Attivisti per i diritti umani palestinesi attaccati con con un sistema di spionaggio elettronico israeliano

Attivisti per i diritti umani palestinesi attaccati con con un sistema di spionaggio elettronico israeliano

Un rapporto di Frontline Defenders rivela che sei attivisti, appartenenti alle sei associazioni della società civile recentemente bollate quali "organizzazioni terroriste" da parte del ministro della Difesa Benny Gantz, sono stati bersaglio del sistema di spionaggio militare Pegasus.

Yumna Patel

8 novembre 2021 – Mondoweiss

Un nuovo rapporto ha rivelato lunedì scorso che sei attivisti per i diritti umani palestinesi sono stati presi di mira con un sistema di spionaggio informatico dell'azienda di sorveglianza israeliana NSO, il primo caso segnalato di attivisti palestinesi nel mirino della compagnia di sorveglianza.

Il rapporto di Frontline Defenders (FLD) [ONG che protegge gli attivisti per i diritti umani a rischio, ndtr.] rivela che sei attivisti, appartenenti alle sei associazioni della società civile recentemente bollate dal ministro della Difesa israeliano Benny Gantz come "organizzazioni terroriste", sono stati bersaglio dello spyware di tipo militare Pegasus.

Secondo FLD, dopo che l'associazione era stata contattata da Al-Haq, organizzazione per i diritti umani di Ramallah, una delle sei prese di mira[dal governo israeliano, ndtr], temendo che il telefono di uno di loro fosse stato infettato da uno spyware aveva fatto esaminare 75 iPhone.

Le rilevazioni di FLD, confermate da Citizen Lab [laboratorio specializzato in

sicurezza del web dell'Università di Toronto, ndtr] e dal laboratorio di sicurezza di Amnesty International, hanno scoperto che sei cellulari erano stati hackerati con uno spyware.

Fra le vittime dell'attacco informatico figurano Ghassan Halaika, ricercatore di Al-Haq, Ubai Al-Aboudi, cittadino palestinese-statunitense che è direttore esecutivo del centro Bisan per la Ricerca & lo Sviluppo, e Salah Hammouri, avvocato franco-palestinese che lavora per il gruppo in difesa dei diritti dei detenuti Addameer.

Il mese scorso Hammouri, originario di Gerusalemme, ha ricevuto una notifica dal ministero degli interni israeliano che il suo status di residente permanente della città è stato revocato per presunta "violazione della fedeltà alla nazione". Salah Hammouri è cittadino francese.

Secondo FLD le altre tre vittime dell'attacco informatico preferiscono rimanere anonime.

In base al rapporto tracce dello spyware nel telefono di Halaika, così come in quello del "difensore dei diritti umani n. 6", come viene chiamato nel rapporto, mostravano segni di spyware Pegasus risalenti al 2020, mentre i dispositivi degli altri quattro attivisti colpiti mostravano prove di attività di Pegasus nel periodo fra febbraio e aprile 2021.

Il rapporto riscontra che alcune delle procedure usate per hackerare i cellulari dei sei attivisti palestinesi sono le stesse usate contro altri difensori dei diritti umani e giornalisti di altri Paesi.

Il rapporto evidenzia che quando Pegasus viene installato sul telefono di qualcuno, l'intruso ottiene "l'accesso completo" a messaggi, mail, contenuti, microfono, fotocamera, passwords, messaggi vocali sulle app di messaggistica, dati di localizzazione, chiamate e contatti.

Pegasus è anche in grado di attivare da remoto fotocamera e microfono sul dispositivo infettato per permettere all'hacker di spiare le chiamate e le attività della vittima.

"In questo modo lo spyware consente di sorvegliare non soltanto la vittima, ma anche chiunque entri in contatto con lei tramite quel dispositivo," osserva FLD.

“Questo significa che, oltre a prendere di mira i palestinesi, compresi quelli con doppia cittadinanza, anche i non-palestinesi (compresi stranieri e diplomatici) con cui queste vittime sono state in contatto, cittadini israeliani inclusi, potrebbero essere stati sottoposti a tale sorveglianza, il che, nel caso dei cittadini israeliani, equivarrebbe ad una violazione della legge israeliana.”

Quindi FLD prosegue ricordando che la ditta NSO ha negato che lo spyware Pegasus sia utilizzato nella sorveglianza di massa dei difensori dei diritti umani, in quanto “esso è destinato ad essere utilizzato solo dai servizi segreti governativi e dalle forze dell’ordine con lo scopo di combattere il terrorismo e il crimine.”

“In questo modo, il fatto che Israele abbia designato “terroriste” queste organizzazioni dopo che sono state scoperte tracce di Pegasus, ma pochi giorni prima della rivelazione di questa indagine, sembra essere uno sforzo evidente di nascondere le proprie azioni e non mostra alcun collegamento a prove che porterebbero discredito a tali organizzazioni,” afferma FLD.

“I difensori dei diritti umani non sono terroristi,” dichiara il gruppo. “Questo sviluppo segna una grave estensione delle politiche e pratiche sistematiche di Israele intese a zittire i difensori dei diritti umani palestinesi che perseguono la giustizia e l’accertamento delle responsabilità per la violazione dei diritti umani dei palestinesi.”

“Arbitraria, oppressiva, angosciante”

In seguito alla pubblicazione del rapporto FLD, le sei organizzazioni della società civile coinvolte hanno rilasciato un comunicato congiunto per condannare le “rivelazioni di una massiccia operazione di sorveglianza arbitraria, oppressiva, angosciante e per sollecitare una risposta ferma, che comprenda azioni concrete, da parte della comunità internazionale.”

“La violazione e il controllo dei dispositivi di difensori dei diritti umani viola non soltanto il diritto alla privacy dei difensori dei diritti umani e dei loro legali, ma anche delle tante vittime che hanno avuto qualche tipo di comunicazione con loro,” affermano le associazioni.

Nel loro comunicato le associazioni fanno notare che, malgrado gli accordi intercorsi fra l’azienda NSO con USA e Francia per escludere la sorveglianza dei cittadini di quei Paesi, nel caso di Ubai Al-Aboudi e Salah Hammouri “la

compagnia ha in seguito infranto tali accordi".

"Il parallelismo nei tempi fra l'inchiesta di FLD e la classificazione delle organizzazioni della società civile da parte del ministero della difesa israeliano a poca distanza dall'inizio di tale indagine potrebbe non essere altro che il tentativo preventivo di nascondere le prove della sorveglianza e di insabbiare le operazioni clandestine condotte mediante lo spyware."

"La sorveglianza dei difensori dei diritti umani palestinesi si unisce ad un'inaccettabile serie infinita di azioni coordinate da parte delle istituzioni governative israeliane e dei loro affiliati volte a istigare e compiere campagne sistematiche e organizzate di calunnie, intimidazioni e persecuzioni contro la società civile palestinese. Negli ultimi decenni tali tecniche hanno comportato campagne di diffamazione tese a bollare i difensori dei diritti umani come "terroristi", di istigazione all'odio razziale e violenza, discorsi d'odio, arresti arbitrari, torture e maltrattamenti, minacce di morte, divieti di viaggiare, revoche di residenza e deportazioni," afferma il comunicato.

Diverse altre organizzazioni per i diritti umani, fra cui Access Now, Human Rights Watch, Masaar – Technology and Law Community, Red Line for Gulf, 7amleh- The Arab Center for the Advancement of Social Media, SMEX, e INSM Network for Digital Rights- Iraq, hanno condannato l'hackeraggio dei telefoni degli attivisti.

Le associazioni hanno diffuso un comunicato congiunto in cui condannano l'attacco informatico che viola il diritto alla privacy degli attivisti, affermando che l'hackeraggio "mina la loro libertà di espressione e di associazione e minaccia la loro sicurezza personale e le loro vite."

"Non pregiudica solo chi viene direttamente colpito, ma ha anche un effetto dannoso su sostenitori e giornalisti, che potrebbero auto-censurarsi per paura di una potenziale sorveglianza," afferma il comunicato.

Le associazioni si sono anche appellate agli Stati affinché "mettano in atto un'immediata moratoria di vendite, trasferimento ed uso delle tecnologie di sorveglianza finché non vengano adottate adeguate tutele in materia di diritti umani", e agli esperti dell'ONU affinché "adottino misure urgenti per denunciare le violazioni dei diritti umani da parte degli Stati agevolate dall'uso del sistema di spionaggio informatico Pegasus dell'azienda NSO e forniscano un sostegno immediato e determinante ad indagini imparziali e trasparenti sugli abusi."

Anche la Campagna USA per i Diritti dei Palestinesi ha condannato l'attacco informatico con la dichiarazione del suo direttore esecutivo Ahmad Abuznaid: "Sappiamo riconoscere la repressione quando la vediamo."

"Calunniare i difensori dei diritti umani e fare propaganda per delegittimare il loro lavoro. Sorvegliare attivisti e giornalisti che osano dire la verità. Tutto mentre continuano a commettere violazioni dei diritti umani giorno dopo giorno. Il regime israeliano è uno Stato di apartheid di separazione e disuguaglianza che impiega ogni tattica autoritaria a sua disposizione, ma noi conosciamo la verità: la liberazione è in arrivo e la Palestina sarà libera," dice Abuznaid.

L'esercito adotta la designazione di "terrorismo" di Gantz

La rivelazione dell'attacco informatico segue immediatamente l'adozione da parte del complesso militare israeliano della precedente ordinanza del ministro della difesa Benny Gantz che definiva come "organizzazioni terroriste" le sei associazioni per i diritti umani palestinesi.

Lo scorso tre novembre il comando militare israeliano in Cisgiordania ha emesso cinque ordinanze militari separate per dichiarare "illegali" le organizzazioni, con l'effetto di mettere fuori legge le attività delle organizzazioni in Cisgiordania, dove hanno sede e dove lavora la maggior parte del loro personale.

Se ad ottobre la designazione di Gantz spianava la strada alla criminalizzazione del lavoro delle organizzazioni all'interno di Israele, le ordinanze militari consentono la chiusura dei loro uffici e il sequestro di ciò che contengono.

Questo mette anche a rischio imminente di arresti e carcerazioni arbitrarie il personale di tali organizzazioni, con la motivazione che lavora", secondo la designazione, per una "organizzazione terrorista".

"In pratica, la designazione attribuita alle organizzazioni palestinesi dà facoltà ad Israele di chiuderne gli uffici, sequestrarne le proprietà, conti bancari compresi, oltre ad arrestarne e trattenerne il personale," affermano in una dichiarazione le organizzazioni.

"Rappresenta inoltre un allarmante tentativo di criminalizzare e minare i loro sforzi di promuovere i diritti umani dei palestinesi e il perseguimento delle responsabilità tramite procedure internazionali, screditandone il fondamentale

lavoro, isolandole dalla comunità internazionale, eliminandone da ultimo le fonti di finanziamento."

Le ordinanze militari sono state emanate alcuni giorni dopo la rivelazione di +972 Magazine e di The Intercept [rivista web USA creata dal fondatore di Ebay, ndtr.] secondo cui un dossier segreto israeliano di cui erano entrati in possesso non forniva alcuna vera prova che giustificasse la designazione delle associazioni quali organizzazioni terroriste.

Le 74 pagine del documento secretato sarebbero state usate dallo Shin Bet, il servizio di intelligence interno israeliano, per cercare di convincere i governi europei ad interrompere il finanziamento delle organizzazioni per i diritti palestinesi.

"Alti funzionari di almeno cinque Paesi europei hanno detto che il dossier non contiene alcuna 'prova concreta' e hanno così deciso di mantenere il sostegno finanziario alle organizzazioni," afferma l'articolo di +972.

Israele rafforza la sorveglianza dei palestinesi con il programma di riconoscimento facciale

Martedì, poche ore prima che venisse rivelato l'attacco informatico della NSO contro i sei attivisti palestinesi, un servizio del Washington Post ha rivelato che l'esercito israeliano sta effettuando una "vasta operazione di controllo" nella Cisgiordania occupata mediante l'uso di tecniche di riconoscimento facciale.

Il *Washington Post ha riferito che da due anni l'esercito sta usando una tecnologia per smartphone chiamata "Blue Wolf", [lupo azzurro, ndtr] che "cattura foto dei volti dei palestinesi e li confronta con un database di immagini così esteso che un ex soldato lo ha definito un 'Facebook per palestinesi' segreto dell'esercito", afferma il servizio.*

Secondo il reportage, i soldati israeliani di stanza in Cisgiordania "l'anno scorso hanno fatto a gara per fotografare i palestinesi, vecchi e bambini compresi, e le unità che raccoglievano più foto venivano premiate."

Il servizio stima che il numero minimo delle persone fotografate per il programma di sorveglianza "è stato dell'ordine di diverse migliaia."

L'articolo afferma che, oltre alla tecnologia *Blue Wolf*, le autorità militari

israeliane hanno installato fotocamere per la scansione facciale nella città di Hebron nel sud della Cisgiordania “per aiutare i soldati dei posti di blocco ad identificare i palestinesi ancor prima che esibiscano i documenti di identità.”

“Una rete ancora più grande di telecamere a circuito chiuso, denominata “Smart City Hebron”, monitora in tempo reale la popolazione cittadina e a volte riesce a vedere all’interno delle case”, ha affermato un ex soldato citato nel servizio.

Hebron è un delicato punto nevralgico all’interno della Cisgiordania, e spesso gli attivisti lo hanno definito un “microcosmo” dell’occupazione israeliana.

La città è divisa fra circa 40.000 autoctoni palestinesi e un gruppo di coloni israeliani tristemente noti per la loro violenza ideologica che vivono nel cuore della Città Vecchia. In seguito al massacro di dozzine di palestinesi per mano di un colono israeliano nel 1994, la città vecchia venne divisa fra aree controllate dai palestinesi e dagli israeliani note come aree H1 e H2, la seconda dove vivono in maggioranza coloni.

I 40.000 palestinesi che vivono nell’area H2 sono perennemente circondati dagli oltre 1.000 soldati israeliani di stanza nell’area e da 20 posti di blocco militari che ne limitano qualsiasi movimento.

L’alta concentrazione di soldati e di coloni armati israeliani ha trasformato la città in uno dei principali luoghi della violenza coloniale e militare in Cisgiordania, dove le violazioni dei diritti umani sono all’ordine del giorno.

(traduzione dall’inglese di Stefania Fusero)

Pegasus: la lunga storia di processi e smentite del Gruppo NSO

Frank Andrews

20 luglio 2021 – Middle east eye

L'azienda israeliana afferma di non poter essere considerata responsabile per il modo in cui gli Stati, "clienti sovrani", utilizzano la sua tecnologia.

Il gruppo NSO non è nuovo agli scandali.

Le affermazioni fatte questa settimana secondo cui la tecnologia *spyware* del programma Pegasus dell'azienda israeliana è stata utilizzata per sorvegliare 50.000 telefoni – appartenenti a capi di stato, giornalisti, attivisti per i diritti umani, oppositori politici e altro – potrebbero rappresentare l'accusa più grave mossa contro l'azienda, ma non sarebbe la prima.

Pegasus, che in vari modi infetta i telefoni con *spyware*, ha rappresentato una manna per i regimi autoritari che usano le tecnologie per tracciare chiunque sia percepito come critico nei confronti del loro potere.

Il Gruppo è stato oggetto di numerose azioni legali e denunce.

