La continua sorveglianza israeliana dei palestinesi ha un ‘effetto dissuasivo’

Usaid Siddiqui

7 maggio 2023 – Al Jazeera

Attivisti palestinesi dicono che il nuovo programma israeliano di riconoscimento facciale, denunciato da Amnesty International, contribuisce a rafforzare ulteriormente l’occupazione

L’ultima rivelazione dell’organizzazione per i diritti umani Amnesty International sull’utilizzo sempre crescente della tecnologia di riconoscimento facciale da parte di Israele contro i palestinesi non è stata una sorpresa per l’attivista Issa Amro.

“Lo vivo, lo sento, ne soffro, il mio popolo ne soffre,” dice ad *Al Jazeera* da Hebron.

Il 2 maggio Amnesty ha pubblicato un rapporto intitolato *Automated Apartheid [Apartheid automatizzato]*, in cui si descrive nei dettagli il funzionamento del programma israeliano *Red Wolf* [Lupo Rosso], una tecnologia di riconoscimento facciale usata dall’anno scorso per tracciare i palestinesi e che sembrerebbe collegata a simili programmi precedenti, noti come *Blue Wolf* e *Wolf Pack* [Lupo blu, Branco di lupi].

La tecnologia è stata utilizzata ai posti di blocco nella città di Hebron e in altre parti della Cisgiordania occupata scansionando i volti dei palestinesi e confrontandoli con i database esistenti.

Amnesty ha rivelato che, se nei database esistenti non si trovano informazioni sull’individuo, lo si registra nel Red Wolf automaticamente e senza consenso e potrebbe persino essere negato il passaggio attraverso il checkpoint.

In una dichiarazione a *The New York Times* l’esercito israeliano ha detto che si eseguono “necessarie operazioni di sicurezza e intelligence, con sforzi notevoli per minimizzare i danni alle normali attività quotidiane della popolazione palestinese’’.

Lo scrittore palestinese Jalal Abukhater ha affermato che i sistemi di sorveglianza sono utilizzati per far capire ai palestinesi di non avere diritti.

“La gente sente questo effetto dissuasivo, non socializza o non si sposta così liberamente come vorrebbe, non vive normalmente come vorrebbe,” ci ha detto Abukhater dalla Gerusalemme Est occupata.

“Questa forma di sistema di sorveglianza è utilizzata proprio per rafforzare l’occupazione… vogliono preservare l’apartheid.”

Secondo Amnesty la rete di sorveglianza con riconoscimento facciale è stata rafforzata anche a Gerusalemme Est, anche nelle vicinanze di luoghi di interesse culturale come la Porta di Damasco, il più ampio ingresso alla Città Vecchia e luogo di frequenti proteste contro le forze di occupazione.

L’anno scorso a febbraio Amnesty ha detto che Israele sta imponendo l’apartheid contro i palestinesi, trattandoli come “un gruppo razziale inferiore”. Altre organizzazioni, fra cui Human Rights Watch, con sede negli USA, e l’associazione israeliana per i diritti umani B’Tselem, sono arrivate a conclusioni simili.

Hebron, occupata da Israele nel 1967, è divisa in due parti: H1, amministrata dall’Autorità Palestinese, e H2, amministrata da Israele in base all’accordo su Hebron del 1997.

Ci sono circa 200.000 palestinesi che vivono in entrambe le parti e parecchie centinaia di coloni israeliani che sono fortemente protetti dall’esercito israeliano.

I palestinesi sono regolarmente costretti a passare tramite i checkpoint e a loro viene impedito di servirsi di parecchie strade importanti e autostrade.

‘Un laboratorio’

L’attivista Amro dice che i palestinesi che vivono a Hebron sono diventati meri “oggetti” di quelli che lui chiama “esperimenti israeliani”.

“Per le loro aziende per soluzioni di sicurezza Hebron è diventato un laboratorio per fare simulazioni, per identificare e risolvere problemi usandoci e commercializzare le loro tecnologie,” dice. “Noi non abbiamo voce in capitolo.”

Israele è annoverato fra i maggiori esportatori di tecnologie cibernetiche di monitoraggio di civili in vari Paesi, tra cui Colombia, India e Messico.

L'azienda di cibersicurezza israeliana NSO Group è stata molto criticata per Pegasus, il suo software di punta, un sistema di spionaggio usato da decine di Paesi per hackerare i telefonini.

Sono stati presi di mira centinaia di giornalisti, attivisti e persino capi di Stato.

Inoltre, aggiunge lo scrittore Abukhater, Israele ha bisogno dei programmi di cibersicurezza come Red Wolf per mantenere i suoi progetti di colonie illegali che si stanno espandendo nei territori occupati.

"Tecnologie di sorveglianza come questa [riconoscimento facciale] sono importanti, specialmente dove Israele sta introducendo coloni nel cuore delle cittadine palestinesi. Il fatto che [le colonie] si addentrino profondamente nei quartieri palestinesi in posti come Gerusalemme Est e Hebron crea un sacco di problemi," dice.

"È [la tecnologia di sorveglianza] un modo per controllare i palestinesi e far sì che l'espansione delle colonie continui senza essere ostacolata dalla resistenza palestinese."

Secondo le Nazioni Unite le colonie israeliane in Cisgiordania sono illegali e in "flagrante violazione" del diritto internazionale.

'Sempre osservati'

Secondo Amro gli apparati di sorveglianza hanno avuto un effetto significativo sui movimenti quotidiani dei palestinesi, lui incluso.

"Mi sento sempre osservato. Mi sento sempre monitorato … inclusi i miei social media, quando entro e esco da casa mia," dice.

