

i giganti della tecnologia archiviano dati di massa per la guerra di Israele

www-972mag-com.translate.google/cloud-israeli-army-gaza-amazon-google-microsoft

August 4, 2024



Soldati dell'unità Sky Rider dell'esercito israeliano visti mentre manovravano un UAV durante un'esercitazione di addestramento presso la base militare di Tze'elim, vicino alla Striscia di Gaza, il 5 agosto 2013. (Miriam Alster/FLASH90)

L'esercito israeliano sta utilizzando il servizio cloud di Amazon per archiviare informazioni di sorveglianza sulla popolazione di Gaza, mentre si procura ulteriori strumenti di intelligenza artificiale da Google e Microsoft per scopi militari, rivela un'indagine.

Di Yuval Abraham 4 agosto 2024

Il 10 luglio, il comandante dell'unità Centro di calcolo e sistemi informativi dell'esercito israeliano – che fornisce l'elaborazione dei dati a tutto l'esercito – ha parlato ad una conferenza intitolata “IT per IDF” a Rishon Lezion, vicino a Tel Aviv. Nel suo discorso davanti a un pubblico di circa 100 militari e industriali, di cui +972 Magazine e Local Call hanno

ottenuto una registrazione , la Col. Racheli Dembinsky ha confermato pubblicamente per la prima volta che l'esercito israeliano sta utilizzando servizi di cloud storage e di intelligenza artificiale forniti da giganti della tecnologia civile nel suo continuo attacco alla Striscia di Gaza. Nelle diapositive delle lezioni di Dembinsky, i loghi di Amazon Web Services (AWS), Google Cloud e Microsoft Azure sono apparsi due volte.

L'archiviazione nel cloud è un mezzo per preservare grandi quantità di dati digitali fuori sede, spesso su server gestiti da un provider di terze parti. Dembinsky inizialmente spiegò che la sua unità militare, conosciuta con l'acronimo ebraico Mamram, utilizzava già un "cloud operativo" ospitato su server militari interni, piuttosto che su cloud pubblici gestiti da società civili. Ha descritto questo cloud interno come una "piattaforma di armi", che include applicazioni per contrassegnare gli obiettivi dei bombardamenti, un portale per visualizzare filmati in diretta dagli UAV sui cieli di Gaza, nonché sistemi di fuoco, comando e controllo.

Ma con l'inizio dell'invasione di terra di Gaza da parte dell'esercito israeliano alla fine di ottobre 2023, ha continuato, i sistemi militari interni sono diventati rapidamente sovraccarichi a causa dell'enorme numero di soldati e personale militare che sono stati aggiunti alla piattaforma come utenti, causando problemi tecnici che minacciavano di rallentare le funzioni militari di Israele.

Il primo tentativo di risolvere il problema, ha spiegato Dembinsky, prevedeva l'attivazione di tutti i server di riserva disponibili nei magazzini dell'esercito e la creazione di un altro data center, ma non era sufficiente. Decisero che dovevano "andare fuori, nel mondo civile". Secondo lei, i servizi cloud offerti dalle principali aziende tecnologiche hanno consentito all'esercito di acquistare server di archiviazione ed elaborazione illimitati con un semplice clic, senza l'obbligo di archiviare fisicamente i server nei centri informatici dell'esercito.

Ma il vantaggio "più importante" offerto dalle società cloud, ha affermato Dembinsky, sono state le loro capacità avanzate nel campo dell'intelligenza artificiale. "La folle ricchezza di servizi, big data e intelligenza artificiale: abbiamo già raggiunto un punto in cui i nostri sistemi ne hanno davvero bisogno", ha detto con un sorriso. Lavorare con queste aziende, ha aggiunto, ha garantito ai militari "un'efficacia operativa molto significativa" nella Striscia di Gaza.

Dembinsky non ha specificato quali servizi siano stati acquistati dalle società cloud o come abbiano aiutato i militari. In un commento a +972 e Local Call, l'esercito israeliano ha sottolineato che le informazioni riservate e i sistemi di attacco archiviati nel cloud interno non sono stati spostati nei cloud pubblici forniti dalle aziende tecnologiche.

Tuttavia, una nuova indagine di +972 e Local Call può rivelare che l'esercito israeliano ha effettivamente archiviato alcune informazioni di intelligence raccolte attraverso la sorveglianza di massa della popolazione di Gaza su server gestiti da AWS di Amazon.

L'indagine può anche rivelare che alcuni fornitori di servizi cloud hanno fornito una vasta gamma di funzionalità e servizi di intelligenza artificiale alle unità dell'esercito israeliano dall'inizio della guerra di Gaza.

