15. Dicembre

Riflessioni a margine di TELETHON: Il Guardian Studys Program

(Parte seconda)

Le previsioni sono estremamente difficili.
Specialmente sul futuro.
Niels Bohr

Negli Stati Uniti, lo **screening neonatale** è un programma sanitario unico che supporta l'equità sanitaria e controlla praticamente ogni bambino dopo la nascita, e ha portato cure tempestive ai bambini sin dagli anni '60.
Il **Newborn Screening Program** identifica efficacemente i bambini con *determinati disturbi* ed è richiesto per tutti i neonati nati nello Stato di New York, a meno che i genitori non confermino, per iscritto, di avere un'obiezione religiosa.

Procedura:
-Un piccolo campione di sangue viene raccolto pungendo il tallone del neonato di solito 24-36 ore dopo la nascita.
-Il sangue viene utilizzato per lo screening di **50 diversi disturbi**.
-Non vi è alcun costo per questo servizio.

I neonati con uno di questi **disturbi** possono sembrare sani alla nascita, pertanto è necessario eseguire il test per intercettare quelli con un disturbo.
Lo *screening* è progettato per identificare tutti i neonati con il potenziale per uno di questi disturbi.
Sono quindi necessari ulteriori test per verificare se il o neonato ha o meno il disturbo.
I genetisti lavorano con gli operatori sanitari per garantire che i neonati con risultati di test anormali ricevano diagnosi e cure di conferma appropriate.

Con la diminuzione del costo del sequenziamento e il miglioramento dei metodi per interpretare i dati genetici, esisterebbe l'opportunità di aggiungere il *sequenziamento del DNA* come metodo di screening per facilitare l'identificazione di bambini con condizioni curabili che non possono essere identificate in nessun altro modo scalabile.

Il **Guardian study** è un progetto per valutare se e come situazioni particolari possono essere effettivamente sottoposti a screening alla nascita, se i genitori desiderano tali informazioni e quale impatto può avere la diagnosi precoce

GUARDIAN STUDY

è uno studio di ricerca che esamina i neonati per oltre **250 condizioni genetiche** non attualmente sottoposte a screening neonatale standard. Lo scopo di questo studio è trovare bambini che hanno queste condizioni in modo che possano avere le migliori possibilità di vivere una vita più

sana. Per le condizioni per le quali è disponibile un trattamento, è importante iniziare presto. Lo studio è gratuito. Non ci sono costi per la famiglia o per la compagnia assicurativa.
Non è necessario alcun campione di sangue aggiuntivo per completare questo studio.
Questo studio è diverso dallo **screening neonatale standard**. Lo screening neonatale standard viene eseguito su tutti i bambini nati negli Stati Uniti e testa circa 50 condizioni diverse e viene eseguito di routine per ogni neonato

Il progetto **Guardian** è guidato dalla prestigiosa genetista della Columbia University **Wendy Chung**,

e sequenzierà il DNA di **100.000** neonati per circa **158 malattie curabili**.
I genitori possono anche chiedere di aggiungere altri **100 disturbi neurologici** che non possono essere curati, ma per i quali una diagnosi precoce e la fisioterapia potrebbero aiutare.

La storia di Cora

Nel 2016 è nata a Boston una ragazza di nome Cora Stetson. Entro 48 ore, il personale dell'ospedale ha puntato il tallone per ottenere una goccia di sangue per cercare molecole che segnalano dozzine di malattie genetiche rare, un test richiesto per tutti i neonati statunitensi.
Poiché i genitori di Cora avevano accettato di iscriverla a uno studio, un ricercatore ha anche prelevato del sangue per un test molto più ampio, uno che ha setacciato il suo genoma per circa 1500 geni della malattia.

Le informazioni genetiche si sono rivelate cruciali. Sebbene il test standard abbia segnalato un disturbo che coinvolge un enzima di elaborazione della **vitamina B chiamato biotinidasi**, un test di follow-up è risultato negativo e il suo pediatra ha concluso che Cora non aveva il disturbo.

