La sorveglianza sui palestinesi e la lotta per i diritti digitali

Nadim Nashif

23 ottobre 2017, Al-Shabaka

Sintesi

La sorveglianza sui palestinesi è sempre stata parte integrante del progetto coloniale israeliano. Prima della creazione dello Stato di Israele, squadre del gruppo paramilitare sionista Haganah percorrevano i villaggi e le città palestinesi, raccogliendo informazioni sui residenti. Questo controllo sulle vite dei palestinesi è continuato dopo l'occupazione israeliana delle Alture del Golan, della Striscia di Gaza e della Cisgiordania, inclusa Gerusalemme est, nel 1967. Gli strumenti utilizzati comprendevano registri della popolazione, carte di identificazione, rilevamenti catastali, torri di controllo, incarcerazione e tortura.

Benché queste tecniche di controllo poco sofisticate siano ancora oggi in uso, una vasta gamma di nuove tecnologie, come il monitoraggio e l'intercettazione per telefono e via internet, la CCTV [televisione a circuito chiuso, ndt.] e la banca dati biometrici, ha messo in grado Israele di sorvegliare la popolazione sotto occupazione su scala massiccia e pervasiva. Israele utilizza in particolare i social media per monitorare ciò che i singoli palestinesi dicono e fanno e per raccogliere ed analizzare informazioni sui comportamenti della popolazione palestinese in generale.

In questo documento Nadim Nashif discute l'uso da parte di Israele dei social media come strumento di controllo dei palestinesi. (1) Prende in esame le tattiche israeliane e gli altri ostacoli digitali ai diritti dei palestinesi, inclusa la parzialità di Facebook a favore di Israele attraverso la censura e la mancanza di trasparenza, nonché la nuova legge sui crimini informatici dell'Autorità Nazionale Palestinese (ANP). Nashif conclude fornendo suggerimenti su come i palestinesi possono contrapporsi all'uso dei social media per la sorveglianza e proteggere i propri diritti informatici.

I social media come ambito di sorveglianza

L’esplosione di rabbia palestinese iniziata nell’ ottobre 2015 in risposta alle incursioni israeliane alla Moschea di Al-Aqsa ha rappresentato una nuova sfida per l’apparato di sicurezza israeliano. Storicamente, gli individui affiliati ai bracci militari delle fazioni palestinesi, come Fatah, Hamas e il Fronte Popolare per la Liberazione della Palestina, hanno condotto attacchi ai quali Israele ha risposto con la violenza, la distruzione e le punizioni collettive. Per esempio, Israele ha scatenato le sue ultime tre guerre nella Striscia di Gaza, nel 2009, 2012 e 2014, con il pretesto di fermare i lanci di razzi da parte di Hamas.

Questa volta, tuttavia, sono stati adolescenti palestinesi, molti dei quali non appartengono ad alcuna fazione politica o ala militare palestinese, a sferrare gli attacchi. Il governo israeliano ha accusato i social media per questa nuova tendenza e l’intelligence militare israeliana ha rafforzato il monitoraggio degli account dei social media palestinesi. In seguito a ciò, Israele ha arrestato 800 palestinesi a causa dei loro post sui social media, soprattutto su Facebook, la piattaforma più seguita dai palestinesi.

All’inizio di quest’anno Haaretz ha rivelato che questi arresti sono il risultato di un metodo poliziesco basato su algoritmi che creano profili di quelli che Israele vede come probabili attentatori palestinesi. Il programma monitora decine di migliaia di account Facebook di giovani palestinesi, cercando termini come *shaheed* (martire), Stato sionista, Al Quds (Gerusalemme) o Al Aqsa. Ricerca anche account che postano foto di palestinesi recentemente uccisi o imprigionati da Israele. Il sistema identifica quindi i “sospetti” basandosi su un possibile atto di violenza, piuttosto che su un attacco reale – o almeno su un piano per realizzare un attacco.[vedi zeitun.info]