"Delle donne mi hanno chiesto se loro possono vederle nelle camere da letto… è straziante sentire che le donne sono preoccupate per la loro intimità con i mariti, per i loro cari," aggiunge.

Secondo l'ingegnere elettronico, 43enne, le famiglie sono state costrette ad andarsene da Hebron, massicciamente sorvegliata, in quartieri meno controllati.

“Non ti sfrattano direttamente da casa tua. Ma ti rendono impossibile restarci… e molto dipende da queste tecnologie [di sorveglianza] e telecamere ovunque,” dice Amro.

Ori Givati, direttore di advocacy di *Breaking The Silence* [Rompere il Silenzio] un’organizzazione per i diritti umani di ex soldati israeliani e lui stesso un ex soldato israeliano, dice che i palestinesi “non hanno più spazio privato”.

“Se nel passato alcuni pensavano che almeno le loro informazioni private erano sotto il loro controllo, noi abbiamo tolto loro anche quello.”

Per parecchi anni Amnesty ha invocato la proibizione dell’uso della tecnologia di riconoscimento facciale per la sorveglianza di massa, dicendo che era usata per “soffocare le proteste” e “tormentare le minoranze”.

Negli Stati Uniti il riconoscimento facciale ha finito per prendere ingiustamente di mira persone di razza mista. Molte città come Portland e San Francisco hanno proibito il suo utilizzo da parte delle forze di polizia locali, mentre altre stanno discutendo misure simili.

L’utilizzo del riconoscimento facciale ha accelerato il passo in India, dove le autorità l’hanno usato per monitorare raduni politici e proteste contro il partito di governo di estrema destra, il Bharatiya Janata Party, sollevando i timori di un giro di vite contro il dissenso e la libertà di espressione.

(Traduzione dall’inglese di Mirella Alessio)

“Per Scopi Medicinali” Il settore militare israeliano e la crisi del

coronavirus.

Rapporto flash

Maggio 2020 – WHO PROFITS

Il Ministero della Difesa israeliano (IMOD), l'esercito e le imprese militari statali e private sono stati in prima linea nella risposta del governo israeliano alla crisi del coronavirus. Il loro cospicuo coinvolgimento, salutato dai media israeliani come dimostrazione di solidarietà sociale e impegno civile, evidenzia il profondo coinvolgimento militare alla base del regime economico e politico israeliano e la simbiosi esistente tra la sfera civile e l'apparato militare. Una delle caratteristiche che spiccano nel caso di Israele è la conversione della produzione e della ricerca e sviluppo (R&S) militare in un'azienda medica nazionale. Apparentemente da un giorno all'altro, il Direttorato per la Difesa (DDR e D) israeliano è stato trasformato in un hub di tecnologia medica, unità top secret di intelligence sono state convertite in centri di raccolta di informazioni mediche e le più grandi imprese militari israeliane sono diventate società appaltatrici per il settore medico. Questi sviluppi rivelano il dominio del settore militare nella ricerca e sviluppo commerciale israeliano e offrono nuove opportunità alle imprese militari di beneficiare materialmente e simbolicamente dalla crisi. In questo flash-report ***Who Profits*** [Centro di ricerca indipendente dedicato alla divulgazione del ruolo del settore privato nell'economia israeliana dell'occupazione, ndt] indaga le attività correlate al coronavirus dell'establishment militare e delle imprese private israeliane, concentrandosi sulle nuove iniziative lanciate, secondo quanto riferito, dalle tre maggiori e più lucrative società militari israeliane: l'*Israel Aerospace Industries* (IAI) di proprietà statale, e *Rafael Advanced Defense Systems* e *Elbit Systems* quotati in borsa.

"Una fusione di medicina e guerra"- La risposta militarizzata di Israele al Coronavirus

L'approccio militarizzato di Israele al virus è vividamente catturato nel *National CoronaPlan for Israel* del Ministero della Difesa israeliano (IMOD), un documento di trentuno pagine pubblicato il 29 marzo 2020. Il documento fa riferimento alla pandemia come "una fusione di medicina e guerra" e prevede un ruolo centrale per l'IMOD in materia di sanità pubblica e politica economica. [1] Tra le altre cose, presenta un'iniziativa pubblico-privata per sviluppare, rendere operativo e potenzialmente esportabile un sistema centralizzato di dati per valutare la probabilità degli individui di essere infettati dal virus. [2] I rapporti dei media hanno rivelato che la società privata coinvolta nel progetto è l'azienda di spionaggio informatico israeliana *NSO Group*. [3] Dall'inizio della crisi, gli organismi governativi di sicurezza nazionale hanno