Fonti del Ministero della Difesa israeliano, dell'industria bellica israeliana, delle tre società cloud e di sette funzionari dell'intelligence israeliana coinvolti nell'operazione dall'inizio dell'invasione di terra in ottobre, hanno descritto a +972 e Local Call come i militari si procurano servizi privati risorse del settore per migliorare le proprie capacità tecnologiche in tempo di guerra. Secondo tre fonti di intelligence, la collaborazione dell'esercito con AWS è particolarmente stretta: il colosso del cloud fornisce alla direzione dell'intelligence militare israeliana una server farm in cui vengono archiviate grandi quantità di informazioni di intelligence che aiutano l'esercito in guerra.

Secondo molteplici fonti, la capacità esponenziale del sistema cloud pubblico AWS consente all'esercito di avere "spazio di archiviazione infinito" per conservare informazioni su quasi "tutti" a Gaza. Una fonte che ha utilizzato il sistema basato su cloud durante l'attuale guerra ha descritto di aver effettuato "ordini da Amazon" per ottenere informazioni durante lo svolgimento dei propri compiti operativi e di aver lavorato con due schermi: uno collegato ai sistemi privati dell'esercito e l'altro collegato ad AWS.

Fonti militari hanno sottolineato a +972 e Local Call che la portata delle informazioni raccolte dalla sorveglianza di tutti i residenti palestinesi di Gaza è così ampia che non può essere archiviata solo sui server militari. In particolare, secondo fonti di intelligence, per conservare miliardi di file audio erano necessarie capacità di archiviazione e potenza di elaborazione molto più estese (invece che solo informazioni testuali o metadati), cosa che ha costretto l'esercito a rivolgersi ai servizi cloud offerti dalle aziende tecnologiche.

La grande quantità di informazioni archiviate nel cloud di Amazon, hanno testimoniato le fonti militari, ha persino contribuito in rare occasioni a confermare attacchi aerei omicidi a Gaza – attacchi che avrebbero ucciso e ferito anche civili palestinesi. Nel complesso, la nostra indagine espone ulteriormente alcuni dei modi in cui le principali società tecnologiche stanno contribuendo alla guerra in corso in Israele, una guerra che è stata segnalata dai tribunali internazionali per sospetti crimini di guerra e crimini contro l'umanità su territori illegalmente occupati .

"Paghi un milione di dollari e hai mille server in più"

Nel 2021, Israele ha firmato un contratto congiunto con Google e Amazon chiamato Project Nimbus. L'obiettivo dichiarato della gara, del valore di 1,2 miliardi di dollari, era quello di incoraggiare i ministeri a trasferire i loro sistemi informativi sui server cloud pubblici delle aziende vincitrici e a ricevere da loro servizi avanzati.

L'accordo è stato molto controverso, con centinaia di lavoratori di entrambe le società che hanno firmato una lettera aperta nel giro di pochi mesi chiedendo di tagliare i legami con l'esercito israeliano. Dal 7 ottobre sono aumentate le proteste dei dipendenti di Amazon e Google, organizzate sotto la bandiera di No Tech For Apartheid . Ad aprile, Google – che è stata brevemente elencata come sponsor della conferenza IT For IDF alla quale ha parlato Dembinsky, prima che il suo logo fosse rimosso – ha licenziato 50 membri dello staff per aver partecipato a una protesta negli uffici della società a New York.

I resoconti dei media affermavano che l'esercito e il ministero della Difesa israeliani avrebbero caricato sul cloud pubblico solo materiali non classificati nell'ambito del progetto Nimbus. Ma la nostra indagine rivela che, almeno dall'ottobre 2023, le grandi società cloud forniscono servizi di archiviazione dati e intelligenza artificiale alle unità dell'esercito che trattano informazioni riservate. Diverse fonti di sicurezza hanno riferito a +972 e Local Call che la pressione sull'esercito israeliano da ottobre ha portato a un drammatico aumento dell'acquisto di servizi da Google Cloud, AWS di Amazon e Microsoft Azure, con la maggior parte degli acquisti dalle prime due società avvenuti attraverso Nimbus. contrarre.

Una fonte della sicurezza ha spiegato che all'inizio della guerra i sistemi dell'esercito israeliano erano così sovraccarichi che hanno considerato di trasferire un sistema di intelligence, che è servito come base per molti attacchi a Gaza, su server cloud pubblici. "C'erano 30 volte più utenti, quindi è semplicemente andato in crash", ha detto la fonte del sistema.

