„Bestellung bei Amazon": Wie Tech-Giganten Massendaten für den israelischen Krieg speichern

Die israelische Armee nutzt den Cloud-Service von Amazon, um Überwachungsdaten über die Bevölkerung des Gazastreifens zu speichern. Gleichzeitig beschafft sie weitere KI-Tools von Google und Microsoft für militärische Zwecke. Dies zeigt eine Recherche.

Yuval Abraham, 972mag/Local Call, 04.08.24

Die direkte militärische Unterstützung Israels durch die Vereinigten Staaten steht immer im Mittelpunkt, aber die Partnerschaften, die sich sowohl auf das zivile als auch auf das militärische Umfeld erstrecken, werden viel weniger beachtet". „Es geht um mehr als nur Komplizenschaft: Es ist eine direkte Beteiligung und Zusammenarbeit mit dem israelischen Militär bei den Werkzeugen, die sie zur Tötung von Palästinensern einsetzen."

Tariq Kenney-Shawa, *Al-Shabaka*

Am 10. Juli sprach die Befehlshaberin des Zentrums für Rechen- und Informationssysteme der israelischen Armee, das für die Datenverarbeitung des gesamten Militärs zuständig ist, auf einer Konferenz mit dem Titel „IT for IDF" in Rishon Lezion in der Nähe von Tel Aviv. In ihrer Rede vor rund 100 Militär- und Industrievertretern, von der die Magazine +972 und Local Call eine Aufzeichnung erhalten haben 1, bestätigte Oberst Racheli Dembinsky zum ersten Mal öffentlich, dass die israelische Armee bei ihren laufenden Angriffen auf den Gazastreifen Cloud-Speicher und Dienste für künstliche nutzt, die von zivilen Tech-Giganten angeboten werden. In Dembinskys Vortragsfolien tauchten zweimal die Logos von Amazon Web Services (AWS), Google Cloud und *Micro-soft Azure* auf.

Bei der Cloud-Speicherung werden große Mengen digitaler Daten außerhalb des Standorts aufbewahrt, oft auf Servern, die von einem Drittanbieter verwaltet werden. Dembinsky erklärte zunächst, dass ihre Armeeeinheit, die unter dem hebräischen Akronym *Mamram* bekannt ist, bereits eine „operative Cloud" verwendet, die auf internen Militärservern gehostet wird und nicht auf öffentlichen Clouds, die von zivilen Unternehmen betrieben werden. Sie beschrieb diese interne Cloud als „Waffenplattform", die Anwendungen zur Markierung von Zielen für Bombardierungen, ein Portal zur Anzeige von Live-Aufnahmen von Drohnen über dem Gazastreifen sowie Feuer-, Befehls- und Kontrollsysteme umfasst.

Mit dem Beginn der Bodeninvasion der israelischen Armee in den Gazastreifen Ende Oktober 2023 seien die internen militärischen Systeme aufgrund der enormen Anzahl von Soldaten und Soldateninnen schnell überlastet gewesen, fuhr sie fort. Der erste Versuch, das Problem zu lösen, so Dembinsky,

bestand darin, alle verfügbaren Ersatzserver in den Lagern der Armee zu aktivieren und ein weiteres Datenzentrum einzurichten - aber das reichte nicht aus. Man beschloss, dass man „nach draußen gehen musste, in die zivile Welt“. Ihr zufolge ermöglichten es die von großen Technologieunternehmen angebotenen Cloud-Dienste der Armee, auf Knopfdruck eine unbegrenzte Anzahl von Speicher- und Verarbeitungsservern zu erwerben, ohne die Server physisch in den Rechenzentren der Armee unterbringen zu müssen.

Der „wichtigste“ Vorteil der Cloud-Firmen, so Dembinsky, seien jedoch ihre fortgeschrittenen Möglichkeiten im Bereich der künstlichen Intelligenz. „Die verrückte Fülle an Diensten, Big Data und KI - wir sind bereits an einem Punkt angelangt, an dem unsere Systeme dies wirklich brauchen“, sagte sie mit einem Lächeln. Die Zusammenarbeit mit diesen Unternehmen, so fügte sie hinzu, habe dem Militär im Gazastreifen eine „sehr große operative Effizienz“ beschert.

Dembinsky gab nicht an, welche Dienste von Cloud-Unternehmen gekauft wurden oder wie sie dem Militär halfen. In einer Stellungnahme gegenüber +972 und Local Call betonte die israelische Armee, dass Verschlusssachen und Angriffssysteme, die in der internen Cloud gespeichert sind, nicht in die von Technologieunternehmen bereitgestellten öffentlichen Clouds verschoben wurden.

Eine neue Untersuchung von +972 und Local Call hat jedoch ergeben, dass die israelische Armee tatsächlich einige nachrichtendienstliche Informationen, die bei der Massenüberwachung der Bevölkerung im Gazastreifen gesammelt wurden, auf Servern gespeichert hat, die von Amazons AWS verwaltet werden. Die Untersuchung kann auch zeigen, dass bestimmte Cloud-Anbieter seit Beginn des Gaza-Krieges eine Fülle von KI-Fähigkeiten und -Diensten an israelische Armeeeinheiten geliefert haben.

