf
695 See for example: Mwatana for Human Rights and PAX for Peace, '"Day of Judgement": The Role of the US and Europe in Civilian Death, Destruction, and Trauma in Yemen', 15 March 2019, https://paxforpeace.nl/

wp-content/uploads/sites/2/import/import/mwatana-day-of-judgement.pdf; Nima Elbagir, Salma Abdelaziz and Laura Smith-Spark, 'Made in America: Shrapnel found in Yemen ties US bombs to string of civilian deaths over course of bloody civil war', CNN, https://edition.cnn.com/interactive/2018/09/world/yemen-airstrikes-intl/

696 Meaghan Tobin, 'How China Built a Chip Industry, and Why It's Still Not Enough', The New York Times, 14 February 2026, https://www.nytimes.com/2026/02/14/business/china-chips-nvidia-huawei.html; Luke Juricic, 'ByteDance and Alibaba to release new AI models for Lunar New Year – Information', Investing.com, 29 January 2026, https://uk.finance.yahoo.com/news/bytedance-alibaba-release-ai-models-155210627.html; Liam Mo and Brenda Goh, 'Alibaba to spend $431 million for Lunar New Year AI push as chatbot war heats up', Reuters, 2 February 2026, https://www.reuters.com/business/media-telecom/alibaba-spend-431-million-lunar-new-year-ai-push-chatbot-war-heats-up-2026-02-02/. Also see the highly informative book 'Chip War' by Chris Miller (Simon & Schuster, London, 2022).

697 The updated 2026 version was put offline just after publication and has not been uploaded again. A copy can be found here: https://d1e00ek4ebabms.cloudfront.net/production/uploaded-files/2026-02991-944fbc39-bffc-4ea9-94af-e0d49be24e45.pdf. See also: Demetri Sevastopulo, 'US concludes Alibaba and BYD have links to Chinese military', The Financial Times, 14 February 2026, https://www.ft.com/content/c80ce7a7-983b-447c-88c2-de5db4cb2e0a; Alexandra Stevenson, 'Pentagon Adds Chinese Social Media Giant to Military Blacklist', The New York Times, 6 January 2025, https://www.nytimes.com/2025/01/06/business/us-chinese-military-companies-tencent-catl.html

698 Xiaoying You, 'China leads research in 90% of crucial technologies — a dramatic shift this century', Nature, 12 December 2025, https://www.nature.com/articles/d41586-025-04048-7

699 Konstantin F. Pilz, Robi Rahman, James Sanders, Luke Emberson, and Lennart Heim, 'The US hosts the majority of GPU cluster performance, followed by China', Epoch AI, 5 June 2025, https://epoch.ai/data-insights/ai-supercomputers-performance-share-by-country

700 See for example: Eduardo Baptista and Fanny Potkin, 'How China could use DeepSeek and AI for an era of war', Reuters, 27 October 2025, https://www.reuters.com/world/asia-pacific/robot-dogs-ai-drone-swarms-how-china-could-use-deepseek-an-era-war-2025-10-27/

701 See: Ralph Jennings, 'Outpaced by the US, China's military places selective bets on artificial intelligence', Defense News, 7 April 2026, https://www.defensenews.com/global/asia-pacific/2026/04/07/outpaced-by-the-us-chinas-military-places-selective-bets-on-artificial-intelligence/; Xiaolong (James) Wang, 'How China's Coming 15th Five-Year Plan Will Reshape Military Innovation', The Diplomat, 25 October 2025, https://thediplomat.com/2025/10/how-chinas-coming-15th-five-year-plan-will-reshape-military-innovation/

702 John Markoff and Matthew Rosenberg, 'China's Intelligent Weaponry Gets Smarter', The New York Times, 3 February 2017, https://www.nytimes.com/2017/02/03/technology/artificial-intelligence-china-united-states.html

703 See for example: US DoD, 'Report to Congress on Military and Security Developments involving the People's Republic of China 2025', December 2025, https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF, 'Huawei to be removed from UK 5G networks by 2027', UK Government press release, 14 July 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027; Meaghan Tobin, 'How China Built a Chip Industry, and Why It's Still Not Enough', The New York Times, 14 February 2026, https://www.nytimes.com/2026/02/14/business/china-chips-nvidia-huawei.html; Bloomberg, 'France's Huawei ban begins to kick in with purge in urban areas', 21 August 2022, https://stg1-tech.hindustantimes.com/tech/news/frances-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas-71614676790623.html and David Shepardson, 'US House to vote to provide $3 billion to remove Chinese telecoms equipment', Reuters, 8 December 2024, https://www.reuters.com/world/us/us-house-vote-provide-3-billion-remove-chinese-telecoms-equipment-2024-12-08/

704 OpenSanctions, 'BIS Entity List', https://www.opensanctions.org/programs/US-BIS-EL/

705 See for example: Ana Swanson and Paul Mozur, 'U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang', The New York Times, 7 October 2019, https://www.nytimes.com/2019/10/07/us/politics/us-to-blacklist-28-chinese-entities-over-abuses-in-xinjiang.html