“Quello che succede nel cloud [pubblico]”, ha continuato la fonte, “è che premi un pulsante, paghi altri mille dollari quel mese e hai 10 server. È iniziata una guerra? Paghi un milione di dollari e hai mille server in più. Questo è il potere del cloud. Ed è per questo che [durante la guerra] le persone dell'IDF hanno davvero spinto per lavorare con il cloud. Era un dilemma”.

Il progetto Nimbus ha alleviato questo dilemma. Secondo i termini della gara, le due società vincitrici, Google e Amazon, avrebbero creato dei data center in Israele rispettivamente nel 2022 e nel 2023 . Anatoly Kushnir, co-fondatore della società tecnologica israeliana Comm-IT, che da ottobre aiuta le unità militari a migrare nel cloud, ha spiegato a +972 e Local Call che Nimbus “ha creato un'infrastruttura” di centri informatici avanzati sotto la giurisdizione israeliana.

Questa disposizione, ha detto, ha reso più facile per “gli enti di sicurezza, anche quelli più sensibili”, archiviare informazioni nel cloud durante la guerra senza timore da parte dei tribunali esteri – che, presumibilmente, potrebbero richiedere le informazioni in caso di causa legale. contro Israele.

“Durante la guerra”, ha continuato Kushnir, “sono sorti bisogni [nell'esercito] che non esistevano [prima], ed è stato molto più facile soddisfarli [usando] questa infrastruttura, perché è l'infrastruttura di un proprietario globale che può portare i servizi dal più semplice al

più complicato". Queste società, ha aggiunto, hanno fornito all'esercito israeliano "i servizi più avanzati" disponibili e che sono stati utilizzati nell'attuale guerra di Gaza.

Questo drammatico cambiamento nelle procedure dell'esercito ha subito un'accelerazione significativa dall'inizio della guerra. In passato, ha detto Kushnir, l'esercito si affidava principalmente a sistemi sviluppati da esso stesso, noti come "on-prem", abbreviazione di "on-premise". Ma questo significava che avrebbe dovuto aspettare mesi, se non anni, per costruire i nuovi servizi che le mancavano. Nel cloud pubblico, invece, le capacità di intelligenza artificiale, archiviazione ed elaborazione sono "molto più accessibili".

Qualificando i suoi commenti, Kushnir ha spiegato che "le informazioni veramente sensibili, le cose più segrete, non sono [sul cloud civile]. Il lato operativo sicuramente non c'è. Ma ci sono cose dell'intelligence che sono parzialmente conservate lì".

Eppure, anche all'interno dell'esercito, alcuni hanno espresso preoccupazione per il potenziale rischio di violazione dei dati. "Quando hanno iniziato a parlarci del cloud e abbiamo chiesto se non ci fosse un problema di sicurezza delle informazioni nell'inviare le nostre informazioni a una società terza, ci è stato detto che questo [rischio] è sminuito dal valore del suo utilizzo ", ha detto una fonte dell'intelligence.



Il fumo si alza dopo gli attacchi aerei israeliani a Khan Younis, nel sud della Striscia di Gaza, il 6 maggio 2024. (Abed Rahim Khatib/Flash90)

"La nuvola ha informazioni su tutti"

Fonti hanno riferito a +972 e Local Call che la maggior parte delle informazioni di intelligence dell'esercito israeliano sugli agenti militari palestinesi sono archiviate sui computer interni dell'esercito piuttosto che sul cloud pubblico, che è connesso a Internet. Tuttavia, secondo tre fonti di sicurezza, uno dei sistemi di dati utilizzati dalla direzione dell'intelligence militare israeliana è archiviato sul cloud pubblico di Amazon, AWS.

L'esercito utilizza questo sistema a Gaza per la sorveglianza di massa almeno dalla fine del 2022, ma non era considerato particolarmente operativo prima dell'attuale guerra. Ora, secondo queste fonti, il sistema Amazon contiene un "archivio infinito" di informazioni che l'esercito può utilizzare.

Fonti della difesa hanno affermato che le informazioni di intelligence conservate su AWS sono ancora considerate "trascurabili" in termini di utilizzo operativo, rispetto a quelle conservate sui sistemi interni dei militari. Tuttavia, tre fonti che hanno preso parte agli attacchi dell'esercito hanno affermato che è stato utilizzato in numerosi casi per fornire "informazioni supplementari" prima degli attacchi aerei contro sospetti agenti militari, alcuni dei quali hanno ucciso molti civili.

Come +972 e Local Call hanno rivelato in una [precedente indagine](#), l'esercito israeliano ha autorizzato l'uccisione di "centinaia di civili" in attacchi contro alti comandanti di Hamas a livello di comandanti di brigata e talvolta anche di comandanti di battaglione. In alcuni di questi casi, hanno spiegato fonti della sicurezza, il cloud di Amazon è stato reso operativo.