Quellen im israelischen Kriegsministerium, in der israelischen Rüstungsindustrie, in den drei Cloud-Unternehmen und sieben israelische Geheimdienstmitarbeiter, die seit Beginn der Bodeninvasion im Oktober an der Operation beteiligt waren, beschrieben gegenüber *+972* und *Local Call*, wie das Militär Ressourcen aus dem Privatsektor beschafft, um seine technischen Kapazitäten im Krieg zu verbessern. Drei Geheimdienstquellen zufolge ist die Zusammenarbeit der Armee mit AWS besonders eng: Der Cloud-Gigant stellt dem israelischen Militärgeheimdienst eine Serverfarm zur Verfügung, auf der massenhaft nachrichtendienstliche Informationen gespeichert werden, die die Armee im Krieg unterstützen.

Mehreren Quellen zufolge ermöglicht die exponentielle Kapazität des öffentlichen AWS-Cloud-Systems der Armee einen „endlosen Speicher“, um Informationen über fast „jeden“ in Gaza zu speichern. Eine Quelle, die das Cloud-basierte System während des aktuellen Krieges nutzte, beschrieb, dass sie während der Ausführung ihrer operativen Aufgaben „Bestellungen bei Amazon“ aufgaben und mit zwei Bildschirmen arbeiteten - einem, der mit den eigenen Systemen der Armee verbunden war, und einem, der mit AWS zusammenarbeitete.

Militärische Quellen betonten gegenüber +972 und Local Call, dass der Umfang der durch die Überwachung aller palästinensischen Bewohner des Gazastreifens gesammelten Informationen so groß ist, dass sie nicht allein auf Militärservern gespeichert werden können. Insbesondere, so die Quellen des

Geheimdienstes, seien sehr viel umfangreichere Speicherkapazitäten und Rechenleistung erforderlich, um Milliarden von Audiodateien (im Gegensatz zu reinen Textinformationen) zu sichern.

Die riesige Menge an Informationen, die in Amazons Cloud gespeichert ist, half den Militärquellen zufolge in seltenen Fällen sogar dabei, tödliche Schläge aus der Luft im Gazastreifen zu bestätigen – Angriffe, die auch palästinensische Zivilisten getötet und geschädigt hätten. Insgesamt deckt unsere Untersuchung einige der Wege auf, mit denen große Technologieunternehmen zum laufendem Krieg des Staates Israel beitragen – einem Krieg, der von internationalen Gerichten wegen mutmaßlicher Kriegsverbrechen und Verbrechen gegen die Menschlichkeit auf völkerrechtswidrig besetztem Gebiet angeklagt wurde.

Du zahlst eine Million Dollar, du hast tausend Server mehr

Im Jahr 2021 unterzeichnete Israel einen gemeinsamen Vertrag mit Google und Amazon namens Project Nimbus. Erklärtes Ziel der Ausschreibung im Wert von 1,2 Milliarden Dollar war es, Ministerien zu ermutigen, ihre Informationssysteme auf die öffentlichen Cloud-Server der Gewinnerunternehmen zu verlagern und von diesen hochentwickelte Dienste zu erhalten.

Das Geschäft war höchst umstritten, und Hunderte von Mitarbeitern beider Unternehmen unterzeichneten innerhalb weniger Monate einen offenen Brief 2, in dem sie dazu aufriefen, die Beziehungen zum israelischen Militär zu beenden. Seit dem 7. Oktober haben die Proteste von Amazon- und Google-Mitarbeitern zugenommen, die unter dem Motto „No Tech For Apartheid“ organisiert wurden 3. Im April entließ Google 50 Mitarbeiter, weil sie an einem Protest in den New Yorker Büros des Unternehmens teilgenommen hatte 4. Google war kurzzeitig als Sponsor der Konferenz „IT For IDF“ aufgeführt, auf der Dembinsky sprach. Das Google-Logo wurde später entfernt 5.

In Medienberichten hieß es, das israelische Militär und das Kriegsministerium würden im Zuge des Projekts Nimbus nur nicht klassifiziertes Material in die öffentliche Cloud hochladen. Unsere Untersuchung zeigt jedoch, dass große Cloud-Unternehmen mindestens seit Oktober 2023 Datenspeicher- und KI-Dienste für Armeeeinheiten anbieten, die mit Verschlusssachen zu tun haben. Mehrere Sicherheitsquellen berichteten +972 und Local Call, dass der Druck auf die israelische Armee seit Oktober zu einem dramatischen Anstieg des Kaufs von Diensten von Google Cloud, Amazons AWS und Microsoft Azure geführt hat, wobei die meisten Käufe von den beiden erstgenannten Unternehmen über den Nimbus-Vertrag erfolgten.

„Was in der [öffentlichen] Cloud passiert“, so die Quelle weiter, „ist, dass man auf einen Knopf drückt, im Monat weitere tausend Dollar bezahlt und schon hat man 10 Server. Ein Krieg beginnt? Man zahlt eine Million Dollar und hat tausend weitere Server. Das ist die Macht der Cloud. Und deshalb haben die Leute in der israelischen Armee [während des Krieges] wirklich auf die Arbeit mit der Cloud gedrängt. Es war ein Dilemma.“

Das Projekt *Nimbus* hat dieses Dilemma gemildert. Zu den Bedingungen der Ausschreibung gehörte, dass die beiden siegreichen Unternehmen, Google und Amazon, 2022 bzw. 2023 Rechenzentren im Staat Israel einrichten. Anatoly Kushnir, Mitbegründer des israelischen Tchnologieunternehmens

Comm-IT, das seit Oktober Militäreinheiten bei der Migration in die Cloud unterstützt, erklärte gegenüber *+972* und L*ocal Call,* dass *Nimbus* „eine Infrastruktur“ fortgeschrittener Rechenzentren unter israelischer Gerichtsbarkeit schaffe. 6

Dieses Arrangement, so sagte er, erleichtere es den „Sicherheitseinheiten, sogar den sensibleren“, während des Krieges Informationen in der Cloud zu speichern, ohne Angst vor ausländischen Gerichten zu haben – die vermutlich die Informationen im Falle eines Prozesses gegen Israel einfordern könnten.

