POLICY BRIEF | ECONOMICS

AI for War: Big Tech Empowering Israel's Crimes and Occupation

By: Marwa Fatafta · October, 2025

Introduction

US technology giants portray themselves as architects of a better world powered by artificial intelligence (AI), cloud computing, and data-driven solutions. Under slogans such as "AI for Good," they pledge to serve as ethical stewards of the technologies reshaping our societies. Yet in Gaza, these narratives have collapsed, alongside international norms and what remains of the so-called rules-based order.

The Israeli regime's genocidal war in Gaza has drawn attention to the role of major technology companies in enabling military operations and sustaining the occupation. Beneath the Israeli destruction lie servers, neural networks, and software systems built and deployed by some of the world's most powerful corporations. The increasing militarization of digital technologies and infrastructures—most visibly in Israel's deployment of AI-driven systems and data analytics in Gaza—has reshaped debates on accountability and exposed critical gaps in existing governance frameworks. This policy brief examines how the frontier of accountability for technology companies now extends to potential complicity in war crimes, crimes against humanity, and genocide, underscoring the

urgent need for new approaches to regulating AI militarization.[1]

An AI-Powered Genocide

The Israeli regime first deployed AI systems to generate and prioritize lethal targets during the 11-day bombardment of Gaza in May 2021—a vicious, unlawful assault the Israeli military later described as its first "AI war." Since then, the occupation forces have significantly expanded their reliance on AI tools, using cloud computing and machine learning to store and process vast volumes of surveillance data—from satellite imagery to intercepted communications—to automate the identification and ranking of targets for attack.

Central to Israel's AI warfare is Project Nimbus—a $1.2 billion contract through which Google and Amazon have provided the Israeli government and military with advanced cloud infrastructure and machine learning capabilities. In the early days of the genocide, Israeli forces reportedly relied almost entirely on AI-powered target-generating systems—such as Lavender, The Gospel, and Where's Daddy—to accelerate mass killing and destruction across Gaza. These platforms ingest mass surveillance data about the entire population of Gaza to algorithmically determine—at scale—who is to be killed, which buildings are to be bombed, and how much "collateral damage" is deemed acceptable.

Alarmingly, these AI-driven systems internalize the genocidal logic of their operators. They are trained to treat civilians as "terrorists," building on the genocidal logic of Israeli officials who declared that "there are no innocent civilians in Gaza." As part of efforts to automate lethal targeting, military commanders reportedly instructed soldiers to identify and feed as many targets as possible into the system. This effectively lowers the threshold for designating individuals as "Hamas militants," casting a wide net of algorithmically flagged subjects. Despite its high error rate, the only criterion Israeli soldiers applied to Lavender's kill list was the target's gender, effectively rendering all Palestinian

males—children and adults alike—legitimate targets. In practice, AI technology has enabled the Israeli regime's genocidal logic to be executed with ruthless, machine-driven efficiency, reducing Palestinians, their families, and their homes to what the military chillingly refers to as "garbage targets."

While many of the technical details of Israel's AI targeting systems remain classified, there is ample credible evidence that their functionality depends on cloud infrastructure and machine-learning capabilities developed and maintained by major technology companies, including Google, Amazon, Microsoft, and Palantir. Consequently, tech companies' direct provision of digital systems used in Israeli warfare raises urgent questions about corporate complicity in grave violations of international law, including acts for which the International Criminal Court (ICC) has issued arrest warrants for Israeli Prime Minister Benjamin Netanyahu and former Defense Minister Yoav Gallant.

From Code to Kill Lists

As Israel intensified its assault on Gaza, its demand for AI and cloud-based technologies, supplied by US tech giants, grew rapidly, embedding corporate infrastructure into the machinery of war. In March 2024, Google deepened its ties with the Israeli Ministry of Defense (IMOD) by signing a new contract to build a specialized "landing zone" into its cloud infrastructure, enabling multiple military units access to its automation technologies. Amazon Web Services (AWS), Google's partner in Project Nimbus, was reported to have supplied Israel's Military Intelligence Directorate with a dedicated server farm capable of endless storage for surveillance data collected on almost everyone in Gaza.