Le fonti affermano che il sistema basato su AWS è particolarmente utile per l'intelligence israeliana perché può contenere informazioni "su tutti", senza limitazioni di archiviazione. Ciò a volte presentava vantaggi operativi: una fonte di intelligence ha descritto un momento "davvero fatidico" della guerra, quando l'esercito ha localizzato un membro anziano dell'ala militare di Hamas all'interno di un grande edificio a più piani pieno di centinaia di rifugiati e malati. La fonte ha descritto l'utilizzo di AWS per raccogliere informazioni su chi si trovava nell'edificio. L'attacco, ha detto, alla fine è stato interrotto perché non era chiaro esattamente dove si nascondesse l'agente senior e l'esercito temeva che portarlo avanti avrebbe ulteriormente danneggiato l'immagine di Israele.

"La nuvola [di Amazon] è lo [spazio] di archiviazione infinito", ha detto un'altra fonte dell'intelligence israeliana. "Ci sono ancora i normali server [dell'esercito], che sono piuttosto grandi... Ma durante la raccolta di informazioni, a volte, trovi qualcuno che ti interessa e dici: 'Che peccato, non è incluso [come obiettivo di sorveglianza], non lo so.'" "non ho informazioni su di lui." Ma la nuvola ti dà informazioni su di lui, perché la nuvola ha [informazioni su] tutti".

In precedenza, l'esercito era solito cancellare le informazioni inutili accumulate nei suoi database per fare spazio a nuove informazioni. Ma nella sua conferenza del 10 luglio, Dembinsky ha osservato che l'esercito sta lavorando da ottobre per "salvaguardare, salvare

e immagazzinare tutto il materiale da combattimento”. Una fonte di sicurezza ha confermato che è proprio così, attribuendo l'aumento dello spazio di archiviazione alle società di cloud pubblico.



Soldati israeliani all'interno di una base militare, maggio 2023. (Unità del portavoce dell'IDF/CC BY-SA 3.0)

Un altro importante incentivo per lavorare con i giganti del cloud sono le loro capacità di intelligenza artificiale e le server farm delle unità di elaborazione grafica (GPU) che li supportano. Una fonte di intelligence, che ha partecipato alle discussioni sullo spostamento dell'intelligence militare sul cloud pubblico, ha affermato che i loro superiori “hanno parlato di come se migrassero sul cloud, allora [le società cloud] avrebbero anche le proprie STT [capacità di sintesi vocale]. Questi sono buoni; hanno molte capacità. Perché sviluppare tutto nell'unità dell'esercito se le capacità esistono già?”

Il flusso di lavoro descritto a +972 e Local Call dagli ufficiali dell'intelligence - "ordinando" i dati dal cloud pubblico AWS e poi inviandoli a una rete militare chiusa - corrisponde ai dettagli in un libro scritto nel 2021 dall'attuale comandante dell'Unità 8200, un'unità d'élite all'interno della direzione dell'intelligence militare israeliana, che recentemente è stato rivelato dal Guardian essere Yossi Sarel .

"Come possono gli istituti di sicurezza utilizzare il 'cloud Amazon' e sentirsi sicuri?" Ha scritto Sarel, sostenendo come soluzione una rete speciale in cui il sistema interno dell'esercito e il cloud pubblico possano "comunicare tra loro in modo sicuro in ogni momento". La portata delle informazioni segrete raccolte dall'intelligence israeliana è così ampia, ha aggiunto, che possono essere archiviate "solo in aziende come Amazon, Google o Microsoft".

Nello stesso anno, scrivendo su un giornale dell'intelligence israeliana, il vice comandante dell'Unità 8200 ha chiesto "nuove partnership" con i fornitori di cloud pubblici, poiché le loro capacità di intelligenza artificiale sono "insostituibili" e superiori a quelle dell'esercito. Ha lasciato intendere che anche le società cloud trarranno vantaggio dalla collaborazione con l'esercito: "Aman [l'intelligence militare] detiene la maggior parte dei dati nell'IDF, compresi i dati sui nemici, da un'ampia varietà di sensori – dati che le società civili pagherebbero un prezzo più alto". fortuna per avere accesso."

"Ciò che utilizzerà l'IDF sarà uno dei migliori argomenti di vendita"

Secondo fonti del settore militare e dell'industria degli armamenti, per anni Microsoft Azure è stato considerato il principale fornitore di servizi cloud in Israele, vendendo i suoi servizi al Ministero della Difesa e alle unità dell'esercito che trattano informazioni riservate. Secondo una fonte, Azure avrebbe dovuto fornire all'esercito israeliano il cloud su cui sarebbero state archiviate le informazioni di sorveglianza, ma Amazon ha offerto un prezzo migliore. Fonti delle società cloud, a conoscenza dei legami con il Ministero della Difesa israeliano, hanno affermato che da quando Amazon ha vinto la gara d'appalto Nimbus, è stata in concorrenza aggressiva con Azure, sperando di sostituirlo come principale fornitore di servizi dell'esercito.