svolto un ruolo di primo piano nella creazione e nell'attuazione dell'agenda coronavirus. Questi includono il *National Security Council* (NSC), operante nell'ufficio del primo ministro, il *Mossad*, l'agenzia di intelligence segreta di Israele e il *General Security Service* (GSS o Shin Bet). Il NSC è stato incaricato del coordinamento generale a livello nazionale, nonostante le dubbie qualifiche nei settori della sanità pubblica e dell'economia. La divisione dei ruoli tra il Mossad e lo Shin Bet nella risposta alla crisi ha riflesso i rispettivi settori di attività, internazionale e nazionale. Il Mossad, che opera una vasta rete globale di agenti segreti regolarmente collegati con casi confermati e presunti di omicidi extragiudiziali [4], è stato impiegato nell'ambito dell'approvvigionamento di attrezzature mediche. [5] Il capo della divisione tecnologica del Mossad ha riferito a un giornalista israeliano che parte dell'attrezzatura è stata ottenuta illecitamente, affermando che "noi attiviamo i nostri collegamenti speciali al fine di […] mettere le mani su partite che qualcun altro ha ordinato."[6] Lo Shin Bet, che opera nel territorio palestinese occupato e all'interno della linea verde, è stato rapidamente autorizzato dal governo israeliano a monitorare i pazienti coronavirus confermati e i probabili contatti.[7] I considerevoli poteri di sorveglianza della Shin Bet precorrono di gran lunga l'attuale pandemia e sono stati a lungo usati contro i palestinesi da entrambe le parti della Linea verde. Secondo Ynet [notiziario e sito web israeliano di contenuti generali, che è l'outlet online per il quotidiano Yedioth Ahronot, ndt], il monitoraggio dei pazienti con coronavirus si affida a un enorme database segreto già esistente, noto come "the Tool" [lo Strumento], che raccoglie dati continui in tempo reale su tutti i cittadini israeliani.[8] Lo Shin Bet è molto coinvolto nella politica israeliana degli omicidi mirati, nella stesura di black-list e a fornire indicazioni per le operazioni dell'aeronautica militare israeliana.[9] A settembre 2019, Amnesty International ha denunciato la tortura autorizzata dallo Stato del detenuto palestinese Samir Arbeed durante gli interrogatori dello Shin Bet.[10] La *Intelligence Division* dell'esercito israeliano è stata anche coinvolta nella risposta nazionale al coronavirus, stabilendo un *National Information and Knowledge Center on Coronavirus*.[11] Secondo quanto riportato dai media, due unità di intelligence d'élite, l'unità 8200, la *Signals Intelligence Uni,t* e l'unità 81, la *Intelligence Division's Technology Unit*, stanno al momento conducendo una ricerca medica correlata al coronavirus.[12] È significativo che gli sforzi tecnologici per affrontare il virus a livello nazionale non siano stati condotti dalla *Israel Innovation Authority* (IIA) o dal *Ministero della scienza e della tecnologia*, ma dal *Directorate of Defence Research and Development* (DDR & D) dell'esercito israeliano.[13] Il direttore della DDR & D, Brigadier-General (Res.) Dani Gold, è stato nominato capo del *National Technological Center to Fight Coronavirus*, che il Ministro della Difesa Naftali Bennett ha definito una "*commando unit*" per individuare tecnologie avanzate. [14] La Direzione ha istituito un "*National Emergency Team*" composto da alcuni ministeri del governo (Difesa, Salute e Finanza), esercito israeliano, industrie militari, IIA, società tecnologiche, ospedali e istituzioni accademiche. Il Centro fornisce la cornice

istituzionale per molte delle recenti collaborazioni tra le compagnie militari israeliane e le imprese medicali civili, gli ospedali e gli accademici in campo medico. Questa cornice fornisce un potenziale modello di sviluppo commerciale per il settore militare israeliano nel mercato medico. Come ha detto il Direttore della *Government Companies Authority* al quotidiano israeliano Globes, "I due tipi di industrie in cui c'è *big money* sono quelle che sviluppano mezzi per uccidere le persone e quelle che sviluppano mezzi per salvarle". [15] Come verrà discusso nella sezione seguente, dal lancio del Centro diretto dal DDR& D c'è stata una rapida proliferazione di proposte, prodotti e progetti relativi al coronavirus, che coinvolgono autorità israeliane di governo, capitale privato, enti accademici di ricerca e ospedali. Va sottolineato che questa sua nuova vocazione medica non ha distolto l'apparato militare israeliano dalla sua funzione primaria e ragion d'essere, ossia il continuo controllo militare sulla popolazione civile palestinese. La repressione quotidiana dei palestinesi rimane il lavoro "essenziale" dell'esercito. Secondo la rivista ufficiale dell'esercito israeliano, l'equipaggiamento di protezione, tra cui maschere e guanti chirurgici e altre misure fanno sì che i soldati possano continuare a compiere incursioni nelle case palestinesi nella Cisgiordania occupata e pattugliare il territorio attorno a Gaza assediata con un minimo di rischio per sé.[16] Inoltre, dal momento della crisi, sono avvenute diverse segnalazioni di attacchi aerei israeliani in Siria [17], che hanno sollevato la possibilità che Israele stia approfittando della crisi sanitaria globale per ottenere benefici geopolitici strategici.[18]

Militarismo nella medicina – Esercito militare israeliano e tecnologia correlata al Coronavirus

La crisi del coronavirus spalanca una finestra su come funziona il trasferimento della conoscenza militare israeliana alle industrie civili, in questo caso l'industria medica. Le ricerche precedenti di ***Who Profits*** hanno messo in luce i modi in cui la commercializzazione del know-how militare israeliano generato dall'occupazione si estenda oltre l'industria della sicurezza e all'interno dei mercati civili. L'apparato militare statale funziona come un laboratorio, un punto di riferimento, un cliente e un incubatore per l'innovazione tecnologica israeliana. Dai muri sottomarini alle armi per il controllo della folla e ai sistemi biometrici, l'occupazione prolungata di Israele fornisce un terreno fertile per lo sviluppo e l'applicazione di nuove tecnologie di controllo. I contratti con le forze armate israeliane fungono da "biglietto da visita" [19] per le aziende con i potenziali clienti, dando loro un vantaggio competitivo. L'importanza di avere l'establishment militare come acquirente di prodotti di sicurezza ha risvolti sia materiali sia in termini di reputazione, creando la domanda locale iniziale e facilitando l'emergere dell'industria locale.[20] Infine, le industrie militari e di proprietà statale rappresentano un campo di addestramento altamente efficace per i lavoratori della tecnologia,

