Un saluto a tutti i presenti, mi dispiace di non essere potuto venire per ascoltare anche gli altri interventi.

Sono Francesco Cibele di Radio Blackout. Cercherò di delineare alcune modalità di interferenza tra apparato tecnico militare sorvegliante israeliano e apparati repressivi europei. Ovviamente, come oramai è già stato definito in modo molto chiaro, Israele utilizza i territori palestinesi come laboratorio di ricerca, sviluppo, perfezionamento e marketing dei suoi prodotti, sia in ambito bellico, sia sorvegliante. La letalità e la sorveglianza di fatto si fondono costantemente. Sappiamo anche benissimo che questa unità di *signal intelligence*, sorveglianza avanzata dell'esercito israeliano, l' "unità 8200" è anche un incubatore di startup. La sua finanziaria si chiama 8200 EISP (*Enterpreneurship and Innovation Support Program*) finanzia startup per veterani e veterane dell'"unità 8200". Questi aspetti, appunto, li diamo abbastanza per scontati.

Cerchiamo di andare a vedere come operino intanto a livello di plasmazione determinate aziende. Non facciamo un elenco, ma stiamo cercando di osservare più che altro delle traiettorie di trasformazione e in parte anche come operi la formazione, la cooperazione tra apparati repressivi e via dicendo. Intanto è chiaro che Israele, al di là degli accordi di cooperazione militare, quindi degli accordi con i governi di turno, seppure dotati di una certa stabilità, e gli accordi con le forze dell'ordine per la formazione, soprattutto in ambito di antiterrorismo, cyber-sicurezza e via dicendo, abbia una fortissima diplomazia industriale all'opera. Non c'è bisogno dei governi che stringono accordi: Israele porta avanti una diplomazia sotterranea con accordi industriali, sostanzialmente sia di partnership con aziende del settore, sia di presenza proprio di stabilimenti delle sue aziende in altri paesi. Pensiamo a tutto il caso di Elbit System nel Regno Unito, dove si crea questa rete di diplomazia industriale sostanzialmente molto forte.

Al di là di questo, Israele accede ai fondi europei per la ricerca e questo è un aspetto molto importante. Israele e le aziende militari, anche israeliane, accedono ai fondi europei Horizon. Diciamo che Israele, associato ai programmi quadro di ricerca e innovazione europei dal '96, inizia a partecipare agli accordi e ai programmi Horizon (quindi finanziati con i fondi Horizon) dal 2014. I programmi Horizon spaziano in diversi generi di contesti, vanno dal medicale all'ambientale, alle tecnologie ambientali, al restauro, alla farmaceutica, eccetera. Quelli che ci interessano maggiormente sono l'ambito della robotica e dell'informatica. Dicevamo che formalmente i programmi militari non possono entrare all'interno dei finanziamenti Horizon. Eppure aziende militari israeliane riescono a bypassare questi limiti. Per esempio, c'è un programma di Elbit System che si occupa dello sviluppo di *head-up display* (quindi di visori che sovrappongono dati alla realtà) che è passato all'interno del capitolo “Sfide della società - Trasporti green” e via dicendo: come se fosse una

tecnologia neutralmente applicabile all'aeronautica. Elbit System, Israeli Aerospace Industries e altre compagnie di scala diversa dell'apparato tecnomilitare israeliano partecipano a questi programmi finanziati dai fondi europei. In particolare, riescono a entrare proprio aziende militari, soprattutto all'interno del portafoglio dell'Internal Security Fund e del Civil Security for Society; sono fondi che si occupano di finanziare ricerca tecnologica in ambito di sorveglianza interna e controllo delle frontiere, quindi biometria, varchi biometrici alle frontiere, accoppiamento di dati raccolti dal volto di una persona rispetto al suo storico di documenti e altre informazioni che riguardano l'individuo.

Al di là di questo, appunto, già si evidenzia molto chiaramente come ci siano delle aree veramente molto liminali tra guerra e repressione. Queste aziende sono settore bellico sorvegliante: sostanzialmente si occupano di tecnologie applicate sia alla letalità sia al controllo e alla repressione.

I programmi dual-use di Horizon non sono solo quelli degli esempi citati dove hanno partecipato aziende israeliane, ma anche contesti quasi incredibili da raccontare: cioè programmi per l'antincendio, droni che calcolano la traiettoria di caduta di oggetti dall'alto: “liquidi antincendio” ovviamente... Peccato che siano aziende come Israely Aerospace Industries che si occupano poi di fare cadere esplosivi addosso alla popolazione di Gaza.