Kushnir, di Comm-IT, ha spiegato che in passato "la maggior parte delle agenzie governative e militari hanno investito molto nello sviluppo e nella creazione di sistemi basati su Azure". Ma poiché Azure non ha vinto la gara d'appalto Nimbus, ha continuato, c'è stato un "certo processo di migrazione" presso il Ministero della Difesa verso i server di Google e Amazon, che ha subito un'accelerazione durante l'attuale guerra.

Fonti del settore high-tech affermano che il Ministero della Difesa israeliano è considerato un cliente importante e "strategico" per le tre società cloud. Ciò non è solo dovuto all'ampia portata finanziaria delle transazioni, ma perché Israele è percepito come influente nel plasmare l'opinione delle agenzie di sicurezza di tutto il mondo e nel guidare le "tendenze" adottate da altre agenzie.

Una delle persone che per anni ha diretto la politica di approvvigionamento del Ministero della Difesa e ha mantenuto i contatti con i giganti del cloud, è il colonnello Avi Dadon, che ha parlato con +972 e Local Call per questa indagine. Fino al 2023 è stato a capo dell'amministrazione degli acquisti del Ministero della Difesa ed è stato responsabile degli appalti militari per un valore di oltre 10 miliardi di shekel (circa 2,7 miliardi di dollari) all'anno.

"Per [le aziende cloud], è il marketing più forte", ha affermato Dadon. "Ciò che utilizza l'IDF era e sarà uno dei migliori punti di vendita di prodotti e servizi nel mondo. Per loro è un laboratorio. Ovviamente vogliono [lavorare con noi]".

Dadon ha affermato di aver tenuto numerosi incontri con rappresentanti di AWS, Microsoft Azure e Google Cloud in Israele, nonché viaggi negli Stati Uniti. Era anche in contatto con i giganti delle nuvole per una gara d'appalto riservata chiamata Progetto Sirius.

Segnalato per la prima volta nel quotidiano finanziario israeliano Globes nel 2021, Sirius è considerato molto più sensibile di Nimbus e non ha ancora firmato un contratto con nessuna delle società tecnologiche. A maggio, l'esercito ha annunciato sul suo sito web che sta cercando di assumere un esperto che "lavorerà con i grandi fornitori di cloud" per "trasferire i sistemi [militari] nel cloud pubblico (Nimbus)" e per "preparare il caricamento dei core , sistemi operativi, nel cloud di sicurezza" nel quadro della gara Sirius.

"Sirius è un cloud di sicurezza privato e isolato [isolato dalle reti pubbliche e di altro tipo], ed è destinato solo all'IDF e al Ministero della Difesa", ha spiegato Dadon. "Ci sono state discussioni per più di un decennio su come sarà". Questo nuovo cloud, secondo tre fonti di sicurezza, dovrebbe essere disconnesso da Internet e costruito sull'infrastruttura dei grandi fornitori di servizi cloud, consentendo a tutte le agenzie di sicurezza israeliane di utilizzarlo per sistemi classificati.

I servizi cloud pubblici, secondo Dadon, hanno il potenziale per aumentare la letalità dei militari. Quando si cerca una persona da "eliminare", ha spiegato, "si raccolgono miliardi di dettagli apparentemente poco interessanti. Ma devi conservarli. Una volta che vuoi elaborare [e] fondere tutto in un prodotto che ti dice che [l'obiettivo] è qui a quest'ora, hai cinque minuti, non hai tutto il giorno e la notte. Quindi ovviamente hai bisogno delle informazioni.

"Non puoi [farlo] sui tuoi server, perché devi eliminare costantemente ciò che ritieni non necessario", ha continuato Dadon. "C'è un compromesso molto critico qui. Una volta effettuato il caricamento sul cloud, tornare a "on-premise" è quasi impossibile. Conosci un nuovo mondo. Hai già caricato informazioni di diversi ordini di grandezza più grandi e cosa farai ora? Iniziare a cancellarlo?"