Martedì i pubblici ministeri francesi hanno annunciato di aver aperto un'indagine con l'accusa secondo cui Pegasus è stato utilizzato dall'intelligence marocchina per spiare i giornalisti francesi, dopo che *F*orbidden Stories, organizzazione senza scopo di lucro [con la missione di "continuare e pubblicare il lavoro di giornalisti minacciati, incarcerati o assassinati", ndtr.] ha condotto

un’inchiesta che ha rivelato come alcuni Stati, tra cui l’Arabia Saudita, gli Emirati Arabi Uniti, il Bahrain e il Marocco, starebbero usando la tecnologia Pegasus per spiare cittadini e dissidenti, inclusi i collaboratori di *Middle East Eye* Madawi al-Rasheed e Azzam Tamimi.

I familiari, gli amici e i contatti più stretti del giornalista saudita assassinato Jamal Khashoggi erano tra le molte migliaia di persone sorvegliate.

Nel corso degli anni, NSO, fondata nel 2010, ha ripetutamente cercato di sottrarsi alle responsabilità riguardo a come gli Stati utilizzino la sua tecnologia per spiare giornalisti e difensori dei diritti umani.

NSO afferma di seguire tutte le normative israeliane che disciplinano l’esportazione dei suoi prodotti e di vendere solo agli alleati di Israele, mai ai suoi nemici. Afferma inoltre di vendere solo a governi e mai a individui o utenti non autorizzati e che Pegasus è destinato esclusivamente a combattere la criminalità e il terrorismo.

Sottolinea tuttavia che una volta venduto il prodotto, non c’è alcun controllo (o almeno così sostiene) su come venga utilizzata la tecnologia.

Middle East Eye ha indagato sulla lunga lista di accuse a cui NSO ha dovuto rispondere nel corso degli anni e su come l’azienda abbia reagito.

2016

Secondo un rapporto di Citizen Lab [laboratorio interdisciplinare dell’Università di Toronto per ricerca, sviluppo e politica strategica di alto livello, ndtr.] e Lookout Security [società californiana che produce software di sicurezza su cloud per dispositivi mobili, ndtr.], si è scoperto che nell’agosto 2016 gli Emirati Arabi Uniti stavano monitorando l’iPhone dell’attivista per i diritti umani negli Emirati Ahmed Mansoor utilizzando lo *spyware* Pegasus.

Mansoor ricevette un sms che gli chiedeva di aprire un link per avere informazioni sui prigionieri torturati negli Emirati Arabi Uniti.

NSO non ha confermato di aver creato lo *spyware* utilizzato per raggiungere Mansoor. Tuttavia ha affermato in una dichiarazione di "vendere solo ad agenzie governative autorizzate e rispettare pienamente le rigorose leggi e regolamenti sul controllo delle esportazioni. Inoltre l'azienda non gestisce nessuno dei suoi sistemi: è un'azienda esclusivamente tecnologica".

Altri Paesi che il rapporto di Citizen Lab ha scoperto potrebbero aver utilizzato questa tecnologia includono Messico, Turchia, Israele, Thailandia, Qatar, Kenia, Uzbekistan, Mozambico, Marocco, Yemen, Ungheria, Arabia Saudita, Nigeria e Bahrein.

In un caso collegato a quello del 2016, anche le autorità degli Emirati Arabi Uniti avrebbero impiegato Pegasus in un tentativo di *phishing* [azione per ottenere con l'inganno dati riservati, ndtr.] contro il giornalista *MEE* Rori Donaghy, che parlava in modo critico degli abusi del regime autocratico del Paese.

Nel corso dell'indagine su questo attacco, Citizen Lab ha scoperto che 1.100 attivisti e giornalisti dell'Emirato erano stati presi di mira allo stesso modo e che per questi attacchi il governo aveva pagato al gruppo NSO 600.000 dollari.

2017

Nel febbraio 2017, Citizen Lab ha rivelato che Pegasus era stato utilizzato per colpire degli attivisti messicani che cercavano di contrastare l'obesità infantile. Il *malware* aveva accesso ai loro telefoni quando aprivano i link con testi che dicevano, ad esempio, "Mentre stai lavorando, sto fottendo la tua vecchia, ecco una foto" e "[tua figlia] ha appena avuto un grave incidente… ecco dove è ricoverata".

Nello stesso anno, il *New York Times* ha riferito che i telefoni di attivisti politici messicani per i diritti umani e anticorruzione, che stavano indagando su possibili crimini commessi dal governo e dai

suoi agenti, erano stati infettati da Pegasus. Il *NYT* ha affermato che le vittime hanno notato le intrusioni per la prima volta nell'estate del 2016.

Il governo messicano ha negato ogni responsabilità in merito allo spionaggio.

2018

Nell'agosto 2018 Amnesty International ha affermato che uno dei membri del suo personale, così come molti sauditi difensori dei diritti umani, erano stati presi di mira con il software Pegasus, utilizzando messaggi di testo con link che dicevano, ad esempio:

"Puoi per favore coprire [la protesta] davanti all'ambasciata saudita a Washington per i fratelli detenuti in Arabia Saudita? Mio fratello sta facendo il Ramadan e io sono qui con una borsa di studio, quindi per favore non taggarmi".

Quando Amnesty ha collegato lo spionaggio alla NSO, l'azienda ha risposto: "Il nostro prodotto è destinato esclusivamente alle indagini e alla prevenzione di crimini e terrorismo. Qualsiasi utilizzo della nostra tecnologia contrario a tale scopo costituisce una violazione delle nostre politiche, dei contratti legali e dei nostri valori come azienda".

In seguito Amnesty ha affermato che alla luce dell'attacco informatico stava considerando un'azione legale per costringere il ministero della Difesa israeliano a revocare la licenza di esportazione a NSO.

Nello stesso mese di agosto, il *New York Times* ha riferito che NSO stava affrontando due cause legali con l'accusa di aver partecipato attivamente allo spionaggio illegale.

Il giornale affermava che le cause, intentate da un cittadino del Qatar e da giornalisti e attivisti messicani, erano state depositate in Israele e a Cipro, e che i documenti presentati a sostegno delle accuse dimostravano che gli Emirati Arabi Uniti avevano utilizzato lo

spyware Pegasus per almeno un anno.

Secondo il *NYT*, gli Emirati avevano intercettato i telefoni dell'emiro del Qatar, di un caporedattore di un giornale con sede a Londra e di un potente principe saudita. Gli Emirati Arabi Uniti, insieme al Bahrain e all'Arabia Saudita, erano a quel tempo coinvolti in una disputa con il Qatar che portò il trio a imporre un blocco terrestre e marittimo contro il loro vicino.

Nell'ottobre 2018 Citizen Lab ha dichiarato che il software Pegasus aveva attaccato il telefono di un caro amico di Jamal Khashoggi, Omar Abdulaziz, prima dell'omicidio del dissidente e che il software aveva preso di mira difensori dei diritti umani in Bahrain, negli Emirati Arabi Uniti e altrove.

Lo stesso mese l'informatore statunitense Edward Snowden aveva affermato che Pegasus era stato utilizzato dalle autorità saudite per sorvegliare Khashoggi prima della sua morte.

"Sono il peggio del peggio", ha detto Snowden dell'azienda. NSO nega che la sua tecnologia sia stata "in alcun modo" utilizzata per l'omicidio.

Sempre a ottobre, Citizen Lab ha affermato che i suoi stessi ricercatori erano stati presi di mira da agenti collegati alla NSO. La NSO ha negato le accuse.

A novembre *Haaretz* ha riferito che nell'estate del 2017 NSO aveva firmato un accordo con l'intelligence saudita.

Rispondendo ad *Haaretz*, NSO ha affermato che "ha operato e opera esclusivamente in conformità con le leggi sull'esportazione della difesa e secondo le linee guida e la stretta supervisione di tutti i componenti dell'establishment della Difesa [israeliana, ndtr.], comprese tutte le questioni relative alle politiche e alle licenze di esportazione. Le informazioni fornite da *Haaretz* sull'azienda, sui suoi prodotti e sul loro utilizzo sono errate, basate su voci e pettegolezzi di parte. Il quadro distorce la realtà".

Poi, secondo quanto riportato dal *New York Times*, a dicembre Abdulaziz ha intentato una causa contro NSO, sostenendo che la società aveva aiutato i sauditi a spiare le sue comunicazioni con Khashoggi.

Il Gruppo NSO ha affermato ancora una volta che la sua tecnologia è stata "concessa su licenza al solo scopo di fornire ai governi e alle forze dell'ordine la capacità di combattere legalmente il terrorismo e la criminalità".

I contratti per l'utilizzo del software, ha aggiunto, "vengono forniti solo dopo un completo controllo e previa autorizzazione da parte del governo israeliano", ha affermato NSO.

"Non tolleriamo un uso improprio dei nostri prodotti. Se c'è il sospetto di un uso improprio, indaghiamo e intraprendiamo le azioni necessarie, inclusa la sospensione o la risoluzione del contratto", ha aggiunto.

L'amministratore delegato della società, Shalev Hulio ha affermato in seguito che NSO non era stata coinvolta nel "terribile omicidio", ma non ha risposto in merito alla segnalazione secondo cui Hulio era andato personalmente a Riyadh per vendere il software Pegasus ai sauditi.

2019

Nel febbraio 2019, una società di *private equity* [che apporta nuovi capitali a una società come investimento finanziario, ndtr.] ha acquistato lo *spyware* NSO e ha dichiarato a Citizen Lab di essere "impegnata ad aiutarla a diventare più trasparente in merito alla sua attività".

E ad aprile, secondo quanto riferito, l'azienda ha congelato dei nuovi accordi con l'Arabia Saudita.

A maggio, Amnesty ha affermato che avrebbe presentato una petizione legale al tribunale distrettuale di Tel Aviv per bloccare le licenze di esportazione di NSO, e uno scrittore satirico saudita che

vive in esilio a Londra ha intentato un'azione legale contro l'Arabia Saudita, accusando il Paese di aver utilizzato lo spyware Pegasus per ottenere informazioni personali dal suo telefono.

Lo stesso mese un'indagine del *Financial Times* ha rivelato che dei malintenzionati stavano sfruttando la funzione di chiamata di WhatsApp telefonando alle vittime per diffondere Pegasus.

"In nessun caso NSO è stata coinvolta nell'operazione o nell'identificazione degli obiettivi della sua tecnologia, che è gestita esclusivamente da agenzie di intelligence e forze dell'ordine", ha risposto la società al *FT*. "NSO non avrebbe, o non potrebbe, utilizzare il software in proprio per prendere di mira qualsiasi persona o organizzazione".

Nell'ottobre dello stesso anno WhatsApp, di proprietà di Facebook, ha intentato una causa contro il gruppo NSO accusandolo di aver cercato illegalmente di sorvegliare giornalisti, attivisti per i diritti umani e altri in 20 Paesi tra cui Messico, Emirati Arabi Uniti e Bahrain.

L'azione legale, intentata in California presso un tribunale federale degli Stati Uniti, accusava il gruppo NSO di aver cercato di infettare circa 1.400 "dispositivi bersaglio" con *spyware* ostile che potrebbe essere utilizzato per rubare informazioni agli utenti di WhatsApp.

"Contestiamo recisamente le accuse odierne e le combatteremo con forza", ha affermato il gruppo NSO in una nota.

"L'unico scopo di NSO è fornire tecnologia all'intelligence governativa autorizzata e alle forze dell'ordine per aiutarli a combattere il terrorismo e gravi forme di criminalità".

Un mese prima, a settembre, NSO aveva messo a punto una politica dei diritti umani, affermando che avrebbe rispettato i principi guida delle Nazioni Unite.

A novembre, un gruppo di dipendenti di NSO ha intentato una causa contro Facebook, affermando che il gigante dei social media aveva

bloccato ingiustamente i loro account privati quando aveva fatto causa a NSO il mese prima, accusando Facebook di “punizione collettiva”.

Il giorno prima, intervenendo a una conferenza sulla tecnologia a Tel Aviv, il presidente della NSO Shiri Dolev aveva difeso la sua azienda, affermando che le tecnologie NSO hanno reso il mondo più sicuro.

Dolev ha anche affermato di auspicare che NSO possa parlare apertamente del ruolo che svolge nell’aiutare le forze dell’ordine a catturare i terroristi.

“Terroristi e criminali usano le piattaforme e le app dei social che usiamo tutti noi ogni giorno”, ha detto.

2020

Nel gennaio 2020 un giudice israeliano ha ordinato a NSO di affrontare la denuncia di pirateria informatica intentata contro il Gruppo dall’attivista saudita Omar Abdulaziz e di pagare le sue spese legali, e un tribunale ha stabilito che la causa legale di Amnesty per impedire a NSO di esportare il suo software si sarebbe dibattuta a porte chiuse.

Lo stesso mese Reuters ha riferito che almeno dal 2017 l’FBI stava indagando su NSO riguardo al suo possibile coinvolgimento in un attacco informatico contro cittadini e società statunitensi, nonché per una sospetta raccolta di informazioni nei confronti di governi.

La società ha affermato di non essere a conoscenza di alcuna inchiesta.

Secondo *The Guardian* ad aprile i documenti del tribunale relativi al caso WhatsApp dimostravano come NSO avesse negato ogni responsabilità per come era stata utilizzata la sua tecnologia, affermando che WhatsApp aveva “confuso” le azioni di NSO con quelle dei suoi “clienti sovrani”.

“I governi clienti agiscono prendendo tutte le decisioni su come

utilizzare la tecnologia", ha affermato la società. "Se qualcuno ha installato Pegasus su un qualche presunto 'dispositivo bersaglio' non sono stati gli imputati [Gruppo NSO] a farlo. Sarebbe stato un ente di un governo sovrano".

"Il Gruppo NSO non gestisce il software Pegasus per i suoi clienti", ha detto a *The Guardian*.

A giugno, un'indagine di Amnesty International ha rivelato che lo *spyware* della NSO era stato utilizzato contro il noto giornalista marocchino e difensore dei diritti umani Omar Radi.

Il rapporto di Amnesty afferma che l'attacco a Radi era avvenuto tre giorni dopo l'annuncio della nuova politica dei diritti umani della NSO.

In risposta, NSO ha dichiarato di essere "profondamente turbata" dalle accuse e che avrebbe immediatamente avviato un'indagine.

"Coerentemente con la propria politica dei diritti umani, il Gruppo NSO considera seriamente la responsabilità di rispettare i diritti umani ed è fortemente impegnata a evitare di causare, contribuire o essere direttamente collegata a effetti negativi sui diritti umani", ha affermato NSO in una nota.

Comunque la società ha preso le distanze dall'accusa di avere legami con le autorità marocchine e ha affermato che, per la natura della sua attività, deve salvaguardare la riservatezza dei suoi clienti.

"Siamo obbligati a rispettare gli interessi di riservatezza degli Stati e non possiamo rivelare l'identità dei clienti", ha affermato NSO.

Martedì Radi è stato condannato a sei anni di carcere per aggressione sessuale e spionaggio, accuse che lui nega.

Nel luglio 2020, un tribunale di Tel Aviv ha respinto la petizione di Amnesty e 30 attivisti per i diritti umani che chiedevano di revocare la licenza di esportazione al gruppo NSO, affermando che non avevano fornito prove del fatto che il software Pegasus fosse stato utilizzato per spiare gli attivisti della ONG britannica.

Le indagini di luglio e agosto hanno rivelato che il software Pegasus era stato utilizzato per spiare politici catalani in Spagna e sacerdoti in Togo.

A dicembre Citizen Lab ha riferito che dozzine di giornalisti dell'agenzia di stampa *Al Jazeera*, finanziata dal Qatar, sono stati presi di mira con un attacco di Pegasus tramite iMessage, attacchi probabilmente collegati ai governi dell'Arabia Saudita e degli Emirati Arabi Uniti.

Un giornalista di *Al Jazeera* ha detto di aver ricevuto minacce di morte sul suo telefono: "Hanno minacciato di farmi diventare il nuovo Jamal Khashoggi".

