Come le tecnologie dello spionaggio israeliano penetrano in modo molto intrusivo nelle nostre vite

Jonathan Cook

Martedì 26 novembre 2019 – Middle East Eye

Israele normalizza nei Paesi occidentali l'uso di tecnologie invasive e oppressive di cui i palestinesi sono vittime da decine di anni

Le armi dell'era digitale sviluppate da Israele per opprimere i palestinesi sono rapidamente riutilizzate in un campo di applicazione molto più ampio, e ciò contro le popolazioni occidentali che considerano tuttavia le loro libertà come acquisite.

Se a Israele già da parecchi anni è stato concesso lo status di "Nazione delle start up", la sua reputazione nel campo delle innovazioni di tecnologia avanzata si è sempre basata su un aspetto oscuro che è vieppiù difficile nascondere.

Qualche anno fa l'analista israeliano Jeff Halper avvertì che Israele aveva giocato un ruolo centrale sulla scena internazionale nella fusione tra le nuove tecnologie digitali e dell'industria della sicurezza interna. Secondo lui il pericolo era che saremmo tutti quanti diventati progressivamente dei palestinesi.

Egli notava che Israele ha effettivamente trattato milioni di palestinesi sottoposti al suo regime militare come delle cavie in laboratori a cielo aperto – e ciò senza doverne rendere conto. I territori palestinesi occupati sono serviti come banco di prova per la messa a punto non solo dei nuovi sistemi d'arma convenzionali, ma anche di nuovi strumenti per la sorveglianza ed il controllo di massa.

Come ha recentemente osservato un giornalista di Haaretz [giornale israeliano di centro sinistra, ndtr.], l'operazione di sorveglianza condotta da Israele contro i

palestinesi figura “tra le più vaste di questo tipo al mondo. Include la sorveglianza dei media, delle reti sociali e della popolazione nel suo insieme.”

Il Grande Fratello fa affari

Tuttavia quello che è iniziato nei territori occupati non doveva affatto essere limitato alla Cisgiordania, a Gerusalemme est e a Gaza. C’erano semplicemente troppo denaro e influenza da guadagnare commercializzando queste nuove forme ibride di tecnologia digitale offensiva.

Per quanto piccolo sia, Israele è da molto tempo uno dei leader mondiali sul mercato estremamente lucrativo degli armamenti e vende a regimi autoritari i suoi sistemi d’arma “testati sul campo di battaglia”, cioè sui palestinesi.

Ora, questo commercio di materiale militare è sempre più eclissato dal mercato dei programmi digitali bellici, cioè gli strumenti che servono a condurre guerre informatiche.

Queste armi di nuova generazione sono molto richieste dagli Stati, che possono utilizzarle non solo contro nemici esterni, ma anche contro dissidenti interni, che siano difensori dei diritti umani o semplici cittadini. Israele può presentarsi a giusto titolo come un’autorità mondiale in questa materia, nella misura in cui controlla ed opprime le popolazioni che vivono sotto il suo dominio. Ma il Paese ha fatto attenzione a non lasciare le sue impronte digitali su gran parte di questa nuova tecnologia degna del Grande Fratello, scegliendo di esternalizzare lo sviluppo di questi strumenti informatici affidandoli agli ufficiali di alto rango delle sue tristemente celebri unità per la sicurezza e l’intelligence militare.

Tuttavia Israele approva implicitamente queste attività fornendo licenze d’esportazione alle imprese che le gestiscono. D’altro canto i maggiori responsabili della sicurezza del Paese sono spesso strettamente legati al lavoro di queste aziende.

Tensioni con la Silicon Valley

Una volta smessa l’uniforme, questi israeliani possono trarre profitto dai loro anni

d’esperienza nel campo dello spionaggio a danno dei palestinesi, creando società il cui obiettivo è sviluppare dei programmi informatici per delle applicazioni più generali.

Queste app, che utilizzano una tecnologia di sorveglianza sofisticata di origine israeliana, sono sempre più frequenti nelle nostre vite digitali. Alcune sono state utilizzate in modo relativamente innocuo. “Waze”, che sorveglia gli ingorghi del traffico, permette ai conducenti di raggiungere la propria destinazione più rapidamente, mentre “Gett” attraverso il loro telefono mette i clienti in contatto con i taxi che si trovano nei dintorni.