Come +972 e Local Call hanno rivelato in una precedente indagine , molti degli attacchi israeliani a Gaza all'inizio della guerra erano basati sulle raccomandazioni di un programma chiamato "Lavender". Con l'aiuto dell'intelligenza artificiale, questo sistema ha elaborato informazioni sulla maggior parte dei residenti di Gaza e ha compilato un elenco di sospetti agenti militari, compresi quelli più giovani, da assassinare. Israele ha attaccato sistematicamente questi agenti nelle loro case private, uccidendo intere famiglie. Col tempo, i militari si resero conto che Lavender non era abbastanza "affidabile" e il suo utilizzo diminuì a favore di altri software. +972 e Local Call non hanno potuto confermare se Lavender sia stato sviluppato con l'aiuto di aziende civili, comprese le società di cloud pubblico.



Palestinesi ispezionano la distruzione della casa appartenente alla famiglia Al-Khatib dopo che fu distrutta da un attacco aereo israeliano, nella città di Rafah, nel sud della Striscia di Gaza, il 29 aprile 2024. (Abed Rahim Khatib/Flash90)

"Stai combattendo dall'interno del tuo laptop"

Nella sua conferenza del mese scorso, Dembinsky ha definito l'attuale operazione militare a Gaza "la prima guerra digitale". Sebbene ciò sembri un'esagerazione, dato che l'offensiva del 2021 sulla Striscia ha utilizzato anche capacità digitali, fonti della difesa israeliane affermano che i processi di digitalizzazione dell'esercito hanno subito un'accelerazione significativa durante l'attuale guerra. Secondo loro, i comandanti sul campo vanno in giro con smartphone crittografati, inviano messaggi in una chat operativa simile a WhatsApp (ma non correlata all'azienda), caricano file su un'unità condivisa e utilizzano innumerevoli nuove applicazioni.

"Stai combattendo dall'interno del tuo laptop", ha detto un ufficiale che ha prestato servizio in una sala operativa di combattimento a Gaza. In passato, "vedresti il bianco degli occhi del tuo nemico, guarderesti attraverso il binocolo e lo vedresti esplodere". Oggi, tuttavia, quando appare un bersaglio, "dici [ai soldati] attraverso il laptop: 'Spara con il carro armato'".

Una delle app sul cloud interno dell'esercito si chiama Z-Tube (Z è l'abbreviazione di Zahal, l'acronimo dell'IDF); è un sito web, che assomiglia molto a Youtube, che consente ai soldati di accedere a filmati in diretta di tutti i dispositivi di ripresa militari a Gaza, compresi gli UAV .

Un'altra app, chiamata "MapIt", consente ai soldati di contrassegnare gli obiettivi in tempo reale su una mappa interattiva e collaborativa. "Gli obiettivi sono lo strato più pesante sulla mappa", ha detto una fonte della sicurezza a +972 e Local Call. "Sembra che ogni casa abbia un obiettivo."

Un'app correlata chiamata "Hunter" viene utilizzata per segnalare obiettivi a Gaza e rilevare modelli di comportamento utilizzando l'intelligenza artificiale. È stato presentato alla conferenza IT for IDF dal colonnello Eli Birenbaum, comandante di un'unità conosciuta con l'acronimo ebraico Matzpen, responsabile dello sviluppo di sistemi per usi operativi.

Il cloud interno dovrebbe essere gestito su server militari e non collegato ai cloud delle società private, ma diverse fonti affermano che esistono modi "sicuri" in cui le società cloud civili possono fornire servizi anche ai sistemi operativi.

"L'IDF non tiene fuori cose molto sensibili e riservate: queste cose rimangono all'interno [delle reti militari con air gap]", ha detto il colonnello Assaf Navot, un ex alto funzionario ICT dell'esercito e ora capo della divisione di difesa di Comm-IT. +972 e chiamata locale. Secondo lui, la sfida è portare il "cervello" delle società cloud civili, come i servizi di intelligenza artificiale, nei sistemi interni dell'esercito, "senza che viva all'esterno. Vive proprio dentro. Quindi non puoi fare tutto in un modo che sia uno a uno [uguale a] ciò che accade fuori, ma riesci a fare progressi pazzeschi.

Nel 2022, Itai Binyamin, un esperto di intelligenza artificiale che all'epoca lavorava con Microsoft Azure e ora lavora con AWS, descrisse a un gruppo di laureati dell'unità Mamram di Dembinsky che questo sistema rende possibile "distribuire le capacità di intelligenza artificiale [di Microsoft] anche su... prem, sui vostri server, in un ambiente disconnesso [da Internet]." Nella sua spiegazione nel video, Binyamin ha mostrato ai laureati come lo strumento di riconoscimento facciale di Microsoft potrebbe analizzare un video di notizie e identificare che il leader di Hamas Ismail Haniyeh vi è apparso.