molti dei quali, dopo aver lasciato il settore militare, vengono ad occupare posizioni chiave nel settore privato dell'alta tecnologia, portando con sé il know-how tecnico e la rete informale ottenuta nel corso della loro carriera militare. Un'indagine della risposta tecnologica israeliana alla pandemia di coronavirus rivela il coinvolgimento dei tre maggiori attori del settore militare israeliano. Secondo quanto riferito, IAI, Rafael ed Elbit Systems sono stati coinvolti in innumerevoli iniziative legate al coronavirus, tra cui la produzione di ventilatori e la conversione di funzionalità di monitoraggio remoto per uso medico. Mentre IAI, Rafael ed Elbit derivano la maggior parte delle loro entrate dai mercati della difesa e della sicurezza, tutti e tre sono attivi nel mercato civile, direttamente o tramite le loro filiali. Nel 2018, IAI ha riferito che il 28% delle sue entrate proveniva dal mercato civile.[21] Rafael detiene il 49,9% di *Rafael Development Corporation* (RDC), una società privata che gestisce un portafoglio di società tecnologiche impegnate nello sviluppo di prodotti basati su tecnologie militari originarie di Rafael per i mercati civili.[22] Elbit Systems fornisce prodotti e soluzioni in una serie di settori commerciali, compresa la strumentazione medica.[23] Precedenti ricerche di ***Who Profits*** hanno dimostrato che tutti e tre hanno adattato le proprie capacità militari ad uso nella crescente industria della tecnologia agroalimentare: IAI ha convertito droni per uso agricolo, la controllata *Rafael mPrest* ha collaborato con *Netafim* su una piattaforma di irrigazione digitale ed Elbit è membro di un consorzio di ricerca sulle tecnologie di identificazione delle piante.[24] L'attuale crisi della sanità pubblica presenta a queste società nuove prospettive di guadagno materiale e simbolico. La capacità di diversificare la loro offerta di prodotti è particolarmente significativa in quanto la pandemia minaccia di avere un impatto sulle catene di approvvigionamento della difesa globale e sulle priorità di bilancio dei governi [25]. Inoltre, con il numero di pazienti in condizioni critiche in Israele [26], il potenziale per future esportazioni è innegabile.

Ventilatori

Una delle prime iniziative intraprese dalla DDR & D è stata abbinare i produttori israeliani di ventilatori alle industrie militari, sfruttando le capacità di produzione di queste ultime per aumentare la produzione [27]. ll Direttore della DDR & D ha riferito ai media israeliani che "le nostre industrie militari hanno capacità straordinarie di produrre rapidamente e in grandi quantità qualsiasi componente, armi o ventilatori, e di eliminare la dipendenza dalle importazioni". [28] Secondo un'intervista al capo della divisione tecnologica del Mossad, anche il Mossad ha procurato, "con mezzi tortuosi", informazioni vitali per la produzione di ventilatori. [29] Il 31 marzo 2020, IAI ha dichiarato in un comunicato stampa che il DDR & D, la Direzione di Produzione e Approvvigionamento dell'IMOD, la società israeliana privata *Inovytec Medical Solutions* e un Dipartimento segreto di produzione di missili IAI hanno istituito una

linea di produzione per i ventilatori *VentwaySparrow*.[30] Secondo *Calcalist*, il dipartimento di produzione in questione fabbrica satelliti di sorveglianza per l'IMOD e clienti internazionali. [31] Secondo quanto riferito, gli ingegneri IAI hanno preso parte a una collaborazione tra la divisione elettronica di *Aeronautica Militare, Microsoft Israel* e altre entità per convertire respiratori manuali in automatici [32] Rafael e le società israeliane private *Flight Medical e Baya Technologies* sono anche coinvolte nella produzione in serie di ventilatori.[33] *Flight Medical* è un produttore di respiratori portatili, [34] mentre *Baya Technologies* è specializzata nella produzione di sistemi elettronici sensibili per l'industria militare e medica. [35] In un blog Rafael ha dichiarato che la società stava fornendo assistenza per i componenti difficili da reperire e nella creazione di infrastrutture di produzione. [36] Infine, la Elbit Systems è stata selezionata dalla IMOD, DDR & D e dal Ministero della Salute per stabilire una linea di produzione seriale per fabbricare grandi quantità di ventilatori *LifeCan One*, basati sulla tecnologia sviluppata dalla start-up medica israeliana *LifeCan Medical*.[37]

Monitoraggio remoto

Mentre la produzione di ventilatori fa leva principalmente sulla capacità produttiva del settore militare, una serie di progetti tecnologici cerca di adattare le tecnologie militari israeliane, sviluppate nel contesto dell'occupazione prolungata di Israele del territorio palestinese e siriano, per uso medico civile. Tra questi progetti c'è un'iniziativa congiunta di Elbit Systems ed Elta Systems, una filiale interamente controllata dell'IAI, condotta nell'ambito del *National Technological Center* DDR & D, per sviluppare un sistema remoto di monitoraggio per pazienti affetti da coronavirus. [38] Secondo *The Marker* [quotidiano economico in lingua ebraica pubblicato dal gruppo Haaretz in Israele, ndt], il sistema si basa sul radar e sui sistemi ottici di *Elbitand Elta*, nonché sulle tecnologie sviluppate dalle startup israeliane *Neteera, Vayyar* ed *EchoCare*. [39] Un sensore altamente sensibile misurerebbe la frequenza cardiaca e respiratoria di un paziente mentre una termocamera misurerebbe la temperatura corporea; nella fase successiva, una componente di Intelligenza Artificiale può essere aggiunta per analizzare i dati. [40] Un'altra azienda che si unisce al business della tecnologia correlata al coronavirus è l'impresa israeliana di riconoscimento facciale *AnyVision*, i cui prodotti di sorveglianza sono stati impiegati nella Cisgiordania occupata, tra cui Gerusalemme est. La tecnologia aziendale è stata utilizzata nei checkpoint militari e nelle reti CCTV esistenti all'interno della Cisgiordania per monitorare e sorvegliare i palestinesi, [41] come anche dalla polizia israeliana per rintracciare i sospetti lungo le strade di Gerusalemme est controllate da Israele, dove tre residenti su cinque sono palestinesi. [42] All'inizio di aprile, Calcalist ha riferito che AnyVision inizierà a distribuire in un ospedale di Tel Aviv termocamere in grado di misurare in remoto la temperatura del corpo e determinare se l'alta temperatura è il risultato