„Während des Krieges“, so Kushnir weiter, „entstanden [in der Armee] Bedürfnisse, die es [vorher] nicht gab, und es war viel einfacher, sie [mit] dieser Infrastruktur zu erfüllen, weil es die Infrastruktur eines globalen Eigentümers ist, der Dienstleistungen von den einfachsten bis zu den kompliziertesten erbringen kann“. Diese Unternehmen, so fügte er hinzu, versorgten das israelische Militär mit den „am weitesten fortgeschrittenen Diensten “, die im aktuellen Gaza-Krieg zum Einsatz kamen.

Dieser dramatische Wandel in den Verfahren der Armee hat sich seit Beginn des Krieges erheblich beschleunigt. In der Vergangenheit, so Kushnir, habe sich die Armee hauptsächlich auf selbst entwickelte Systeme verlassen, die als „on-prem“, kurz für „on premises“, bekannt sind. Dies bedeutete jedoch, dass sie Monate, wenn nicht sogar Jahre warten musste, um neue Dienste zu erstellen, die ihr fehlten. In der öffentlichen Cloud hingegen sind die KI-, Speicher- und Verarbeitungsfunktionen „viel leichter zugänglich“.

Kushnir schränkte ein, dass „die wirklich sensiblen Informationen, die geheimsten Dinge, nicht [in der zivilen Cloud] sind. Die operative Seite ist definitiv nicht dort. Aber es gibt nachrichtendienstliche Dinge, die teilweise dort aufbewahrt werden“.

Doch selbst innerhalb der Armee haben einige ihre Besorgnis über das Potenzial für Datensicherheitsverletzungen zum Ausdruck gebracht. „Als sie begannen, mit uns über die Cloud zu sprechen, und wir fragten, ob es nicht ein Informationssicherheitsproblem gäbe, wenn wir unsere Daten an ein Drittunternehmen senden, wurde uns gesagt, dass dieses [Risiko] durch den Wert der Nutzung in den Schatten gestellt wird“, so eine Geheimdienstquelle.

Die Cloud hat Informationen über jeden

Quellen sagten gegenüber *+972* und *Local Call*, dass die meisten nachrichtendienstlichen Informationen der israelischen Armee über palästinensische Kämpfer auf den internen Computern der Armee gespeichert seien und nicht in der öffentlichen Cloud, die mit dem Internet verbunden ist. Drei Sicherheitsquellen zufolge ist jedoch eines der vom israelischen Militärgeheimdienst verwendeten Datensysteme in der öffentlichen Cloud von Amazon, AWS, abgelegt.

Das Militär nutzt dieses System in Gaza mindestens seit Ende 2022 zur Massenüberwachung, aber vor dem aktuellen Krieg galt es nicht als besonders einsatzfähig. Diesen Quellen zufolge enthält das Amazon-System nun einen „unendlichen Vorrat“ an Informationen, die die Armee nutzen kann.

Militärische Quellen bestätigten, dass die nachrichtendienstlichen Informationen, die auf AWS gespeichert sind, im Vergleich zu denen, die auf den internen Systemen des Militärs gelagert werden, immer

noch als „vernachlässigbar“ angesehen werden, was ihre operative Nutzung angeht. Drei Quellen, die an den Angriffen der Armee beteiligt waren, sagten jedoch, dass die AWS in einer Reihe von Fällen genutzt wurde, um „zusätzliche Informationen“ im Vorfeld von Luftangriffen gegen mutmaßliche Kämpfer zu liefern, wobei in einigen Fällen zahlreiche Zivilisten getötet wurden.

Wie *+972* und *Local Call* 7 in einer früheren Untersuchung aufdeckten, genehmigte die israelische Armee die Tötung von „Hunderten von Zivilisten“ bei Angriffen gegen hochrangige Hamas-Kommandeure auf der Ebene von Brigadekommandeuren und manchmal sogar Bataillonskommandeuren. In einigen dieser Fälle, so erklärten Sicherheitsquellen, wurde die Amazon-Cloud eingesetzt

Quellen sagten, dass das AWS-basierte System für den israelischen Geheimdienst besonders nützlich ist, weil es Informationen „über jeden“ speichern kann, ohne Speicherbeschränkungen. Dies hatte manchmal operative Vorteile: Eine Geheimdienstquelle beschrieb einen „wirklich schicksalhaften“ Moment im Krieg, als die Armee ein hochrangiges Mitglied des militärischen Flügels der Hamas in einem großen, mehrstöckigen Gebäude mit Hunderten von Flüchtlingen und Kranken ausfindig machte. Die Quelle beschrieb den Einsatz von AWS, um Informationen darüber zu sammeln, wer sich in dem Gebäude befand. Der Angriff sei schließlich abgebrochen worden, weil unklar war, wo genau sich der hochrangige Agent versteckt hielt, und die Armee befürchtete, dass ein weiterer Angriff dem Ansehen des Staates Israel schaden würde.