Recent reporting has further documented the rapid expansion of Israel's AI-driven military capabilities, underscoring how growing partnerships with technology companies have accelerated the deployment of advanced systems in its war on Gaza. According to leaked documents, Microsoft hosted elements of the Israeli

military's mass surveillance program on its cloud servers, storing recordings of millions of intercepted phone calls from Palestinians in Gaza and the West Bank. The Israeli occupation forces reportedly used these files to identify bombing targets, blackmail individuals, place people in detention, and also to justify killings after the fact. The Israeli military's reliance on Microsoft Azure surged accordingly: in the first six months of the war, its average monthly use rose by 60%, while use of Azure's machine-learning tools increased 64-fold compared to prewar levels. By March 2024, the use of Microsoft and OpenAI technological tools by Israeli forces was nearly 200 times higher than it had been in the week preceding October 7, 2023. In addition, the amount of data stored on Microsoft's servers had doubled to more than 13 petabytes.

The results of Microsoft's own internal review, announced in September 2025, ultimately confirmed that a unit of the Israeli defense ministry had indeed used some of its services for prohibited surveillance purposes. Consequently, the company suspended certain cloud and AI services, admitting that its technology was complicit in practices that contravened its terms of service. Yet Microsoft's suspension of services to the Israeli military was minimal: many contracts and functions with the Israeli military and other government bodies responsible for gross human rights abuses and atrocity crimes remain intact. While the review itself is still ongoing, this narrow admission lays bare the company's complicity in Israel's military machinery.

Moreover, big tech's involvement in Israel's war appears to extend beyond standard service provision. Microsoft engineers have reportedly provided both remote and on-site technical assistance to Israeli forces, including Unit 8200 (cyber operations and surveillance) and Unit 9900 (geospatial intelligence and targeting). In fact, the Israeli defense ministry procured approximately 19,000 hours of Microsoft engineering and consultancy services, valued at around $10 million. Amazon has likewise been implicated, reportedly providing not only cloud

infrastructure but also direct assistance in verifying targets for airstrikes. Google's role raises additional concerns: according to internal documents, the company created a classified team composed of Israeli nationals with security clearances, tasked explicitly with receiving sensitive information from the Israeli government that could not be shared with the broader company. This team is set to deliver "specialized training with government security agencies" and to participate in "joint drills and scenarios tailored to specific threats." No comparable arrangement seems to exist between Google and any other state, underscoring the exceptional depth of its collaboration with the Israeli regime.

Profit is not the sole driver of big tech's deepening entanglement with Israel's military; political affinity plays a role as well. Palantir Technologies, a US-based data analytics and surveillance company known for its close ties to intelligence and defense agencies, has openly expressed support for Israel throughout the Gaza genocide. Palantir has partnered with AWS to deliver tools designed to help clients, such as the Israeli military, "win in the warfighting context." The company signed a strategic partnership with the Israeli defense ministry to provide technologies directly supporting the genocidal campaign. Microsoft, too, has longstanding ties with Israel's military and security apparatus—ties so close that Netanyahu once described the relationship as "a marriage made in heaven but recognized here on earth."

By providing direct support to Israeli military operations, tech companies are not merely supplying infrastructure; they are actively facilitating and aiding the surveillance, targeting, and execution of actions that violate international law. In a grim evolution, the deployment of commercial AI in Gaza marks a chilling frontier: systems once designed to optimize logistics and decision-making at scale are now generating kill lists, erasing families, and leveling entire neighborhoods. Technology developed and maintained by big tech now underpins warfare, ethnic cleansing, and genocide in Palestine, serving as a prototype for the future of

automated warfare.

The Future of Warfare

The Israeli regime has formalized its push toward automated warfare by creating a dedicated AI research division within the IMOD, tasked with advancing military capabilities for a future in which "battlefields will see integrated teams of soldiers and autonomous systems working in concert." This initiative marks a significant shift toward the normalization of AI-driven combat. Western governments, including France, Germany, and the US, are pursuing similar trajectories, racing to integrate artificial intelligence into their weapons systems and armed forces. Together, these developments position Israel not only as an early adopter but as a model for the coming era of algorithmic warfare.

In parallel, major tech companies are abandoning their self-imposed ethical boundaries in pursuit of military contracts. Earlier this year, both Google and OpenAI quietly abandoned their voluntary commitments not to develop AI for military use, signaling a broader realignment with the security and defense sectors. Within weeks of amending its AI principles, Google signed a formal partnership with Lockheed Martin, the world's largest arms manufacturer and a major supplier of weapons to the Israeli military. In November 2024, Meta announced that it would make its large language models, called Llama, available to US government agencies and contractors working on national security. Lockheed Martin has since integrated Llama into its operations.