di una malattia o di uno sforzo fisico. [43] Il sistema si basa sulle telecamere termiche *MiniIOP44* dell'IAI. Secondo Calcalist, la tecnologia è stata originariamente sviluppata per navi da guerra e droni militari. [45] Un prodotto simile, progettato per identificare le persone con febbre nei luoghi pubblici, è stato sviluppato dalla Rafael utilizzando le termocamere della sua parzialmente controllata (49,9%) Opgal. Secondo il blog dell'azienda "queste telecamere ad alta sensibilità, utilizzate nei dispositivi di tracciamento collegati ai nostri missili, sono in grado di rilevare e misurare il calore da una distanza significativa". [46] A seguito di uno studio pilota in due ospedali israeliani, il prodotto è attualmente operativo. In futuro, secondo il blog, tali telecamere potranno anche essere installate in luoghi come centri commerciali e negozi. Mentre la presenza dei maggiori attori militari israeliani nelle iniziative del *National Technological Center to Fight Coronavirus* è stata di vasta portata e onnipresente, esistono canali aggiuntivi per il trasferimento di conoscenze dall'apparato militare statale al settore medico privato. Diverse unità israeliane di *intelligence* militare, ingegneria informatica e programmi di addestramento funzionano da "nastro trasportatore" per centinaia di israeliani, molti dei quali migrano verso l'industria privata dell'alta tecnologia. [47] Un caso emblematico è la start-up israeliana *Sensible Medical*, composta in gran parte da veterani dell'Unità 81, l'unità tecnologica top-secret della divisione di *intelligence* dell'esercito israeliano. [48] Haaretz ha riferito che in un certo numero di ospedali israeliani la società sta testando l'uso del suo monitor del fluido polmonare ReDS per monitorare i polmoni dei pazienti affetti da coronavirus. [49] Secondo quanto riferito, il sistema ReDS è già in uso in Italia e negli Stati Uniti. [50] Il CEO di Sensible Medical, Amir Ronentold ha detto a Haaretz che la tecnologia di base del sistema è una tecnologia militare, "intesa a vedere attraverso i muri in condizione di guerra urbana o per localizzare i sopravvissuti sotto i detriti". [51]

1 National Corona Plan for Israel . Israeli Ministry of Defense. 29 March 2020.

2 Ibid. "This is why we have established in the IMOD in collaboration with the IDF [sic] and civilian

companies a centralized data system, into which we will 'spill' all the data…The system is ready to be operationalized. It is the most advanced system in the world, in my opinion, and will be replicated later (gladly!) all over the world."

3 Goichman, Rafaela. Ministry of Defense Teamed Up with NSO to Rate the Probability of You Catching Coronavirus. The Marker, 29 March, 2020. For more on the involvement of NSO Group, see NSO Group: Technologies of Control, Who Profits, May 2020. https://whoprofits.org/updates/nso-group-technologies-of-control/

4 Black, Ian. Rise and Kill First: The Secret History of Israel's Targeted Assassinations – review . The

Guardian. 22 July 2018. https://www.theguardian.com/books/2018/jul/22/rise-kill-first-secret-history-israel-targeted-assassinations-ronen-bergman-review-mossad

5 Holmes, Oliver. Israeli spies source up to 100,000 coronavirus tests in covert mission. The Guardian. 19 March 2020. https://www.theguardian.com/world/2020/mar/19/israeli-spies-source-100000-coronavirus-tests-covert-foreign-mission

6 Dayan, Ilana. Commander of Mossad war room for fighting coronavirus, in an interview with Uvda: Globally people are dying due to shortage of ventilators. That won't happen in Israel. Channel 12, 31 March 2020 (Hebrew).

7 Konrad, Ido. Equating coronavirus with terror, Netanyahu turns surveillance powers on Israelis. +972 Magazine, 15 March 2020. https://www.972mag.com/netanyahu-surveillance-coronavirus/

8 Bergman, Ronen and Shvartztuch, Ido. "The Tool" is exposed: The secret GSS database that collects your SMS texts, calls and locations. Ynet+, 27 March 2020 (Hebrew).

9 Weizman, Eyal. Hollow land: Israel's architecture of occupation. Verso books, 2012, p. 241. 10 Israel/ OPT: Legally-sanctioned torture of Palestinian detainee left him in critical condition. Amnesty International, 30 October 2019. https://www.amnesty.org/en/latest/news/2019/09/israel-opt-legally-sanctioned-torture-of-palestinian-detainee-left-him-in-critical-condition/

11 National Information and Knowledge Center on Coronavirus. Gov.il (Hebrew).

12 Berkovitz, Uri. Hush-hush IDF intel unit takes on Covid-19. Globes, 20 April 2020. https://en.globes.co.il/en/article-hush-hush-idf-intel-unit-takes-on-covid-19-1001325867

13 DDR&D- Directorate of Defense Research & Development. Israeli Ministry of Defense. Accessed 11 May 2020. https://english.mod.gov.il/About/Innovative_Strength/Pages/Directorate-_of_Defense_Research_Development.aspx

14 DDR&D: Emergency team to address the COVID-19 pandemic. Israeli Ministry of Defense. Accessed 11 May 2020.

15 Barkat, Amiram. Weapons against coronavirus. Globes, 1 April 2020. https://en.globes.co.il/en/article-weapons-against-coronavirus-1001324270

16 Barel, Merav, Van Zayden, Batya, Greenberg Cohen, Einav and Neustein, Lior. Adjusted training, surgical gloves and dispersing the force: How does one maintain operational preparedness under the coronavirus pandemic?. IDF [sic] Editorial Board, 22 March 2020 (Hebrew).

