



20 Sekunden bis zum Tod: Die KI-Infrastruktur des Silicon Valley hinter dem Völkermord in Gaza

von Legi-Team | 3. Nov. 2025

Die Werbevideos zeigen lächelnde Ingenieure. Die Pressemitteilungen versprechen „KI für das Gute“. Aber in Gaza kollidiert die beschönigende Sprache der technologischen Innovation mit einer brutalen Realität, in der künstliche Intelligenzsysteme, die im Silicon Valley entwickelt wurden, nun darüber entscheiden, wer lebt und wer stirbt. Marwa Fatafta, eine palästinensische Forscherin und Politikanalystin mit Sitz in Berlin, hat monatelang dokumentiert, wie es dazu gekommen ist. Ihr neuer Bericht enthüllt etwas, das uns alle erschüttern sollte. Die Cloud-Computing- und KI-Tools der großen Tech-Unternehmen werden nicht nur im Krieg Israels gegen Gaza eingesetzt, sondern sind zu einer unverzichtbaren Infrastruktur für das geworden, was mehrere UN-Gremien als Völkermord bezeichnet haben.

Zwanzig Sekunden, um einen Menschen

zum Tode zu verurteilen

In den israelischen Militärkommandozentralen laufen rund um die Uhr KI-Systeme mit Namen wie „Lavender“, „The Gospel“ und „Where’s Daddy?“. Sie unterstützen menschliche Entscheidungen nicht etwa, sondern ersetzen sie vielmehr. Lavender kann ein Ziel in nur 20 Sekunden identifizieren und genehmigen. Denken Sie darüber nach. In der Zeit, die Sie zum Lesen dieses Absatzes benötigen, hat das System bereits entschieden, dass jemand sterben soll.

Das Ausmaß ist atemberaubend in seinem Schrecken. Laut Berichten israelischer Militärquellen erstellte Lavender eine Liste mit 37.000 Personen, die es als Hamas-Mitglieder identifizierte. Viele waren niedrigrangig. Einige hatten überhaupt keine bestätigten militärischen Funktionen. Das israelische Militär griff täglich bis zu 250 Ziele an, mehr als doppelt so viele wie in früheren Konflikten. Bis Dezember 2023 wurden mehr als 22.000 Ziele in Gaza getroffen, ein Tempo, das ohne algorithmische Automatisierung unmöglich wäre.

Dann gibt es noch „Where’s Daddy?“, ein System, das Berichten zufolge Militante über ihre Mobiltelefone verfolgt und wartet. Es wartet, bis sie nach Hause gehen. Bis sie bei ihren Familien sind. Das System bestätigt ihre Anwesenheit zu Hause als Bestätigung ihrer Identität. Und dann schlägt es zu. Ein hochrangiger israelischer Militärvertreter beschrieb, wie es funktioniert: Jedes Ziel wird mit einer „Kollateralschaden-Punktzahl“ versehen, einer Berechnung, wie viele Zivilisten wahrscheinlich sterben werden. Die Bediener, so der Vertreter, verwenden „sehr genaue“ Messungen, wie viele Zivilisten kurz vor einem Angriff ein Gebäude evakuieren. Ein anderer Militärinsider verglich es mit einer „Ampel“. Familien werden zu akzeptablen Verlusten. Häuser werden zu Todesfallen. Kinder werden zu Kollateralschäden, deren Tod im Voraus berechnet und als akzeptabel angesehen wird.

Die Cloud-Dienste hinter dem Mord

An dieser Stelle kommen amerikanische Unternehmen ins Spiel. Zwischen dem 7. Oktober 2023 und dem folgenden März stieg die Nutzung von Microsoft- und OpenAI-Künstlicher Intelligenz durch das israelische Militär

auf fast das 200-Fache des Vorkriegsniveaus. Die auf Microsoft-Servern gespeicherten Daten verdoppelten sich bis Juli 2024 und erreichten mehr als 13,6 Petabyte, was etwa dem 350-fachen des digitalen Speichers entspricht, der benötigt wird, um alle Bücher der Library of Congress zu speichern. Die KI-Modelle, die diese Systeme antreiben? Sie stammen von OpenAI, dem Hersteller von ChatGPT, werden über die [Azure-Cloud-Plattform](#) von Microsoft bereitgestellt und vom israelischen Militär gekauft.

Dies ist die erste Bestätigung, die wir erhalten haben, dass kommerzielle KI-Modelle direkt in der Kriegsführung eingesetzt werden, sagt Heidy Khlaaf, leitende Wissenschaftlerin für künstliche Intelligenz am AI Now Institute.

Auf einer Militärkonferenz mit dem Titel „IT for IDF“ im Jahr 2014 wurden die Auswirkungen deutlich sichtbar, als Oberst Racheli Dembinsky, eine hochrangige israelische Militär-IT-Offizierin, beschrieb, wie KI in Gaza zu einer „sehr bedeutenden operativen Effektivität“ beigetragen hatte, während hinter ihr die Logos von Microsoft Azure, Google Cloud und [Amazon Web Services](#) auf dem Bildschirm erschienen.