„Die [Amazon]-Cloud ist ein endloser Speicherplatz“, sagte eine andere Quelle des israelischen Geheimdienstes. „Es gibt immer noch die regulären [Armee-]Server, die ziemlich groß sind ... Aber beim Sammeln von Geheimdienstinformationen findet man manchmal jemanden, der einen interessiert, und sagt: ‚Wie schade, er ist nicht dabei [als Überwachungsziel], ich habe keine Informationen über ihn.‘ Aber die Cloud gibt Ihnen Informationen über ihn, denn die Cloud hat [Informationen über] jeden.“

Früher hat die Armee üblicherweise die in ihren Datenbanken angesammelten nutzlosen Informationen gelöscht, um Platz für neue Informationen zu schaffen. In ihrem Vortrag am 10. Juli wies Dembinsky jedoch darauf hin, dass die Armee seit Oktober daran arbeitet, „das gesamte Kampfmaterial zu sichern, zu speichern und aufzubewahren“. Eine Sicherheitsquelle bestätigte, dass dies tatsächlich so ist, und führte die Vergrößerung des Speicherplatzes auf die öffentlichen Cloud-Unternehmen zurück.

Ein weiterer wichtiger Anreiz für die Zusammenarbeit mit den Cloud-Giganten sind deren Fähigkeiten im Bereich der künstlichen Intelligenz und die Serverfarmen mit Grafikprozessoren (GPU), die sie unterstützen. Eine Geheimdienstquelle, die an Diskussionen über die Verlagerung militärischer Nachrichtendienste in die öffentliche Cloud teilnahm, sagte, dass ihre Vorgesetzten „darüber sprachen, dass sie, wenn sie in die Cloud migrieren, [die Cloud-Unternehmen] auch ihre eigenen STT [Speech-to-Text-Funktionen] haben. Diese sind gut; sie haben viele Fähigkeiten. Warum alles in der Armeeeinheit entwickeln, wenn die Fähigkeiten bereits vorhanden sind?“

Der Arbeitsablauf, den die Geheimdienstoffiziere gegenüber *+972* und *Local Call* beschrieben haben – das „Bestellen“ von Daten aus der öffentlichen AWS-Cloud und das anschließende Senden an ein ge-

schlossenes militärisches Netzwerk – stimmt mit den Details in einem Buch überein, das der derzeitige Kommandeur der Einheit 8200, einer Eliteeinheit innerhalb des israelischen Militärgeheimdienstes, Yossi Sariel, im Jahr 2021 verfasst hat, wie der Guardian kürzlich aufdeckte. 8

„Wie können die Sicherheitsorgane die ‚Amazon-Cloud' nutzen und sich sicher fühlen?" schrieb Sariel und plädierte als Lösung für ein spezielles Netzwerk, in dem das interne System des Militärs und die öffentliche Cloud sicher „die ganze Zeit miteinander kommunizieren" könnten. Der Umfang der geheimen Informationen, die der israelische Geheimdienst sammelt, sei so groß, dass sie „nur in Unternehmen wie Amazon, Google oder Microsoft gespeichert werden können."

Im selben Jahr rief der stellvertretende Kommandeur der Einheit 8200 in einer israelischen Geheimdienstzeitschrift zu „neuen Partnerschaften" mit öffentlichen Cloud-Anbietern auf, da deren KI-Fähigkeiten „unersetzlich" und denjenigen der Armee überlegen seien. Er deutete an, dass auch die Cloud-Unternehmen von einer Partnerschaft mit dem Militär profitieren werden: „Aman [der militärische Geheimdienst] verfügt über die meisten Daten der IDF, einschließlich der Daten über die Feinde, die von einer Vielzahl von Sensoren stammen - Daten, für die zivile Unternehmen ein Vermögen zahlen würden, um Zugang zu erhalten."

Was die IDF nutzt, wird eines der besten Verkaufsargumente sein"

Quellen aus dem Militär und der Waffenindustrie zufolge galt *Microsoft Azure* jahrelang als wichtigster Cloud-Anbieter des Staates Israel, der seine Dienste an das Kriegsministerium und Armeeeinheiten verkauft, die mit geheimen Informationen arbeiten. Einer Quelle zufolge sollte *Azure* dem israelischen Militär die Cloud zur Verfügung stellen, in der die Überwachungsdaten gespeichert werden sollten – doch Amazon bot einen besseren Preis. Quellen in den Cloud-Unternehmen, die in die Beziehungen mit dem israelischen Kriegsministerium eingeweiht waren, sagten, dass Amazon, seit es die *Nimbus*-Ausschreibung gewonnen hat, aggressiv mit *Azure* konkurriert, in der Hoffnung, es als Top-Dienstleister der Armee zu ersetzen.

Kushnir von *Comm-IT* erklärte, dass in der Vergangenheit „die meisten Regierungs- und Militärbehörden viel in die Entwicklung und Erstellung von Systemen auf der Grundlage von *Azure* investiert haben". Da *Azure* jedoch die Nimbus-Ausschreibung nicht gewonnen habe, habe es im Verteidigungsministerium einen „gewissen Migrationsprozess" zu den Servern von Google und Amazon gegeben, der sich während des aktuellen Krieges beschleunigt habe.