17 Salama, Daniel, Zeitoun, Yoav and Blumenthal, Itay. Syria: Israel attacked in the northern region. Ynet, 5 May 2020 (Hebrew).

18 Harel, Amos. Analysis Under Cover of COVID-19, Israel Seems to Intensify Its Attacks Against Iran in Syria. 5 May 2020.

19 Israel Aerospace Industries, 2018 Annual Report, p. 124. On file with Who Profits.

20 Gordon, Neve. "The political economy of Israel's homeland security/surveillance industry." The New Transparency: Surveillance and Social Sorting 28 (2009). P. 24

21 Israel Aerospace Industries, 2018 Annual Report, p. 154. On file with Who Profits.

22 Rafael Advanced Defense Systems, 2018 Annual Report, p. 13. On file with Who Profits.

23 Elbit Systems, 2019 Annual Report. On file with Who Profits.

24 Agribusiness as Usual Agricultural Technology and the Israeli Occupation. Who Profits, January 2020. https://whoprofits.org/report/agribusiness-as-usual/

25 Sreekumar, Arjun. How COVID-19 Will Impact the Defense Industry. The Diplomat, 27 March 2020. https://thediplomat.com/2020/03/how-covid-19-will-impact-the-defense-industry/

26 Covid-19 in Israel. Haaretz. Accessed 11 May 2020. https://www.haaretz.com/israel-news/EXT-INTERACTIVE-coronavirus-tracker-israel-world-updates-real-time-statistics-covid-19-cases-deaths-1.8763410

27 Etzion, Udi. Head of MOD emergency team: "We will supply ventilators in a short period time". Calcalist, 29 March 2020 (Hebrew).

28 Etzion, Udi. A peek into Israel's ventilators production line.Calcalist, 6 April 2020 (Hebrew).

29 Dayan, Ilana. Commander of Mossad war room for fighting coronavirus, in an interview with Uvda: Globally people are dying due to shortage of ventilators. That won't happen in Israel. Channel 12, 31 March 2020 (Hebrew).

30 In Accordance with the Directive of the Minister of Defense, Naftali Bennett: The Ministry of Defense, IAI and Invoytec will Begin the Serial Production of Israeli-developed Ventilators. Press release. Israel Aerospace Industries. 31 March 2020. Accessed 11 May 2020. https://www.iai.co.il/serial-production-of-israeli-developed-ventilators

31 Etzion, Urdi. Coronavirus brings military industries into a new battlefield. Calcalist, 31 March

2020 (Hebrew).

32 Ibid; Etzion, Udi. Head of MOD emergency team: "We will supply ventilators in a short period time". Calcalist, 29 March 2020 (Hebrew).

33 Ibid.

34 Flight Medical Homepage . Accessed 11 May 2020. https://www.flight-medical.com/

35 Etzion, Udi. A peek into Israel's ventilators production line. Calcalist, 6 April 2020 (Hebrew).

36 Fighting the Coronavirus with Powerful Technologies . Rafael Blog. Rafael Advanced Defense Systems, 16 April 2020. Accessed 11 May 2020. https://www.rafael.co.il/blog/rafael-fighting-the-coronavirus-with-powerful-technologies/

37 Globes Correspondent. Elbit Systems to produce LifeCan Medical ventilators . Globes , 10 April 2020. https://en.globes.co.il/en/article-elbit-systems-to-produce-lifecan-medical-ventilators-1001325034

38 Cohen, Sagi. Without a doctor's touch: An Israeli system will remotely monitor temperature and breathing in coronavirus patients . TheMarker , 31 March 2020 (Hebrew).

39 Ibid.

40 Ibid.

41 Ziv, Amitai. Scoop: The curious Israeli startup that operates clandestinely in the territories and surveils Palestinians. TheMarker, 14 July 2019 (Hebrew).

42 Solon, Olivia. Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians? NBC News, 28 October 2019. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

43 Kabir, Omer. Face Recognition Startup AnyVision to Deploy Thermal Cameras at Tel Aviv Hospital. CTech, 7 April 2020. https://www.calcalistech.com/ctech/articles/0,7340,L-3806587,00.html

44 MiniPOP Lightweight Payload for Day/Night Observation System. Israel Aerospace Systems. Accessed 11 May 2020. https://www.iai.co.il/p/minipop

45 Kabir, Omer. Face Recognition Startup AnyVision to Deploy Thermal Cameras at Tel Aviv Hospital. CTech, 7 April 2020. https://www.calcalistech.com/ctech/articles/0,7340,L-3806587,00.html

46 Fighting the Coronavirus with Powerful Technologies. Rafael Blog. Rafael Advanced Defense Systems, 16 April 2020. Accessed 11 May 2020.

47 Gordon, Neve. "The political economy of Israel's homeland security/surveillance industry." The New Transparency: Surveillance and Social Sorting 28 (2009).

48 Cohen, Sagi. Pilot in hospitals: A radar to warn about deteriorating condition of coronavirus patients. Haaretz, 30 April 2020 (Hebrew).