In una dichiarazione il gruppo NSO ha messo in dubbio le accuse di Citizen Lab, ma ha affermato di "non essere in grado di commentare un rapporto che non abbiamo ancora visto".

L'azienda ha affermato di fornire software al solo scopo di consentire "alle forze dell'ordine governative di affrontare la criminalità organizzata e l'antiterrorismo".

All'inizio di quel mese, una conduttrice televisiva di *Al Jazeera* ha intentato un'altra causa negli Stati Uniti, sostenendo che il gruppo NSO ha hackerato il suo telefono tramite WhatsApp a causa delle sue critiche al potente principe ereditario dell'Arabia Saudita Mohammed bin Salman.

A dicembre, una coalizione di associazioni per i diritti umani, tra cui il gruppo per i diritti sulla rete Access Now, Amnesty International, il Comitato per la Protezione dei Giornalisti e Reporter senza Frontiere, si è unita alla lotta legale di Facebook contro NSO, sostenendo che la società dà la priorità ai profitti rispetto ai diritti umani, facendo seguito a un'azione simile promossa da una serie di grandi aziende tecnologiche tra cui Google e Microsoft.

2021

A marzo *The Guardian* ha riferito che il Dipartimento di Giustizia degli

Stati Uniti ha ripreso le indagini sul gruppo NSO, dopo mesi in cui le principali società tecnologiche statunitensi andavano affermando che l'azienda israeliana è "potente e pericolosa" e non dovrebbe avere l'immunità per il suo ruolo nelle operazioni di pirateria informatica.

Il *Guardian* ha riferito che all'inizio del 2020 il gruppo NSO era stato oggetto di un'indagine dell'FBI, che però sembrava essersi arenata e il Dipartimento di Giustizia stava ora mostrando un nuovo interesse per il caso.

A luglio, un'indagine condotta da Forbidden Stories e Amnesty International ha rivelato che i telefoni di migliaia di giornalisti, attivisti e funzionari sono stati presi di mira o violati utilizzando Pegasus.

In risposta, NSO ha respinto le "false affermazioni", ha definito le accuse "teorie non provate" e parte di una "narrazione oscena... strategicamente inventata da diversi gruppi di interessi specifici strettamente allineati".

"Le tecnologie vengono utilizzate ogni giorno anche per spezzare i circuiti di pedofilia, sesso e traffico di droga, individuare i bambini scomparsi e rapiti e i sopravvissuti intrappolati sotto edifici crollati e proteggere lo spazio aereo dalla dannosa penetrazione di pericolosi droni", ha aggiunto.

"In parole povere, NSO ha una missione salvavita e la società proseguirà imperterrita ad adempiere a questa missione, nonostante i continui tentativi di screditarla su false basi ".

"Nonostante quanto sopra", ha aggiunto, "NSO continuerà a indagare su tutte le affermazioni credibili di un uso scorretto e a intraprendere azioni appropriate in base ai risultati di quelle indagini".

(traduzione dall'inglese di Luciana Galliano)

Tribunale israeliano consente alla NSO di continuare a vendere tecnologia per lo spionaggio ai governi autoritari

13 lug 2020 – Al Jazeera

Amnesty afferma che il sistema di spionaggio tecnologico Pegasus viene utilizzato dai governi repressivi per colpire attivisti e giornalisti a favore dei diritti umani.

Un tribunale israeliano ha respinto la richiesta di togliere alla controversa società israeliana di tecnologia per lo spionaggio NSO Group la licenza di esportazione per sospetto uso della tecnologia dell'azienda ai danni di giornalisti e dissidenti in tutto il mondo.

L'istanza legale, presentata da Amnesty International a gennaio, richiedeva al tribunale di impedire a NSO di vendere la sua tecnologia all'estero, in particolare a governi repressivi.

Il tribunale del distretto di Tel Aviv ha stabilito che gli avvocati di Amnesty non hanno fornito prove sufficienti "per dimostrare l'affermazione che fosse stato fatto un tentativo di rintracciare un attivista per i diritti umani cercando di hackerare il suo cellulare" o che l'hackeraggio fosse stato effettuato da NSO.

"La concessione di una licenza viene effettuata dopo un'indagine estremamente rigorosa e anche dopo la concessione dell'autorizzazione le autorità conducono dei controlli e rigorose indagini, se necessario", ha affermato il tribunale. In caso di violazione dei diritti umani, ha aggiunto, tale permesso può essere sospeso o annullato.

Il tribunale ha emesso la sentenza domenica, ma l'ha resa pubblica solo lunedì.

Gil Naveh, portavoce di Amnesty International Israel, ha dichiarato che l'organizzazione è rimasta delusa ma non sorpresa.

"È una tradizione di lunga data da parte dei tribunali israeliani avvallare burocraticamente le decisioni del Ministero della Difesa israeliano", ha detto.

L'organizzazione non è a conoscenza delle prove fornite dalla NSO o dal Ministero della Difesa alla corte, perché le udienze si sono tenute a porte chiuse. "Anche se lo sapessimo, non potremmo parlarne", ha detto.

Nel 2018 Amnesty ha denunciato che uno dei suoi dipendenti è stato preso di mira dal sistema di spionaggio di NSO, affermando che un hacker ha cercato di penetrare nello smartphone del membro dello staff usando come esca un messaggio su WhatsApp riguardante una protesta davanti all'ambasciata saudita a Washington.

NSO, una società israeliana di noleggio hacker, utilizza il suo sistema di spionaggio Pegasus per prendere il controllo di un telefono, delle sue videocamere e dei suoi microfoni e per ricavarne i dati personali dell'utente.

L'azienda è stata accusata di vendere il suo software di sorveglianza a governi repressivi che lo usano contro i dissidenti. La clientela non viene rivelata, ma si ritiene che includa Stati mediorientali e latinoamericani. La società ha dichiarato di vendere la propria tecnologia ai governi approvati da Israele per aiutarli a combattere criminalità e terrorismo.

NSO Group ha affermato in una dichiarazione che la società "continuerà a lavorare per fornire tecnologia agli Stati e alle organizzazioni di intelligence", aggiungendo che il suo scopo è "salvare vite umane".

In un rapporto pubblicato il mese scorso Amnesty International ha affermato che il telefono del giornalista marocchino Omar Radi è stato violato con l'uso della tecnologia dell'NSO nell'ambito degli sforzi del governo per reprimere il dissenso.

Un dissidente saudita ha accusato l'NSO di essere coinvolta nell'omicidio del giornalista saudita Jamal Khashoggi nel 2018.

(traduzione dall'inglese di Aldo Lotta)

Nel 2019 la censura delle IDF ha cancellato duemila notizie

Haggai Matar

March 9, 2020 – +972

Secondo dati ufficiali, la censura militare israeliana ha vietato del tutto la pubblicazione di oltre 200 articoli e ne ha parzialmente censurati altri 2.000.

Il 2019 è stato un anno di relativa calma per la censura delle IDF [Forze di Difesa Israeliane, l'esercito israeliano, ndtr.]. Secondo i dati ufficiali forniti lo scorso mese a +972 Magazine, Local Call [edizione di +972 in ebraico, ndtr.] e al Movimento per la Libertà di Informazione in seguito a una richiesta in base alla legge sulla libertà di informazione, il censore ha vietato del tutto la pubblicazione di 202 articoli sui mezzi di comunicazione e ne ha in parte censurati altri 1.973.

Rispetto ai dati che avevamo raccolto dal 2011, lo scorso anno ha visto il minor numero di censure dirette di mezzi di informazione dell'ultimo decennio.

In Israele a tutti i mezzi di comunicazione viene richiesto di sottoporre articoli relativi alla sicurezza ed alla politica estera alla censura delle IDF per un controllo prima della pubblicazione. Il censore ricava la sua autorità dalle "regole d'emergenza" emanate dopo la fondazione di Israele e che sono rimaste in vigore fino ad oggi.

Queste norme consentono al censore di cancellare totalmente o parzialmente un articolo, impedendo al contempo ai mezzi di comunicazione di indicare in qualche modo se un articolo è stato modificato. Tuttavia, mentre i criteri giuridici che definiscono la competenza della censura delle IDF sono sia stringenti che piuttosto ampi, la decisione di quali articoli sottomettere al controllo dipende dalla discrezionalità dei direttori dei mezzi di comunicazione.

La riduzione dell'intervento della censura militare nel 2019 è ancora più evidente se confrontata al 2018, l'anno di punta degli interventi censori. Quell'anno ha

visto 363 notizie di cui è stata vietata la pubblicazione (circa una al giorno), mentre altre 2.712 sono state parzialmente censurate.

La contrazione dell'ampiezza della censura è stata anche accompagnata da un calo del numero di materiale presentato al censore dai mezzi di comunicazione. Nel 2019 le pubblicazioni hanno sottoposto 8.127 notizie al controllo della censura – circa il 25% in meno dell'anno precedente – che di per sé è stato un numero relativamente basso.

Eppure, persino in un anno "fiacco", ciò significa che ci sono oltre 200 articoli che i giornalisti hanno considerato degni di nota ma che non hanno potuto rendere pubblici e più di 2.000 articoli che hanno subito un certo tipo di interferenza esterna.

Si tratta ancora di un grande numero, considerando che nessun altro Paese al mondo che si definisca una democrazia impone un simile obbligo ai giornalisti di ricevere l'approvazione ufficiale del governo prima della pubblicazione. Dal 2011 2.863 articoli sono stati eliminati dalla censura e 21.683 sono stati censurati.

Ovviamente la censura militare non condivide informazioni sulla natura delle notizie che nasconde all'opinione pubblica né stila un rapporto mensile di queste attività. Ciò rende ancora più difficile capire perché quest'anno ci sia un simile calo degli interventi censori.

Nel nostro rapporto sul 2018 abbiamo ipotizzato che il picco della censura potesse essere in rapporto con gli attacchi aerei israeliani in Siria e in Libano. Nel 2019 tuttavia i politici israeliani, soprattutto nel periodo delle elezioni di aprile e di settembre, si sono vantati di aver intrapreso tali azioni militari. Questo aspetto pubblico potrebbe fornire una sorta di spiegazione.

"I dati che abbiamo visto un anno dopo l'altro indicano un fenomeno complesso e problematico," afferma Or Sadan, un giurista del Movimento per la Libertà di Informazione, che guida anche il "Centro per la Libertà d'informazione" alla Scuola di gestione in Israele. "Il censore militare impedisce letteralmente al pubblico di avere a disposizione molte informazioni che i mezzi di comunicazione avevano ritenuto valesse la pena raccontare. La stampa libera è uno strumento con cui il pubblico viene a conoscenza degli sviluppi nel Paese, anche su argomenti legati alla sicurezza."

“A dispetto degli aspetti sensibili per la sicurezza,” continua Sadan, “gli organi competenti devono ridurre al minimo possibile i casi in cui l’informazione è oscurata dalla censura e solo in casi estremi, quando c’è un reale timore per la sicurezza nazionale. Continueremo a monitorare questi dati per capirne gli sviluppi nel corso degli anni.”

Un altro aspetto del lavoro del censore sono i suoi interventi negli archivi nazionali israeliani. Da quando gli archivi sono stati messi totalmente in rete e non hanno più una biblioteca fisica aperta al pubblico, il censore militare ha controllato tutto il materiale declassificato, che l’ha a volte portato a nascondere documenti che erano già stati resi pubblici.

Quando nel 2016 è iniziata la digitalizzazione degli archivi, le autorità archivistiche hanno sottoposto al controllo del censore circa 7.800 documenti. A differenza degli articoli, il censore si è rifiutato di informarci su quanto materiale d’archivio sia stato censurato, rispondendo solo che “la grande maggioranza dei documenti è stata approvata per la pubblicazione senza modifiche.”

La crescente mancanza di trasparenza della censura militare è di per sé una causa di preoccupazione. Il censore è totalmente esente dalla legge israeliana sulla libertà d’informazione, e, benché negli ultimi anni si sia offerto volontariamente di rispondere alle domande di +972, le sue risposte nel corso dell’anno si stanno riducendo.

Nelle prime reazioni alle nostre richieste, nel 2016, il censore ha reso pubblico il numero dei documenti di archivio che sono stati censurati e il numero di casi in cui il censore ha chiesto che i mezzi di comunicazione eliminassero informazioni pubblicate senza la precedente approvazione (una media di 250 casi all’anno). Nonostante ripetuti tentativi, negli ultimi anni questi dati non ci sono stati forniti.

Nell’ultima risposta del censore, datata febbraio 2020, non abbiamo neppure ricevuto informazioni sul numero di libri censurati dal censore, un numero che in precedenza era arrivato a varie decine all’anno.

La direttrice della censura militare, generalessa di brigata Ariella Ben-Avraham, nelle prossime settimane darà le dimissioni dal suo incarico, prima del previsto. Secondo varie notizie dei media, andrà a far parte del gruppo israeliano “NSO”, un’impresa informatica che produce materiale spionistico ed è stata associata ai tentativi di molte dittature di spiare giornalisti e difensori dei diritti umani.

Durante il suo primo anno come dirigente della censura, Ben-Avraham ha esteso la sua giurisdizione dai principali mezzi d'informazione alle reti sociali e agli organi d'informazione indipendenti, compreso +972Magazine, chiedendo che sottoponessero alla censura articoli per l'approvazione. Ben-Avraham ha anche deciso di smettere di rispondere alle nostre domande sul numero di volte in cui il censore ha attivamente eliminato articoli che erano già stati pubblicati.

Haggai Matar è un pluripremiato giornalista israeliano e un attivista politico, oltre ad essere direttore esecutivo di "+972 – Promozione del giornalismo dei cittadini", l'associazione no-profit che pubblica +972 Magazine.

(traduzione dall'inglese di Amedeo Rossi)

Scienza, guerra, società. Secondo incontro. 5 febbraio, incontro con Jeff Halper

13 febbraio 2020 – Scienceground

Genova, 5 febbraio 2020. Incontro con Jeff Halper, antropologo e attivista pacifista [americano che vive] in Israele, autore di "War against the people" Pluto press, 2015 ["La guerra contro il popolo", trad. it. Ester Garau, Ed. Epoké, 2017, ndt]

La guerra come questione internazionale

Questo libro deriva dal mio lavoro su Palestina e Israele. Sono un attivista da molti anni. Sono il presidente di un'organizzazione chiamata Israeli Committee Against House Demolitions [Comitato israeliano contro la demolizione delle case, ndt]. Cerchiamo di combattere la politica israeliana di demolizione delle case palestinesi. E la domanda che sorge spontanea ogni volta è: come fa Israele a passarla liscia? Perché il mondo permette a Israele di mantenere l'occupazione da

oltre cinquant'anni, di violare il diritto internazionale, di reprimere un intero popolo? Non solo [il mondo] glielo permette, ma Israele ottiene sempre più sostegno internazionale, il suo status è in costante miglioramento all'interno della comunità internazionale.

La gente si dà ogni tipo di spiegazione, per esempio la potente lobby ebraica negli Stati Uniti. Ma questo non spiega il sostegno italiano a Israele. E non spiega il sostegno a Israele da parte di Paesi in cui non ci sono ebrei: oggi India e Cina sono due tra i più forti sostenitori di Israele nella comunità internazionale.

C'è poi l'idea del senso di colpa per l'Olocausto. Questo può avere forse un peso, fino a un certo punto, in Germania, o in Polonia e negli Stati Uniti, ma non in America Latina, dove Israele oggi ha un sostegno enorme: è il primo Paese non latinoamericano a far parte del mercato latinoamericano. Un'altra spiegazione potrebbe essere costituita dai fondamentalisti cristiani: gli evangelici, i cristiani di destra: di nuovo, è un elemento importante negli Stati Uniti, ma non ha molta importanza in altri Paesi che continuano a sostenere Israele. Quindi era un aspetto difficile da spiegare. Secondo me, per trovare il bandolo della matassa bisogna focalizzarsi sulla domanda: qual è il ruolo di Israele nel mondo? In altre parole, noi consideriamo sempre Israele per ciò che sta facendo ai palestinesi: le demolizioni, il muro, le colonie, ecc. Non capita spesso di analizzare il suo ruolo internazionale.