Ma alcune delle tecnologie più segrete prodotte dagli sviluppatori israeliani rimangono molto più vicine al loro format militare originario.

Questi programmi offensivi sono venduti ai Paesi che desiderano spiare i loro stessi cittadini o Stati nemici, come anche a società private che sperano così di conquistarsi un notevole vantaggio sui concorrenti o di manipolare e sfruttare meglio dal punto di vista commerciale i loro clienti.

Una volta integrati nelle piattaforme delle reti sociali, che contano miliardi di utenti, questi programmi spionistici offrono ai servizi statali della sicurezza un raggio d’azione potenziale quasi universale. Ciò implica una relazione a volte tesa tra le società israeliane e la Silicon Valley [centro di ideazione e produzione delle innovazioni digitali negli USA, ndtr.], con quest’ultima che lotta per prendere il controllo di questi programmi “malintenzionati” – come dimostrano due esempi diversi dell’attualità recente.

“Sistema di spionaggio” per telefonini

Indice di queste tensioni, WhatsApp, una piattaforma di reti sociali appartenente a Facebook, molto di recente ha intentato il primo processo di questo tipo davanti a un tribunale californiano contro NSO, la più grande impresa di sorveglianza israeliana.

WhatsApp accusa NSO di attacchi informatici. Nel lasso di tempo di sole due settimane fino all’inizio di maggio esaminato da WhatsApp, NSO avrebbe preso di mira i telefonini di più di 1.400 utenti in 20 Paesi.

Il programma di spionaggio digitale di NSO, chiamato “Pegasus”, è stato utilizzato contro difensori dei diritti umani, avvocati, responsabili religiosi, giornalisti e operatori umanitari. La Reuter [agenzia di stampa inglese, ndtr.] ha rivelato alla fine di ottobre che alti responsabili di Paesi alleati degli Stati Uniti sarebbero stati anche loro presi di mira da NSO.

Dopo aver preso il controllo del telefono di un utente a sua insaputa, “Pegasus” ne copia i dati e attiva il microfono dell’apparecchio al fine di controllarlo. La rivista “Forbes” [rivista USA di economia, ndtr.] lo ha descritto come “il sistema di spionaggio mobile più invasivo al mondo”.

NSO ha concesso la licenza di utilizzazione del programma a decine di governi, in particolare a regimi noti per le violazioni dei diritti umani come l’Arabia Saudita, il Bahrein, gli Emirati Arabi Uniti, il Kazakistan, il Messico e il Marocco. Amnesty International si è lamentata che i suoi funzionari figurano tra le persone prese di mira dal programma spia di NSO. L’Ong per la difesa dei diritti dell’uomo attualmente sostiene un’azione legale contro il governo israeliano perché ha concesso alla società una licenza d’esportazione.

Rapporti con i servizi di sicurezza israeliani

NSO è stata fondata nel 2010 da Omri Lavie e Shalev Hulio, entrambi ufficiali della famosa Unità 8200 di intelligence militare israeliana. Nel 2014 degli informatori che hanno lanciato l’allarme hanno rivelato che l’unità spiava regolarmente i palestinesi, cercando nei loro telefoni e computer delle prove di comportamenti sessuali devianti, di problemi di salute o di difficoltà finanziarie che potevano essere utilizzate per spingerli a collaborare con le autorità militari israeliane.

I soldati hanno scritto che i palestinesi erano “totalmente esposti allo spionaggio e alla sorveglianza dei servizi di intelligence israeliani. Questi sono utilizzati per perseguitare gli avversari politici e per creare divisioni all’interno della società palestinese reclutando collaboratori e spingendo le diverse componenti della società palestinese le une contro le altre.”

Benché le autorità abbiano concesso a NSO delle licenze d’esportazione, Ze’ev Elkin [del partito di destra Likud, ndtr.], ministro israeliano per la Protezione

dell'Ambiente, per Gerusalemme e per l'Integrazione, ha negato "il coinvolgimento del governo israeliano" nello spionaggio di WhatsApp. "Tutti capiscono che non si tratta dello Stato d'Israele," ha dichiarato a una radio israeliana all'inizio di novembre.