Ma il test del genoma ha rivelato che aveva effettivamente mutazioni che causavano il deficit di biotinidasi, una forma lieve che tuttavia poteva provocare "*cattiva vista e difficoltà a scuola*", dice la madre di Cora.
Cora ora prende una compressa di **biotina** al giorno ed è una bambina dell'asilo "coraggiosa, pazza, sfacciata"

Il **caso di Cora** illustra l' enorme potenzialità del sequenziamento dell' intero genoma dei neonati: scoprire una quantità di informazioni genetiche che potrebbero identificare i bambini che necessitano di cure e migliorare la salute più avanti nella vita.

l sequenziamento del genoma ha mostrato che **Cora Stetson** ha ereditato una carenza enzimatica dai suoi genitori. Ora ha 5 anni, prende un integratore e sta crescendo senza alcun problema

Cora Stetson con i suoi genitori oggi

Allegato
Wendy Chung

Wendy Chung è una genetista clinica e molecolare certificata dal consiglio di amministrazione dell'ABMG con 20 anni di esperienza nella ricerca genetica umana di tratti monogenici e complessi tra cui malattie come cancro al seno, cancro al pancreas, cardiopatie congenite, ipertensione polmonare, aritmie ereditarie, cardiomiopatie, obesità, diabete, ernie diaframmatiche congenite e autismo.

Ha una vasta esperienza nella mappatura e clonazione di geni negli esseri umani, nella descrizione delle caratteristiche cliniche e nella storia naturale di nuove condizioni genetiche e nella caratterizzazione dello spettro delle malattie, nonché nello sviluppo di cure e trattamenti su misura per le malattie genetiche rare.

Chung dirige i programmi di ricerca finanziati dal NIH sulla genetica umana dei difetti congeniti tra cui l'ernia diaframmatica congenita, le cardiopatie congenite, l'atresia esofagea, l'autismo, disturbi dello sviluppo neurologico, ipertensione polmonare, cardiomiopatia, obesità, diabete e cancro al seno. Dirige la Precision Medicine Resource presso l'Irving Institute della Columbia University.

Ha ricevuto l'American Academy of Pediatrics Young Investigator Award, il Medical Achievement Award da Bonei Olam, la New York Academy Medal for Distinguished Contributions in Biomedical Science e il Rare Impact Award dalla National Organization of Rare Disorders.

La dottoressa Chung è rinomata per il suo insegnamento e tutoraggio e ha ricevuto il più alto riconoscimento per l'insegnamento della Columbia University, il Presidential Award for Outstanding Teaching.

Ha guidato lo studio pilota di screening neonatale dell'atrofia muscolare spinale a New York, che ha contribuito a portare all'adozione nazionale di questo test nei neonati.

. Chung apprezza le sfide della genetica come campo della medicina in rapida evoluzione e si impegna a facilitare l'integrazione della medicina genetica in tutte le aree dell'assistenza sanitaria in modo medico, scientifico ed etico valido, accessibile ed economico. Ha conseguito la laurea in biochimica ed economia presso la Cornell University, la laurea in medicina presso il Cornell University Medical College e il dottorato di ricerca. dalla Rockefeller University in genetica.
Primo consulente medico della Casa bianca è nell'elenco dei primi dieci medici degli Stati Uniti

Un anno fa… Baedeker/Replay del 15. Dicembre
Perché nei prossimi giorni sarà indispensabile monitorare la diffusione di Omicron in tempo reale