Le forze israeliane osservano i palestinesi fuggire da Khan Younis nel sud della Striscia di Gaza, il 30 gennaio 2024. (Atia Mohammed/Flash90)

Il sito web di Microsoft Azure fa riferimento a strumenti chiamati “contenitori disconnessi”, progettati per “partner strategici” che hanno bisogno di mantenere le proprie informazioni al sicuro. Gli strumenti, secondo il sito Web, includono funzionalità di trascrizione, traduzione, riconoscimento dei sentimenti, lingua, riepilogo, analisi di documenti e immagini e altro ancora.

Navot ha spiegato che il ritmo di sviluppo della tecnologia digitale è così rapido che l’unico modo per l’esercito di “recuperare il ritardo” è acquistare servizi dal mercato civile e dalle società cloud. “Guarda l’M16 [fucile d’assalto]. L’ultima volta che hanno realizzato un M16 è stato durante la guerra del Vietnam. Non è cambiato molto”. Ma per quanto riguarda il software digitale, dice, le cose cambiano “in mesi, non in anni”.

Il fatto stesso che materiale di intelligence, anche se non direttamente operativo, venga caricato su un cloud civile ha sollevato preoccupazioni tra alcuni membri dell’esercito israeliano. “C’è qualcosa di spaventoso in questo”, ha detto una fonte dell’esercito. “Le informazioni di cui dispone oggi l’esercito sono informazioni intime su molte persone [nei territori occupati]. Quindi cederlo a gigantesche aziende private e commerciali che hanno l’obiettivo di fare soldi?”

Altre fonti di sicurezza, d'altro canto, hanno affermato che l'intelligence grezza raccolta su vasta scala piuttosto che su obiettivi specifici non è particolarmente sensibile, poiché lo diventa solo quando viene tradotta in obiettivi di attacco. "Non è poi così spaventoso se gli iraniani avessero [accesso a] queste informazioni", ha affermato una delle fonti.

Brigantino. Il generale Yael Grossman, comandante della Divisione dell'esercito per il rafforzamento della tecnologia operativa - conosciuta con l'acronimo ebraico Lotem - che è responsabile di Mamram, ha affermato in un podcast di maggio che la dipendenza dalle tecnologie civili nell'attuale guerra ha consentito un "salto pazzesco in un breve periodo di tempo. Ma Dadon paragona il caricamento di materiali sul cloud alla "consegna delle chiavi di una Mercedes a qualcun altro. Non dovremmo usare la Mercedes? Abbiamo bisogno di. Così come? Non lo so."

"È partecipazione diretta sugli strumenti usati per uccidere i palestinesi"

Negli ultimi anni Amazon è diventata non solo partner dell'esercito israeliano, ma anche fornitore di servizi cloud per diverse agenzie di intelligence occidentali. Nel 2021, AWS ha firmato un accordo con le agenzie di intelligence del Regno Unito GCHQ, MI5 e MI6 per archiviare informazioni "classificate" e accelerare l'uso degli strumenti di intelligenza artificiale. Allo stesso modo, il governo australiano ha annunciato questo mese che investirà 1,3 miliardi di dollari per costruire un cloud per materiale di intelligence "top secret" sui server di Amazon. Il colosso della tecnologia ha anche firmato un accordo con il Pentagono, insieme ad altre tre grandi aziende, per costruire un gigantesco cloud che servirebbe al Dipartimento della Difesa degli Stati Uniti per "tutti i livelli di classificazione".

Amazon pubblica regole vaghe per "Costruire l'intelligenza artificiale in modo responsabile", che si riferiscono solo a "ottenere, utilizzare e proteggere i dati in modo appropriato" e a "prevenire risultati dannosi e usi impropri del sistema". I principi e l'approccio responsabile dell'intelligenza artificiale di Microsoft affermano: "Ci impegniamo a garantire che i sistemi di intelligenza artificiale siano sviluppati in modo responsabile e in modi che garantiscano la fiducia delle persone".

Google pubblica anche un elenco dei suoi principi sull'intelligenza artificiale in cui si afferma più chiaramente che Google "non progetterà né implementerà l'intelligenza artificiale in... tecnologie che causano o potrebbero causare danni complessivi; ... armi o altre tecnologie il cui scopo o implementazione principale è causare o facilitare direttamente lesioni alle persone ... tecnologie che raccolgono o utilizzano informazioni per la sorveglianza che violano le norme accettate a livello internazionale ... [o] tecnologie il cui scopo contravviene ai principi ampiamente accettati del diritto internazionale e dei diritti umani. "

Tuttavia, Gabriel Schubiner, attivista e organizzatore di No Tech For Apartheid, afferma che questi principi "non hanno alcun effetto reale" perché le società cloud "li usano come PR per dimostrare quanto sono responsabili". Secondo lui le aziende non hanno modo di sapere in

tempo reale come i loro clienti utilizzano i loro servizi.