706 Anton Oksentiuk, 'Military Cooperation Between Russia and China and Its Impact on the Russia-Ukraine War', 23 April 2025, https://prismua.org/en/english-military-cooperation-between-russia-and-china-and-its-impact-on-the-russia-ukraine-war/
707 See for example: Subhodip Das, 'China's Reverse Engineered Weapons – A Land of Larceny', Defence XP (Indian Defence Network), 5 February 2024, https://www.defencexp.com/chinas-reverse-engineered-weapons-a-land-of-larceny/
708 Chun Han Wong, 'How China Built an Arms Industry to Rival the West', The Wall Street Journal, 21 December 2025, https://www.wsj.com/world/china/how-beijing-built-arms-industry-to-rival-the-west-2ef824c7
709 Fanny Potkin, 'Exclusive: How China built its 'Manhattan Project' to rival the West in AI chips', Reuters, 18 December 2025, https://www.reuters.com/world/china/how-china-built-its-manhattan-project-rival-west-ai-chips-2025-12-17/
710 Fanny Potkin, 'Exclusive: How China built its 'Manhattan Project' to rival the West in AI chips', Reuters, 18 December 2025, https://www.reuters.com/world/china/how-china-built-its-manhattan-project-rival-west-ai-chips-2025-12-17/
711 Eduardo Baptista and Fanny Potkin, 'How China could use DeepSeek and AI for an era of war', Reuters, 27 October 2025, https://www.reuters.com/world/asia-pacific/robot-dogs-ai-drone-swarms-how-china-could-use-deepseek-an-era-war-2025-10-27/
712 Eduardo Baptista and Fanny Potkin, 'How China could use DeepSeek and AI for an era of war', Reuters, 27 October 2025, https://www.reuters.com/world/asia-pacific/robot-dogs-ai-drone-swarms-how-china-could-use-deepseek-an-era-war-2025-10-27/
713 A thinktank based at Georgetown University's School of Foreign Service in Washington, D.C.
714 Cole McFaul, Sam Bresnick, and Daniel Chou, 'Pulling Back the Curtain on China's Military-Civil Fusion - How the PLA Mobilizes Civilian AI for Strategic Advantage', Center for Security and Emerging Technology, September 2025, https://cset.georgetown.edu/wp-content/uploads/CSET-Pulling-Back-the-Curtain-on-Chinas-Military-Civil-Fusion.pdf
715 SIPRI, 'The SIPRI Top 100 Arms Producing and Military Services Companies in the World', 2024, https://www.sipri.org/visualizations/2025/sipri-top-100-arms-producing-and-military-services-companies-world-2024
716 Patrick Tucker, 'The big threat left out of Xi's parade: China's weaponized AI startups', Defense One, 4 September 2025, https://www.defenseone.com/threats/2025/09/big-threat-left-out-xis-parade-chinas-weaponized-ai-startups/407916/
717 Chen Chuanren, 'China Unveils New UCAV, CCA Designs In Victory Day Parade', Aviation Week, 3 September 2025, https://aviationweek.com/defense/aircraft-propulsion/china-unveils-new-ucav-cca-designs-victory-day-parade
718 William Langley and Joe Leahy, 'China's 'loyal wingman' drones open new front in military competition with US', Financial Times, 15 December 2024, https://www.ft.com/content/5687a223-6115-4cbc-86d2-2e17aaa54dc1
719 Tye Graham and Peter W. Singer, 'New products show China's quest to automate battle', Defense One, 2 March 2025, https://www.defenseone.com/threats/2025/03/new-products-show-chinas-quest-automate-battle/403387/
720 Tye Graham and Peter W. Singer, 'New products show China's quest to automate battle', Defense One, 2 March 2025, https://www.defenseone.com/threats/2025/03/new-products-show-chinas-quest-automate-battle/403387/
721 Rahul Udoshi, 'Crash attack - Loitering munitions on the rise in Asia', Janes Defence Weekly, 20 December 2023.
722 Akhil Kadidal, 'China developing 'super long-range' loitering munition', Janes Defence Weekly, 9 August 2023, https://www.janes.com/defence-intelligence-insights/defence-news/defence/china-developing-long-range-loitering-munition
723 Rahul Udoshi, 'Crash attack - Loitering munitions on the rise in Asia', Janes Defence Weekly, 20 December 2023, https://www.janes.com/
724 Dake Kang and Yael Grauer, 'Detailed findings from AP investigation into how US tech firms enabled

China's digital police state', AP, 9 September 2025, https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-a80904158b771a14d5a734947f28d71b

725 Eduardo Baptista and Fanny Potkin, 'How China could use DeepSeek and AI for an era of war', Reuters, 27 October 2025, https://www.reuters.com/world/asia-pacific/robot-dogs-ai-drone-swarms-how-china-could-use-deepseek-an-era-war-2025-10-27/

726 Steve Holland and Alexandra Alper, 'Exclusive: China's top chipmaker has supplied chipmaking tech to Iran military, US officials say', Reuters, March 27, 2026, https://www.reuters.com/world/asia-pacific/chinas-top-chipmaker-has-supplied-chipmaking-tech-iran-military-us-officials-say-2026-03-27/

727 Joseph Wilde-Ramsing, Katharine Booth and Omid Shams (Justice for Iran), 'Caught on camera: How CCTV tech contributes to human rights abuse in Iran', SOMO, 30 January 2023, https://www.somo.nl/caught-on-camera-how-cctv-tech-contributes-to-human-rights-abuse-in-iran/

PAX
+31 (0)30 - 233 33 46
info@paxvoorvrede.nl
paxforpeace.nl

Privacy International
+44 (0)20 3422 4321
info@privacyinternational.org
privacyinternational.org