Wir haben bereits einen Punkt erreicht, an dem unsere Systeme dies wirklich benötigen.
(Vgl. [youtube.com](#))

Auch Google und Amazon sind keine unbeteiligten Zuschauer. Im Rahmen des „Projekts Nimbus“, einem 2021 unterzeichneten Vertrag im Wert von 1,2 Milliarden Dollar, stellen beide Unternehmen Cloud-Computing- und KI-Dienste direkt für die israelischen Streitkräfte bereit. Und es gibt Hinweise darauf, dass sogar Meta daran beteiligt ist: Metadaten von WhatsApp könnten in das Lavender-Zielsystem einfließen. (Vgl. [haaretz.com](#))

Gaza als Versuchslabor

Für Gaza ist das nichts Neues. Seit Jahrzehnten nutzt Israel den Gazastreifen als eine Art lebendes Testgelände für Waffen und Überwachungstechnologien. Was in Gaza getestet wird, wird verfeinert, verpackt und weltweit verkauft. Die Überwachung, die diese KI-Systeme

speist, ist ebenso erschreckend. Eine Untersuchung der *New York Times* ergab:

Dass israelische Militär hat ein umfangreiches Gesichtserkennungssystem in Gaza eingesetzt um die Gesichter von Palästinensern, ohne deren Wissen oder Zustimmung, zu sammeln und zu katalogisieren.

Aktivitäten in sozialen Medien, Telefonaufzeichnungen, Tagesabläufe – all das wird erfasst, analysiert und in KI-Systeme eingespeist, die das normale Leben in Ziel-Daten verwandeln. Ihr morgendlicher Weg zur Arbeit, Ihre Telefonate, wo Sie beten und wo Ihre Kinder zur Schule gehen – all das wird zu Informationen, die Sie zu einem Ziel machen.

Die rechtliche Einschätzung

Im September 2025 kam die Unabhängige Internationale Untersuchungskommission der Vereinten Nationen für die besetzten palästinensischen Gebiete zu dem Schluss, dass Israel Völkermord an den Palästinensern im Gazastreifen begangen hat. Die Kommission stellte fest, dass die israelischen Behörden vier der fünf in der Völkermordkonvention von 1948 definierten Völkermordhandlungen begangen haben.

Ein von den Menschenrechtsorganisationen [Al-Haq](#) und [SOMO](#) in Auftrag gegebenes Rechtsgutachten legt nahe, dass Technologieunternehmen, die für israelische Militäroperationen unverzichtbare Dienstleistungen erbringen, möglicherweise direkt zu Verstößen gegen das humanitäre Völkerrecht und möglicherweise zu Völkermordhandlungen beitragen. Die Analyse stellt fest:

Nach internationalem Strafrecht erfordert direkte Mittäterschaft eine vorsätzliche Beteiligung, aber nicht unbedingt die Absicht, Schaden zuzufügen, sondern nur die Kenntnis vorhersehbarer schädlicher Auswirkungen.

Mit anderen Worten: Unwissenheit ist keine Rechtfertigung. Die UN-Sonderberichterstatteerin Francesca Albanese hat 48 Unternehmen, darunter Microsoft und Googles Muttergesellschaft [Alphabet](#), namentlich

genannt, die Israels Krieg gegen Gaza unter Verstoß gegen das Völkerrecht unterstützen. Ihr Bericht fand „begründete Anhaltspunkte“ für die Annahme, dass Palantir Technologie für automatisierte Entscheidungen auf dem Schlachtfeld und die Erstellung von Ziellisten durch KI-Systeme wie Lavender bereitgestellt hat.

Ben Saul, ein weiterer UN-Sonderberichterstatter, brachte es auf den Punkt:

Wenn die Berichte über Israels Einsatz von KI zutreffen, würden viele israelische Angriffe auf Gaza Kriegsverbrechen in Form von unverhältnismäßigen Angriffen darstellen.

Die menschlichen Opfer

Die Zahlen sind erschütternd, aber sie geben nicht die Realität wieder. Seit Beginn des Krieges sind mehr als 60.000 Menschen in Gaza ums Leben gekommen, ganz zu schweigen von denen, die im Libanon ihr Leben verloren haben. Einige Berichte gehen davon aus, dass weitere hunderttausend Menschen unter den Trümmern im Gazastreifen begraben sind, während Daten zeigen, dass fast 70% der Gebäude in Gaza zerstört oder beschädigt wurden.

Hinter jeder Statistik steht ein Name. Ein Gesicht. Ein Leben. Wenn ein dreijähriges Mädchen in einem Haus in Gaza getötet wird, dann deshalb, weil jemand in der Armee entschieden hat, dass es keine große Sache ist, wenn sie getötet wird, dass es ein Preis ist, den es zu zahlen gilt, um [ein anderes] Ziel zu treffen, erklärte eine Quelle aus dem israelischen Militärgeheimdienst gegenüber [+972Magazine](#). Das sind keine zufälligen Raketen. Alles ist absichtlich. Wir wissen genau, wie hoch der Kollateralschaden in jedem Haus ist.