Quellen in der High-Tech-Branche sagten, dass das israelische Kriegsministerium als wichtiger und „strategischer" Kunde für die drei Cloud-Unternehmen gilt. Dies liege nicht nur an dem großen finanziellen Umfang der Transaktionen, sondern auch daran, dass der Staat Israel als einflussreich bei der Meinungsbildung unter den Sicherheitsbehörden weltweit und als Vorreiter bei „Trends" gilt, die andere Behörden übernehmen.

Einer der Personen, die jahrelang die Beschaffungspolitik des Kriegsministeriums leiteten und Kontakte zu den Cloud-Giganten pflegten, ist Oberst Avi Dadon, der für diese Recherche mit *+972* und *Local Call* sprach. Bis 2023 leitete er die Beschaffungsverwaltung des Kriegsministeriums und war für

militärische Anschaffungen in Höhe von mehr als 10 Mrd. NIS (rund 2,7 Mrd. USD) pro Jahr verantwortlich.

„Für [die Cloud-Unternehmen] ist es das stärkste Marketing", sagte Dadon. „Was die IDF nutzt, war und wird eines der besten Verkaufsargumente für Produkte und Dienstleistungen in der Welt sein. Für sie ist es ein Labor. Natürlich wollen sie [mit uns] zusammenarbeiten."

Dadon sagte, dass er viele Treffen mit Vertretern von AWS, *Microsoft Azure* und Google Cloud im Staat Israel sowie auf Reisen in die Vereinigten Staaten hatte. Er stand auch mit den Cloud-Giganten wegen einer geheimen Ausschreibung namens Project *Sirius* in Kontakt.

Sirius, über das die israelische Finanzzeitung Globes erstmals im Jahr 2021 berichtete, gilt als wesentlich sensibler als Nimbus und muss noch mit einem der Technologieunternehmen unterzeichnet werden. Im Mai gab das Militär auf seiner Website bekannt, dass es einen Experten sucht, der „mit den großen Cloud-Anbietern zusammenarbeitet", um „die [militärischen] Systeme in die öffentliche Cloud (Nimbus) zu übertragen" und „den Upload der operativen Kernsysteme in die Sicherheits-Cloud vorzubereiten", und zwar im Zuge der Sirius-Ausschreibung.

„*Sirius* ist eine private, von öffentlichen und anderen Netzen abgeschottete Sicherheits-Cloud, die nur für die IDF und das Kriegsministerium bestimmt ist", erklärte Dadon. „Es gibt seit mehr als einem Jahrzehnt Diskussionen darüber, wie diese aussehen wird". Diese neue Cloud soll nach Angaben von drei Sicherheitsquellen vom Internet getrennt sein und auf der Infrastruktur der großen Cloud-Anbieter aufbauen, so dass alle israelischen Sicherheitsbehörden sie für klassifizierte Systeme nutzen können.

Dadon zufolge haben die öffentlichen Cloud-Dienste das Potenzial, die Tödlichkeit des Militärs zu erhöhen. Bei der Suche nach einer Person, die „eliminiert" werden soll, erklärt er, „sammelt man Milliarden von Details, die scheinbar uninteressant sind. Aber man muss sie speichern. Wenn man alles zu einem Produkt verarbeiten [und] zusammenfügen will, das einem sagt, dass [die Zielperson] zu dieser Stunde hier ist, hat man fünf Minuten Zeit, man hat nicht den ganzen Tag und die ganze Nacht. Also braucht man natürlich die Informationen.

„Sie können das nicht auf Ihren Servern machen, weil Sie ständig löschen müssten, was Sie für unnötig halten", so Dadon weiter. „Hier gibt es einen sehr kritischen Kompromiss. Wenn man einmal in die Cloud hochgeladen hat, ist der Weg zurück zu ‚on-prem' fast unmöglich. Man lernt eine neue Welt kennen. Sie haben bereits Informationen hochgeladen, die um mehrere Größenordnungen umfangreicher sind, und was werden Sie jetzt tun? Anfangen, sie zu löschen?"

Wie +972 und Local Call in einer früheren Untersuchung aufdeckten, basierten viele der israelischen Angriffe in Gaza zu Beginn des Krieges auf den Empfehlungen eines Programms namens „Lavender". Mit Hilfe von künstlicher Intelligenz verarbeitete dieses System Informationen über die meisten Bewohner des Gazastreifens und erstellte eine Liste von mutmaßlichen Militärangehörigen, darunter auch Nachwuchskräfte, die ermordet werden sollten. Das israelische Militär griff diese Personen systematisch in ihren Privathäusern an und tötete ganze Familien. Mit der Zeit erkannte die Armee, dass

Lavender nicht „zuverlässig“ genug war, und sein Einsatz ging zugunsten anderer Software zurück. +972 und Local Call konnten nicht bestätigen, ob Lavender mit Hilfe von zivilen Firmen, einschließlich öffentlicher Cloud-Unternehmen, entwickelt wurde.