Sappiamo ancora poco su Omicron, ma una tendenza preoccupante diventa sempre più precisa : questa variante si sta sicuramente diffondendo rapidamente in sud Africa, Regno Unito e Danimarca i paesi con la migliore sorveglianza (sequenziamento) delle varianti che lo cercano con maggiore impegno e quindi probabilmente sta crescendo silenziosamente ovunque. La variante in sud Africa ha superato la già alta trasmissibilità della Delta e potrebbe presto fare lo stesso altrove. Secondo stime preliminari, ogni persona con Omicron ne sta infettando almeno 3 dato approssimativamente pari con la velocità con cui il coronavirus si è diffuso quando è diventato globale per la prima volta all'inizio del 2020. In altre parole, Omicron si sta diffondendo in popolazioni altamente immunizzate con la stessa rapidità del virus originale in popolazioni prive di immunità. Se questo trend viene lasciato incontrollato, dobbiamo aspettarci una grande ondata di Omicron, più grande di quanto ci saremmo aspettati con Delta. Ciò non significa che l'orologio della pandemia sia stato riportato all'inizio del 2020. I vaccini e le infezioni precedenti possono attenuare gli effetti peggiori del virus. Anche se la protezione contro le infezioni viene erosa, come si aspettano gli esperti, data la proteina spike fortemente mutata di Omicron, la protezione contro le malattie gravi e la morte dovrebbe essere più duratura. I ricoveri, piuttosto che i casi, potrebbero essere una misura più veritiera dell'impatto del virus, . Ma se i casi dovessero aumentare in maniera esponenziale, anche una piccola percentuale di pazienti che si ammalano gravemente può trasformarsi in troppi ricoveri tutti in una volta. Qui sta il pericolo possibile con Omicron.
Questa è la semplice matematica che dobbiamo tenere a mente: una piccola percentuale di un numero enorme è ancora un numero grande. Un'ondata di Omicron in gran parte lieve ma incontrollata potrebbe causare molto dolore, ricoveri e morte in un paese. L'impatto finale di Omicron dipenderà da quanto piccola sia quella piccola percentuale e da quanto sia enorme quel numero enorme. Allo stesso tempo, Omicron non sembra molto virulento finora, tuttavia i medici in Sud Africa, dove Omicron è già dominante dicono che non hanno visto tanti casi gravi come nelle ondate precedenti. Anche altri paesi con un piccolo numero di Omicron non hanno trovato molti pazienti gravi. Ma ci sono diversi motivi per ritenere che le notizie sulla gravità potrebbero rivelarsi meno rosee di quanto appaia attualmente. Prima di tutto, è presto. Le infezioni impiegano settimane per evolvere in infezioni gravi che portano a morte. Nel 2020, il 20 gennaio è stato confermato il primo caso di COVID negli Stati Uniti ; la prima morte ufficiale per COVID non è stata segnalata fino al 29 gennaio I primi dati sulla gravità sono ancora "confusi". Le persone che contraggono il virus all'inizio di un'ondata possono essere sproporzionatamente giovani e sane perché probabilmente stanno prendendo meno precauzioni di una persona anziana o di qualcuno che è immuno

compromesso", La popolazione del Sudafrica è di per sé abbastanza giovane, con un'età media di 28 anni, rispetto ai 38,5 degli Stati Uniti. E sebbene i tassi di vaccinazione siano bassi in Sud Africa, dove meno di un quarto è completamente vaccinato , l'immunità dall'infezione precedente è molto alta, con una stima che si attesta intorno al 62% È probabile che un buon numero di casi di Omicron siano delle re-infezioni. I casi in persone giovani o che sono state precedentemente infettate o entrambi dovrebbero essere in gran parte lievi. Se i casi di Omicron in questa popolazione fossero per lo più gravi, sarebbe un segnale catastrofico. Il fatto che non lo siano in questo momento è moderatamente rassicurante. Gli scienziati stanno ora lavorando alacremente per comprendere l'effetto di Omicron sulle persone vaccinate. Anche se la maggior parte dei nuovi casi continua a essere lieve nei vaccinati, un piccolo aumento di quanti non sono lievi può comunque avere un impatto sui ricoveri in base alla regola della "piccola percentuale di un numero enorme".

La protezione contro l'infezione dopo due dosi non sembra essere molto buona. I virologi evoluzionisti sono concordi nell'affermare che Omicron rappresenta un enorme salto nell'evoluzione, in solo pochi mesi, il virus è cambiato tanto quanto molti ricercatori si aspettavano che cambiasse nell'arco di quattro o cinque anni. In una serie di studi delle ultime settimane sembrerebbe che la potenza degli anticorpi in grado di neutralizzare il virus in vitro sia diminuita di 41 volte. E' importante sottolineare che un calo di 41 volte nell'attività degli anticorpi neutralizzanti dopo due dosi non significa un corrispettivo calo di 41 volte nell'efficacia del vaccino. L'impatto nel mondo reale è difficile da prevedere, ma l'effetto è abbastanza grande che la protezione contro le infezioni potrebbe essere piuttosto bassa, afferma Florian Krammer, virologo del Icahn School of Medicine del Monte Sinai. E sospetta che abbiamo a che fare con una variante che non ha problemi a infettare gli individui vaccinati. I primi dati reali sulla gravità arriveranno probabilmente nei prossimi giorni dal Regno Unito, che sta seguendo da vicino la diffusione di Omicron. La protezione contro le malattie gravi generalmente tende a essere più duratura a causa della risposta immunitaria. Le difese di prima linea degli anticorpi neutralizzanti potrebbero diminuire, ma altri settori del sistema immunitario, come le cellule T, possono ancora resistere a malattie gravi. In questo caso un richiamo potrebbe rafforzare la risposta immunitaria complessiva I dati preliminari attuali sembrano confermare che due dosi più l'infezione o tre dosi portano le persone a un livello di base più alto di anticorpi neutralizzanti, che possono resistere meglio all'erosione di Omicron. I primi scorci dei dati sulla gravità di Omicron non possono ancora dirci come la variante colpisca gli anziani e i non vaccinati, ma tutto ciò che riguarda la nostra esperienza finora con COVID suggerisce che c'è una estrema variabilità in rapporto all'età.