Appena ho iniziato a farlo, è apparso molto chiaro che Israele ha un ruolo chiave nelle funzioni di polizia militare di sicurezza del sistema mondiale.

È interessante notare che non esistono molti studi sul ruolo della guerra e della sicurezza nelle questioni internazionali, mentre ce ne sono molti sulle ragioni della guerra e sulla storia della guerra. Ci sono studi sulle tecnologie militari. Ma quale ruolo giochi la guerra – e non solo la guerra, ma anche la sicurezza – nella politica internazionale non è sufficientemente approfondito. Per esempio, Marx quasi non nomina neppure la guerra. Immanuel Wallerstein, nella sua teoria del moderno sistema-mondo, non sfiora nemmeno il tema della guerra. La guerra è vista come disgregante, come una brutta cosa, ma mai come parte integrante del modo in cui gira il mondo.

Quindi ho voluto vedere qual è il ruolo della guerra e della sicurezza nel mondo moderno. Ho provato a inserire il mio lavoro nella cornice del capitalismo

transnazionale perché per la prima volta, forse dagli anni ‘70 del 1800, si inizia ad avere un sistema mondiale. In particolare con la fine della Guerra Fredda e con la nascita del neoliberismo e del capitalismo mondiale. E di sicuro, come ben sappiamo, il capitalismo globale è un bene per pochi, ma non per tutti.

Umanità eccedente e risorse

C’è questo concetto dell’eccesso, o eccedenza, di umanità. Risulta che l’80% della popolazione mondiale è umanità in eccesso. Il sistema capitalista non ha bisogno di questa gente. Non saranno mai consumatori in modo significativo. Non saranno mai davvero istruiti o produttivi nel senso capitalista di produttività. Sono superflui, sono in eccesso. L’80% della popolazione mondiale vive con meno di 10 dollari al giorno. Il 50% della popolazione mondiale vive con meno di 2 dollari al giorno. La stragrande maggioranza della popolazione non è in grado di provvedere al proprio sostentamento.

Il sistema [capitalista] non va molto d’accordo con questa gente, ma si tratta pur sempre dell’80% della popolazione, bisogna controllarla in qualche modo. Per esempio, sappiamo che l’economia mondiale è per lo più concentrata nelle mani di specifiche imprese e società e gente ricca, circa 147 aziende – ce n’è anche qualcuna italiana, da qualche parte – che controllano il 40% dell’economia mondiale.

Oggi abbiamo quelle che vengono definite “guerre per le risorse”. Le guerre oggi sono meno guerre per l‘ideologia e più guerre per le risorse, perché le risorse sono sempre più scarse – e ovviamente la maggior parte delle risorse mondiali confluiscono nel Nord del mondo – ed ecco il motivo di lotte tremende: acqua, minerali, legno e, ovviamente, petrolio. Secondo Michael Klare [professore di studi universitari sulla pace e sulla sicurezza del Five College, corrispondente della difesa della rivista The Nation, ndt] c’è una fascia lungo l’Equatore in cui si trovano alcune delle più importanti risorse del mondo. In altre parole, i più poveri del mondo vivono dove sono concentrate le risorse più preziose. Il sistema mondiale è in gran parte basato sulla sottrazione di tali risorse a quei popoli, e conosciamo i conflitti che ne derivano in quell’area.

Il sistema capitalista quindi ha un problema, e il problema è che solo una piccola percentuale dell’umanità ne trae beneficio, mentre la maggioranza è esclusa. Il

che comprende anche la classe media, come in Italia e in Europa. I giovani della classe media del Nord del mondo stanno diventando sempre più marginali per il mercato del lavoro: i sindacati si stanno indebolendo, c'è il modello economico di McDonald, in cui la gente viene assunta solo temporaneamente, i giovani non guadagnano abbastanza per vivere, non riescono a trovare una casa, ecc. Quindi non è solo una questione di "Terzo mondo" o di Sud del mondo, ma è qualcosa che sta succedendo in realtà anche nel Nord del mondo.

Guerre securocratiche esterne

E qui il problema diventa: in che modo il sistema capitalista si garantisce l'egemonia?

Perché c'è un'egemonia sul sistema mondiale. Non è che possiamo controllare tutto, non è che andiamo lì e conquistiamo. Non come Hitler, che voleva conquistare qualsiasi cosa per controllarla. Qui non c'è da conquistare: bisogna aumentare la propria egemonia sul mondo in un modo più politico, economico e culturale, per avere il controllo. Ma il problema è che la gente che viene esclusa dal sistema resiste sempre di più.

Quindi quel che abbiamo è ciò che io chiamo una guerra contro il popolo. Da altri è stata chiamata "guerra quotidiana" o "guerra permanente". Di sicuro è una guerra securocratica, questo è il termine che uso io. È una guerra per la sicurezza.

Non mi riferisco, in realtà, alla guerra come siamo abituati a immaginarla. Le guerre tra potenze, di solito condotte con eserciti che combattono battaglie e una parte vince. Le guerre convenzionali tra Stati appartengono al passato. L'ultima grande guerra tra Stati nella quale due o più grandi potenze si sono combattute è stata la Seconda Guerra Mondiale. Forse la [guerra di] Corea, in un certo senso. Ma tutte le altre guerre tra Stati, anche se hanno avuto un numero di morti non certo esiguo, sono state "piccole" in quanto a episodi. Erano circoscritte: la guerra Iran-Iraq, le Falklands, le guerre arabo-israeliane, quelle tra la Georgia e la Russia, o con l'Ucraina.

È successo qualcosa tra gli Stati? Per prima cosa, le guerre di questo tipo non coinvolgono solo due superpotenze. A volte c'è una superpotenza e un Paese più piccolo, come ad esempio gli Stati Uniti e l'Iraq o gli Stati Uniti in Afghanistan. E,

secondo, sono molto circoscritte.

Quindi non sto parlando esattamente delle guerre convenzionali. Ma la guerra cronica per la sicurezza si realizza principalmente in due modi.

Primo: le guerre si combattono altrove, fuori dal proprio Paese. Ci sono molte definizioni: “guerre asimmetriche”, “guerre limitate”, “operazioni”. La prima guerra in Iraq è stata chiamata “operazione Desert Storm [Tempesta nel Deserto, ndt]”. Spesso non vengono nemmeno dichiarate. Le guerre vere, o tra Stati, di solito vengono dichiarate. Ci sono delle regole d’ingaggio. Ma oggi le guerre non vengono quasi mai dichiarate. Le “guerre di guerriglia’, “guerre sporche”, “piccole guerre”. A volte sono definite “guerre coloniali”, “conflitto”. O “conflitti a bassa intensità”: ciò significa che ci può essere una guerra senza le regole della guerra, relativamente ai prigionieri, per esempio. Non si è limitati dalle regole del diritto internazionale. “Operazioni militari”, “contro-insurrezione”, “guerra a bassa intensità”, “antiterrorismo”.

Tutte queste sono tipologie di guerra che si combattono fuori dal Primo Mondo, di solito tra grandi potenze in Paesi o aree in cui ci sono le risorse di cui si ha bisogno. E si domano le popolazioni, si creano le condizioni per estrarre le risorse, avendo a disposizione una popolazione schiava per il lavoro a basso costo. Queste sono le guerre securocratiche che rafforzano l’egemonia del capitalismo delle multinazionali in tutto il mondo.

Oggi abbiamo a disposizione tipologie di armi che sono immediate, siano esse droni o altri tipi di robot, hanno la capacità di risposta immediata ovunque nel mondo. Le definisco securocratiche perché l’idea non è di vincere, né di colpire l’altra parte. Non c’è nessuna ideologia qui. L’idea è di creare le condizioni di controllo ed egemonia, per sempre. A tempo indefinito.

Guerre securocratiche interne

Il secondo tipo di guerra si svolge all’interno, come qui in Italia. Una volta, nel Nord del mondo, esisteva una separazione tra le istituzioni militari e quelle di sicurezza interna, per esempio le forze di polizia. L’esercito all’esterno e le forze nazionali all’interno, e non si parlavano molto tra loro. Questo deriva dall’idea di Stato in Occidente: bisogna stare alla larga dagli affari interni di altri Paesi. Per esempio, negli Stati Uniti, la CIA non è autorizzata a parlare con l’FBI, se non

attraverso determinati canali. Non ci si aspetta che le forze militari interagiscano con le forze di polizia, ma di sicuro, dopo l'11 settembre, queste differenze hanno iniziato ad essere meno nitide, e l'esercito, la sicurezza interna e la polizia sono diventate una cosa sola.

Quindi quello che succede oggi nelle guerre securocratiche è che i militari stanno diventando come le forze di polizia. I militari americani in Iraq o Afghanistan non stanno più, in realtà, combattendo battaglie. Sono forze di polizia. Si tratta, in parte, di addestramento, in parte mantengono l'ordine e in parte portano avanti operazioni di peacekeeping, che è un'altra forma securitaria dell'ONU. Quindi l'esercito si sta "poliziottizzando": agisce come una forza di polizia.

Ma nello stesso tempo le forze di polizia del vostro Paese si stanno militarizzando. Stanno iniziando ad indossare divise e a portare armi e a fare cose che, solo una generazione fa, non erano considerate di competenza della polizia.

Quindi sta avvenendo la militarizzazione della polizia e la poliziottizzazione dell'esercito. Ecco che tutto inizia a quadrare. La guerra securocratica interna ha a che fare con la sicurezza interna: antiterrorismo, di nuovo. Pensate alla "guerra alla droga". Alla "lotta al crimine". Al "contrasto all'immigrazione". Queste metafore vengono utilizzate perché queste cose minacciano il controllo interno delle multinazionali su un Paese. E quindi si arriva a cose come la disciplina, le prigioni, a quello che viene definito complesso dell'industria carceraria.

Cosa si fa in un Paese come l'Italia, in cui molti giovani – non solo immigrati – non hanno un futuro assicurato? O in Europa in generale?

Questa è la guerra securocratica per rafforzare l'egemonia nel sistema capitalistico in cui la maggior parte delle persone sono escluse. Questo è il ruolo della guerra oggi. La chiamo guerra contro il popolo. Diversa da una guerra come la Seconda Guerra mondiale. È così che l'ho concettualizzata.

Tecnologia bellica

In tutto ciò, Israele ha un ruolo chiave. Non affronterò l'argomento Israele. Ma Israele ha un ruolo chiave in tutto questo. Perché Israele è un Paese che ricopre una posizione fondamentale. Israele sta combattendo una guerra contro il popolo palestinese da cent'anni. Quindi ha più esperienza.

L’Europa ha combattuto le guerre coloniali. Cosa che è finita molto tempo fa, forse 60-70 anni fa, o più. L’Italia è stata in Etiopia e in Libia per un po’. Ma l’Europa non ha tutta quell’esperienza. E neanche gli Stati Uniti ce l’hanno. L’ultima volta che gli Stati Uniti hanno avuto a che fare con quel genere di guerra è stato in Vietnam, e non è andata molto bene. E nemmeno oggi sta andando molto bene in Afghanistan.

Israele ha l’esperienza di una guerra interna, contro un altro popolo, ma contemporaneamente ha un’altissima capacità tecnologica. È in grado di sviluppare sistemi d’armi e di sicurezza, nonché tattiche e strategie, che altri Paesi trovano utili.

Ed è qui che trovo la risposta: come fa Israele a farla franca? Perché altri Paesi usano queste tecnologie!

Inclusa la Cina, dove la tecnologia israeliana viene impiegata contro gli uiguri [minoranza di religione musulmana che vive nella regione dello Kinjiang, nel nord ovest della Cina, ndt]. Israele ha uno strettissimo legame con la Cina in tema di sicurezza. Dopo la Russia, Israele è il secondo fornitore di armi alla Cina. O l’India, che è oggi il più grande compratore di armi da Israele. È sorprendente, perché Israele non vende armi costose, carri armati e navi, e aerei da guerra. Non produce quel genere di armamenti, sono troppo costosi per Israele. Produce radar, sistemi di sicurezza e sorveglianza. E componenti per tali sistemi (se prendete i sistemi più piccoli, in quello Israele è il numero due dopo la Cina). Potete immaginare quanto è profonda l’infiltrazione della tecnologia israeliana nell’esercito cinese, nella sicurezza cinese, nella polizia cinese. Dopo la Russia, Israele è il secondo fornitore di armamenti all’India.

Così, la “piccola Israele” è il secondo fornitore di due delle più grandi Nazioni militarizzate del mondo. Specialmente per quanto riguarda i sistemi di sorveglianza con riconoscimento fisico e facciale. In Israele, c’è un’azienda che si chiama Nice Systems [Bei sistemi, ndt] – che nome! – che produce una tecnologia digitale in grado di captare chiunque attraverso le sole telecamere. Tutti hanno qualcosa di speciale. Altezza, peso, fisionomia, tutto. Alcuni sbattono le palpebre, o camminano zoppicando, o hanno un tic. Qualunque cosa sia (e il sistema si accorge di tutto!), con questo tipo di tecnologia digitale non è necessario riavvolgere e rivedere i filmati di milioni di individui. Si rilevano le caratteristiche e si identificano immediatamente le persone. Sono sistemi davvero sofisticati.

Israele esporta praticamente in ogni parte del mondo. Anche in Paesi con cui non intercorrono relazioni diplomatiche. Per esempio, Israele e Arabia Saudita. Di fatto, era nei notiziari proprio la settimana scorsa, il telefono usato da bin Salman per scovare Kashoggi a Istambul era dotato di sistemi di sorveglianza israeliani e di NSO [compagnia israeliana di cyber-sicurezza, i cui prodotti consentono – tra le altre cose – la sorveglianza remota degli smartphone, ndt]. Ha semplicemente usato quello stesso sistema per entrare nel telefono di Jeff Bezos [CEO di Amazon] e trovare i dati sulla sua vita sentimentale. Jeff Bezos ha divorziato, e le informazioni sulla relazione che stava portando avanti con quella donna sono uscite dal suo telefono, collegato a quello di bin Salman in Arabia Saudita attraverso una società israeliana.

Ci sono davvero di mezzo società israeliane. Non parlerò adesso di tutto questo, però commerciano con quasi tutti i Paesi del mondo. Ma in cosa è specializzato Israele, in particolare?

Una cosa sono i droni. Il 60% dei droni nel mondo sono israeliani. Infatti, la tecnologia per i droni prodotta in Europa e negli Stati Uniti è israeliana. Il drone Watchkeeper, che si sta sviluppando in Europa, è per il 51% di una società israeliana, la Elbit Systems. Una parte di esso viene dal Technion, il politecnico considerato il laboratorio dell'esercito israeliano e dell'industria della difesa.

È interessante capire come il concetto di guerra influisca sugli armamenti. La tecnologia dei droni è conosciuta da anni. C'erano perfino droni rudimentali nella Seconda Guerra Mondiale. Ma l'Europa e specialmente gli Stati Uniti avevano deciso che non avrebbero continuato a sviluppare i droni, perché questi sono molto vulnerabili. Cos'è un drone? È un aereo che sta fermo in un posto. Per giorni e settimane sorveglia semplicemente cosa succede. Questa è la sua funzione principale. In inglese, lo chiamiamo "facile preda". È molto semplice per l'aviazione, o anche per l'artiglieria, abbattere un drone. Gli Stati Uniti direbbero "Perché dovremmo avere uno stupido aereo che costa un miliardo di dollari se lo si può abbattere?"