Ogni profilo Facebook segnalato come sospetto dal sistema è un potenziale bersaglio di un arresto e la principale accusa di Israele alle persone arrestate è “incitamento alla violenza”. Poiché l’incitamento è definito in modo vago, il termine include tutte le forme di resistenza alle politiche ed alle pratiche israeliane. La “popolarità”, o il livello di influenza che una persona esercita sui social media, è un fattore che conta nella decisione di Israele di sporgere denuncia contro i palestinesi accusati di incitamento. Per esempio, più alto è il numero di ‘like’, di commenti e di condivisioni che ha un’utenza, maggiore è la possibilità che le persone vengano denunciate – e più lunga e pesante sarà la condanna.

L’intelligence israeliana inoltre crea falsi account Facebook per tracciare e ottenere accesso a profili Facebook per poter comunicare con palestinesi e ricavare informazioni private che altrimenti essi non condividerebbero. Nell’ottobre 2015, per esempio, parecchi attivisti palestinesi hanno riferito di aver ricevuto messaggi da account Facebook con nomi arabi e fotografie di bandiere palestinesi, che chiedevano i nomi dei palestinesi che partecipano alle proteste.

Inoltre Israele si introduce negli account Facebook per accedere ad informazioni private, come l’orientamento sessuale, le condizioni di salute e mentali e lo status coniugale e finanziario. Un veterano dell’Unità 8200, un corpo d’elite dell’intelligence dell’esercito israeliano, spesso paragonato all’Agenzia per la Sicurezza Nazionale USA, ha testimoniato che questo materiale viene raccolto come mezzo di pressione. “Ogni informazione che possa consentire di ricattare una persona è considerata un’informazione rilevante”, ha detto. “ Sia che tale individuo abbia un certo orientamento sessuale, tradisca sua moglie o necessiti di cure in Israele o in Cisgiordania – è un bersaglio per essere ricattato.” L’intelligence israeliana ha preso di mira soprattutto palestinesi omosessuali, minacciando di pubblicare le loro foto intime per costringerli a collaborare con Israele.

Una simile intrusione nella vita privata dei palestinesi è resa possibile dal fatto che Israele occupa e controlla l’intera infrastruttura delle telecomunicazioni usata dalle compagnie e dai gestori del servizio di internet palestinesi. La mancanza di qualunque limitazione legale o etica sul punto fino al quale Israele può spingersi nella sorveglianza sui palestinesi nel 2014 ha addirittura portato 43 veterani dell’Unità 8200 ad inviare una lettera al primo ministro israeliano Benjamin Netanyahu per contestare “il continuo controllo di milioni di persone ed un’intrusione profondamente invasiva in quasi tutti gli ambiti della vita.”

Il complesso militare industriale del Paese è uno strumento ancor più pervasivo per il controllo digitale sui palestinesi. Israele produce ed esporta un’enorme quantità di tecnologie di sicurezza militare e cibernetica. Secondo un rapporto del 2016 di ‘Privacy International’, una Ong che indaga sui controlli da parte del governo e sulle imprese che lo consentono, Israele è la sede di 27 imprese di sorveglianza – il più alto numero pro capite di tutti i Paesi del mondo. Nel 2014 le esportazioni israeliane di tecnologie di sicurezza informatica e di sorveglianza all’estero, come il monitoraggio di telefoni e internet, hanno superato le esportazioni di armamenti. Queste tecnologie sono state vendute a regimi

autoritari e repressivi in Colombia, Kazakhstan, Messico, Sud Sudan, Emirati Arabi Uniti e Uzbekistan, tra gli altri.

Ambigui legami tra l'esercito israeliano ed il settore tecnologico rafforzano l'importanza del Paese nell'industria della sorveglianza. I veterani dell'Unità 8200 hanno fondato alcune delle principali compagnie israeliane di sicurezza informatica, come le imprese Mer e NSO. I veterani trasferiscono le loro competenze militari e di intelligence sviluppate nell'unità di elite al settore privato, dove non ci sono ostacoli legali relativamente alla sovrapposizione tra industria militare e di sorveglianza.