Altri programmi molto importanti sono quelli che riguardano la robotica e l'informatica. Attualmente sono in corso diverse partecipazioni di Israele nei programmi finanziati dai pacchetti dei fondi Horizon (che potete trovare su Cordis, che è il portale in cui vengono pubblicati tutti i progetti e i loro avanzamenti) dove Israele partecipa a diversi progetti in ambito di *quantum computing* e soprattutto di crittografia. Perché è importante la crittografia? Come i Large Language Models, i chatbot sostanzialmente, programmi importanti perché fanno parte dell'arsenale operativo israeliano per modificare, diciamo, il consenso attraverso la moltiplicazione di pareri, opinioni favorevoli online attraverso chatbot e via dicendo… ma soprattutto perché la maggior parte dei prodotti che Israele vende all'apparato repressivo riguardano proprio il "bucare" le protezioni dei dispositivi.

Diciamo che ci sono due grandi famiglie di prodotti di questo tipo: ci sono quelli come *Cellebrite* che si chiamano Mobile Devices Forensic Tools, quindi dispositivi per l'analisi forense delle tecnologie mobili dei telefonini, e in questo caso *Cellebrite* è il prodotto più noto, che abbiamo visto venire progressivamente sempre più impiegato, il cui l'uso viene sempre più normalizzato in Italia.

E se *Cellebrite* viene definita una tecnologia di grado militare, adesso vediamo che molte forze di polizia locale e di polizia stradale, hanno licenze Cellebrite in Italia –

per esempio – per entrare nei dispositivi dopo gli incidenti e vedere se una persona era al telefonino mentre si è schiantata contro un lampione. *Cellebrite* non si occupa solo di quella parte, cioè di estrarre i dati con un cavo USB da un telefono, si occupa anche poi di organizzare questi dati, di elaborarli, di conservarli, e quindi vende strumenti alle forze dell'ordine basati su intelligenza artificiale per osservare ricorrenze, ad esempio all'interno dei dati: vedere all'interno di un set di dati, raccolto magari all'interno anche di indagini diverse, se ci sono corrispondenze tra immagini, tra indirizzi, tra messaggi, tra persone citate nei messaggi su WhatsApp, per esempio. Tutto questo compone appunto un'architettura informatica che va a plasmare l'operatività stessa delle forze dell'ordine grazie a questi strumenti.

Ovviamente un altro contesto importantissimo (poi arriveremo anche agli spyware, appunto ai malware di Stato, gli strumenti per prendere il controllo dei dispositivi) e fondamentale è quello della biometria: trasformare il corpo (l'immagine) in dati, trasformare di fatto un individuo in un codice che lo rende riconoscibile appena supera un varco biometrico. L'attore più interessante da studiare in ambito di aziende israeliane di sorveglianza biometrica è *Corsight*.

Corsight nasce nel 2019 in quel contesto, appunto, come dicevamo prima, di incubazione di startup militari sorveglianti per il riconoscimento biometrico, non solo riconoscimento facciale. Inizia con il riconoscimento facciale, vende i suoi prodotti alle forze dell'ordine in giro per il mondo; sviluppa progressivamente testandoli proprio in West Bank, in Cisgiordania, degli algoritmi di analisi biometrica delle condotte, quindi analisi delle immagini non solo per riconoscere chi sia una persona, ma per capire che cosa stia facendo in modo automatico, visto che per osservare la mole di dati prodotti dai flussi video costanti di centinaia di telecamere, servirebbero molti operatori umani. L'automazione serve proprio a quello. L'automazione serve, così come per i sistemi d'arma autonomi, a disaccoppiare quantità di umani da quantità di letalità allo stesso modo, in ambito sorvegliante-repressivo, l'automazione serve a disaccoppiare operatori umani, che devono guardarsi degli schermi, rispetto invece a delle intelligenze artificiali che ti mandano una segnalazione.

Corsight fa analisi biometrica delle condotte: dove sta guardando un individuo, se sta afferrando degli oggetti, se più individui si stanno radunando, si stanno accorpando, se si sta per esempio per formare un corteo. Tutti questi sono parametri che questi software analizzano e riconoscono in modo automatico e possono così mandare delle segnalazioni automatizzate a forze di intervento, forze di sicurezza umane. Le tecnologie di questo tipo di *Corsight*, non pensiamo siano circoscritte all'antiterrorismo più oscuro, col passamontagna che ti piomba in casa con la corda.