Du kämpfst von deinem Laptop aus

In ihrem Vortrag im vergangenen Monat bezeichnete Dembinsky die aktuelle Militäroperation im Gazastreifen als „den ersten digitalen Krieg“. Dies scheint zwar übertrieben, da bei der Offensive auf den Gazastreifen im Jahr 2021 auch digitale Möglichkeiten genutzt wurden, aber israelische Militärquellen sagten, dass sich die Digitalisierungsprozesse der Armee während des aktuellen Krieges erheblich beschleunigt haben. Ihnen zufolge laufen die Kommandeure im Feld mit verschlüsselten Smartphones herum, schreiben Nachrichten in einem operativen Chat, der WhatsApp ähnelt (aber nichts mit dem Unternehmen zu tun hat), laden Dateien auf ein gemeinsames Laufwerk hoch und nutzen unzählige neue Anwendungen.

„Du kämpfst von deinem Laptop aus“, sagte ein Offizier, der in einem Einsatzraum in Gaza diente. Früher sah man das Weiße in den Augen des Gegners, schaute durch ein Fernglas und sah ihn explodieren“. Wenn heute jedoch ein Ziel auftaucht, „sagt man [den Soldaten] über den Laptop: ‚Schieß mit dem Panzer“‘.

Eine der Apps in der internen Cloud des Militärs heißt *Z-Tube* (Z ist die Abkürzung für *Zahal*, das Akronym für die israelische Armee); es handelt sich um eine Website, die ähnlich wie Youtube aussieht und es den Soldaten ermöglicht, auf Live-Filmmaterial aller militärischen Filmgeräte im Gazastreifen zuzugreifen, einschließlich UAVs. Mit einer anderen App namens „MapIt“ können die Soldaten Ziele in Echtzeit auf einer interaktiven Karte markieren. „Ziele sind die schwerste Ebene auf der Karte“, so eine Sicherheitsquelle gegenüber +972 und Local Call. „Es sieht so aus, als ob jedes Haus ein Ziel hat.“

Eine verwandte App namens „Hunter“ dient dazu, Ziele in Gaza zu signalisieren und mithilfe von KI Verhaltensmuster zu erkennen. Sie wurde auf der Konferenz IT for IDF von Oberst Eli Birenbaum vorgestellt, dem Kommandeur einer Einheit, die unter dem hebräischen Akronym *Matzpen* bekannt ist und für die Entwicklung von Systemen für den operativen Einsatz zuständig ist.

Die interne Cloud soll auf militärischen Servern verwaltet werden und nicht mit den Clouds privater Unternehmen verbunden sein, aber mehrere Quellen sagten, dass es „sichere“ Möglichkeiten gebe, dass auch zivile Cloud-Unternehmen Dienste für operative Systeme anbieten könnten.

„Die IDF nimmt keine sehr sensiblen, geheimen Dinge mit nach draußen – diese Dinge bleiben innerhalb [der luftüberwachten militärischen Netzwerke]“, sagte Oberst Assaf Navot, ein ehemaliger hochrangiger ICT-Beamter der Armee und jetzt Leiter der Militärabteilung von *Comm-IT*, gegenüber *+972* und *Local Call*. Ihm zufolge besteht die Herausforderung darin, das „Gehirn“ ziviler Cloud-Unternehmen, wie z. B. KI-Dienste, in die internen Systeme der Armee einzubringen, „ohne dass es draußen bleibt. Es lebt direkt im Inneren. Man kann nicht alles so machen, dass es eins zu eins mit dem übereinstimmt, was draußen passiert, aber man schafft es, verrückte Fortschritte zu machen.“

Im Jahr 2022 beschrieb Itai Binyamin, ein KI-Experte, der damals für *Microsoft Azure* arbeitete und heute für AWS tätig ist, einer Gruppe von Absolventen von Dembinskys Mamram-Einheit, dass dieses System es ermöglicht, „die KI-Fähigkeiten von [Microsoft] sogar vor Ort einzusetzen, auf Ihren Servern, in einer Umgebung, die nicht [mit dem Internet] verbunden ist." In seiner Erklärung in dem Video zeigte Binyamin den Absolventen, wie Microsofts Gesichtserkennungstool ein Nachrichtenvideo analysieren und erkennen konnte, dass der Hamas-Führer Ismail Haniyeh darin zu sehen war.

Die Website von Microsoft Azure verweist auf Tools mit der Bezeichnung „Disconnected Containers", die für „strategische Partner" entwickelt wurden, die ihre Informationen sicher verwahren müssen. Die Tools umfassen laut der Website Funktionen für Transkription, Übersetzung, Stimmungserkennung, Sprache, Zusammenfassung, Dokumenten- und Bildanalyse und mehr.

Navot erklärte, dass die Entwicklung der digitalen Technologie so schnell voranschreite, dass die einzige Möglichkeit für die Armee, den Rückstand aufzuholen, darin bestehe, Dienstleistungen vom zivilen Markt und von Cloud-Unternehmen zu erwerben. „Schauen Sie sich das M16 [Sturmgewehr] an. Das letzte Mal, dass ein M16 hergestellt wurde, war im [Vietnam-]Krieg. Da hat sich nicht viel geändert." Aber bei digitaler Software, sagt er, ändern sich die Dinge „in Monaten, nicht in Jahren".

Allein die Tatsache, dass nachrichtendienstliches Material, auch wenn es nicht direkt einsatzfähig ist, in eine zivile Cloud hochgeladen wird, hat bei einigen Mitgliedern des israelischen Militärs Besorgnis ausgelöst. „Das hat etwas Beängstigendes", sagte eine Quelle der Armee. „Die Informationen, die die Armee heute hat, sind intime Informationen über viele Menschen in [den besetzten Gebieten]. Sollen wir sie also riesigen privaten und kommerziellen Unternehmen überlassen, deren Ziel es ist, Geld zu verdienen?"