L'idea che sta prendendo corpo è che la popolazione non vaccinata sia vulnerabile all'Omicron, così come le persone immunocompromesse che non hanno una buona risposta al vaccino.

Una ulteriore preoccupazione è che Omicron sta arrivando anche in coincidenza delle festività natalizie, quando una considerevole fetta di italiani si sta preparando per feste e i viaggi. È un momento particolarmente poco indicato per una nuova variante perché la gente sta già andando in giro. Hanno già fatto dei programmi e sarà difficile interrompere questi piani vacanzieri. Inoltre sono in aumento anche le altre malattie respiratorie stagionali come l'influenza, che può gravare anche sulla tenuta degli ospedali. Il problema della "piccola percentuale di un numero enorme" è stato con noi fin dall'inizio della pandemia. Il coronavirus è molto meno mortale di altri virus emergenti che hanno suonato campanelli d'allarme in passato (SARS, MERS o Ebola) ma è molto più trasmissibile. In tutta la popolazione, in un passato recente questo si è sommato a tanti casi gravi da sopraffare il nostro sistema sanitario. I pazienti COVID hanno ricevuto cure peggiori, così come chiunque sia stato abbastanza sfortunato da ammalarsi durante queste grandi ondate. Non vogliamo che questo si ripeta. Ma fortunatamente non siamo nella stessa posizione dell'inizio del 2020 perché ora abbiamo gli strumenti per controllare Omicron. E grazie ai ricercatori Sud Africani che hanno visto molto presto il rischio di questa variante, abbiamo tempo per metterli in atto. I vaccini probabilmente continueranno a proteggere dalle infezioni gravi e un ulteriore booster potrebbe aumentare tale protezione. I produttori stanno lavorando su un booster specifico per Omicron. Inoltre conosciamo meglio come avviene la trasmissione del virus per via aerea e come fermarla con mascherine e ventilazione. Abbiamo antivirali all'orizzonte e speriamo in test rapidi affidabili. Sappiamo che il distanziamento sociale ha già frenato il Sars-cov-2. Omicron si sta diffondendo velocemente, ma sappiamo come rallentarlo. Tutto andrà bene alla fine. Se non va bene, allora non è la fine. (John Lennon)

L’ autocrate nel tuo iPHONE

Ronald J . Deibert

Nell'estate del 2020, un complotto ruandese per catturare il leader dell'opposizione in esilio Paul Rusesabagina ha attirato i titoli dei giornali internazionali. *Rusesabagina* è meglio conosciuto come difensore dei diritti umani e vincitore della medaglia presidenziale della libertà degli Stati Uniti che ha ospitato più di 1.200 hutu e tutsi in un hotel durante il genocidio ruandese del 1994. Ma nei decenni successivi al genocidio, divenne anche un importante critico statunitense del presidente ruandese Paul Kagame. Nell'agosto 2020, durante uno scalo a Dubai, *Rusesabagina è stato indotto con false pretese* a salire su un aereo diretto a Kigali, la capitale del Ruanda, dove le autorità governative lo hanno immediatamente arrestato per la sua affiliazione a un gruppo di opposizione. L'anno successivo, un tribunale ruandese lo ha condannato a 25 anni di carcere, suscitando la condanna di gruppi internazionali per i diritti umani, del Parlamento europeo e degli Stati Uniti