Die Systeme selbst weisen grundlegende Mängel auf. Ein Bericht des *Jewish Institute for National Security of America* ([JNSA](#)) hat ein kritisches Problem aufgezeigt: Das System verfügte über Daten darüber, was ein Ziel darstellte, aber nicht darüber, *was kein Ziel war*. Informationen, die von menschlichen Analysten geprüft und als nicht bedrohlich eingestuft

worden waren, wurden einfach verworfen. Die KI lernte nur aus positiven Beispielen für Ziele, was zu einer unvermeidlichen Verzerrung führte.

Die Tatsache, dass KI-Systeme eingesetzt werden, zeigt, dass es dem israelischen Staat an Rücksichtnahme mangelt, sagte Ramesh Srinivasan, Professor an der UCLA. Jeder weiß, dass diese KI-Systeme Fehler machen werden.

Dennoch vertrauten Berichten zufolge viele Betreiber Lavender so sehr, dass sie dessen Ziele ohne jegliche Überprüfung genehmigten.

Widerstand von innen

Nicht alle Mitarbeiter dieser Unternehmen fühlen sich wohl dabei. Mitarbeiter von Amazon, Google, Microsoft und Palantir haben öffentlich die Rolle ihrer Arbeitgeber in der KI-gestützten Kriegsführung in Frage gestellt. Einige haben eine mögliche Mittäterschaft an Kriegsverbrechen angeführt. Microsoft sah sich internen Gegenreaktionen ausgesetzt, weil es Azure-Dienste für die israelische Signalaufklärungseinheit Unit 8200 bereitgestellt hatte. Nachdem *The Guardian* berichtet hatte, dass Daten aus der Massenüberwachung in Gaza und im Westjordanland, darunter auch Telefonaufzeichnungen, zur Identifizierung von Bombenzielen verwendet wurden, leitete Microsoft eine Untersuchung ein. Im September 2024 beendete das Unternehmen den Zugang der Einheit 8200 zu Azure-Diensten.

Paul Scharre vom „Center for a New American Security“ ([CNAS](#)) warnt jedoch:

Das Tempo der technologischen Entwicklung übertrifft bei weitem das Tempo der politischen Entwicklung.

Der Schaden ist angerichtet. Der Präzedenzfall ist geschaffen.

Der Zusammenbruch von „KI für das Gute“

Unter Slogans wie „KI für das Gute“ haben uns Technologieunternehmen ethische Innovationen und sozialen Fortschritt versprochen. Sie sprachen von der Demokratisierung von Informationen, der Vernetzung der Menschheit und der Lösung globaler Herausforderungen. In Gaza jedoch liegen diese Versprechen buchstäblich in Trümmern, inmitten der Ruinen von Häusern, die algorithmisch ins Visier genommen wurden.

Was wir derzeit erleben, ist die Apotheose der gefährlichsten Trends der KI: Biometrische Massenüberwachung, prädiktive Polizeiarbeit und automatisierte Entscheidungen über Leben und Tod. Technologien, die laut Menschenrechtsaktivisten selbst in Friedenszeiten verboten werden sollten, werden nun in einem Konflikt eingesetzt, den UN-Experten eindeutig als Völkermord bezeichnen.

Wenn eindeutige Anzeichen und Beweise für einen Völkermord vorliegen, kommt Untätigkeit gleich einer Mittäterschaft, sagte die Vorsitzende der Kommission, Navi Pillay. Jeder Tag der Untätigkeit kostet Menschenleben und untergräbt die Glaubwürdigkeit der internationalen Gemeinschaft.

Was kommt als Nächstes?

Gaza hat eine Frage eindeutig beantwortet: KI kann und wird für Massenmord als Waffe eingesetzt werden. Zwei Fragen bleiben jedoch offen. Werden wir zulassen, dass die Unternehmen, die von dieser Gewalt profitieren, sich ihrer Verantwortung entziehen? Werden die Giganten aus dem Silicon Valley für die Bereitstellung der Infrastruktur für Völkermord zur Rechenschaft gezogen oder werden sie weiterhin ihre Milliardenverträge einfahren und gleichzeitig hohle Erklärungen über ethische KI abgeben? Und wird die internationale Gemeinschaft zulassen, dass dieses neue Paradigma des automatisierten, algorithmischen Tötens zur Normalität wird? Werden „Where’s Daddy?“ und ähnliche Systeme zum Vorbild für die Kriege von morgen?