Facebook: neutrale o di parte?

Facebook si pubblicizza come una piattaforma aperta, al servizio di tutti. Il fondatore e amministratore delegato di Facebook, Mark Zuckerberg, ha detto recentemente: "Lavoro ogni giorno per unire le persone e creare una comunità per tutti. Speriamo di dare voce a tutto il popolo e di creare una piattaforma per tutte le idee."

Gli affari del gigante dei social media con Israele mettono in discussione tale affermazione. Mentre Facebook ha dei chiari protocolli e meccanismi per le richieste da parte di governi di rimuovere contenuti, e addirittura pubblica un rapporto biennale delle richieste dei governi, l'azienda viene spesso criticata per la sua mancanza di trasparenza e le sue decisioni arbitrarie. Un'inchiesta del *Guardian* ha rivelato le norme riservate di Facebook per limitare argomenti relativi a violenze, discorsi di odio, terrorismo e razzismo – norme che dimostrano la sua parzialità a favore di Israele.

Per esempio, Facebook segnala i sionisti come "gruppo globalmente protetto", il che significa che i contenuti che li attaccano devono essere rimossi. Un'altra regola spiega che "le persone non devono elogiare, sostenere o raffigurare un membro…di un'organizzazione terrorista, o di qualunque organizzazione che abbia lo scopo principale di intimidire una popolazione, un governo, o di usare violenza per resistere all'occupazione di uno Stato riconosciuto a livello internazionale." Di conseguenza, Facebook ha censurato attivisti e giornalisti in territori oggetto di disputa, come Palestina, Kashmir, Crimea e Sahara occidentale. Secondo rapporti dei media, Facebook ha rivisto la definizione di terrorismo per includervi l'uso di violenza premeditata da parte di organizzazioni

non governative “allo scopo di raggiungere un obiettivo politico, religioso o ideologico.” In ogni caso, la definizione permette di punire coloro che resistono all’occupazione e all’oppressione, mentre non include il terrorismo di Stato e la violenza inflitti ai palestinesi da parte di Israele.

Inoltre nel 2016 la ministra della Giustizia Ayelet Shaked ed il ministro della Pubblica Sicurezza Gilad Erdan hanno annunciato un accordo tra Israele e Facebook per creare delle squadre di monitoraggio e rimozione dei contenuti “che favoriscono l’incitamento [alla violenza]”.

Il direttore politico di Facebook, Simon Milner, nega l’esistenza di qualunque accordo speciale tra il suo datore di lavoro e Israele. Ha anche ribadito che tutti gli utenti di Facebook sono soggetti alle stesse politiche per la comunità di utilizzatori. Tuttavia un recente rapporto di Adalah [*organizzazione per i diritti umani e centro legale per i diritti degli arabi in Israele, ndtr.*] rivela che fin dalla seconda metà del 2015 l’ufficio del procuratore generale di Israele ha gestito un’unità informatica in collaborazione con Facebook e Twitter, per rimuovere contenuti online. Il resoconto finale annuale del 2016 dell’unità si fa vanto di aver trattato 2.241 casi e rimosso il contenuto in 1.554 di essi.

La collaborazione tra Israele e Facebook è dovuta probabilmente a molteplici ragioni. Anzitutto Israele ha una fiorente industria di alta tecnologia e rappresenta un lucroso mercato per Facebook. In secondo luogo, l’ufficio di Facebook a Tel Aviv rende la compagnia più soggetta all’influenza dei decisori israeliani. La nomina di Jordana Cutler, da lungo tempo principale consigliera di Netanyahu, a capo della politica e comunicazione di Facebook nell’ufficio israeliano è un caso emblematico.