Inseguiti dalle telecamere

La settimana in cui WhatsApp ha lanciato la sua azione legale, la catena televisiva americana NBC ha rivelato che la Silicon Valley intende comunque lavorare con delle start-up israeliane profondamente coinvolte negli abusi legati all'occupazione.

Microsoft ha investito parecchio in AnyVision, una società che sviluppa una sofisticata tecnologia di riconoscimento facciale usata dall'esercito israeliano per opprimere i palestinesi.

I rapporti tra AnyVision e i servizi di sicurezza israeliani sono a malapena nascosti. Il consiglio consultivo della società conta tra i suoi membri Tamir Pardo, ex-capo del Mossad, l'agenzia di spionaggio israeliana. Il suo presidente, Amir Kain, era in precedenza alla testa del "Malmab", il dipartimento del ministero della Difesa israeliano incaricato della sicurezza.

Il principale programma di AnyVision, "Better Tomorrow" [Futuro Migliore], è stato soprannominato "Google dell'Occupazione", perché la società sostiene che può identificare e seguire qualunque palestinese grazie alle immagini prodotte dalla vasta rete di telecamere di sorveglianza sistemate dall'esercito israeliano nei territori occupati.

A dispetto degli evidenti problemi etici, l'investimento di Microsoft suggerisce che il suo obiettivo potrebbe essere integrare questo programma all'interno dei suoi. Ciò ha provocato viva preoccupazione tra i gruppi di difesa dei diritti umani.

Shankar Narayan, dell'American Civil Liberties Union [ACLU, ong Usa per la difesa dei diritti e delle libertà individuali, ndtr.], ha messo in guardia in particolare contro un avvenire fin troppo familiare ai palestinesi che vivono sotto il controllo di Israele: "L'uso generalizzato della sorveglianza facciale sovverte il principio di libertà e genera una società in cui tutti sono seguiti in continuazione,

indipendentemente da quello che fanno," ha dichiarato alla NBC.

"Il riconoscimento facciale è forse lo strumento più perfetto per il controllo totale del governo nei luoghi pubblici."

Secondo Yael Berda, ricercatore dell'università di Harvard, Israele dispone di una lista di circa 200.000 palestinesi in Cisgiordania che desidera sorvegliare 24 ore al giorno. Le tecnologie come AvyVision sono considerate essenziali per mantenere questo vasto gruppo sotto una sorveglianza continua.

Un ex dipendente di AvyVision ha dichiarato alla NBC che i palestinesi sono stati trattati come cavie. "La tecnologia è stata testata sul terreno in uno dei contesti della sicurezza più esigenti al mondo, e ora noi la utilizziamo sul resto del mercato," ha dichiarato.

Il 15 novembre Microsoft ha annunciato il lancio di un'indagine sulle accuse secondo cui la tecnologia di riconoscimento facciale messa a punto da AnyVision violerebbe il suo codice etico a causa del suo utilizzo in operazioni di sorveglianza nella Cisgiordania occupata.

Interferenza nelle elezioni

Utilizzare queste tecnologie di spionaggio negli Stati Uniti e in Europa interessa sempre di più il governo israeliano stesso, nella misura in cui l'occupazione dei territori palestinesi è ormai oggetto di una polemica e di un controllo minuzioso nel discorso politico prevalente.

In gran Bretagna i cambiamenti di clima politico sono stati messi in evidenza dall'elezione alla testa del partito Laburista di Jeremy Corbyn, militante di lunga data per i diritti dei palestinesi. Negli Stati Uniti un piccolo gruppo di parlamentari che appoggiano in modo palese la causa palestinese ha di recente fatto il suo ingresso al Congresso, in particolare Rashida Tlaib, la prima donna americana-palestinese a occupare tale ruolo.

Più in generale Israele teme il BDS (Boicottaggio, Disinvestimento e Sanzioni), movimento di solidarietà internazionale che chiede un boicottaggio di Israele, sul modello del boicottaggio contro il Sud Africa durante l'apartheid, finché non cesserà la repressione del popolo palestinese. Il BDS è in piena espansione,

soprattutto negli Stati Uniti, dove si è notevolmente sviluppato in molti campus universitari.