In Gaza spielt gerade ein Kind. Möglicherweise wird es bereits von einem Algorithmus beobachtet. Möglicherweise berechnet eine Serverfarm in Kalifornien bereits seinen Tod. Möglicherweise profitiert bereits ein Unternehmen davon. Die Zukunft der Kriegsführung kommt nicht erst. Sie ist bereits da. Und sie wird von Unternehmen aufgebaut, deren Logos wir

jeden Tag sehen, deren Produkte wir in unseren Taschen tragen, deren Dienste wir ohne nachzudenken nutzen. Die einzige Frage, die noch offen ist, lautet: *Was werden wir dagegen tun?*

Freddie Ponton

(Vgl. 21stcenturywire.com)



Marwa Fatafta berichtet für [Al-Shabaab](#): KI für den Krieg: Big Tech unterstützt Israels Verbrechen und Besatzung

Zusammenfassung

US-amerikanische Technologiekonzerne präsentieren sich als ethische Innovatoren, die durch künstliche Intelligenz (KI) und Cloud Computing eine bessere Welt gestalten. In Gaza jedoch sind diese Narrative zusammengebrochen. KI-Systeme, Cloud-Infrastrukturen und Überwachungsinstrumente, die von Technologieunternehmen wie Google, Amazon, Microsoft und Palantir bereitgestellt werden, sind zu einem integralen Bestandteil der Völkermordkampagne Israels gegen die Palästinenser geworden.

Einleitung

Die US-amerikanischen Technologiegiganten präsentieren sich als Architekten einer besseren Welt, die von künstlicher Intelligenz (KI), Cloud Computing und datengesteuerten Lösungen angetrieben wird. Unter Slogans wie „AI for Good“ versprechen sie, als ethische Verwalter der Technologien zu fungieren, die unsere Gesellschaften neu gestalten. In Gaza jedoch sind diese Narrative zusammengebrochen, ebenso wie internationale Normen und die Überreste der sogenannten „regelbasierten Ordnung“.

Der Völkermordkrieg des israelischen Regimes in Gaza hat die Aufmerksamkeit auf die Rolle großer Technologieunternehmen bei der Ermöglichung militärischer Operationen und der Aufrechterhaltung der Besatzung gelenkt. Hinter der Zerstörung durch Israel stehen Server, neuronale Netzwerke und Softwaresysteme, die von einigen der mächtigsten Unternehmen der Welt entwickelt und eingesetzt werden. Die zunehmende Militarisierung digitaler Technologien und Infrastrukturen, die am deutlichsten in Israels Einsatz von KI-gesteuerten Systemen und Datenanalysen in Gaza zum Ausdruck kommt, hat die Debatten über Rechenschaftspflicht neu geprägt und kritische Lücken in den bestehenden Governance-Rahmenwerken aufgedeckt. Dieser Policy Brief untersucht, wie sich die Grenze der Rechenschaftspflicht für Technologieunternehmen nun auf eine mögliche Mittäterschaft an Kriegsverbrechen, Verbrechen gegen die Menschlichkeit und Völkermord ausweitet, und unterstreicht die dringende Notwendigkeit neuer Ansätze zur Regulierung der Militarisierung der KI.

Ein KI-gestützter Völkermord

Das israelische Regime setzte KI-Systeme erstmals während der elf Tage andauernden Bombardierung des Gazastreifens im Mai 2021 ein, um tödliche Ziele zu generieren und zu priorisieren. (vgl. [jpost.com](https://www.jpost.com)) Ein brutaler, rechtswidriger Angriff, den das israelische Militär später als seinen ersten „KI-Krieg“ bezeichnete. Seitdem haben die Besatzungstruppen ihre Abhängigkeit von KI-Tools erheblich ausgeweitet und nutzen Cloud Computing und maschinelles Lernen, um riesige Mengen an Überwachungsdaten von Satellitenbildern, bis hin zu abgefangenen Kommunikationen, zu speichern und zu verarbeiten, um die Identifizierung und Einstufung von Angriffszielen zu automatisieren. (Vgl. [theguardian.com](https://www.theguardian.com))

Im Mittelpunkt der KI-Kriegsführung Israels steht das „Projekt Nimbus“ – ein 1,2 Milliarden Dollar schwerer Auftrag, durch den Google und Amazon der israelischen Regierung und dem Militär fortschrittliche Cloud-Infrastruktur und maschinelle Lernfähigkeiten zur Verfügung gestellt haben. (vgl. [wired.com](https://www.wired.com)) In den frühen Tagen des Völkermords stützten sich die israelischen Streitkräfte Berichten zufolge fast ausschließlich auf KI-gestützte Zielgenerierungssysteme, wie Lavender, The Gospel und Where's Daddy, um die Massenvernichtung und Zerstörung in Gaza zu beschleunigen. Diese Plattformen nehmen Massenüberwachungsdaten über die gesamte Bevölkerung Gazas auf, um algorithmisch zu bestimmen, wer getötet, welche Gebäude bombardiert und wie viel „Kollateralschaden“ als akzeptabel angesehen wird. (Vgl. [972mag.com](https://www.972mag.com))