Terzo, forse Facebook teme azioni legali. Nel 2015 un’organizzazione filoisraeliana, ‘Shurat HaDin-Israel Law Center’, ha intentato una causa contro Facebook negli Stati Uniti a nome di 20.000 querelanti israeliani, che accusavano la compagnia di “incitamento ed incoraggiamento alla violenza contro gli israeliani.” Il timore di Facebook di un’azione legale è espresso in un documento interno, che è trapelato, relativo ad un contenuto negazionista dell’Olocausto. Il documento spiega che Facebook semplicemente nasconderà o rimuoverà tale contenuto in quattro Paesi – Austria, Francia, Germania e Israele – per evitare cause legali.

Infine, benché Facebook neghi ogni discriminazione tra palestinesi ed israeliani, gli utenti palestinesi raccontano una storia diversa. Per esempio, poco dopo che una delegazione di Facebook aveva incontrato rappresentanti del governo israeliano nel settembre 2016, gli attivisti palestinesi hanno documentato interruzioni degli account personali su Facebook di giornalisti e di organizzazioni di informazione. Gli account di quattro giornalisti dell'agenzia di notizie palestinese Shehab e di tre giornalisti della rete Al Quds News sono stati chiusi. In seguito a proteste online e campagne con gli hashtag #FBCensorsPalestine e #FacebookCensorsPalestine, Facebook si è scusata per l'interruzione, spiegando che si era trattato di un errore.

La nuova legge sui crimini informatici dell'Autorità Nazionale Palestinese

Non è soltanto Israele a reprimere gli utenti palestinesi dei social media: lo fa anche l'ANP, per cassare opinioni politiche sfavorevoli o critiche verso la leadership palestinese. Tuttavia c'è una differenza fondamentale tra la portata del controllo digitale israeliano e le violazioni della libertà di espressione online da parte dell'ANP. Mentre il controllo digitale globale di Israele fa di ogni palestinese un sospetto ed un bersaglio, l'ANP utilizza le informazioni condivise pubblicamente per prendere di mira il dissenso politico.

L'ANP ha recentemente approvato una legge che limita ancor di più la libertà dei palestinesi di esprimersi online. La controversa legge sui crimini informatici è stata firmata dal Presidente palestinese Mahmoud Abbas il 24 giugno 2017, senza alcuna consultazione pubblica con le organizzazioni della società civile palestinese o con i gestori dei servizi internet. E' stata pubblicata con decreto presidenziale due settimane dopo la firma ed è entrata immediatamente in vigore.

Il pretesto della nuova legge è quello di combattere i reati informatici come l'estorsione per motivi sessuali, la frode fiscale e il furto di identità. Però l'utilizzo di termini vaghi come "armonia sociale", "modalità pubbliche", "sicurezza dello Stato" e "ordine pubblico" indica che la legge ha scopi differenti, in particolare eliminare la libertà di espressione online e reprimere ogni critica politica. Essa rende gli utenti palestinesi di internet, specialmente gli attivisti e i giornalisti, passibili di incriminazione da parte dell'ANP, che può interpretare le disposizioni della legge come vuole.

I primi due casi intentati in base alla legge rivelano il suo scopo. In entrambi è

stato utilizzato l'art. 20, che stabilisce che ogni utente di internet che possiede o gestisce un sito web che pubblica "notizie che mettono a rischio la sicurezza dello Stato, il suo ordine pubblico, o la sicurezza interna o esterna" può essere arrestato per un anno o multato fino a circa 1.400 dollari. Nel primo caso sono stati arrestati sei giornalisti palestinesi che lavorano per organi di stampa legati ad Hamas in Cisgiordania. Nel secondo caso, i servizi di sicurezza preventiva dell'ANP hanno arrestato Issa Amro, importante difensore dei diritti umani ed attivista politico nonviolento palestinese di Hebron, che aveva protestato con un post su Facebook per l'arresto da parte dell'ANP di un giornalista.