Quindi non hanno mai approfondito questo tipo di tecnologia. Ma Israele sta combattendo una guerra diversa. Israele combatte una guerra contro i palestinesi, che non hanno un'aviazione e quindi non possono abbattere un drone israeliano. Per Israele i droni sono stati molto utili per quel tipo di guerriglia in cui si cerca di mantenere il controllo su tutti i movimenti e su tutto quel che

succede. Ecco perché Israele ha conquistato quel mercato: perché per le guerre contro il popolo queste sono armi eccezionali. Per le guerre convenzionali sono pessime, perché basta abbatterli. Il Pentagono si prepara ancora a combattere guerre convenzionali contro la Cina, contro l'Unione Sovietica. Stanno ancora sviluppando armamenti che sono inutili in un sistema di guerra asimmetrica. L'F-35, ultimo modello di stealth americano [velivolo invisibile ai radar, ndt], è inutile.

Un altro tipo di prodotto israeliano sono i muri e le barriere: stupidi muri ciechi di confine, ma anche muri intelligenti con sensori. Potete trovare muri israeliani in tutta Europa, per lo più contro gli immigrati. La maggior parte dei muri in Europa viene realizzata con tecnologia israeliana. C'è anche il muro sul confine tra Messico e Stati Uniti, che stanno costruendo insieme la Boeing e la Elbit Systems. Questa è un'intera tecnologia che Israele sta vendendo all'Europa e in altri luoghi, basata su sensori più che su muri fisici. Fuoco automatizzato, ma non ne parlerò.

La responsabilità dello scienziato

Sistemi di sorveglianza. La sorveglianza urbana è un'altra grande industria in Israele. Il concetto è che il più grande pericolo che minaccia lo Stato di polizia è il cosiddetto spazio di anonimato. Quando lo Stato non sa dove sei, non sa con chi stai parlando, con chi sei.

Sono cose molto pericolose. L'idea del sistema di sicurezza israeliano è di sapere tutto. Quindi Israele non solo esporta tecnologie per la guerra contro il popolo, ma anche sistemi di sorveglianza. Ce ne sono di tutti i tipi. Non parlerò adesso di tutti, ma ci sono i mini droni, che sembrano insetti o uccelli. Si trasformano in armi insetti veri. O si costruisce un insetto – che te ne pare come drone?!

Non solo, ma Israele è anche uno dei leader mondiali, con l'Italia, nel campo delle nanotecnologie. L'Italia è uno dei leader mondiali nelle nanotecnologie a scopo medico. Anche Grenoble e altri centri europei. Israele è uno dei leader mondiali in campo militare. Così ora hanno aperto un centro italo-israeliano di ricerca in nanotecnologie a Firenze. Non sono sicuro di tutto perché è tutto molto segreto. Questo è un drone [mostra l'immagine], una piccola zanzara. Queste sono le telecamere. La Elbit Systems produce obiettivi che vengono utilizzati nei satelliti, in grado di mostrarvi, dallo spazio, cosa c'è su questo tavolo.

Sono molto bravi in questo. Ma ecco quel che chiamiamo un becher con un ago. Con le nanotecnologie possiamo prendere una malattia come l'antrace, che non ha antidoto, che non può essere curata, e in questo piccolo contenitore possiamo metterne abbastanza da ammazzare oltre centinaia di migliaia di persone. Si potrebbe metterla nella rete idrica, o nelle persone, in modo da creare un virus contagioso come quello che c'è oggi in Cina. "Nano" è un miliardesimo di metro, la dimensione di una molecola. Oggi potete immaginare armi della dimensione di una molecola. Ecco il punto d'incontro con la prospettiva biomedica. Perché nano è così importante in medicina?

Non ho intenzione di tenere una lezione di medicina, ma il punto è che le nanotecnologie sono così piccole da poter essere introdotte nel sistema circolatorio e monitorare l'afflusso di sangue senza interferire con esso. Bene, oggi è possibile armarle, con malattie o spray. Abbiamo il sospetto, ma non possiamo provarlo, che Israele abbia usato queste armi a Gaza. Si può caricare il DNA di qualcuno. Mettiamo che tu stia cercando qualcuno a Gaza. È come inserire questa informazione nel pulviscolo o nel vapore, e poi spruzzarla con l'aereo su Gaza. Quando [il pulviscolo o il vapore, ndt] tocca terra, la persona che ha quel DNA apparirà a chi sta facendo il monitoraggio. Quindi, in altre parole, si può adottare quel sistema e trovare chiunque. Oppure si può modificare il DNA. Si può utilizzare una nano-sostanza che potrebbe provocare amnesia generale, o portare le persone a ridere in modo incontrollato, o avere cose che influenzano la mente o il cervello attraverso una specie di nano-distanza.

È qualcosa contro cui non si può combattere.

Oggi, quella "nano" è la parte più finanziata della ricerca sugli armamenti. In Italia, Israele, Stati Uniti, Cina, Germania, riceve la maggior parte dei fondi rispetto ad ogni altra branca della ricerca per lo sviluppo di armamenti.

In un convegno di ricercatori sponsorizzato dal "Future of Humanity Institute" [Istituto per il Futuro dell'Umanità, centro di ricerca interdisciplinare sull'umanità e sulle sue prospettive, Università di Oxford, ndt] nel 2008, è stato chiesto agli scienziati cosa ne pensassero della probabilità che gli umani si estinguano entro il 2100 e quale sarà la causa di estinzione. Qual è il più grande pericolo per la sopravvivenza umana? Gli scienziati hanno risposto che c'è il 19% di probabilità di estinzione. Non so se è alta o bassa, ma siccome stavano discutendo di come succederà, è interessante scoprire che la ragione principale

per cui potremmo estinguerci sono le armi molecolari nanotecnologiche. Questa era la causa più pericolosa. Perché pensiamo sempre alle armi nucleari come a quelle più pericolose. Poi scorri la lista e scopri che c'è anche un'intelligenza artificiale super-intelligente, ma che prima vengono le pandemie studiate a tavolino, il che ci riporta a ciò che stavo dicendo su come si potrebbe utilizzare il DNA per diffondere pandemie. In fondo alla lista, non molto più in là, ci sono gli incidenti nanotecnologici.

In altre parole, le nanotecnologie sono in cima alla lista in termini di rischio piuttosto grande, e noi non ne parliamo. Uno dei motivi per cui ho scritto questo libro, comunque, è che sono di sinistra. La sinistra non sa nulla di queste cose. Io non ne sapevo niente finché non ho scritto il libro. Non conosciamo i sistemi d'arma, non conosciamo queste tecnologie, e sicuramente non conosciamo le nanotecnologie. La maggior parte di noi di sinistra proviene dalle scienze sociali, da discipline umanistiche, e non conosciamo davvero la "vera scienza". Non sappiamo che cosa bolle in pentola da 25 anni a questa parte nei laboratori scientifici, e nello stesso tempo spesso gli scienziati non vengono posti di fronte alle più grandi questioni di etica, storia e politica. Loro se ne stanno nei loro laboratori, a fare le loro cose, e non capiscono veramente le implicazioni di tutto questo. Penso che sia un aspetto veramente importante.

Esportazione dello Stato di polizia

E veniamo alla militarizzazione della polizia, a cui ho accennato prima. Israele, per esempio – ma non solo Israele – sta sviluppando armi che una volta erano armi militari e che oggi sono fatte per la polizia. Così per esempio il più famoso mitra israeliano è l'Uzi – la mafia lo ama, tutti amano l'Uzi. È una piccola mitragliatrice. Adesso la stanno facendo a forma di pistola, una pistola a mano. Così un poliziotto potrà portarla nella fondina e tirarla fuori così. Ma è un mitra, non spara solo un colpo alla volta. Stiamo iniziando ad avere sempre più armi da guerra nelle forze di polizia.

Torniamo indietro un secondo. Israele non esporta solo tecnologia per la guerra securocratica, nella quale è particolarmente bravo perché ha a disposizione un laboratorio: la Cisgiordania e Gaza. Milioni di persone su cui poter fare esperimenti. Nel mio libro, mostro tutte le armi che sono state usate per la prima volta a Gaza, nelle diverse operazioni. C'è un'intera popolazione e nessun

controllo, ci puoi fare quello che vuoi, con loro.

Ma non è solo questo: Israele ha una concezione di Stato di sicurezza che sta esportando. Non solo la tecnologia di sicurezza, ma il concetto di Stato di sicurezza, nel quale fondamentalmente la sicurezza diventa l'elemento centrale. Si può anche avere una democrazia, ma la democrazia viene dopo la sicurezza. Tutto viene dopo la sicurezza. Ne risente l'equità dei processi, ne risentono le leggi, e ne risentono i diritti umani. Il punto è che la sicurezza diventa la cosa principale. Vedete come Israele si sta comportando in Europa, per esempio.

Quando, un paio di anni fa, c'è stato l'attentato a Bruxelles, all'aeroporto e poi in città, Israele ha detto ai belgi: "Smettetela di mangiare cioccolato e unitevi al mondo". E ha aggiunto: "Avete un problema con il terrorismo. Tutti voi europei avete un problema con il terrorismo. E non lo state affrontando molto bene. Criticate Israele per l'occupazione. Non dovreste criticare Israele.

Dovreste prendere esempio da Israele. Dovreste fare quello che fa Israele, perché, sapete, avete un quartiere di musulmani a Bruxelles che fa del terrorismo. Noi abbiamo una Nazione tra il Mediterraneo e il fiume Giordano, abbiamo una democrazia – l'unica democrazia in Medio Oriente, giusto? -, abbiamo una fiorente economia, la nostra gente prova davvero una sensazione di sicurezza e incolumità. In un Paese in cui metà della popolazione è terrorista! Se stabilisci che i palestinesi siano terroristi per definizione… Possiamo creare sicurezza in un Paese in cui metà della popolazione è terrorista, immaginate cosa potrebbe fare il nostro modello per voi a Bruxelles, o in Francia, o in qualsiasi altro posto."

Israele sta davvero lavorando con le destre in tutto il mondo. Israele collabora con la destra italiana, ovviamente. Con Orban, e tutto l'est Europa, la Polonia e anche con la destra austriaca, gli ungheresi, e così via. Israele lavora a strettissimo contatto con la destra britannica, negli Stati Uniti con Trump naturalmente, e Bolsonaro è uno dei suoi migliori amici, lui ama Netanyahu! Quindi le cose stanno così: esiste il reale pericolo di una sorta di aggregazione delle ideologie nazionaliste di destra, che iniziano ad avere un concetto [univoco] di Stato di sicurezza che li guida. Non è solo un manipolo di gente di destra che non vuole l'immigrazione – e di questo c'è una versione francese, una polacca, una italiana – ma di persone che iniziano ad adottare la stessa ideologia, lo stesso progetto di Stato di sicurezza e le tecnologie che Israele sta sviluppando. Non è solo Israele che sta sviluppando un complesso globale securocratico: e capite che questo

diventa un pericolo reale per tutti noi.

La guerra contro il popolo non è solo un piccolo ramo della politica internazionale. È il modo in cui il capitalismo delle multinazionali rafforza la sua egemonia. Ne è parte integrante. Non è solo un elemento collaterale: e su questo non ci si sofferma molto nella ricerca, né nell'agenda politica di sinistra. Non stiamo capendo il significato di tutto questo a livello internazionale.

(Traduzione dall'inglese di Elena Bellini)

Il processo contro il software di sorveglianza israeliano si svolge a porte chiuse

Pegasus è collegato allo spionaggio politico in Messico, Emirati Arabi e Arabia Saudita: Citizen Lab dell'università di Toronto.

16 gennaio 2020 – Al Jazeera

Giovedì un tribunale israeliano ha disposto le udienze a porte chiuse del processo intentato da Amnesty International per bloccare le esportazioni del gruppo NSO [dalle iniziali dei fondatori dell'azienda: Niv, Shalev e Omri, è una società tecnologica israeliana, ndtr.] di software di spionaggio, che le associazioni per i diritti affermano vengano usati per spiare giornalisti e dissidenti in tutto il mondo.

Una giudice della Corte Distrettuale di Tel Aviv ha citato preoccupazioni relative alla sicurezza nazionale quando ha escluso il pubblico e i media dalle udienze. L'iniziativa ha comportato un'immediata condanna da parte dell'associazione di attivisti.

"È vergognoso che veniamo costretti al silenzio", ha detto ai giornalisti Gil Naveh, un portavoce di Amnesty.

Il Ministero della Difesa di Israele – che ha richiesto il divieto della Corte – e NSO hanno rifiutato di commentare la causa intentata da Amnesty. La causa potrebbe stabilire se il governo debba inasprire i controlli sulle esportazioni di strumenti informatici – un settore in cui Israele è leader mondiale.

Amnesty afferma che i governi hanno usato il software di hackeraggio dei cellulari della società israeliana per reprimere gli attivisti in tutto il mondo. Uno studio di Citizen Lab [Laboratorio dei Cittadini, associazione che difende i cittadini dallo spionaggio illecito dei governi, ndtr.] dell'università di Toronto ha collegato Pegasus allo spionaggio politico in Messico, Emirati Arabi e Arabia Saudita.

NSO ha affermato di vendere la propria tecnologia solo ad enti statali e alle forze dell'ordine per "aiutarle nella lotta al terrorismo e alla criminalità organizzata."

La giudice Rachel Barkai inizialmente aveva detto che avrebbe permesso che le argomentazioni di Amnesty fossero ascoltate dal pubblico, ma gli avvocati del governo hanno sostenuto che sarebbe parso che lo Stato stesse accettando le accuse di Amnesty e Barkai ha cambiato idea.

NSO è finita sotto esame quando un dissidente saudita legato al giornalista assassinato Jamal Khashoggi ha intentato causa sostenendo che NSO aveva aiutato la corte reale ad entrare nel suo cellulare e a spiare le sue comunicazioni con Khashoggi.

NSO ha negato che la sua tecnologia sia stata utilizzata nell'omicidio di Khashoggi.

In ottobre WhatsApp, che è di proprietà di Facebook Inc., ha fatto causa a NSO presso la corte federale degli Stati Uniti a San Francisco. WhatsApp ha accusato NSO di aiutare le spie governative ad entrare nei telefoni di circa 1.400 utenti in quattro continenti.

Nella causa di Amnesty, intentata da membri e sostenitori del suo ufficio di Israele, l'organizzazione ha affermato che NSO continua a trarre profitti dal suo programma spia che viene usato per commettere violazioni contro attivisti in tutto il mondo e che il governo israeliano "è rimasto a guardare senza fare niente."

"Il modo migliore per impedire che i potenti prodotti di spionaggio di NSO arrivino ai governi repressivi è revocare la licenza di esportazione della società, e

questo è esattamente ciò che questa causa legale intende fare", ha detto Danna Ingleton, vicedirettrice di Amnesty Tech.

Amnesty Tech è descritta sul sito web di Amnesty International come una collettività globale di avvocati, esperti di informatica, ricercatori e tecnologie che sfidano "la sistematica minaccia ai nostri diritti" da parte delle imprese di spionaggio.

NSO, che l'anno scorso è stata acquisita dalla società privata Novalpina Capital con sede a Londra, a settembre ha annunciato che avrebbe iniziato ad attenersi alle linee guida dell'ONU sulle violazioni dei diritti umani.

FONTE: Agenzia di informazioni Reuters

(Traduzione dall'inglese di Cristiana Cavagna)

Fine modulo

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.