Es ist alarmierend, dass diese KI-gesteuerten Systeme die genozidale Logik ihrer Betreiber verinnerlichen. (vgl. [haaretz.com](https://www.haaretz.com)) Sie sind darauf trainiert, Zivilisten als „Terroristen“ zu behandeln, und bauen damit auf der genozidalen Logik israelischer Beamter auf, die erklärten, dass es „keine unschuldigen Zivilisten in Gaza gibt“. (vgl. [middleeasteye.net](https://www.middleeasteye.net)) Im Rahmen der Bemühungen, tödliche Angriffe zu automatisieren, sollen Militärkommandanten Soldaten angewiesen haben, so viele Ziele wie möglich zu identifizieren und in das System einzugeben. Dies senkt effektiv die Schwelle für die Einstufung von Personen als „Hamis-Kämpfer“ und wirft ein breites Netz algorithmisch markierter Personen auf.

Trotz der hohen Fehlerquote war das einzige Kriterium, das israelische Soldaten auf Lavenders Todesliste anwandten, das Geschlecht des Ziels, wodurch effektiv alle palästinensischen Männer – Kinder und Erwachsene

gleichermaßen – zu legitimen Zielen wurden. In der Praxis hat die KI-Technologie es dem israelischen Regime ermöglicht, seine genozidale Logik mit rücksichtsloser, maschinengesteuerter Effizienz umzusetzen und Palästinenser, ihre Familien und ihre Häuser zu dem zu reduzieren, was das Militär erschreckenderweise als „Müllziele“ bezeichnet.

Obwohl viele technische Details der israelischen KI-Zielerfassungssysteme weiterhin geheim sind, gibt es zahlreiche glaubwürdige Hinweise darauf, dass ihre Funktionsweise von Cloud-Infrastrukturen und maschinellen Lernfähigkeiten abhängt, die von großen Technologieunternehmen, wie Google, Amazon, Microsoft und Palantir entwickelt und gewartet werden. (vgl. business-humanrights.org) Folglich wirft die direkte Bereitstellung digitaler Systeme durch Technologieunternehmen, die in der israelischen Kriegsführung eingesetzt werden, dringende Fragen hinsichtlich der Mitschuld von Unternehmen an schweren Verstößen gegen das Völkerrecht auf. Darunter Handlungen, für die der Internationale Strafgerichtshof (IStGH) Haftbefehle gegen den israelischen Premierminister Benjamin Netanjahu und den ehemaligen Verteidigungsminister Yoav Gallant erlassen hat. (Vgl. icc-cpi.int)

Vom Code zur Tötungsliste

Als Israel seine Angriffe auf Gaza verstärkte, stieg auch der Bedarf an KI- und Cloud-basierten Technologien, die von US-amerikanischen Tech-Giganten bereitgestellt wurden, rapide an. (vgl. 972mag.com) Dadurch die Infrastruktur von Unternehmen in die Kriegsmaschinerie eingebunden wurde. Im März 2024 vertiefte Google seine Beziehungen zum israelischen Verteidigungsministerium (IMOD) durch die Unterzeichnung eines neuen Vertrags über den Aufbau einer speziellen „Landezone“ in seiner Cloud-Infrastruktur, die mehreren Militäreinheiten den Zugang zu seinen Automatisierungstechnologien ermöglicht. (vgl. time.com) Amazon Web Services (AWS), Googles Partner im Projekt Nimbus, soll Israels Militärgeheimdienst eine dedizierte Serverfarm zur Verfügung gestellt haben, die unbegrenzte Speicherkapazität für Überwachungsdaten bietet, die über fast alle Menschen in Gaza gesammelt wurden.

Jüngste Berichte belegen die rasante Ausweitung der KI-gestützten militärischen Fähigkeiten Israels und unterstreichen, wie die zunehmende

Zusammenarbeit mit Technologieunternehmen den Einsatz fortschrittlicher Systeme im Krieg gegen Gaza beschleunigt hat. Laut durchgesickerten Dokumenten hat Microsoft Teile des Massenüberwachungsprogramms des israelischen Militärs auf seinen Cloud-Servern gehostet und Aufzeichnungen von Millionen abgehörter Telefongespräche von Palästinensern in Gaza und im Westjordanland gespeichert. Die israelischen Besatzungstruppen sollen diese Dateien genutzt haben, um Bombenziele zu identifizieren, Personen zu erpressen, Menschen in Haft zu nehmen und auch um Tötungen nachträglich zu rechtfertigen.

Die Abhängigkeit des israelischen Militärs von Microsoft Azure stieg entsprechend an: In den ersten sechs Monaten des Krieges stieg die durchschnittliche monatliche Nutzung um 60%, während die Nutzung der Machine-Learning-Tools von Azure im Vergleich zum Vorkriegsniveau um das 64-fache zunahm. Bis März 2024 war die Nutzung der technologischen Tools von Microsoft und OpenAI durch die israelischen Streitkräfte fast 200-mal höher, als in der Woche vor dem 7. Oktober 2023. Darüber hinaus hatte sich die auf den Servern von Microsoft gespeicherte Datenmenge auf mehr als 13 Petabyte verdoppelt.