Andere Quellen aus dem Sicherheitsbereich erklärten hingegen, dass rohe Informationen, die auf breiter Basis und nicht über spezifische Ziele gesammelt wurden, nicht besonders sensibel sind, sie würden erst dann sensibel, wenn sie in Angriffsziele umgesetzt werden. „Es wäre nicht wirklich beängstigend, wenn die Iraner [Zugang zu] diesen Informationen hätten", so eine der Quellen.

Brigadegeneral Yael Grossman, Kommandeur der für *Mamram* zuständigen Abteilung der Armee für die Stärkung der operativen Technologie – bekannt unter dem hebräischen Akronym *Lotem* –, sagte in einem Podcast im Mai, dass der Rückgriff auf zivile Technologien im aktuellen Krieg einen „verrückten Sprung in kurzer Zeit" ermöglicht habe. Doch Dadon vergleicht das Hochladen von Materialien in die Cloud mit der „Übergabe der Schlüssel eines Mercedes an jemand anderen". „Sollten wir den Mercedes nicht benutzen? Wir müssen es. Und wie? Ich weiß es nicht."

Es ist eine direkte Beteiligung an den Werkzeugen, die zur Tötung von Palästinensern verwendet werden

In den letzten Jahren ist Amazon nicht nur ein Partner der israelischen Armee, sondern auch ein Anbieter von Cloud-Diensten für mehrere westliche Geheimdienste geworden. Im Jahr 2021 unterzeichnete AWS eine Vereinbarung mit den britischen Geheimdiensten GCHQ, MI5 und MI6, um „geheime" Informationen zu speichern und den Einsatz von KI-Tools zu beschleunigen. 9 Die australische Regie-

rung kündigte diesen Monat ebenfalls an, dass sie 1,3 Milliarden US-Dollar investieren würde, um eine Cloud für „streng geheimes“ Geheimdienstmaterial auf den Servern von Amazon aufzubauen. Der Tech-Gigant unterzeichnete auch eine Vereinbarung mit dem Pentagon, zusammen mit drei anderen großen Unternehmen, um eine riesige Cloud zu bauen, die dem US-Verteidigungsministerium für „alle Klassifizierungsstufen“ dienen würde. 10

Amazon veröffentlicht vage Regeln für den „verantwortungsvollen Aufbau von KI“, die sich nur auf die „angemessene Beschaffung, Nutzung und den Schutz von Daten“ und die „Verhinderung von schädlichen Systemausgaben und Missbrauch“ beziehen 11. In Microsofts Grundsätzen und Herangehensweise für verantwortungsvolle KI heißt es: „Wir setzen uns dafür ein, dass KI-Systeme verantwortungsvoll und auf eine Weise entwickelt werden, die das Vertrauen der Menschen rechtfertigt.“ 12

Google veröffentlicht auch eine Liste seiner KI-Prinzipien, in der es klarer heißt, dass Google „keine KI in ... Technologien entwickeln oder einsetzen wird, die allgemeinen Schaden verursachen oder wahrscheinlich zufügen; ... Waffen oder andere Technologien, deren Hauptzweck oder Implementierung darin besteht, Menschen zu verletzen oder dies direkt zu ermöglichen ... Technologien, die Informationen für die Überwachung sammeln oder nutzen, die gegen international anerkannte Normen verstoßen ... [oder] Technologien, deren Zweck gegen weithin anerkannte Grundsätze des Völkerrechts und der Menschenrechte verstößt.“ 13

Gabriel Schubiner, ein Aktivist und Organisator von *No Tech For Apartheid*, meint jedoch, dass diese Grundsätze „keine reale Wirkung“ haben, weil Cloud-Unternehmen sie „als PR benutzen, um zu zeigen, wie verantwortungsbewusst sie sind“. Seiner Meinung nach haben die Unternehmen keine Möglichkeit, in Echtzeit zu erfahren, wie ihre Kunden ihre Dienste nutzen.

Schubiner – der früher bei Google arbeitete und an einem Protest von Google-Mitarbeitern gegen die Lieferung von Technologie teilnahm, die ihrer Meinung nach vom israelischen Militär im Gaza-Krieg eingesetzt wird – sagt, 14 dass Google bei der Erklärung seiner ethischen Grundsätze immer eine „vage Sprache“ verwendet habe. Außerdem behaupte das Unternehmen weiterhin, dass seine Verträge mit dem Staat Israel „in erster Linie für zivile Zwecke bestimmt sind, obwohl klar ist, dass viele der Aktionen bei *Nimbus* militärischen Zwecken dienen“.

Eine Quelle aus dem Verteidigungsbereich erklärte gegenüber *+972* und *Local Call*, dass die meisten neuen Verträge zwischen dem Militär und Cloud-Unternehmen seit Beginn des Krieges im Zusammenhang mit der Nimbus-Ausschreibung geschlossen wurden. Das Militär kann jedoch auch durch Ausschreibungen des Kriegsministeriums oder durch Verträge, die vor dem Projekt *Nimbus* geschlossen wurden, Beziehungen zu Cloud-Unternehmen knüpfen und vertiefen. *+972* und *Local Call* konnten nicht überprüfen, ob die AWS-Cloud, die für die Speicherung nachrichtendienstlicher Informationen genutzt wird, im Zusammenhang mit dem Projekt *Nimbus* erworben wurde.