(traduzione dall'inglese di Amedeo Rossi)

Un sistema di spionaggio del

gruppo NSO sarebbe stato utilizzato in attacchi informatici contro avvocati e giornalisti

Nick Hopkins *e* **Stephanie Kirchgaessner**

Martedì 29 ottobre 2019 – The Guardian

WhatsApp denuncia un'impresa israeliana accusandola di aver violato i telefoni di attivisti

WhatsApp ha iniziato un'azione legale senza precedenti contro un'impresa di armi informatiche accusata di essere dietro attacchi segreti contro più di 100 attivisti per i diritti umani, avvocati, giornalisti e docenti universitari in sole due settimane all'inizio dell'anno.

L'impresa di social media ha presentato una denuncia contro NSO Group, una compagnia israeliana della sorveglianza, affermando che essa è responsabile di una serie di attacchi informatici molto complessi che a suo parere hanno violato le leggi americane con una "inconfondibile modalità di uso illecito".

WhatsApp afferma di ritenere che durante il periodo di due settimane tra la fine di aprile e metà maggio questa tecnologia venduta da NSO sia stata usata per prendere di mira i telefonini di oltre 1.400 suoi utenti in 20 diversi Paesi.

WhatsApp pensa che in questo breve periodo tra quanti sono stati sottoposti agli attacchi informatici ci siano importanti difensori ed avvocati per i diritti umani, illustri personalità religiose, famosi giornalisti e funzionari di organizzazioni umanitarie.

Secondo quanto ritiene la compagnia, sono state vittime di attacchi anche un certo numero di donne precedentemente prese di mira dalla violenza informatica e personalità che hanno subito tentativi di assassinio e minacce di violenza, così come i loro parenti.

La denuncia di WhatsApp, presentata martedì a un tribunale californiano, chiede un'ingiunzione permanente che vieti a NSO di tentare di accedere ai sistemi su

computer WhatsApp e Facebook, ad esso legato.

Ha anche chiesto al tribunale di sentenziare che NSO ha violato le leggi federali USA e della California contro frodi informatiche, ha violato i suoi contratti con WhatsApp ed ha "indebitamente abusato" di proprietà di Facebook.

"Questa è la prima volta che un fornitore di messaggistica criptata ha preso un'iniziativa legale contro un ente privato che ha perpetrato questo tipo di attacchi contro i suoi utenti," ha affermato un portavoce di WhatsApp. "Nella nostra denuncia spieghiamo come NSO abbia messo in atto il suo attacco, compresa l'ammissione di un dipendente di NSO che le nostre iniziative per porre rimedio all'attacco sono state efficaci."

La compagnia sta anche appoggiando richieste del relatore speciale ONU per il diritto di espressione, David Kaye, per una moratoria di questo tipo di programmi di spionaggio invasivo.

"Ci deve essere un deciso controllo giudiziario su armi informatiche come quella usata in questo attacco, per garantire che non vengano usate per violare i diritti individuali e le libertà a cui le persone hanno diritto ovunque nel mondo," ha affermato WhatsApp.

"Gruppi per i diritti umani hanno documentato una preoccupante tendenza in base alla quale tali strumenti sono stati usati per attaccare giornalisti e difensori dei diritti umani."

WhatsApp ha sostenuto di aver lavorato con "Citizen Lab", un gruppo di ricerca universitario con sede presso la Munk School di Toronto, per identificare le vittime degli attacchi e la tecnologia utilizzata contro di loro. L'organizzazione ha iniziato a contattare membri della società civile che siano stati colpiti dai presunti hacker.

John Scott-Railton, un ricercatore esperto di "Citizen Lab", ha detto che l'azione legale di WhatsApp è stata "un importante passo positivo per la protezione dei diritti umani in rete e rappresenterà sicuramente un precedente." Egli ha accusato NSO di agire con spregio nei confronti delle persone prese di mira. "Mentre dice all'opinione pubblica di essere preoccupata dei diritti umani, la società privata di sistemi di spionaggio ha cercato di ritagliarsi una nicchia di impunità, per cui, in virtù della sua vicinanza ad alcuni governi, sostiene di agire

in modo legale, ma quando le fa comodo preferisce disconoscere qualunque responsabilità per questo comportamento.

L'annuncio di WhatsApp giunge sei mesi dopo che ha comunicato di aver scoperto un punto debole che ha consentito ad aggressori informatici di installare programmi di spionaggio sui telefoni con il programma sia iPhone che Android, chiamando destinatari che usano la funzionalità telefonica dell'applicazione. In quel momento non era ancora chiaro come molti degli 1,5 miliardi di utenti di WhatsApp siano stati colpiti.

Da allora WhatsApp, in collaborazione con "Citizen Lab", nei giorni prima che la vulnerabilità venisse bloccata, ha cercato di capire come siano stati lanciati molti attacchi. Si ritiene che l'azienda sia rimasta scioccata da quello che ha scoperto.

Nella sua azione legale ha accusato NSO di "accesso e uso illegali dei computer di WhatsApp, molti dei quali si trovano in California."

Sostiene anche che NSO "ha preso una serie di iniziative, utilizzando senza autorizzazione server di WhatsApp e il suo servizio, per spedire singoli componenti del programma ostile ('codice dannoso') per prendere di mira dispositivi elettronici" – e che ciò è stato fatto in modo da "occultare l'identità e il coinvolgimento degli accusati."

La denuncia di WhatsApp non è l'unica rivolta contro NSO. L'impresa è stata accusata di aver preso di mira Omar Abdulaziz, uno stretto collaboratore di Jamal Khashoggi prima che il giornalista del Washington Post venisse assassinato l'anno scorso nel consolato saudita di Istanbul.

NSO ha affermato di prendere in esame le accuse nei confronti dei propri clienti e di riservarsi il diritto di ritirare agli utenti i permessi di utilizzo.

All'inizio di quest'anno l'azienda è stata acquistata da un'impresa privata con sede a Londra denominata "Novalpina Capital", che in giugno ha affermato che avrebbe svelato nuove regole di governo dell'azienda. Nel passato NSO ha tenacemente difeso l'utilizzo della sua tecnologia e del sistema informatico di sorveglianza, noto come "Pegasus", in quanto strumento di messa in pratica della legge che potrebbe contribuire a prevenire attacchi criminali e terroristici. "Novalpina" ha attribuito alla tecnologia di NSO il merito di aver bloccato piani di un attacco terroristico in uno stadio affollato in Europa e, citando il governo

messicano, ha affermato che nel 2011 ha contribuito all'arresto del boss della droga noto come "El Chapo".

In novembre l'impresa israeliana ha reso nota una "nuova politica per i diritti umani", che a suo dire è fondata su un "rispetto incondizionato per i diritti umani". Tra le altre iniziative, si è impegnata a inserire nuove procedure corrette di controllo per identificare, prevenire e mitigare "effetti contrari ai diritti umani" a causa del possibile abuso della sua tecnologia.

Ha anche affermato che avrebbe condotto una valutazione del "potenziale di effetti contrari ai diritti umani" dovuti ad un uso scorretto dei prodotti di NSO, così come avrebbe imposto "obblighi contrattuali" che impedirebbero ai clienti di NSO di utilizzare i suoi prodotti per qualcosa di diverso da un'inchiesta su gravi delitti.

Ma la nuova politica è stata criticata da alcuni esperti dei diritti umani e della sorveglianza informatica, compreso Kaye dell'ONU.

In una lettera del 18 ottobre a Shalev Hulio, uno dei fondatori di NSO, Kaye ha sollevato dubbi sull'efficacia di queste nuove linee guida sui i diritti umani e delle procedure basate sulla necessaria attenzione, ed ha suggerito che [NSO] sembrava affidarsi totalmente ai suoi stessi clienti per l'autocertificazione sull'uso scorretto dei suoi prodotti.

NSO Group ha affermato: "Contestiamo con la massima fermezza le attuali accuse e ci opporremo fortemente ad esse. L'unico scopo di NSO è fornire una tecnologia ad agenzie di intelligence e forze dell'ordine governative per aiutarle a combattere il terrorismo e la grande criminalità. La nostra tecnologia non è destinata o autorizzata ad essere usata contro gli attivisti per i diritti umani e i giornalisti. Negli ultimi anni ha contribuito a salvare migliaia di vite.

"La verità è che piattaforme fortemente criptate sono spesso utilizzate da circoli di pedofili, boss della droga e terroristi per proteggere le proprie attività criminali. Senza tecnologie sofisticate, gli organi di polizia che devono garantire la nostra sicurezza devono affrontare ostacoli insormontabili. Le tecnologie di NSO forniscono soluzioni adeguate e legali a questo problema.

"Noi consideriamo ogni uso dei nostri prodotti diverso dalla prevenzione della grande criminalità e del terrorismo una misura vietata dai termini contrattuali. Se

lo individuiamo, interveniamo. Questa tecnologia è radicata nella protezione dei diritti umani – compresi il diritto alla vita, alla sicurezza ed all'integrità fisica – ed è per questo che abbiamo cercato di adeguarci ai principi delle linee guida dell'ONU su attività economiche e diritti umani, per garantire che i nostri prodotti rispettino *tutti* i diritti umani fondamentali."

Se siete stati colpiti da presunto hackeraggio di WhatsApp o avete informazioni su di esso contattate *Nick.Hopkins@theguardian.com* oppure *Stephanie.Kirchgaessner@theguardian.com*

(traduzione dall'inglese di Amedeo Rossi)

Esportare la tecnologia dell'occupazione

Antony Loewenstein

4 gennaio 2019 **The New York Review of Books**

Parlando recentemente via satellite da Mosca ad un pubblico di Tel Aviv poco dopo l'assassinio del giornalista Jamal Khashoggi nel consolato dell'Arabia Saudita ad Istanbul, l'informatore della National Security Agency [ente governativo USA che si occupa di sicurezza nazionale, ndtr.] Edward Snowden ha sostenuto che l'Arabia Saudita ha utilizzato un software-spia prodotto in Israele per tracciare i movimenti di Khashoggi prima della sua morte. Snowden ha detto che l'agenzia israeliana di intelligence informatica 'NSO Group Technologies' ha sviluppato un software noto come Pegasus che è stato venduto ai sauditi ed ha consentito che Khashoggi fosse monitorato infettando lo smartphone di uno dei suoi contatti, un altro oppositore del regime saudita, che vive in Canada.

Questo dissidente, Omar Abdulaziz, alla fine del 2018 ha promosso un'azione legale in Israele sostenendo che il gruppo NSO ha violato le leggi internazionali vendendo la propria tecnologia a regimi oppressivi. "NSO dovrebbe rispondere

riguardo alla protezione delle vite di dissidenti politici, giornalisti ed attivisti per i diritti umani", ha detto il suo avvocato di Gerusalemme, Alaa Mahajna. Il gruppo NSO risulta di proprietà di un'impresa americana, la Francisco Partners, e sia Goldman Sachs che Blackstone vi investono. Il giornalista di *The Washington Post* David Ignatius, da tempo sostenitore dei sauditi, ha confermato le affermazioni di Snowden circa gli affari dell'impresa israeliana con il Regno [saudita].

Questo è solo uno dei tanti sinistri esempi di un lucroso affare. Secondo il *Jerusalem Post*, Israele recentemente ha venduto all'Arabia Saudita sofisticati impianti di spionaggio per un valore di 250 milioni di dollari, e *Haaretz* ha anche riferito che al Regno è stato offerto un software per intercettazioni telefoniche del gruppo NSO poco prima che il principe ereditario Mohammed Bin Salman iniziasse le purghe contro gli oppositori nel 2017. Sia Israele che l'Arabia Saudita considerano l'Iran come un'eccezionale minaccia che giustifica la loro cooperazione.

Oltre a software di spionaggio e strumenti informatici, Israele ha sviluppato una crescente industria nell'ambito della sorveglianza, inclusi spionaggio, operazioni psicologiche e disinformazione. Una di queste imprese, Black Cube, un'agenzia di intelligence privata con legami con il governo israeliano (due ex capi del Mossad hanno fatto parte del suo comitato consultivo internazionale), di recente ha acquisito notorietà – soprattutto per aver spiato donne che avevano accusato il magnate di Hollywood Harvey Weinstein di violenza sessuale. Alcuni reportage hanno anche rivelato l'attività dell'impresa per il governo autoritario ungherese, così come una presunta campagna di 'operazioni sporche' contro funzionari dell'amministrazione Obama legati all'accordo nucleare iraniano e contro un ricercatore anti-corruzione in Romania. Black Cube ed altre agenzie simili hanno stretti legami con lo Stato di Israele in quanto impiegano molti dipendenti che hanno fatto parte dell'intelligence.

In più di mezzo secolo di occupazione Israele ha perfezionato l'arte di monitorare e sorvegliare milioni di palestinesi in Cisgiordania, Gaza e nello stesso Israele. Adesso confeziona e vende queste conoscenze a governi che ammirano la capacità del Paese di reprimere e gestire la resistenza. Così l'occupazione israeliana è diventata globale. Le esportazioni del Paese per la difesa hanno raggiunto un record di 9,2 miliardi di dollari nel 2017, il 40% in più del 2016 (in un mercato di armamenti globale che ha registrato le vendite più alte di sempre nel 2017, con la cifra di 398,2 miliardi di dollari). La maggioranza di queste vendite sono avvenute

in Asia e nella regione del Pacifico. I sistemi militari, come missili e difesa aerea, sono stati il settore principale con il 31%, mentre i sistemi di intelligence, informatici e di spionaggio hanno rappresentato il 5%. L'industria di Israele è sostenuta da un'abbondante spesa interna: nel 2016 la spesa per la difesa ha rappresentato il 5,8% del PIL del Paese. A titolo di confronto, nel 2017 il settore della difesa americano ha assorbito il 3,6% del PIL degli USA.

Nonostante i loro occasionali gesti diplomatici di opposizione all'occupazione israeliana dei territori palestinesi, molte Nazioni sono diventate acquirenti bendisposti di armamenti informatici israeliani e di know-how per lo spionaggio. Secondo il New York Times, anche il governo messicano ha utilizzato, almeno in un caso, strumenti del gruppo NSO, verosimilmente per spiare un giornalista d'inchiesta che è stato in seguito ucciso; sono stati presi di mira anche avvocati per i diritti umani ed attivisti anti-corruzione. Amnesty International ha accusato il gruppo NSO di aver cercato di spiare uno dei suoi dipendenti. Un gruppo di ricerca canadese, 'The Citizen Lab', ha scoperto che sono comparsi apparecchi telefonici infettati in Bahrein, Brasile, Egitto, Palestina, Turchia, Emirati Arabi, Regno Unito, USA e altrove.

Durante le recenti proteste a Gaza un ex amministratore delegato dell'impresa che ha costruito la barriera che circonda parte della Striscia di Gaza, Saar Korush della 'Magal Security Systems', ha detto all'agenzia Bloomberg che Gaza era una vetrina per la sua "recinzione intelligente", perché i clienti apprezzavano che fosse stata sperimentata sul campo di battaglia e si fosse dimostrata in grado di tenere i palestinesi fuori da Israele. La Magal (insieme ad un'altra impresa israeliana) è tra le imprese candidate a costruire il muro di confine col Messico del presidente Trump ed ha creato un business internazionale sulla base della sua capacità di bloccare gli "infiltrati", un termine comunemente usato in Israele per definire i rifugiati. Un'altra nuova arma utilizzata lungo la barriera tra Israele e Gaza è il "Mare di Lacrime", un drone che sgancia candelotti lacrimogeni sui dimostranti. Secondo il sito israeliano Ynet il suo produttore ha presto ricevuto centinaia di ordini per questi droni. La Germania sta già noleggiando droni israeliani, mentre l'agenzia europea Frontex sta testando droni simili per sorvegliare i confini europei nel tentativo di impedire l'ingresso di migranti e rifugiati.