Meno notato all'epoca, tuttavia, era che questa sfacciata operazione transfrontaliera poteva anche aver impiegato una sorveglianza digitale altamente sofisticata. Dopo la condanna di Rusesabagina, Amnesty International e il Citizen Lab dell'Università di Toronto, un gruppo di ricerca sulla sicurezza digitale da me fondato e diretto, hanno scoperto che ***gli smartphone appartenenti a diversi membri della famiglia di Rusesabagina che vivevano anche all'estero***

erano stati violati da un programma spyware avanzato chiamato Pegasus . Prodotto dal gruppo NSO con sede in Israele, Pegasus offre a un operatore un accesso quasi totale ai dati personali di un bersaglio. L'analisi forense ha rivelato che il telefono appartenente alla figlia di *Rusesabagina,* Carine Kanimba, era stato infettato dallo spyware nel periodo in cui suo padre era stato rapito e di nuovo quando lei stava cercando di ottenere il suo rilascio e stava incontrando funzionari di alto livello aL'Europa e il Dipartimento di Stato degli Stati Uniti, compreso l'inviato speciale degli Stati Uniti per gli affari con gli ostaggi. NSO Group non identifica pubblicamente i suoi clienti governativi e il governo ruandese ha negato di aver utilizzato Pegasus, ma forti prove circostanziali indicano il regime di Kagame.

In effetti, l'incidente è solo uno delle dozzine di casi in cui Pegasus o altre tecnologie spyware simili sono state trovate sui dispositivi digitali di importanti esponenti dell'opposizione politica, giornalisti e attivisti per i diritti umani in molti paesi. Fornendo la possibilità di infiltrarsi clandestinamente anche negli smartphone più aggiornati (l'ultima versione "zero click" dello spyware può penetrare in un dispositivo senza alcuna azione da parte dell'utente), ***Pegasus è diventato lo strumento di sorveglianza digitale preferito dai regimi repressivi in circolazione il mondo.*** È stato usato contro i critici del governo negli Emirati Arabi Uniti (UAE) e i manifestanti pro-democrazia in Thailandia. È stato schierato dall'Arabia Saudita di Mohammed bin Salman e dall'Ungheria di Viktor Orban.

Ma l'uso dello spyware non è limitato agli autoritari del mondo. Come hanno rivelato i ricercatori, nell'ultimo decennio anche molte democrazie, tra cui Spagna e Messico, hanno iniziato a utilizzare lo spyware, *in modi che violano norme consolidate sui diritti umani e sulla responsabilità pubblica.* I documenti del governo degli Stati Uniti divulgati dal New York Times nel novembre 2022 mostrano che l'FBI non solo ha acquisito servizi di spyware da NSO, forse per scopi di controspionaggio, ma ha anche pensato di implementarli, anche su obiettivi statunitensi. (Un portavoce dell'FBI ha detto al Times che "non c'è stato alcun uso operativo del prodotto NSO per supportare alcuna indagine dell'FBI.")

L'avvento dello spyware avanzato ha trasformato il mondo dello spionaggio e della sorveglianza. Riunendo un settore in gran parte non regolamentato con un ecosistema digitale invasivo in cui ***smartphone e altri dispositivi personali contengono i dettagli più intimi della vita delle persone,*** la nuova tecnologia può tracciare quasi chiunque, ovunque nel mondo. I governi hanno preso atto. Per Israele, che approva le licenze di esportazione per ***Pegasus*** di NSO Group, la vendita di spyware a governi stranieri ha portato nuova influenza diplomatica in paesi diversi come India e Panama; un'indagine del New York Times ha scoperto che gli accordi NSO hanno aiutato il primo ministro israeliano **Benjamin Netanyahu** a siglare gli accordi di Abramo con il Bahrain, il Marocco e gli Emirati Arabi Uniti. A loro volta, gli stati clienti hanno usato ***Pegasus*** contro non solo gruppi di opposizione, giornalisti, e organizzazioni non governative (ONG) ma anche rivali geopolitici. Nel 2020 e nel 2021, il Citizen Lab ha scoperto che diversi dispositivi appartenenti a funzionari del Foreign Commonwealth and Development Office del Regno Unito erano stati violati con ***Pegasus*** e che un cliente di NSO Group nelGli Emirati Arabi Uniti avevano utilizzato lo spyware per infiltrarsi in un dispositivo situato al 10 di Downing Street, la residenza del primo ministro britannico. Nel novembre 2021, il gigante della tecnologia Apple ha notificato a 11 membri dello staff dell'ambasciata americana in Uganda che i loro iPhone erano stati violati con ***Pegasus.***