„Keines der beiden Unternehmen hat öffentlich bekannt gegeben, welche menschenrechtliche Sorgfaltsprüfung sie vor der Teilnahme am Projekt Nimbus vorgenommen haben, wenn überhaupt“, er-

klärte Zach Campbell, ein Experte für digitale Rechte bei *Human Rights Watch*. „Sie haben nicht angegeben, ob und wenn ja, welche roten Linien es für die zulässige Nutzung ihrer Technologie gibt."

Kushnir, der israelische Militäreinheiten bei der Umstellung auf die Cloud unterstützt, befürchtet nicht, dass die Proteste gegen die Partnerschaften der Cloud-Unternehmen mit dem Staat Israel Erfolg haben werden. „Man muss bedenken, dass dieselben Unternehmen ähnliche Regierungs- und Militär-Clouds in den Vereinigten Staaten, Großbritannien und der NATO betreiben", sagte er. „Das sind keine Start-up-Unternehmen, sondern globale ICT-Kraftpakete."

Nadim Nashif, der geschäftsführende Direktor von *7amleh – The Arab Center for the Advancement of Social Media*, das sich mit den digitalen Rechten der Palästinenser befasst, sagte, seine grundlegende Forderung an die Cloud-Unternehmen sei, dass sie „sicherstellen, dass ihre Produkte nicht zum Schaden von Menschen eingesetzt werden". Das sei aber derzeit nicht die Praxis. Ihm zufolge werden die Produkte der Cloud-Giganten trotz der Rhetorik der Sorge um die Menschenrechte „an Regierungen und Regime verkauft, die Menschen unterdrücken" - darunter auch die israelische Armee.

Mit Blick auf die fehlende Kontrolle der Projekte und Partnerschaften der Cloud-Unternehmen fügte Nashif hinzu: „Im lokalen Kontext, im Falle einer Besatzung, wird die Frage, ob [diese Dienste] für militärische Zwecke, an die Besatzungsarmee, oder für zivile Zwecke verkauft werden, viel wichtiger". Ihm zufolge erleichtert die im Staat Israel bestehende Nähe zwischen dem Privatsektor und dem Militär die Zusammenarbeit ohne rote Linien, was zu „mehr Kontrolle über [die Palästinenser] führt – erst recht in Zeiten des Krieges".

„Die direkte militärische Unterstützung Israels durch die Vereinigten Staaten – die Munition, die Kampfjets und die Bomben – steht immer im Mittelpunkt, aber diese Partnerschaften, die sich sowohl auf das zivile als auch auf das militärische Umfeld erstrecken, werden viel weniger beachtet", so Tariq Kenney-Shawa, US-amerikanischer Mitarbeiter bei der palästinensischen Denkfabrik *Al-Shabaka*. „Es geht um mehr als nur Komplizenschaft: Es ist eine direkte Beteiligung und Zusammenarbeit mit dem israelischen Militär bei den Werkzeugen, die sie zur Tötung von Palästinensern einsetzen.

Google und Microsoft lehnten es ab, auf die verschiedenen Anfragen an ihre Büros im Staat Israel und den Vereinigten Staaten zu antworten. *Amazon Web Services* erklärte: „AWS konzentriert sich darauf, die Vorteile unserer weltweit führenden Cloud-Technologie allen unseren Kunden zur Verfügung zu stellen, egal wo sie sich befinden. Wir setzen uns dafür ein, dass unsere Mitarbeiter sicher sind, unterstützen unsere Kollegen, die von diesen schrecklichen Ereignissen betroffen sind, und arbeiten mit unseren unterstützenden humanitären Partnern zusammen, um denjenigen zu helfen, die von dem Krieg getroffen wurden."

1 https://www.youtube.com/watch?v=qLBDfnZJrC8

2 https://www.theguardian.com/commentisfree/2021/oct/12/google-amazon-workers-condemn-project-nimbus-israeli-military-contract

3 https://www.notechforapartheid.com/

4 https://www.404media.co/google-cloud-listed-then-removed-as-sponsor-of-israeli-military-tech-conference/#:~:text=The%20conference%2C%20organized%20by%20the,and%20security%E2%80%9D%20on%20its%20website.

5 https://www.theguardian.com/technology/2024/apr/27/google-project-nimbus-israel

6 https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-in-israel-is-now-open?hl=en

https://www.timesofisrael.com/israel-signs-deal-for-cloud-services-with-google-amazon/#:~:text=Israel%20on%20Monday%20officially%20announced%20its%20signing%20of,giants%20come%20under%20pressure%20to%20boycott%20the%20country

7 https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

8 https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse

9 https://www.theguardian.com/uk-news/2021/oct/26/amazon-web-services-aws-contract-data-mi5-mi6-gchq

10 https://www.wsj.com/tech/amazon-to-build-1-3-billion-top-secret-cloud-for-australias-government-699ec515

11 https://aws.amazon.com/de/machine-learning/responsible-ai/

12 https://www.microsoft.com/en-us/ai/principles-and-approach

13 https://ai.google/responsibility/principles/

14 https://www.thenation.com/article/activism/google-firings-gaza-project-nimbus/

Quelle: https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft

Übersetzung: Pako – palaestinakomitee-stuttgart.de