Die Ergebnisse der internen Überprüfung von [Microsoft](#), die im September 2025 bekannt gegeben wurden, bestätigten letztendlich, dass eine Abteilung des israelischen Verteidigungsministeriums tatsächlich einige seiner Dienste für verbotene Überwachungszwecke genutzt hatte. Infolgedessen stellte das Unternehmen bestimmte Cloud- und KI-Dienste ein und räumte ein, dass seine Technologie an Praktiken beteiligt war, die gegen seine Nutzungsbedingungen verstießen. Die Aussetzung der Dienste für das israelische Militär durch Microsoft war jedoch minimal: Viele Verträge und Funktionen mit dem israelischen Militär und anderen Regierungsstellen, die für schwere Menschenrechtsverletzungen und Gräueltaten verantwortlich sind, bleiben unverändert bestehen. Während die Überprüfung selbst noch andauert, offenbart dieses begrenzte Eingeständnis die Komplizenschaft des Unternehmens mit der israelischen Militärmaschinerie.

Darüber hinaus scheint die Beteiligung der großen Technologieunternehmen am Krieg Israels über die normale Erbringung von Dienstleistungen hinauszugehen. Berichten zufolge haben Microsoft-

Ingenieure den israelischen Streitkräften, darunter der Einheit 8200 (Cyberoperationen und Überwachung) und der Einheit 9900 (geografische Informationen und Zielerfassung), sowohl technische Fernunterstützung als auch Vor-Ort-Unterstützung geleistet. Tatsächlich hat das israelische Verteidigungsministerium etwa 19.000 Stunden an Ingenieurs- und Beratungsdienstleistungen von Microsoft im Wert von rund 10 Millionen US-Dollar in Anspruch genommen.

Auch Amazon ist in diese Angelegenheit verwickelt und hat Berichten zufolge nicht nur Cloud-Infrastruktur bereitgestellt, sondern auch direkte Unterstützung bei der Überprüfung von Zielen für Luftangriffe geleistet. Die Rolle von Google gibt Anlass zu zusätzlicher Besorgnis: Internen Dokumenten zufolge hat das Unternehmen ein geheimes Team aus israelischen Staatsangehörigen mit Sicherheitsfreigabe gebildet, das ausdrücklich damit beauftragt ist, sensible Informationen von der israelischen Regierung entgegenzunehmen, die nicht an das gesamte Unternehmen weitergegeben werden dürfen. Dieses Team soll „spezielle Schulungen mit staatlichen Sicherheitsbehörden“ durchführen und an „gemeinsamen Übungen und Szenarien teilnehmen, die auf bestimmte Bedrohungen zugeschnitten sind“. Eine vergleichbare Vereinbarung scheint zwischen Google und keinem anderen Staat zu bestehen, was die außergewöhnliche Tiefe seiner Zusammenarbeit mit dem israelischen Regime unterstreicht.

Gewinn ist nicht der einzige Grund für die zunehmende Verflechtung der großen Technologieunternehmen mit dem israelischen Militär. Auch politische Affinität spielt eine Rolle. Palantir Technologies, ein in den USA ansässiges Datenanalyse- und Überwachungsunternehmen, das für seine engen Verbindungen zu Geheimdiensten und Verteidigungsbehörden bekannt ist, hat während des Völkermords im Gazastreifen offen seine Unterstützung für Israel bekundet. (vgl. [businessinsider.com](https://www.businessinsider.com)) Palantir hat sich mit AWS zusammengetan, um Tools zu entwickeln, die Kunden wie dem israelischen Militär helfen sollen, „im Krieg zu gewinnen“. Das Unternehmen hat eine strategische Partnerschaft mit dem israelischen Verteidigungsministerium geschlossen, um Technologien bereitzustellen, die die Völkermordkampagne direkt unterstützen. (vgl. [bloomberg.com](https://www.bloomberg.com)) Auch Microsoft unterhält langjährige Beziehungen zum israelischen Militär und Sicherheitsapparat – Beziehungen, die so eng sind, dass Netanjahu sie einmal als „eine Ehe, die im Himmel geschlossen, aber hier auf Erden

anerkannt wurde“ beschrieb. (Vgl. jpost.com)

Durch die direkte Unterstützung israelischer Militäroperationen liefern Technologieunternehmen nicht nur Infrastruktur, sondern fördern und unterstützen aktiv die Überwachung, Zielauswahl und Durchführung von Maßnahmen, die gegen das Völkerrecht verstoßen. In einer düsteren Entwicklung markiert der Einsatz kommerzieller KI in Gaza eine erschreckende Grenze: Systeme, die einst zur Optimierung der Logistik und Entscheidungsfindung in großem Maßstab entwickelt wurden, erstellen nun Todeslisten, löschen Familien aus und zerstören ganze Stadtviertel. Die von den großen Tech-Unternehmen entwickelte und gewartete Technologie unterstützt heute Kriegführung, ethnische Säuberungen und Völkermord in Palästina und dient als Prototyp für die Zukunft der automatisierten Kriegführung. (Vgl. universiteitleiden.nl)