No, vengono sviluppate in un contesto di oppressione e di forza letali, vengono poi vendute in giro per il mondo. Per esempio, la suite di *Corsight* sul riconoscimento biometrico viene utilizzata nei casinò per osservare condotte fraudolente. Vende tantissimi dei prodotti nel contesto dell'antitaccheggio: quindi vedere come una persona in un negozio si sta comportando, se ha delle condotte sospette, se si sta infilando qualcosa sotto la giacca, addirittura per quello che si definisce *sweethearting* (cuore d'oro), ovvero se i commessi fanno dei regalini impropri a dei loro amici, o trattano in modo preferenziale alcuni clienti. Tutto questo tipo di condotte all'interno dei negozi può essere controllato da tecnologie *Corsight*, che appunto nascono, vengono testate e hanno come spinta di marketing la letalità oppressiva dei territori palestinesi e finiscono poi nelle catene di negozi, per esempio nel Regno Unito, nei casinò in Australia e via dicendo.

Il sistema di riconoscimento facciale di Corsight si chiama Fortify (usato dal DHS), e vende ad ICE la versione *Mobile Fortify* [nota: attribuita a NEC] che sta appunto all'interno dei dispositivi dei miliziani di ICE per i rastrellamenti all'interno dei territori statunitensi.

La ministra degli interni britannica, la Home Secretary, ha appena pubblicato le linee guida per la riforma delle forze dell'ordine britanniche in chiave di normazione dell'utilizzo (già in corso da anni, ma che esce da una zona grigia e si moltiplica) del riconoscimento biometrico e dell'intelligenza artificiale. Tecnologie predittive per riformare appunto le forze dell'ordine britanniche: è uno dei cambiamenti più radicali nella storia recente delle forze dell'ordine in generale, perché viene appunto progettato nell'insieme questo corpo di trasformazione. All'interno di questo corpo di trasformazione, di questa traiettoria, un ruolo centrale ce l'avrà appunto *Corsight*, come già emerso.

Dagli elementi preliminari sappiamo anche che i carabinieri italiani utilizzano tecnologia di riconoscimento facciale *Corsight*, come è uscito, anche se con pochi dati, da una recente inchiesta su Fanpage.

Oltre appunto però alla biometria, torniamo al discorso degli spyware. Abbiamo visto che all'interno dei fondi di ricerca europei Horizon, Israele partecipa a programmi per la crittografia e il *quantum computing*: gli strumenti più venduti dell'apparato industriale sorvegliante israeliano sono appunto gli spyware. All'interno del mondo degli spyware ci sono quelli di *Candiru*, ci sono quelli di *NSO Group*... NSO Group sono un po' i cattivi, sono quelli che sono balzati maggiormente all'onore delle cronache perché vendono le loro licenze per questo strumento – teoricamente antiterrorismo – più o meno a chiunque gliele chieda, per monitorare giornalisti, attivisti, e via dicendo. Il software Pegasus di *NSO Group* è stato trovato nel telefono

della moglie del giornalista Khashoggi, prima che appunto venisse smembrato in un consolato saudita ad Istanbul. E poi c'è *Paragon Solutions*.

Paragon Solutions, invece, cercano di porsi un po' come quelli corretti, come i buoni nel mercato degli Spyware rispetto ai cattivi di *NSO Group*. *Paragon Solution*, ricordiamo, in Italia è stato al centro di questo teatrino: il suo software di spionaggio dei dispositivi **Graphite** è stato trovato sui telefoni di giornalisti di Fanpage invisi al governo Meloni per le inchieste su Gioventù Nazionale, oltre che trovato sui dispositivi di attivisti di ONG per il soccorso di migranti, e di fronte a ciò, Mantovano, il Sottosegretario alla Presidenza del Consiglio ha detto: «Noi non possiamo dire nulla, diciamo che alcuni fenomeni riguardano la sicurezza nazionale, altri no. Non abbiamo mai acquistato licenze per spiare i giornalisti. Provate il contrario».

Sarebbe abbastanza semplice provare il contrario, perché *Paragon Solutions* evidentemente avrà un registro di cosa è avvenuto. Ad acquistare le licenze dicono che magari non sia stata l'Italia...

Di fatto, comunque, *Paragon Solutions* vende i suoi prodotti alle forze dell'ordine e se fino a qualche anno fa l'utilizzo dei captatori informatici, appunto degli spyware, era limitato, sia perché il mercato era meno esteso, sia perché non c'era una normazione chiara a riguardo, adesso vengono sostanzialmente equiparate alle intercettazioni ambientali. Sono in grado di attivare e disattivare i microfoni e le videocamere dei telefoni in momenti specifici, sono in grado di controllare tutta la corrispondenza delle telecomunicazioni.

