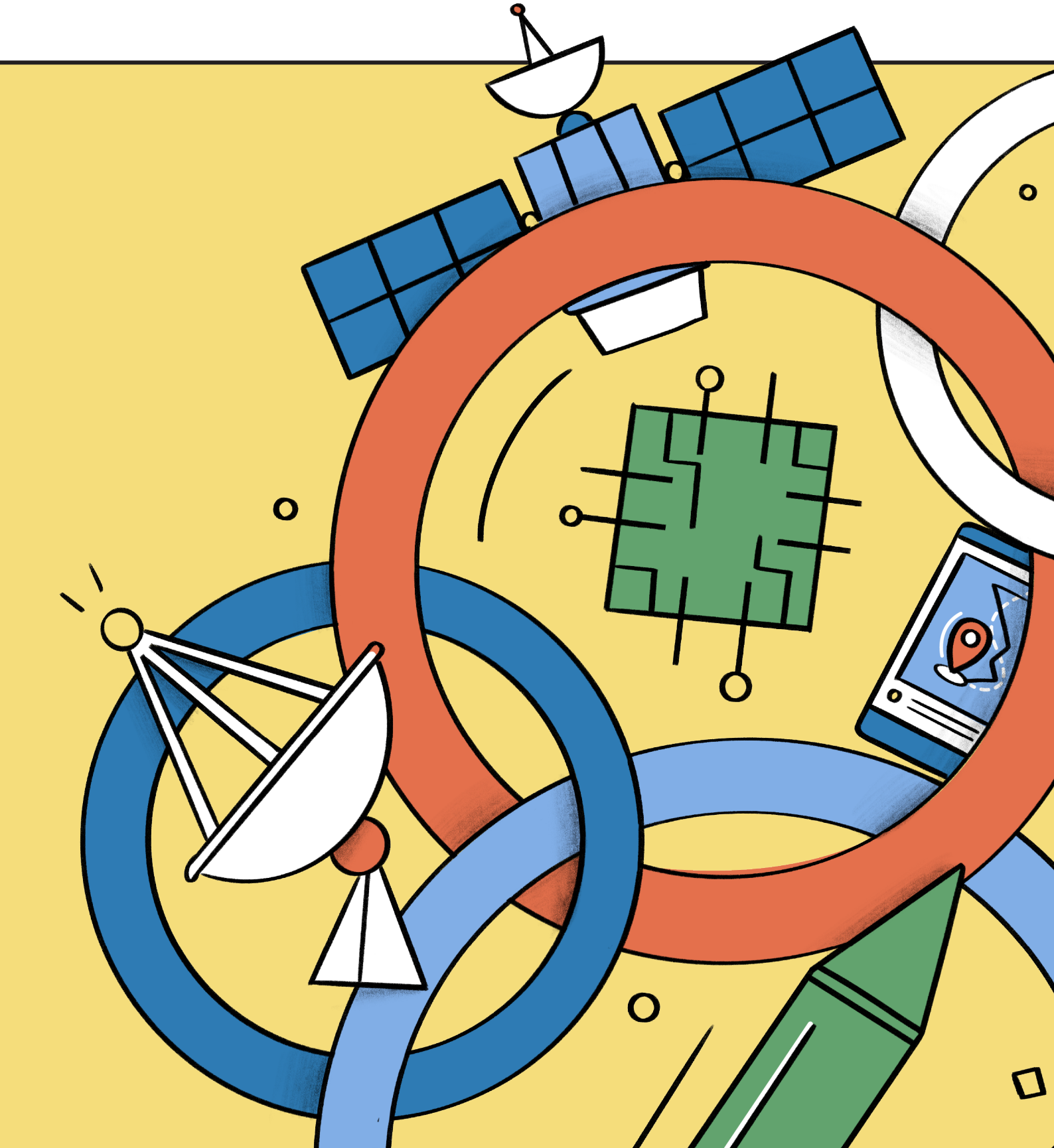
# WHEN ALGORITHMS GO TO WAR

Tech giants, the arms industry and the weaponisation of AI

June 2026



Scan for further information

# 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.

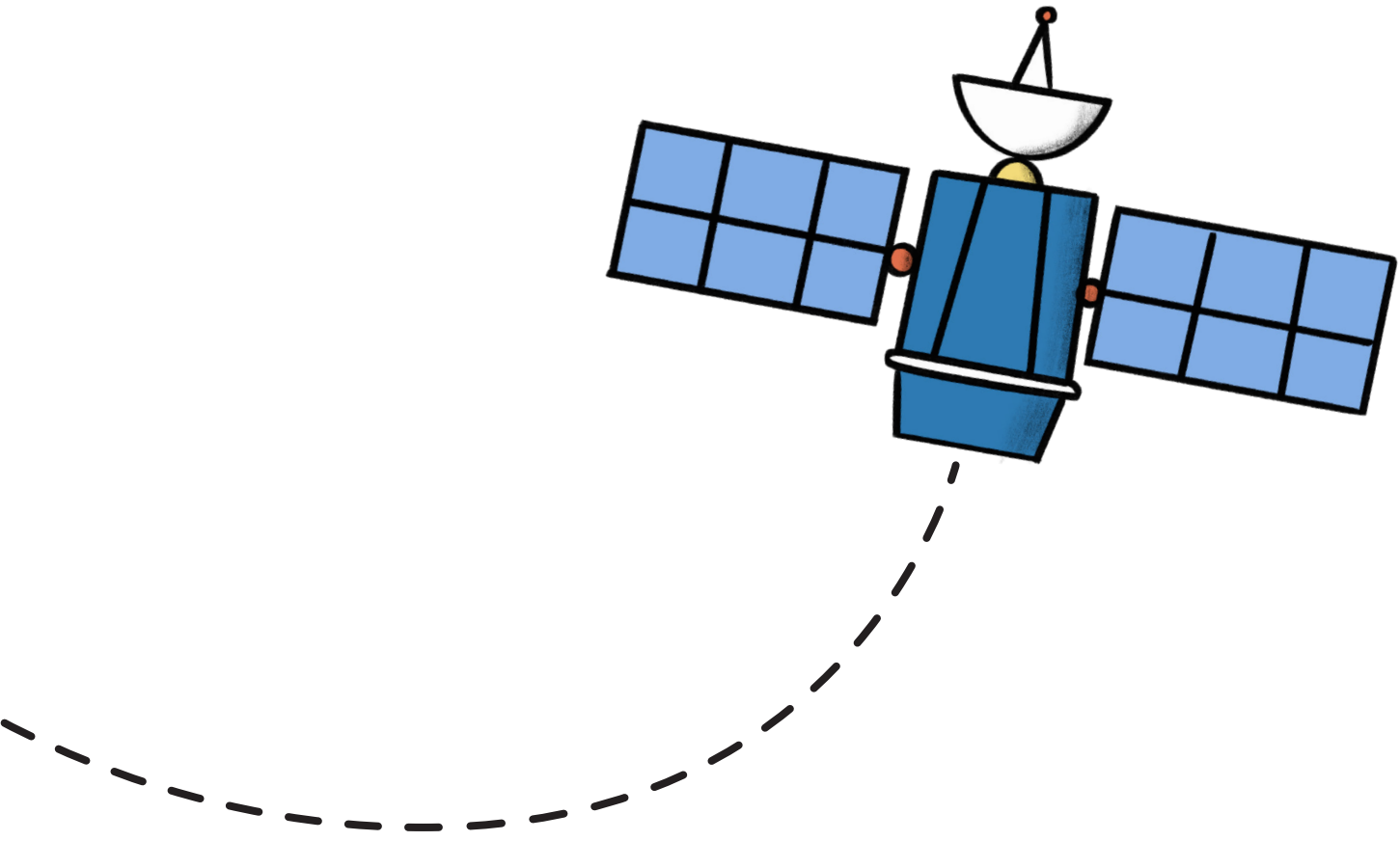
## The case for international guidelines

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.


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

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