49 Ibid.

50 Sensible Medical ReDS Lung Fluid Monitor to Help COVID-19 Patients in Italy, US and Other Countries. News. Sensible Medical. 16 April 2020. Accessed 11 May 2020. https://sensible-medical.com/sensible-medical-reds-lung-fluid-monitor-to-help-covid-19-patients-in-italy-us-and-other-countries/

51 Cohen, Sagi. Pilot in hospitals: A radar to warn about deteriorating condition of coronavirus patients. Haaretz, 30 April 2020 (Hebrew).

(Traduzione dall'inglese di Angelo Stefanini)

WhatsApp: azienda israeliana ‘pesantemente coinvolta’ nello spionaggio dei nostri utenti

Stephanie Kirchgaessner da **Washington**

29 aprile 2020 – The Guardian

La NSO Group accusata di aver hackerato 1400 persone, inclusi attivisti per i diritti umani

Nuove deposizioni processuali presentate da WhatsApp rivelerebbero che una azienda israeliana specializzata in spyware usava server con sede negli USA e che era “pesantemente coinvolta” nell’hackeraggio di telefonini di 1.400 utenti di WhatsApp, inclusi funzionari governativi di alto livello, giornalisti e attivisti per i diritti umani.

Le nuove affermazioni sul NSO Group sostengono che l’azienda israeliana sarebbe responsabile di serie violazioni dei diritti umani, incluso l’hackeraggio di oltre una decina di giornalisti indiani e dissidenti del Rwanda.

Per anni, NSO Group ha detto che il suo software di sorveglianza è acquistato dai governi per rintracciare terroristi e altri criminali e di non avere a disposizione informazioni indipendenti riguardo a come tali clienti, che in passato avrebbero incluso l’Arabia Saudita e il Messico, usino il suo software.

Ma la causa intentata l’anno scorso da Whatsupp contro NSO, la prima nel suo genere intentata da una grande azienda tecnologica, sta rivelando altri dettagli su come lo spyware Pegasus verrebbe utilizzato contro obiettivi precisi.

La scorsa settimana WhatsApp ha rivelato come le proprie indagini su come Pegasus sia stato usato l’anno scorso contro 1.400 utenti mostrerebbero che i server controllati da NSO Group, non i governi suoi clienti, erano parte integrante di come si effettuavano gli hackeraggi.

WhatsApp ha detto che le vittime ricevevano telefonate tramite l’app di

messaggistica ed erano infettatate da Pegasus. Ha poi aggiunto: “NSO usava una rete di computer per monitorare e aggiornare Pegasus dopo che era stato impiantato sui dispositivi degli utenti. Tali computer erano controllati da NSO e servivano come centro nevralgico attraverso cui controllava le operazioni dei propri clienti e l’uso di Pegasus.”

Secondo l’accusa di WhatsApp, NSO otteneva un “accesso non autorizzato” ai suoi server tramite il processo di reverse engineering dell’app di messaggistica e poi eludeva le funzioni di sicurezza che impediscono la manomissione delle funzioni di chiamata della compagnia. Un tecnico di WhatsApp che aveva indagato sugli hackeraggi ha dichiarato in una deposizione giurata presentata al tribunale che in 720 casi l’indirizzo IP di un server in remoto era stato incluso nel codice malevolo usato negli attacchi. Secondo il tecnico, il server remoto con sede a Los Angeles era di proprietà di una azienda il cui data centre era usato da NSO.

NSO ha sostenuto nella sua deposizione di non avere informazioni su come i governi suoi clienti usino i suoi strumenti di hackeraggio e perciò non può sapere chi siano i loro bersagli.

Ma John Scott-Railton, un esperto che lavora per Citizen Lab [centro canadese che si occupa della difesa dei diritti dei cittadini contro l’uso improprio delle informazioni, ndtr.] e ha collaborato al caso con WhatsApp, ha detto che il controllo dei server coinvolti da parte di NSO suggerisce che l’azienda avrebbe avuto i log, inclusi gli indirizzi IP [etichetta numerica dei dispositivi informatici, ndtr.] che identificavano gli utenti oggetto della sorveglianza.

“Chi può sapere se NSO guarda quei log? Ma il semplice fatto che potrebbe avvenire smentisce quello che dicono,” fa notare Scott-Railton.

In una dichiarazione al *Guardian* NSO conferma quelle che aveva fatto in precedenza. “I nostri prodotti sono utilizzati per porre fine al terrorismo, limitare il crimine violento e salvare vite. NSO Group non gestisce il software Pegasus per i propri clienti,” afferma l’azienda. “Le nostre affermazioni precedenti sulle nostre attività, e la portata delle nostre interazioni con la nostra intelligence governativa e i clienti appartenenti alle forze dell’ordine sono corrette.”

L’azienda ha detto che avrebbe presentato la propria replica al tribunale nei prossimi giorni.

I nuovi sviluppi del caso arrivano nello stesso momento in cui NSO deve rispondere a domande, in sede separata, sull'accuratezza di un prodotto di tracciamento lanciato in seguito all'insorgere del Covid-19. Si chiama Fleming e usa i dati dei telefonini e le informazioni sulla salute pubblica per identificare con quali individui infettati si è venuti in contatto. Lo scorso finesettimana, un reportage dell'emittente NBC [rete televisiva US, ndtr.] ha affermato che la nuova app di tracciamento di NSO era commercializzata negli USA.

Ma in un thread su Twitter Scott-Railton ha sostenuto che la sua analisi rivelava che essa si basa su dati che sembrano molto imprecisi.

"Quando stai lavorando con dati che incorporano tante imprecisioni, sarebbe molto laborioso lanciare un allarme ogni volta che ciò accade. O chiedere la quarantena. O un test. La percentuale di falsi positivi esploderebbe. Ma … anche quella dei falsi negativi," ha aggiunto.

Interrogato sui tweet, NSO ha detto che le "accuse infondate" erano basate su "supposizioni e schermate non aggiornate e non su fatti".