Die Zukunft der Kriegführung

Das israelische Regime hat seine Bemühungen um eine automatisierte Kriegführung formalisiert, indem es innerhalb des IMOD eine eigene KI-Forschungsabteilung eingerichtet hat, deren Aufgabe es ist, die militärischen Fähigkeiten für eine Zukunft voranzutreiben, in der „auf den Schlachtfeldern integrierte Teams aus Soldaten und autonomen Systemen zusammenarbeiten werden“. (vgl. linkedin.com) Diese Initiative markiert eine bedeutende Wende hin zur Normalisierung KI-gesteuerter Kampfhandlungen. Westliche Regierungen, darunter [Frankreich](#), [Deutschland](#) und die [USA](#), verfolgen ähnliche Strategien und bemühen sich um die Integration künstlicher Intelligenz in ihre Waffensysteme und Streitkräfte. Zusammen genommen positionieren diese Entwicklungen Israel nicht nur als Vorreiter, sondern auch als Vorbild für die kommende Ära der algorithmischen Kriegführung.

Parallel dazu geben große Technologieunternehmen ihre selbst auferlegten ethischen Grenzen auf, um Militärverträge zu erhalten. Anfang dieses Jahres haben sowohl [Google](#), als auch [OpenAI](#) stillschweigend ihre freiwilligen Verpflichtungen aufgegeben, keine KI für militärische Zwecke zu entwickeln, was eine umfassendere Neuausrichtung auf den Sicherheits- und Verteidigungssektor signalisiert. Innerhalb weniger Wochen nach der Änderung seiner KI-Grundsätze unterzeichnete [Google](#)

eine formelle Partnerschaft mit Lockheed Martin, dem weltweit größten Waffenhersteller und einem wichtigen Lieferanten von Waffen für das israelische Militär. Im November 2024 kündigte [Meta](#) an, dass es seine großen Sprachmodelle namens Llama US-Regierungsbehörden und Auftragnehmern, die im Bereich der nationalen Sicherheit tätig sind, zur Verfügung stellen werde. Lockheed Martin hat Llama seitdem in seine Abläufe integriert.

Meta hat sich dem Wettlauf um KI für Kriegszwecke angeschlossen und eine Partnerschaft mit Anduril, einem Start-up-Unternehmen für Verteidigungstechnologie, geschlossen, um Virtual- und Augmented-Reality-Geräte für die US-Armee zu entwickeln. Trotz seines Status als gemeinnützige Organisation arbeitete OpenAI mit Anduril zusammen, um seine Technologie auf dem Schlachtfeld einzusetzen. (vgl. [technologyreview.com](https://www.technologyreview.com)) Darüber hinaus kündigten [Palantir](#) und Anthropic – ein von Google unterstütztes KI-Forschungs- und Entwicklungsunternehmen – eine Partnerschaft mit AWS an, um „US-Geheimdiensten und Verteidigungsbehörden Zugang“ zu seinen KI-Systemen zu gewähren.

Ein deutlicher Indikator für die zunehmende Annäherung zwischen Big Tech und Kriegsministerien ist die Entscheidung der US-Armee, Führungskräften von Palantir, Meta, OpenAI und Thinking Machines Labs den Rang eines Oberstleutnants zu verleihen und sie als Berater in die Streitkräfte einzubinden. (vgl. [defensescoop.com](https://www.defensescoop.com)) Die Initiative, die als Bemühung um „schnelle und skalierbare technische Lösungen für komplexe Probleme“ dargestellt wird, zielt darauf ab, das US-Militär „schlanker, intelligenter und tödlicher“ zu machen. (vgl. [usar.army.mil](https://www.usar.army.mil)) Die Symbolik ist kaum zu übersehen: Die Führungskräfte aus dem Silicon Valley entwickeln nicht mehr nur Werkzeuge für das Schlachtfeld, sondern werden offiziell in dessen Kommandostruktur integriert.

Militarisierung der KI in einem regulatorischen Vakuum

Die Militarisierung der KI schreitet ohne wirksame regulatorische Rahmenbedingungen rasch voran. Während die Staaten bei den Vereinten Nationen weiterhin über Normen für autonome Waffen beraten, gibt es

keinen verbindlichen internationalen Vertrag, der deren Entwicklung oder Einsatz konkret regelt. (vgl. docs.un.org) Noch weniger reguliert sind Dual-Use-Technologien, wie LLMs und Cloud-Infrastrukturen, die mittlerweile in militärische Operationen eingebunden werden. Aktuelle nationale und [globale Diskussionen](#) und [Regulierungsvorschläge](#) zur KI-Governance, die sich oft auf die Wahrung der Privatsphäre und der Menschenrechte konzentrieren, umgehen weitgehend die verheerenden Auswirkungen von KI-Systemen in Konfliktgebieten. (vgl. accessnow.com)