La legge è in netto contrasto con la legge fondamentale di tutela della privacy e della libertà di espressione. Conferisce alle istituzioni dello Stato un ampio potere di monitoraggio, raccolta e conservazione di dati relativi alle attività online di palestinesi nei Territori Palestinesi Occupati (TPO), e di fornire, su loro richiesta, tali informazioni alle autorità preposte all'applicazione della legge. Anche i gestori privati del servizio internet sono obbligati a cooperare con le agenzie di sicurezza raccogliendo, conservando e condividendo i dati informativi sugli utenti per almeno 3 anni, oltre che bloccando qualunque sito web su ordine della magistratura.

L'applicabilità della legge si estende oltre i confini legali dei territori controllati dall'ANP e consente di perseguire palestinesi che vivono all'estero. Ciò costituisce una reale minaccia per gli attivisti politici palestinesi che vivono all'estero, ma che hanno una notevole influenza sui social media in patria. Comunque la legge non specifica se le autorità possano tentare di ottenere l'estradizione di palestinesi che risiedono all'estero per aver commesso un crimine informatico.

Contrastare il controllo digitale

Mentre la violazione dei diritti digitali dei palestinesi è un caso unico, data l'occupazione militare israeliana, la lotta per questi diritti è globale. I governi, le organizzazioni della società civile, le agenzie di social media e gli utenti di internet hanno tutti un ruolo importante nella protezione della libertà di espressione online e della privacy dal controllo e dalla censura dello Stato.

In Palestina l'ANP deve revocare immediatamente la legge sui crimini informatici. Per adempiere meglio allo scopo che esplicitamente si propone – combattere il crimine informatico – l'ANP dovrebbe consultare le organizzazioni della società

civile ed altri importanti attori coinvolti per assicurarsi che ogni legge collegata all'informatica riduca effettivamente i crimini informatici senza violare i diritti politici dei palestinesi e le libertà pubbliche. Invece di reprimere i palestinesi per aver espresso le proprie opinioni politiche, l'ANP dovrebbe cercare di proteggere il suo popolo dagli arresti e dalle incriminazioni da parte di Israele con accuse senza fondamento di incitamento e terrorismo.

I diritti digitali, che sono parte del complesso dei diritti umani, sono un concetto relativamente nuovo nei Territori Palestinesi Occupati. Le organizzazioni palestinesi della società civile hanno la responsabilità di creare consapevolezza circa questi diritti, soprattutto riguardo alla sicurezza digitale. Proteggere gli account di un individuo e mantenere tali le informazioni private dovrebbe essere una priorità, soprattutto per giornalisti ed attivisti. Questo è particolarmente vero nel contesto di un'occupazione in cui l'occupante dispone di potenti capacità di controllo e controlla tutta l'infrastruttura delle telecomunicazioni.

La società civile palestinese ed i media devono anche smascherare e mobilitarsi contro le immorali pratiche di sorveglianza israeliane, la censura e la repressione della libertà di espressione dei palestinesi. Campagne online cresciute dal basso, come #FBCensorsPalestine e #FacebookCensorsPalestine, si sono dimostrate efficaci nell'attaccare le violazioni dei diritti digitali delle aziende di social media, dovute a prese di posizione faziose, nonostante le dichiarazioni di neutralità. I palestinesi hanno anche bisogno di coalizzarsi con organizzazioni internazionali per i diritti digitali, che possono aiutare a fare pressione sulle aziende di social media e sul governo israeliano perché interrompano le violazioni.

Note:

1. Questo scritto si basa su una tavola rotonda organizzata nel maggio 2017 da Al-Shabaka e dalla Fondazione Heinrich Boell a Ramallah, in collaborazione con "7amleh: Centro arabo per lo sviluppo dei social media". Le opinioni espresse in questo scritto sono dell'autore e non riflettono necessariamente l'opinione della Fondazione Heinrich Boell

(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)