Joining the AI-for-warfare race, Meta has also partnered with Anduril, a defense technology startup, to develop virtual and augmented reality devices for the US Army. Despite its nonprofit status, OpenAI collaborated with Anduril to deploy its technology on the battlefield. In addition, Palantir and Anthropic—an AI research and development company backed by Google—announced a partnership with AWS to "provide US intelligence and defense agencies access" to its AI systems.

A telling indicator of the deepening convergence between big tech and ministries of war is the US Army's decision to grant senior executives from Palantir, Meta, OpenAI, and Thinking Machines Labs the rank of lieutenant colonel and to embed them as advisors within the armed forces. Framed as an effort to "guide rapid and scalable tech solutions to complex problems," the initiative seeks to make the US military "leaner, smarter, and more lethal." The symbolism is hard to miss: Silicon Valley leaders are no longer merely building tools for the battlefield; they are being formally integrated into its command structure.

AI Militarization in a Regulatory Vacuum

AI militarization is rapidly unfolding in the absence of effective regulatory frameworks. While states continue to deliberate norms for autonomous weapons at the UN, no binding international treaty specifically governs their development or deployment. Even less regulated are dual-use technologies, such as LLMs and cloud infrastructure, which are now being embedded in military operations. Recent national and global conversations and regulatory proposals regarding AI governance, which often focus on upholding privacy and human rights, largely sidestep the devastating impact of AI systems in conflict zones. The most illustrative example of this disconnect is Israel's signing of the Council of Europe's AI treaty, which addresses human rights, democracy, and the rule of law, at a time when credible reports were emerging about its use of AI-driven targeting in Gaza. While the treaty contains numerous caveats that limit its effectiveness, Israel's signature amid an ongoing campaign of genocide underscores the profound disconnect between the legal norms being crafted and the battlefield deployment of the technologies they seek to regulate.

Meanwhile, voluntary guidelines or soft-law mechanisms are routinely discarded. The UN Guiding Principles on Business and Human Rights (UNGPs), which outline both state obligations and corporate responsibilities to identify and mitigate

human rights risks, are frequently ignored by tech companies. While these principles clearly state that companies operating in conflict zones must treat the risk of contributing to gross human rights abuses and violations of international humanitarian law as a legal compliance issue, tech companies continue to comply selectively. Microsoft's belated admission that the Israeli regime used its cloud infrastructure for mass surveillance in Gaza is a case in point. In May 2025, Microsoft denied enabling the Israeli regime to inflict harm on Palestinians through mass surveillance, only to reverse course months later with a narrow admission of misuse of its technology. As mentioned, this admission exposes the extent to which companies fail to fulfil their responsibility under the UNGPs to identify and mitigate such harm.

In this context, international criminal law remains inadequate to address corporate complicity in war crimes. Both customary law and the Rome Statute restrict criminal liability to natural persons, excluding corporations as legal entities. As a result, pursuing corporate accountability for the involvement in committing and perpetuating atrocity crimes, including genocide, war crimes, and crimes against humanity, is a legal struggle of its own.

While the prospect of seeing a tech executive stand trial for aiding and abetting international crimes may seem remote, even modest calls for regulation and accountability are increasingly under attack. The Trump administration has folded big tech into its broader pursuit of global dominance, effectively rendering the industry giants untouchable. In alignment with industry lobbyists, Trump has pledged to resist state-level regulation of the tech sector and has already begun rolling back oversight mechanisms. The sanctioning of the UN Special Rapporteur for Palestine, Francesca Albanese, following the release of her report on corporate complicity in Israel's unlawful occupation and genocide, further illustrates the current climate in which the US government and corporations close ranks to shield themselves from any pursuit of justice and

accountability. Compounded by entrenched anti-Palestinian bias and the persistent double standards surrounding Israel's crimes and occupation, these dynamics have created a permissive legal and political environment that shields the tech sector from scrutiny. As a result, tech companies can continue to design, deploy, and support AI-driven targeting systems and mass surveillance technologies in direct collaboration with the Israeli military occupation, without oversight or accountability.