Perché è interessante proprio *Paragon Solutions*? Non solo perché il suo software spia è stato trovato in contesti di – diciamo – repressione del dissenso in Italia in particolar modo, mentre invece l'altra gamma in cui sicuramente opera è per il discorso della “sicurezza nazionale” e come tendono a definire loro i fenomeni... Ma Paragon Solution è fondata non da un militare qualunque dell'esercito israeliano, è fondata da Ehud Barak. **Ehud Barak** è sia un ex militare, sia un ex primo ministro israeliano. Ehud Barak, tra l'altro, è una persona che ha dei canali di collegamento con l'apparato di sicurezza italiano, oltre a essere tra l'altro probabilmente uno dei burattinai dietro l'asset Jeffrey Epstein come asset di dossieraggio e ricatto delle persone più potenti al mondo, visto che appunto ci sono contatti dimostrati tra Ehud Barak e Jeffrey Epstein... Ehud Barak che fonda un'azienda di spyware che vende alle forze dell'ordine anche italiane. Barak è anche una persona che lo stragista miliardario dell'amianto Schmidt Diney, ha contattato per essere assolto (ed è stato poi assolto in Italia) dalla strage dell'amianto che ha compiuto.

Al di là di tutto questo, per concludere, un contesto veramente importante sono le forze dell'ordine locali.

Le forze dell'ordine locali, perché sono molto permeabili sia al lobbying, sia all'introduzione di nuove tecnologie. Per esempio, una tecnologia che si sta diffondendo all'interno dei comuni italiani è *Safer Place*. Vi leggo un breve estratto di un articolo del 2023 del prestigioso quotidiano "La Provincia di Cremona": «Il Comune di Cremona doterà una parte delle auto della polizia municipale con questo sistema derivato dal settore militare (non si specifica settore militare israeliano), nel quale viene utilizzato in particolare nella lotta contro il terrorismo. A Cremona, anziché monitorare situazioni di potenziale pericolo legato ad attentati, *Safer Place* sarà utilizzato per individuare e nel caso sanzionare comportamenti scorretti alla guida; il dispositivo è già in utilizzo in vari capoluoghi italiani». Siamo nel 2023… grazie alla connessione tra quanto registrato dalle videocamere e il software di elaborazione, la capacità di scansionare tutte le targhe visibili, di collegarsi al database ministeriale e di controllare in automatico se dovessero esserci problemi per la mancanza di revisione, assicurazione o addirittura auto nelle liste nere, quindi auto – per esempio – che possono essere veicoli che devono essere bloccati perché sospetti di essere stati coinvolti in dei reati. Sostanzialmente questo sistema si basa sulla lettura di targhe e la lettura di targhe è quella forma di riconoscimento degli oggetti molto affine al riconoscimento facciale: se il nostro volto viene trasformato in un codice, il nostro volto diventa la nostra targa.

Sostanzialmente, adesso si stanno normalizzando all'interno dei comuni italiani degli strumenti di riconoscimento automatizzato. I primi sono stati attivati con le ZTL semplicemente per riconoscere se determinati veicoli potevano accedere a delle “zone rosse”. Si stanno moltiplicando le Zone Rosse per umani e stanno moltiplicando tecnologie in grado di automatizzare il riconoscimento e l'analisi dei dati che riguardano un veicolo.

Ci sarebbe poi tutta una parte sulla formazione delle forze dell'ordine, i corsi antiterrorismo, i contatti, appunto, tra forze dell'ordine e l' apparato sionista, o per esempio i corsi di indottrinamento recentemente emersi per – di fatto – formare le forze dell'ordine in un'ottica di rappresentazione delle mobilitazioni per Gaza come eterodirette dal Qatar e dai Fratelli Musulmani, sostenendo che il genocidio non è mai avvenuto. Ci sono poi dei corsi professionali di formazione del comando interforze (e quindi funzionari di polizia, carabinieri, Guardia di Finanza) che vanno in Israele a farsi addestrare dalle truppe delle forze speciali israeliane, e ci sono anche quei corsi privati fatti da aziende della formazione israeliana. Per esempio, c'è questa azienda che si chiama *Cherries* (come “ciliegie”) *Counter Terror*, che rilascia attestati con il grado di «addestramento israeliano per il riconoscimento dei comportamenti». Il loro

motto è: «una delle differenze fondamentali nella metodologia israeliana di sicurezza è che noi non cerchiamo armi, ma cerchiamo terroristi» e quindi tutta una formazione sulla lettura della comunicazione non verbale e via dicendo. Non mi dilungo oltre.

Grazie mille per questa iniziativa veramente importante. Buona lotta a tutte le compagne e i compagni. Ciao.