Il primo ministro israeliano Benjamin Netanyahu, nel corso dei suoi quasi dieci anni al potere, ha favorito la trasformazione del suo Paese in una potenza

tecnologica che promuove orgogliosamente i suoi strumenti di occupazione sul mercato mondiale e interno. Parlando a novembre ai suoi colleghi parlamentari in Israele, Netanyahu ha detto che "il potere è la componente più importante della politica estera. 'L'occupazione' è una cavolata. Ci sono Paesi che hanno conquistato e deportato intere popolazioni ed il mondo resta in silenzio. La chiave è la forza, fa la differenza nella nostra politica verso il mondo arabo." Ha concluso che ogni accordo di pace con i palestinesi potrebbe avvenire solamente con "interessi comuni basati sulla potenza tecnologica."

Nel 2017 Israele ha ammorbidito le sue regole per concedere licenze di esportazione ad una serie di produttori di strumenti di spionaggio, sorveglianza e armamenti, benché sostenga di farlo tenendo conto delle implicazioni per i diritti umani. Ma questo non è credibile, dato che proprio negli scorsi anni Israele ha venduto armi a Paesi che commettono gravi violazioni, come Filippine, Sud Sudan e Myanmar. Netanyahu ha stretto amicizia con il dittatore del Ciad Idriss Déby, e i prossimi della lista potrebbero essere il regime del Bahrein e il dittatore sudanese Omar al-Bashir, che è ricercato dalla Corte Penale Internazionale per crimini contro l'umanità.

Il ministero della Difesa israeliano rilascia difficilmente informazioni su come o perché le sue esportazioni vengano concesse. *Haaretz* ha recentemente scoperto che sono stati venduti sistemi di spionaggio a parecchi regimi non democratici, compresi Bangladesh, Angola, Bahrein, Nigeria, Emirati Arabi, Vietnam ed altri. In alcuni casi, questi governi ed altri hanno usato i sistemi per prendere di mira dissidenti e cittadini LGBTQ e anche per fabbricare false accuse di blasfemia. All'inizio del 2019 *Haaretz* ha anche rivelato l'esistenza di un'altra azienda israeliana di sicurezza informatica, di nome Candiru, che commercializza strumenti di hackeraggio e si basa ampiamente sul reclutamento di veterani dell'esercito del reparto d'elite dello spionaggio Unit 8200.

Da quando è scoppiata la bolla tecnologica nel 2000, il governo israeliano ha spinto imprese locali ad investire nelle industrie di sicurezza e di intelligence. Secondo un rapporto di "Privacy International" [organizzazione inglese che si occupa delle garanzie della privacy in tutto il mondo, ndtr.] del 2016, il risultato è stato che, su 528 imprese attive nel mondo in questo settore, 27 hanno sede in Israele –facendo del Paese quello con il tasso di imprese di sorveglianza e di intelligence pro capite di gran lunga più alto al mondo. E nel 2016, riferisce *Haaretz*, il 20% degli investimenti mondiali nel settore sono stati in start-up

israeliane.

In quello stesso anno l'avvocato per i diritti umani Eitay Mack, uno dei pochi israeliani famosi che sfidi pubblicamente la politica di esportazione di armi di Israele, e Tamar Zandberg, presidentessa del partito di sinistra Meretz, si sono rivolti all'Alta Corte di Giustizia israeliana nel tentativo di ottenere una sospensione della licenza all'esportazione del gruppo NSO. Il governo ha chiesto che il processo si tenesse a porte chiuse e la sentenza della corte non è stata resa pubblica. La giudice che presiede la Corte Suprema Esther Hayut ha spiegato che "la nostra economia, guarda caso, si basa non poco su quelle esportazioni."

Infatti nel 2017 Israele è stato secondo solo agli USA, raggiungendo quasi 1 miliardo di dollari in capitale di rischio e azioni private per imprese di sicurezza informatica. Informazioni diffuse l'anno scorso dall'impresa di dati di New York "CB Insights" mostrano che Israele è stato il secondo maggior firmatario di accordi di sicurezza informatica al mondo dopo gli USA. Benché gli USA siano i primi con largo margine, con il 69% del mercato globale, il 7% di Israele lo piazza davanti al Regno Unito.

L'occupazione ha quindi alimentato la politica israeliana dell'industria e della difesa attraverso un boom economico che ha beneficiato le imprese che costruiscono, conducono e gestiscono l'impresa coloniale. Ma per Shir Hever, autore di '*The privatization of israeli security*' [La privatizzazione della sicurezza israeliana] (2017) ed esperto mondiale del commercio di armi israeliano, l'occupazione sta diventando meno un'opportunità che un peso. Molti venditori di armi israeliani, mi ha detto, "stanno esprimendo la loro frustrazione per il fatto che i clienti non sono entusiasti dei prodotti israeliani perché non riescono a fermare la resistenza palestinese. La Russia ha sviluppato un sistema di vendita equa di armi 'collaudate in battaglia' nella guerra in Siria ed è riuscita ad aumentare le vendite in Turchia e India, entrambi mercati molto importanti per le imprese israeliane. Quindi perché gli importatori di armi dovrebbero considerare speciali gli armamenti israeliani?"

Hever riconosce che "i regimi autoritari vogliono sicuramente ancora imparare come Israele gestisce e controlla i palestinesi, ma più imparano, più si rendono conto che Israele in realtà non controlla i palestinesi molto efficacemente. Il sostegno ad Israele da parte dei gruppi e dei politici di destra nel mondo è ancora forte – il nuovo presidente del Brasile, Jair Bolsonaro, ne è un esempio

particolarmente deprimente – ma io penso che vi sia più attenzione al razzismo, alla discriminazione razziale e al nazionalismo, e meno attenzione e ammirazione per 'l'esercito più forte del mondo."" Egli mette anche in discussione la narrazione del governo israeliano riguardo al successo del settore degli armamenti e dell'intelligence e sostiene che l'industria sia in declino perché è troppo dipendente da alleanze di breve termine e ad hoc.

Il Sudafrica dell'apartheid e il suo declino sono un avvertimento della storia che Israele sarebbe incauto ad ignorare. Al suo apice, il Sudafrica è stato uno dei maggiori mercanti di armi al mondo, dopo il Brasile e Israele, e questo è stato ottenuto attraverso ingenti sussidi statali. Nonostante un embargo ONU sulle armi, secondo un recente volume, '*Apartheid guns and money: a tale of profit*' *(Fucili e denaro dell'apartheid: una storia di profitto*), di Hennie van Vuuren, direttore dell'organizzazione di controllo sudafricana non profit 'Open Secrets', il regime sudafricano alla fine degli anni '80 ha speso il 28% del bilancio statale nella sua industria della difesa. Un'economia costruita sul know-how militare e sulla competenza nelle tecniche di repressione interna può sembrare una fonte di invincibile potenza, ma l'apartheid è finita meno di cinque anni dopo.

Oggi un crescente numero di ebrei americani sta prendendo le distanze da Israele, rifiutando l'adesione del governo al nazionalismo etnico e sostenendo invece una soluzione di uno Stato unico. Per il momento Israele appare nella posizione di restare un importante soggetto mondiale nella produzione e vendita di sistemi di armi e di dispositivi e competenze di sorveglianza – che è ora uno dei modi principali in cui il Paese si autodefinisce sul piano internazionale. Ma l'opposizione internazionale sta crescendo, grazie soprattutto agli appelli del movimento di Boicottaggio, Disinvestimento e Sanzioni (BDS) per un embargo militare contro Israele e la sua industria della difesa. Una delle imprese del settore della difesa più grandi del Paese, Elbit Systems, ha già subito boicottaggi alle sue attività nel mondo. Pochi giorni fa il colosso bancario HSBC ha annunciato il proprio disinvestimento da Elbit Systems. Campagne di alto profilo come questa inizieranno sicuramente a modificare i calcoli sui costi economici e morali dell'occupazione – ancor di più se Israele proseguirà il suo attuale percorso politico verso l'annessione de facto della Palestina.

(Traduzione di Cristiana Cavagna)

Acquirente fai attenzione: l'impresa israeliana che aiuta i governi a spiare i loro stessi cittadini

Richard Silverstein ,martedì 22 agosto 2017, Middle East Eye

Consentendo ai governi di violare i telefoni dei loro cittadini, un'azienda israeliana di sicurezza informatica ha presumibilmente reso il mondo più pericoloso per gli attivisti a favore dei diritti umani che lottano contro l'impunità delle imprese e degli Stati.

Dato che negli ultimi anni gli smartphone si sono moltiplicati e sono diventati un mezzo di comunicazione indispensabile per tutti noi, si sono moltiplicate anche le nuove aziende che si dedicano a violare questi telefoni a favore di governi – compresi i servizi militari, dello spionaggio e della polizia.

I clienti di queste imprese innovative utilizzano la nuova tecnologia per sorvegliare criminali e terroristi, per individuare e far fallire i loro piani. Questo è un uso legittimo. Ma ce ne sono altri che sono molto più redditizi per le imprese – e molto meno accettabili per le società democratiche.

Prendiamo per esempio l'attivista per i diritti umani degli Emirati [Arabi Uniti] Ahmed Mansoor. Nell'agosto 2016 ha ricevuto un messaggio ingannevole [phishing message] che sembrava provenire da una fonte fidata. Ma si è insospettito ed ha immediatamente inviato il suo telefono a "Citizen's Lab" [Laboratorio del Cittadino, centro studi interdisciplinare che si occupa del controllo sulle informazioni, ndt.] dell'università di Toronto per un'analisi forense.

Da questa verifica è risultato che le autorità degli Emirati si erano procurate "Pegasus", il più potente programma di malware [sistemi usati per apportare modifiche indesiderate ad un apparecchio informatico, ndt.] mai creato che si

possa trovare sul mercato e venduto dall'azienda israeliana "NSO Group".

Se Mansoor avesse aperto il link, esso avrebbe preso il controllo del suo telefono e consentito alla polizia di accedere non solo a tutto quanto vi si trovava (email, contatti e messaggi di testo, per esempio), ma anche alla macchina fotografica, al video e all'audio. La polizia avrebbe sentito e visto tutto quello che faceva e sarebbe stata in grado di prevenire ogni sua azione.

1. Attacchi di "Pegasus"

In un caso collegato del 2016, le autorità degli EAU hanno anche utilizzato "Pegasus" in un tentativo di intrusione che ha preso di mira il giornalista di MEE Rory Donaghy, che informava in modo critico sui soprusi del regime autocratico del Paese. Nel pieno di un'inchiesta su questo attacco, il "Citizen's Lab" ha scoperto che 1.100 attivisti e giornalisti del regno erano stati presi di mira allo stesso modo e che il governo aveva pagato a "NSO Group" 600.000 dollari per questi tentativi [di intercettazione].

Anche se è un prodotto commerciale, "Pegasus" – come molti altri strumenti simili per lo spionaggio ora sul mercato – è chiaramente anche un mezzo politico che consente a regimi autoritari di spiare i propri cittadini.

Infatti potrei andare anche oltre e dire che "Pegasus" è spesso utilizzato come arma informatica offensiva usata dall'élite mondiale per proteggere i propri interessi e contrastare il legittimo controllo da parte delle Ong e di altre associazioni di attivisti.

"Il governo compra (la tecnologia) e può usarla come vuole," ha detto a "HuffPost" Bill Marczak, un ricercatore di "Citizen's Lab" che ha analizzato molte campagne di controllo che secondo lui sono state condotte con "Pegasus".

"Sono praticamente dei mercanti di armi digitali."

Nelle ultime settimane il gruppo finanziario privato che possiede "NSO Group", valutato oggi 1 miliardo di dollari, ha cercato di vendere la compagnia, sollevando grandi questioni tra gli attivisti dei diritti digitali in merito a se un nuovo investitore ridurrà il sospetto uso del sistema di spionaggio dell'azienda contro dissidenti politici ed attivisti da parte di alcuni governi.

2. Dall’esercito alla tecnologia

Ci sono parecchie imprese che creano questo tipo di software maligni in vari Paesi, ma alcune di quelle di maggior successo sono israeliane.

Ciò è principalmente un risultato della “SIGINT-Unità 8200”, la più numerosa dell’esercito israeliano, che spia i segnali elettromagnetici, monitora, intercetta e sorveglia i nemici di Israele in Medio Oriente e in tutto il mondo.

I suoi ufficiali ricevono l’addestramento più sofisticato nello spionaggio ed uso dei segnali e creano la tecnologia più avanzata per farlo. Quando lasciano il servizio attivo trovano le porte aperte nel mondo tecnologico. Possono avere un lavoro molto ben remunerato nelle grandi imprese o utilizzare le competenze che hanno acquisito nell’esercito per fondare un’azienda innovativa propria.

Alcune delle aziende di maggiore successo includono Waze, Wix, Taboola, NICE Systems, Amdocs, Onavo (acquistata da Facebook per 150 milioni di dollari), Checkpoint, Mirabilis e Verint.

Molti dei progetti riguardano la sicurezza informatica, che è quello che l’ “Unità 8200” è stata costituita per debellare nei suoi tentativi di intercettare le comunicazioni delle forze nemiche di Israele. Alcune iniziative sono concentrate sulla protezione della sicurezza informatica. Questi sono i bravi, o i “cappelli bianchi” nella terminologia degli hacker.

Ma altri continuano lungo la direzione che gli hacker dell’”Unità 8200” perseguono durante il servizio militare: sono destinati ad aggirare le funzioni di sicurezza di vari sistemi.

Forse quella che ha avuto più successo tra queste imprese è “NSO Group” che si trova a Herziliya [importante università privata israeliana in stretti rapporti con i servizi di sicurezza, ndt.], il cui motto è “rendi il mondo un posto più sicuro.” Ma l’azienda ha reso sicuramente il mondo molto più pericoloso per un gran numero di attivisti politici e per i diritti umani che lottano contro l’impunità di imprese e governi.

3. Vulnerabilità da miliardi di dollari

“NSO” è stata fondata nel 2010 da due veterani dell’esercito israeliano, Shalev Hulio and Omri Lavie, che non erano stati nell’“Unità 8200” (nonostante informazioni in contrario). Secondo la rivista israeliana “Globes” [quotidiano di informazioni finanziarie, ndt], Lavie ha fatto il militare nei corpi di artiglieria e Hulio nel servizio di ricerca e soccorso.

Alle scuole superiori né Hulio né Lavie erano studenti particolarmente brillanti e, secondo le informazioni del “Globes”, hanno passato un sacco di tempo insieme sulla spiaggia. Dopo aver lasciato l’IDF, hanno deciso di diventare imprenditori di servizi in rete.

“NSO” è la loro terza e di gran lunga più importante iniziativa imprenditoriale di successo. Secondo i fondatori, la sua nascita è avvenuta per puro caso. Vari clienti avevano chiesto loro se ci fosse un modo per prendere il controllo di un cellulare senza avere accesso fisico all’apparecchio reale.

Benché avessero sentito dire che c’era [questa possibilità], non riuscivano a trovare nessun ingegnere informatico che avesse idea di come farlo, finché un giorno, seduti in un caffè, i due udirono per caso parlarne veterani dell’“Unità 8200”. Così nel 2010, proprio quando gli smartphone stavano per essere trasformati da oggetti per un solo uso in apparecchi quotidiani potenti, multiuso e indispensabili, fondarono “NSO”.

Iniziarono a farsi una clientela tra le forze di polizia di vari Paesi, offrendo la possibilità di spiare criminali sospetti in modi che nessuno aveva mai previsto. Fondarono una succursale per le vendite negli USA, “WestBridge Technologies”, per incentivare la penetrazione commerciale in uno dei loro maggiori mercati potenziali.