Di conseguenza le imprese informatiche israeliane sono state coinvolte sempre di più nei tentativi intesi a manipolare il discorso pubblico su Israele, in particolare interferendo nelle elezioni all'estero.

Due esempi noti sono per breve tempo finiti sulle prime pagine. Psy-Group, che si presentava come un "Mossad privato in affitto", è stato chiuso l'anno scorso dopo che l'FBI ha aperto un'inchiesta su di esso per aver interferito nelle elezioni presidenziali americane del 2016. Secondo il New Yorker [prestigiosa rivista USA, ndtr.], il suo "Project Butterfly" [Progetto Farfalla] intendeva "destabilizzare e sconvolgere i movimenti antisraeliani dall'interno."

E l'anno scorso la società "Black Cube" [Cubo Nero] è stata accusata di controllo ostile su importanti membri della precedente amministrazione americana guidata da Barack Obama. "Black Cube" sembra essere strettamente legata alle aziende della sicurezza e per un certo periodo i suoi uffici sono stati dislocati in una base militare israeliana.

Vietato da Apple

Un certo numero di altre aziende israeliane cerca di attenuare la distinzione tra spazio privato e spazio pubblico.

"Onavo", una società israeliana di raccolta dati creata da due veterani dell'Unità 8200, è stata acquistata da Facebook nel 2013. L'anno dopo Apple ha vietato la sua applicazione VPN dopo che è stato rivelato che offriva un accesso illimitato ai dati degli utenti.

Secondo un articolo di Haaretz, l'anno scorso il ministro israeliano degli Affari Strategici, Gilad Erdan, che dirige una campagna segreta intesa a demonizzare i militanti del BDS all'estero, ha tenuto regolarmente riunioni con un'altra società, "Concert". Questo gruppo segreto, esentato dalle leggi israeliane sulla libertà d'informazione, ha ricevuto circa 36 milioni di dollari di finanziamenti da parte del governo israeliano. I suoi dirigenti e i suoi azionisti sono "la crema" dell'élite israeliana per la sicurezza e l'intelligence.

Un’altra società israeliana di primo piano, “Candiru” – che deve il suo nome a un piccolo pesce amazzonico famoso per infiltrarsi segretamente nel corpo umano, dove diventa un parassita – vende principalmente i propri strumenti di pirateria informatica ai governi occidentali, anche se le sue operazioni sono circondate dal segreto.

Il suo personale proviene quasi esclusivamente dall’Unità 8200. A prova dello stretto rapporto tra le tecnologie pubbliche e segrete sviluppate dalle aziende israeliane, il direttore generale di “Candiru”, Eitan Achlow, dirigeva in precedenza “Gett”, l’applicazione dei servizi per i taxi.

L’élite della sicurezza israeliana trae profitto da questo nuovo mercato della guerra informatica, sfruttando – come ha fatto per il commercio di armamenti convenzionali – una popolazione palestinese a sua disposizione e prigioniera su cui può testare la sua tecnologia.

Non è sorprendente che Israele renda progressivamente normale nei Paesi occidentali l’uso di tecnologie invasive e oppressive, di cui i palestinesi sono le vittime da decine di anni.

I programmi di riconoscimento facciale permettono una profilazione razziale e politica sempre più sofisticata. Le operazioni segrete e la raccolta dati e di sorveglianza cancellano le tradizionali frontiere tra gli spazi privati e quelli pubblici. E le campagne di raccolta di informazioni che ne sono il risultato permettono d’intimidire, minacciare e screditare gli oppositori o chi, come la comunità dei difensori dei diritti umani, cerca di mettere i potenti di fronte alle loro responsabilità.

Se questo avvenire distopico continua a svilupparsi, New York, Londra, Berlino e Parigi assomiglieranno sempre di più a Nablus, Hebron, Gerusalemme est e Gaza. E noi finiremo tutti col capire cosa significhi vivere in uno Stato di polizia impegnato in una guerra informatica contro quelli che domina.

Jonathan Cook è un giornalista britannico residente dal 2001 a Nazareth. Ha scritto tre libri sul conflitto israelo-palestinese. È stato vincitore del Martha Gellhorn Special Prize for Journalism.

Le opinioni espresse in questo articolo impegnano solo il suo autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(traduzione dall'inglese di Amedeo Rossi)