"Fleming, il nostro prodotto contro il Covid-19, si è nel frattempo rivelato fondamentale per governi in tutto il mondo, contribuendo a contenere la pandemia. Stimati giornalisti di vari Paesi l'hanno esaminato, hanno capito come funziona la tecnologia e hanno riconosciuto che si tratta della più recente evoluzione dei software di analisi e che non mette in pericolo la privacy," ha concluso l'azienda.

(traduzione dall'inglese di Mirella Alessio)

Facebook censura un'importante operazione di fake news condotta

da Israele

Ali Abunimah

17 maggio 2019, Electronic Intifada

Facebook ha scoperto un'importante campagna israeliana per influenzare politici ed elezioni in tutti i Paesi del mondo.

Giovedì il gigante dei social media ha annunciato di aver rimosso 265 accounts di Facebook e Instagram con un seguito complessivo di 2.8 milioni di utenti, per coinvolgimento in "comportamento fraudolento coordinato."

"Questa attività ha avuto origine in Israele e si è concentrata su Nigeria, Senegal, Togo, Angola, Niger e Tunisia, oltre ad alcune azioni in America Latina e sudest asiatico", ha affermato Facebook.

Coloro che agiscono in rete si sono falsamente "presentati come soggetti locali, incluse agenzie di notizie locali, e hanno pubblicato presunte indiscrezioni su politici" e su "elezioni in diversi Paesi, opinioni di candidati e critiche di oppositori politici."

Facebook ha detto che "i soggetti che stanno dietro a questa rete hanno cercato di nascondere la propria identità", ma l'indagine della compagnia li ha collegati a "un ente commerciale israeliano" chiamato Gruppo Archimede.

Venezuela connection?

Il Gruppo Archimede è una società di consulenza con sede a Tel Aviv, che si vanta sul suo sito web di "condurre campagne vincenti in tutto il mondo", ma fornisce poche altre informazioni su di sé.

Interessante notare che uno dei filmati sul suo sito web mostra una manifestazione in Venezuela, suggerendo un segreto ruolo di Israele nel tentativo a guida statunitense di rovesciare il governo del presidente Nicolas Maduro.

Il *Times of Israel* [quotidiano israeliano on-line in lingua inglese, ndtr.] ha individuato l'amministratore delegato del Gruppo Archimede in Elinadav Heymann, citando la società svizzera di consulenza 'Negotiations.CH' che lo

annovera tra i suoi consulenti.

“Una biografia pubblicata sul sito web della compagnia lo descrive come ex direttore del gruppo lobbistico ‘Amici europei di Israele’, con sede a Buxelles, ex consulente politico del parlamento israeliano ed ex agente segreto delle forze aeree israeliane.”

Comunque dopo quell’articolo ‘Negotiations.CH’ sembra aver rimosso la biografia di Heymann dal suo sito web.

Sembra che Heymann stia cercando di far perdere le proprie tracce.

Su internet è ancora visibile una copia archiviata della sua biografia.

All’inizio di questo decennio Heymann era uno dei principali lobbisti a favore di Israele a Bruxelles. L’organizzazione che guidava, ‘Amici Europei di Israele’, era un’alleanza interpartitica di politici ostili ai diritti dei palestinesi.

Al momento apparentemente inattiva, ‘Amici europei di Israele’ è stata modellata sull’esempio di gruppi analoghi attivi a Washington. Heymann ha anche lavorato come consulente di politica estera per rappresentanti del partito conservatore britannico nel Parlamento Europeo.

Più grande del Russiagate

Secondo Facebook la campagna di condizionamento israeliana dal 2012 ha speso più di 800.000 dollari per annunci falsi – otto volte di più di quanto si dice abbia speso un’azienda gigante russa per inserzioni sui social media, soprattutto dopo le elezioni USA del 2016, un intervento insignificante che i politici USA e gli opinionisti favorevoli a Hillary Clinton hanno pubblicizzato come paragonabile all’attacco a Pearl Harbour.

Eppure è certo che l’ultima prova dell’inganno ideato da Israele attirerà una minima parte dell’attenzione suscitata dalla sterile ricerca di una presunta interferenza e collusione russa che ha ossessionato i media e le elite politiche americane negli ultimi tre anni.

Ma questa operazione è ben lungi dall’essere solo un tentativo nascosto di Israele di influenzare e sabotare le politiche e l’attivismo in tutto il mondo.

L’annuncio di Facebook di aver fermato l’operazione di ‘Archimede’ giunge solo pochi giorni dopo che WhatsApp, di proprietà di Facebook, ha rivelato che aveva identificato una grave falla nel sistema che l’azienda di spionaggio israeliano NSO Group stava usando per installare programmi spia sugli smartphone delle persone.

Il documentario riservato di Al Jazeera sulla lobby israeliana, reso pubblico l’anno scorso da *The Electronic Intifada* nonostante gli sforzi per censurarlo, ha rivelato che diversi gruppi lobbistici con sede negli USA stanno lavorando in segreto in coordinamento con il Ministero israeliano per gli Affari Strategici per spiare e monitorare cittadini statunitensi impegnati nel sostegno di cause legittime.

Il documentario ha mostrato che uno di quei gruppi lobbistici, ‘Il Progetto Israele’, ha condotto un’importante campagna segreta di condizionamento su Facebook.

Ma, in contrasto con la sua pronta azione di interruzione dell’operazione Archimede, Facebook ha detto a *The Electronic Intifada* di non aver riscontrato alcuna violazione nel modo in cui ‘Il Progetto Israele’ stava utilizzando segretamente la sua piattaforma.

(Traduzione di Cristiana Cavagna)