Attraverso la “Francisco Partners”, la società di capitale di rischio che nel 2015 ha comprato “NSO”, questa è finita sotto l’egida di un’impresa che possiede una serie di altre compagnie di telecomunicazioni che hanno fornito informazioni sensibili per fare passi avanti nelle possibilità di hackeraggio. Per esempio, “Intelligence Online” [rivista informativa nel campo dell’informatica, ndt.] riporta che Boaz Goldman è presidente del consiglio di amministrazione di “Inno Networks”, che installa reti di comunicazione mobile (3G e 4G). E’ appena entrato nel consiglio di amministrazione di una holding con sede in Lussemburgo che include “NSO Group” in un complicato rapporto finanziario. Questo accordo

d’affari fornisce all’azienda di armi informatiche un accesso diretto a grandi reti (SS7 – Signal System 7) utilizzate per trasmettere testi, email, chiamate telefoniche, dati di geo-localizzazione e chiavi di cifratura.

“NSO” ha anche iniziato a crearsi fonti che gli forniscono accesso a prototipi di modelli di cellulari prima che vengano immessi sul mercato, il che gli permette di fare analisi scientifiche in modo che gli ingegneri di “NSO” possano cercare falle di vulnerabilità che consentano un accesso totale ai telefoni che i loro clienti desiderano prendere di mira.

4. Zona grigia

Si potrebbe pensare che i produttori di telefonini intendano proteggere i propri prodotti come Fort Knox [area militare in cui sono conservate le riserve auree e monetarie degli USA, ndt.] e vietarli agli sguardi loschi di hacker come “NSO”. Ma l’impresa opera in una zona grigia e cerca di garantirsi quello di cui ha bisogno da varie fonti sia all’interno che all’esterno delle industrie produttrici.

Prima dei portatili, i criminali comunicavano nel modo in cui lo facevano tutti: con telefoni fissi, mail o di persona. La tecnologia per intercettare o controllare queste comunicazioni era semplice e primitiva: per i telefoni si usava una “cimice” [microspie per l’ascolto di conversazioni private, ndt.] su una linea telefonica.

La cimice avrebbe dovuto presumibilmente essere approvata da un giudice ed essere messa in funzione con l’aiuto di una compagnia telefonica. C’era un processo di controllo e questo veniva in genere rispettato, almeno nelle società democratiche.

La comunicazione elettronica ha cambiato tutte le regole, aprendo nuove modalità per spiare le singole persone. Si possono intercettare dall’esterno i segnali di comunicazione tra chi parla. “NSO” ne ha approfittato, sviluppando un programma che, una volta scaricato, prenderà il controllo del telefonino di chi lo utilizza.

Così non c’è più bisogno di intercettare telefonate, perché il cliente di “NSO” è effettivamente all’interno dello stesso telefono. Le forze di polizia ed i governi possono distruggere i piani per commettere reati o attacchi terroristici prima che avvengano e preservare l’ordine pubblico.

5. Una breccia delle dimensioni di un camion

Ma c'è un aspetto problematico in questa tecnologia per altri versi benefica: "NSO Group" controlla solo quelli che l'hanno comprata, non l'utilizzatore finale. Il primo cliente può offrirla ad altri individui o enti nel suo governo, o creare un'identità commerciale fittizia per celare l'uso finale che farà di "Pegasus".

"NSO" sostiene di seguire tutte le regole israeliane che governano l'esportazione dei suoi prodotti e vende solo agli alleati di Israele e mai ai suoi nemici. Sostiene anche di vendere solo a governi e mai a singoli individui o ad utilizzatori non autorizzati. Afferma che "Pegasus" è previsto solo per lottare contro criminali e terroristi e mai per essere usato a fini politici.

Tuttavia sottolinea che, una volta che ha venduto il prodotto, non ha il controllo (o per lo meno questo sostiene) su chi usa la tecnologia o sul come. Questa è una breccia abbastanza grande da farci passare un camion Mack [marca che produce negli USA camion enormi, ndt.], e consente ad "NSO" – e a decine di altre imprese di spionaggio informatico che offrono programmi simili – di evitare la responsabilità sui modi ripugnanti in cui la loro tecnologia viene usata.

Nel caso di Mansoor l'hackeraggio è stato diretto contro un cittadino considerato un criminale dallo Stato. Ma egli non lo è da nessun punto di vista riconosciuto da una società democratica. Non è stato imputato di nessun reato, di aver rapinato qualcuno o di aver messo una bomba. Nel 2011 è stato condannato a tre anni con l'accusa di oltraggio allo Stato (in seguito è stato amnistiato e liberato) – e ciò a quanto pare è stato sufficiente in un regime autocratico come quello degli EAU per considerarlo sospetto.

La tecnologia dell'"NSO" è caduta in cattive mani anche in Messico. Come ha informato il "New York Times", i telefoni di attivisti politici, per i diritti umani e contro la corruzione messicani che stavano facendo un'inchiesta su possibili delitti commessi dal governo e dai suoi agenti sono stati infettati da "Pegasus". Il "Times" afferma che le vittime se ne sono accorte per la prima volta nell'estate 2016.

Una di queste era l'avvocato che rappresenta i genitori di 43 studenti medi uccisi dalla polizia messicana in un caso per cui non è mai stata perseguita. Altri

stavano facendo un'inchiesta sulla corruzione di dirigenti d'azienda collusi con rappresentanti eletti.

Secondo mail interne della "NSO" datate a partire dal 2013 e lette dal "New York Times", il governo messicano ha pagato alla "NSO" più di 15 milioni di dollari per tre progetti. Funzionari messicani hanno negato di essere coinvolti nello spionaggio ed hanno aperto un'inchiesta.

Questi usi violano le disposizioni della licenza di esportazione israeliana in base alla quale "NSO" vende i propri prodotti. Ma ci sono scarse possibilità che i funzionari israeliani intervengano in questo caso. Sono interessati a promuovere le esportazioni israeliane, non a limitarle. Né vedono il proprio ruolo come un servizio di censori nei confronti del comportamento delle imprese israeliane.

"Middle East Eye" ha contattato l'agenzia di controllo dell'esportazione per la difesa del Ministero della Difesa israeliano per chiedere di commentare i suoi rapporti con "NSO". Non ha risposto prima che questo articolo venisse pubblicato. Abbiamo anche posto delle domande all'ufficio stampa del Ministero della Difesa, e neppure questo ha risposto a tempo per la pubblicazione.

Per esempio, molti esportatori di armi israeliani sono sospettati di essere impegnati in truffe e altre pratiche corruttive per ottenere contratti per la vendita di armamenti con eserciti stranieri. Poche tra queste imprese sono state messe sotto inchiesta dalle autorità israeliane, benché a parecchie sia stato vietato di fare affari in vari Paesi.

"Citizen Lab" ha detto a "Forbes" che "NSO" ha registrato domini in Israele, Kenya, Mozambico, Yemen, Qatar, Turchia, Arabia Saudita, Uzbekistan, Thailandia, Marocco, Ungheria, Nigeria e Bahrain, suggerendo che "Pegasus" potrebbe essere stato usato in questi Paesi, anche se non ci sono prove evidenti.

Secondo email interne, contratti e proposte di "NSO" visionate dal "New York Times", "NSO" fa pagare ai clienti 650.000 dollari per spiare i proprietari di 10 iPhone, più 500.000 dollari di commissione per la configurazione.

E' evidente quanto questo affare possa essere una miniera d'oro – ed anche perché "NSO" potrebbe essere tentata di allentare le considerazioni etiche per massimizzare il suo profitto potenziale. "Middle East Eye" ha cercato un cofondatore di "NSO" e l'addetto stampa dell'impresa per un

commento. Nessuno ha risposto.

Da imprenditori astuti quali sono, Lavie e Hulio hanno deciso di poter giocare da entrambi i lati. E' così che nel 2013 hanno fondato "Kaymera", un'altra azienda tecnologica con sede nell'università di Herzilya destinata a proteggere i clienti contro intrusioni informatiche indesiderate.

Nella maggior parte delle iniziative imprenditoriali, questo passaggio del confine avrebbe fatto scattare l'allarme. Ci potrebbero essere dei vantaggi nel condividere informazioni: non appena un ingegnere dell' "NSO" ha individuato il punto debole di un'impresa, potrebbe condividerlo con "Kaymera" per risolverlo.

Ma con la stessa facilità potrebbe succedere il contrario: "Kaymera" potrebbe informare "NSO" dei punti deboli che ha scoperto nei sistemi informatici o di comunicazione di un cliente. Questa informazione potrebbe effettivamente essere monetizzata a favore di entrambe le aziende. Middle East Eye ha contattato "Kaymera" per avere un commento e l'impresa non ha risposto.

Il problema è che, in uno Stato di sicurezza nazionale come Israele, considerazioni etiche come queste passano in secondo piano rispetto ai benefici per la sicurezza *e* finanziari.

6. Unicorni e galline dalle uova d'oro

La crescente clientela di "NSO" e i profitti che genera hanno attirato l'attenzione di società di capitale di rischio alla ricerca di opportunità di investimenti lucrosi. Una di queste è stata la società privata di investimenti "Francisco Partners" con sede negli USA.

Nel 2014 la società ha comprato una quota di maggioranza in "NSO" per 120 milioni di dollari. Le migliori società finanziarie investono in un'impresa per un lungo periodo, offrendo non solo un investimento di capitale, ma anche consulenza strategica e gestionale. Ma altre investono a breve termine. "Francisco" è una di queste.

Cosa interessante, "Francisco Partners" e un ramo di "NSO" hanno un passato di rapporti con l'ex consigliere per la sicurezza nazionale dell'amministrazione Trump Michael Flynn, che ha dato le dimissioni in febbraio dopo indiscrezioni sui

suoi rapporti con la Russia.

Secondo moduli informativi finanziari, una controllata di "NSO" con sede in Lussemburgo, "OSY Group", ha pagato a Flynn 40.280 dollari per il suo ruolo come membro del consiglio di amministrazione dal maggio 2016 al gennaio scorso. Flynn – che avrebbe lavorato per molte imprese di sicurezza informatica – è stato anche consulente del socio proprietario di "NSO", "Francisco Partners", ma non ha mai rivelato quanto lo hanno pagato.

Un mese prima che Flynn entrasse nel consiglio di amministrazione di "OSY", "NSO Group" ha aperto una nuova branca nella zona di Washington chiamata "WestBridge Technologies" che, secondo l' "Huffington Post", è "in lizza per contratti con il governo federale per prodotti del gruppo "NSO". Assumere Flynn avrebbe messo a disposizione di "NSO Group" una figura con ottimi contatti a Washington, per aiutarla a inserirsi nel mondo notoriamente esclusivo della destinazione dei fondi dei servizi segreti."

"Francisco Partners" ha tenuto "NSO" solo per un anno prima di iniziare a venderla con una valutazione di un miliardo di dollari. Nelle scorse settimane "Blackstone Group", una delle più grandi società finanziarie di Wall Street, avrebbe accettato di acquistare una quota del 40% in "NSO".

Un investimento di 400 milioni di dollari da parte di "Blackstone" avrebbe fatto diventare "NSO" un "unicorno" (una startup che ha raggiunto il valore di un miliardo di dollari o più) ed offerto ai suoi fondatori – e a "Francisco Partners" – un enorme guadagno.

Data la maggiore penetrazione nel mercato mondiale che l'investitore "Blackstone" avrebbe fornito a "NSO", le notizie hanno preoccupato gli attivisti per la libertà nella rete.

"Access Now", una Ong statunitense che sostiene un internet libero e democratico, ha dato vita ad una petizione on line ed a una campagna con l'intenzione di informare l'opinione pubblica sul modello di attività di "NSO". "Citizen Lab" si è unito al progetto scrivendo una lettera aperta al consiglio di amministrazione di "Blackstone", invitandolo a "considerare con attenzione le implicazioni etiche e per i diritti umani" del loro potenziale investimento.

7. “Blackstone” si ritira

Questa settimana sono comparse notizie secondo cui “Blackstone” è uscita dalle trattative con “NSO” senza arrivare ad un accordo. Rispondendo ad una richiesta di commento da parte di “Middle East Eye” nel giorno in cui è stata annunciata la fine dei colloqui, un rappresentante di “Blackstone” ha rifiutato di commentare l’affare. Un’altra società di investimenti, “ClearSky Technologies”, avrebbe accettato di acquistare una quota del 10% in “NSO”. Ma anch’essa ha confermato a “Middle East Eye” che non investirà nell’azienda.

Un portavoce di “NSO” ha rifiutato di discutere con la Reuters [agenzia di stampa inglese, ndt.] dei colloqui o del perché sono saltati.

Ma pare probabile che la polemica generata da “Access Now” e le questioni sollevate dai giornalisti abbiano reso prudente la società sulla responsabilità che si sarebbe accollata.

“Finché ‘Blackstone’ non parla,” ha detto Peter Micek, consulente legale di ‘Access Now’, “non sapremo se hanno ascoltato le voci di difensori dei diritti umani, giornalisti e vittime di reati le cui vite sono state sconvolte dagli strumenti di ‘NSO Group’”.

“Ma questo accordo defunto dimostrerà ad altri investitori, compreso l’attuale proprietario di ‘NSO’, ‘Francisco Partners’, che non c’è niente da guadagnare – e tutto da perdere – nell’investire nelle violazioni dei diritti umani.”

Tutto ciò mette in luce nuove domande su come “NSO” fa affari e sull’inconsistenza del suo modello etico. Perché, per esempio, “Pegasus” perde il simbolo e il controllo di “NSO” una volta che viene concessa la licenza ad un cliente? Perché l’azienda non può fissare condizioni esplicite nei suoi contratti stabilendo da chi e come sarà utilizzato?

8. Condizioni di utilizzo

Sembra ridicolo che un’impresa, la cui tecnologia è destinata a infiltrarsi e controllare le attività di singole persone prese di mira, non sia in grado di monitorare gli usi a cui vengono destinati i suoi prodotti.

Ovviamente, se “NSO” potesse controllare come i clienti utilizzano i suoi prodotti, potrebbe essere ritenuta responsabile se violano le condizioni di utilizzo. Gli attivisti per i diritti umani presi di mira o imprigionati a causa di “Pegasus” potrebbero forse fare causa per le proprie sofferenze a “NSO” in qualche sede giurisdizionale. Questa sarebbe un’ulteriore ragione per cui “NSO” preferisce non sapere quello che succede una volta che il suo malware lascia i suoi server.

E’ indispensabile che il futuro acquirente ne sia consapevole e risponda a queste preoccupazioni in modo costruttivo. Inoltre gli Stati che sono già clienti di “NSO” devono fare un lavoro molto migliore per monitorare come la tecnologia per la sorveglianza viene utilizzata nelle zone di loro competenza.

Gli Stati che stanno pensando di diventare clienti di “NSO” devono anche fornire tutele per garantire che “Pegasus” venga usato unicamente contro i veri cattivi, ma non contro civili, fautori del benessere pubblico, avvocati, giornalisti o attivisti politici.

Richard Silverstein *scrive sul blog “Tikun Olam”, dedicato a smascherare gli eccessi dello Stato della sicurezza nazionale israeliano. Il suo lavoro è comparso su “Haaretz”, “Forward”, “Seattle Times” e “Los Angeles Times”. Ha contribuito alla raccolta di saggi dedicata alla guerra in Libano del 2006, “A Time to Speak Out” [Il momento di far sentire la propria voce] (Verso), e a un altro saggio nella raccolta di prossima pubblicazione “Israel and Palestine: Alternative Perspectives on Statehood” [Israele e Palestina: prospettive alternative di sovranità nazionale] (Rowman & Littlefield).*

Le opinioni espresse in questo articolo sono dell’autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(traduzione di Amedeo Rossi)