Amid this accountability crisis, tech workers are increasingly at the forefront of challenging corporate complicity. While executives double down on their business ties with the Israeli regime, dissent within the tech industry continues to grow, as more employees refuse to build the tools that enable genocide, colonization, and apartheid. The recent termination of Microsoft workers who protested the company's role in Israel's genocide in Gaza was mirrored at Google, where employees have faced retaliation for opposing collaboration with Israeli military and security agencies. Organizers from groups such as No Tech for Apartheid and the Tech Workers Coalition have been central in exposing the industry's deep entanglement with state violence, often carried out through opaque and undisclosed military contracts.

Recommendations

While resistance within the tech industry continues to grow, Palestinian civil society and global solidarity movements must intensify efforts to dismantle the structures that dehumanize Palestinians and treat them as test subjects for new war technologies.

First, addressing corporate complicity requires confronting the research partnerships involving private entities, including business enterprises and academic institutions, which collaborate in developing and scaling militarized technologies. It also requires examining the funding streams, trade flows, and

broader economic ties that sustain and legitimize Israel's militarized tech sector. Often described as the "engine of growth", Israel's high-tech industry is structurally reliant on private and foreign capital. Around 91% of its funding comes from the private sector, and roughly 80% of venture capital investments originate from abroad. These figures underscore how international investors, universities, and corporations are directly implicated in financing and legitimizing Israel's military-tech apparatus. Governments, regulators, and civil society should press for transparency in financial flows, condition partnerships on compliance with international law, and pursue divestment or sanctions against companies complicit in atrocity crimes and systemic human rights violations.

Second, civil society efforts and legal initiatives focused on accountability must place greater emphasis on the digital infrastructures underpinning Israel's crimes, not only in Gaza but also in the West Bank. The Office of the Prosecutor at the ICC recently published its first draft policy on investigating and prosecuting cyber-enabled crimes—an overdue acknowledgment of the digital dimensions of today's atrocity crimes. While prosecuting tech executives for complicity in such crimes is a complex and long-term undertaking—fraught with challenges of evidence, intent, and jurisdiction—it offers a path worth exploring.

The 2024 International Court of Justice advisory opinion on the illegality of Israel's occupation makes clear that states are obligated to refrain from supporting or sustaining that unlawful presence. This opinion opens the door to legal challenges not only against governments that maintain economic or military ties with Israel, but also against corporations domiciled in those states whose technologies materially facilitate ethnic cleansing and occupation. Civil society actors should use this opinion to pressure states to regulate such corporate involvement, pursue litigation where companies fail to comply, and advocate for divestment from firms that continue to provide digital infrastructure to the Israeli regime.

Third, fostering stronger alliances between legal advocates and tech workers is

crucial. These collaborations can expose opaque military contracts, strengthen evidence gathering, and amplify internal dissent within the industry. By connecting legal strategies with worker-led resistance, such alliances can both challenge the complicity embedded in the digital infrastructures of war and apartheid and lay the groundwork for future accountability mechanisms.

Ultimately, establishing clear accountability mechanisms for military AI requires governments, regulators, and civil society to collaborate in closing legal loopholes and reshaping the global tech landscape to uphold international law. Big tech accountability is particularly urgent given the accelerating use of AI in warfare, and consequently the heightened scale, speed, and opacity of AI-driven lethal force. In the case of Palestine, AI technologies supplied by major tech companies have played a central role in enabling the Israeli regime to wage a genocidal campaign in Gaza with unprecedented scale and ruthlessness. Holding these companies accountable is therefore a core component of the broader pursuit of justice and accountability for Israel's war crimes.

1. *To read this piece in French, please click here. Al-Shabaka is grateful for the efforts by human rights advocates to translate its pieces, but is not responsible for any change in meaning.*

Al-Shabaka: The Palestinian Policy Network, is an independent, non-profit organization. Al-Shabaka convenes a multidisciplinary, global network of Palestinian analysts to produce critical policy analysis and collectively imagine a new policymaking paradigm for Palestine and Palestinians worldwide.

Al-Shabaka materials may be circulated with due attribution to Al-Shabaka: The Palestinian Policy Network. The opinion of individual members of Al-Shabaka's policy network do not necessarily reflect the views of the

organization as a whole.