Das anschaulichste Beispiel für diese Diskrepanz ist die Unterzeichnung des [KI-Vertrags](#) des Europarats durch [Israel](#), der sich mit Menschenrechten, Demokratie und Rechtsstaatlichkeit befasst, zu einem Zeitpunkt, als glaubwürdige Berichte über den Einsatz von KI-gesteuerten Zielsystemen im Gazastreifen auftauchten. Obwohl der Vertrag zahlreiche Vorbehalte enthält, die seine Wirksamkeit einschränken, unterstreicht die Unterzeichnung durch Israel inmitten einer anhaltenden Völkermordkampagne die tiefe Kluft zwischen den ausgearbeiteten Rechtsnormen und dem Einsatz der Technologien, die sie regulieren sollen, auf dem Schlachtfeld.

Gleichzeitig werden freiwillige Richtlinien oder Soft-Law-Mechanismen routinemäßig verworfen. Die Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte (UNGPs) – die sowohl die Verpflichtungen der Staaten als auch die Verantwortung der Unternehmen zur Identifizierung und Minderung von Menschenrechtsrisiken umreißen – werden von Technologieunternehmen häufig ignoriert. Obwohl diese Prinzipien klar festlegen, dass Unternehmen, die in Konfliktgebieten tätig sind, das Risiko, zu schweren Menschenrechtsverletzungen und Verstößen gegen das humanitäre Völkerrecht beizutragen, als Frage der Rechtskonformität behandeln müssen, halten sich Technologieunternehmen weiterhin nur selektiv daran.

Ein typisches Beispiel dafür ist das verspätete Eingeständnis von Microsoft, dass das israelische Regime seine Cloud-Infrastruktur für die Massenüberwachung in Gaza genutzt hat. Im Mai 2025 bestritt Microsoft, dem israelischen Regime durch Massenüberwachung Schaden zuzufügen, nur um Monate später mit einem knappen Eingeständnis des Missbrauchs seiner Technologie eine Kehrtwende zu machen. Wie bereits erwähnt, zeigt dieses Eingeständnis, in welchem Ausmaß Unternehmen ihrer

Verantwortung gemäß den UNGPs, solche Schäden zu erkennen und zu mindern, nicht nachkommen.

Lesen Sie den gesamten Artikel der [Al-Shabaka News](#).

Quelle: [Activist Post](#)

Telegram zensiert nicht! Wenn du diese Information wichtig findest, kannst du Legitim auf Telegram kostenlos abonnieren: [hier anmelden](#) ([Telegram herunterladen](#))

teilen

teilen

teilen

teilen

E-Mail

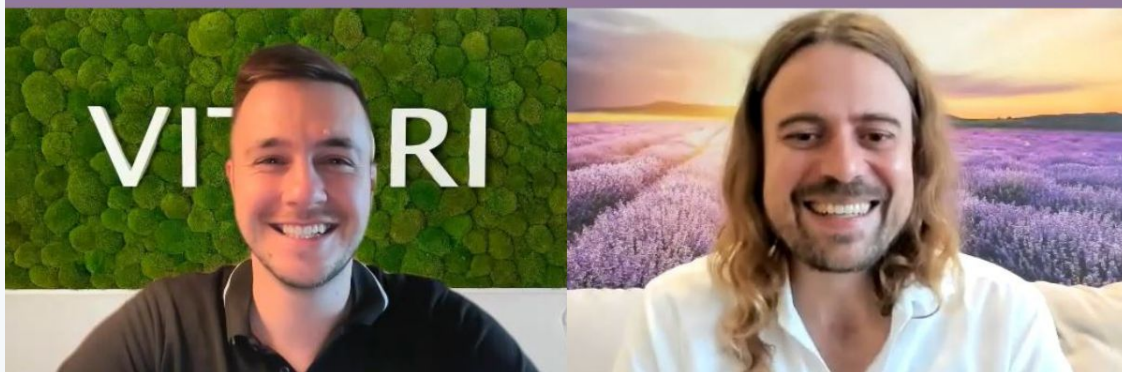
drucken



Die unglaubliche Überlieferung eines längst vergessenen Naturheilmittels

von Jan Walter | 1. Nov. 2024

WAHRE GESUNDHEIT GEHT ÜBER DEN LICHTKÖRPER



Die Frequenz-Medizin ist auf dem Vormarsch! (Inkl. Blick hinter die Kulissen)

von Jan Walter | 2. Nov. 2023

MARVIN ALBERG IM GESPRÄCH



BIOPHOTONEN – Das magische Licht in deinem Körper (Interview)

von Jan Walter | 3. Nov. 2023

Informationen

[Redaktion](#)

[Impressum](#)

[Datenschutzerklärung](#)

[Newsletter abonnieren](#)

Social Media

[Rumble](#)

[Telegram](#)

[Youtube](#)