Schubiner – che in precedenza ha lavorato presso Google e ha preso parte a una protesta dei dipendenti di Google contro la fornitura di tecnologia che sostengono venga utilizzata dall'esercito israeliano nella guerra di Gaza – afferma che Google ha sempre utilizzato un "linguaggio vago" quando afferma i suoi principi etici . Inoltre, dice, la compagnia continua a sostenere che i suoi contratti con Israele sono "prima di tutto per uso civile, anche se è chiaro che molte delle azioni della Nimbus sono finalizzate all'uso militare".

Una fonte della difesa ha detto a +972 e Local Call che la maggior parte dei nuovi contratti tra l'esercito e le società cloud dall'inizio della guerra sono stati realizzati attraverso la gara Nimbus. Tuttavia, le forze armate possono anche creare e approfondire i legami con le società cloud attraverso gare d'appalto del Ministero della Difesa o attraverso contratti precedenti al Progetto Nimbus. +972 e Local Call non sono riusciti a confermare se il cloud AWS, utilizzato per archiviare informazioni di intelligence, sia stato acquistato come parte del progetto Nimbus.

"Nessuna delle due società ha rivelato pubblicamente quali attività di due diligence sui diritti umani hanno effettuato prima di partecipare al progetto Nimbus", ha spiegato Zach Campbell, esperto di diritti digitali presso Human Rights Watch. "Non hanno menzionato quali, se esistono, linee rosse ci siano in termini di quale sarebbe l'uso consentito della loro tecnologia."

Kushnir, che ha aiutato le unità militari israeliane a migrare verso il cloud, non ha paura del successo delle proteste contro le partnership delle società cloud con Israele. "Bisogna ricordare che le stesse aziende gestiscono cloud governativi e militari simili negli Stati Uniti, nel Regno Unito e nella NATO", ha affermato. "Queste non sono start-up, sono potenze globali dell'ICT".

Nadim Nashif, direttore esecutivo di 7amleh – Centro arabo per l'avanzamento dei social media, che si concentra sui diritti digitali palestinesi, ha affermato che la sua richiesta fondamentale da parte delle società cloud è che "si assicurino che i loro prodotti non vengano utilizzati per danneggiare le persone". , cosa che attualmente nella pratica non avviene. Secondo lui, nonostante la retorica sulla preoccupazione per i diritti umani, i prodotti dei giganti del cloud vengono venduti "a governi e regimi che opprimono le persone" – compreso l'esercito israeliano.



Protesta contro i legami di Google con Israele davanti all'ufficio del CEO di Google Cloud a Sunnyvale, California, 14 giugno 2024. (Per gentile concessione di No Tech for Apartheid)

Riguardo alla mancanza di supervisione dei progetti e dei partenariati delle società cloud, Nashif ha aggiunto: “Nel contesto locale, in caso di occupazione, la questione se [questi servizi] siano venduti per uso militare, all’esercito di occupazione, o se poi viene venduto per uso civile, diventa molto più importante”. Secondo lui, la vicinanza che esiste in Israele tra il settore privato e quello militare facilita la cooperazione senza linee rosse, che porta a “un maggiore controllo sui [palestinesi] – ancora di più durante la guerra”.

“C’è sempre molta attenzione sull’assistenza militare diretta che gli Stati Uniti forniscono a Israele – munizioni, aerei da combattimento e bombe – ma è stata prestata molta meno attenzione a queste partnership che abbracciano sia ambienti civili che militari”, ha affermato Tariq Kenney-Shawa, membro della politica statunitense presso il think tank palestinese Al-Shabaka. “È più che complicità: è partecipazione diretta e collaborazione con l’esercito israeliano sugli strumenti che stanno usando per uccidere i palestinesi”.

Google e Microsoft hanno rifiutato di rispondere a molteplici richieste di commento provenienti dai loro uffici in Israele e negli Stati Uniti. Amazon Web Services ha dichiarato: “AWS è focalizzata nel rendere disponibili i vantaggi della nostra tecnologia cloud leader a livello mondiale a tutti i nostri clienti, ovunque si trovino. Ci impegniamo a garantire la sicurezza dei nostri dipendenti, a sostenere i nostri colleghi colpiti da questi terribili eventi e a collaborare con i nostri partner umanitari per aiutare le persone colpite dalla guerra”.

Questa indagine è stata co-pubblicata in ebraico su Local Call. Leggilo [qui](#). Yuval Abraham è un giornalista e regista con sede a Gerusalemme.