In risposta a queste rivelazioni, le aziende di spyware hanno generalmente negato la responsabilità per gli abusi dei loro clienti o si sono rifiutate di commentare. In una dichiarazione al New Yorker nell'aprile 2022, **NSO Group** ha dichiarato: *"Abbiamo ripetutamente collaborato con indagini governative, laddove meritano accuse credibili, e abbiamo imparato da ciascuno di questi risultati e rapporti e migliorato le salvaguardie nelle nostre tecnologie".* La società israeliana ha anche affermato che la sua tecnologia è progettata per aiutare i governi a indagare su criminalità e terrorismo. Ma lo spyware avanzato *è stato ora implicato in violazioni dei diritti umani* e spionaggio interstatale in dozzine di paesi, e le società di spyware hanno pochi obblighi legali o incentivi per la trasparenza pubblica o la responsabilità.

Le conseguenze della rivoluzione dello spyware sono profonde. Nei paesi con poche risorse, le forze di sicurezza possono ora svolgere operazioni ad alta tecnologia utilizzando *una tecnologia standard che è facile da acquistare quasi quanto le cuffie di Amazon*. Tra le democrazie, la tecnologia è diventata uno strumento irresistibile che può essere utilizzato con poca supervisione; solo nell'ultimo anno, le agenzie di sicurezza in almeno quattro paesi europei - Grecia, Ungheria, Polonia e Spagna - sono state coinvolte in scandali in cui le agenzie statali sono state accusate di dispiegare spyware contro giornalisti e esponenti dell'opposizione politica. Un mercato globale per lo spyware significa anche che forme di sorveglianza e spionaggio che una volta erano limitate a poche grandi potenze sono *ora disponibili in quasi tutti i paesi e potenzialmente anche in un numero ancora maggiore di aziende private.*

SPIEREMO PER TE

La rivoluzione dello spyware è emersa come sottoprodotto di una notevole convergenza di sviluppi tecnologici, sociali e politici nell'ultimo decennio. Gli smartphone e altri dispositivi digitali sono vulnerabili alla sorveglianza perché le loro applicazioni spesso contengono difetti e perché trasmettono continuamente dati attraverso reti cellulari e Internet non sicure. Sebbene i produttori di queste piattaforme tecnologiche impieghino ingegneri per trovare e correggere le vulnerabilità, tendono a dare la priorità allo sviluppo del prodotto rispetto alla sicurezza. Scoprendo e sfruttando come arma i "giorni zero", difetti del software sconosciuti ai loro progettisti, le aziende di spyware ***sfruttano l'insicurezza intrinseca del mondo dei consumatori digitali.***

Ma la straordinaria crescita del mercato dello spyware è stata guidata anche da diverse tendenze più ampie. In primo luogo, lo spyware sfrutta una cultura digitale globale che si basa su smartphone sempre attivi e sempre connessi. Hackerando un dispositivo personale, lo spyware può fornire ai suoi operatori l'intero modello di vita di un utente in tempo reale. In secondo luogo, lo spyware offre alle agenzie di sicurezza un modo elegante per eludere la crittografia end-to-end, che è diventata una barriera crescente per i programmi di sorveglianza di massa del governo che dipendono dalla raccolta di telecomunicazioni e dati Internet. Inserendosi all'interno del dispositivo di un utente, ***lo spyware consente ai suoi operatori di leggere i messaggi o ascoltare le chiamate prima che siano stati cifrati o dopo che siano stati decifrati***; se l'utente può vederlo sullo schermo, lo può fare anche lo spyware.

Un terzo fattore che ha guidato la crescita del settore è stato l'aumento dei movimenti di protesta abilitati digitalmente. Sconvolgimenti popolari come le rivoluzioni colorate negli ex stati sovietici nel primo decennio di questo secolo e la primavera araba nel 2010-2011 hanno colto di sorpresa molti autocrati e gli organizzatori hanno spesso utilizzato i telefoni per mobilitare i manifestanti. Offrendo un modo quasi divino per entrare nelle reti di attivisti, lo spyware ha

aperto un nuovo potente metodo ai governi ***per monitorare il dissenso e adottare misure per neutralizzarlo prima che si verifichino grandi proteste***.

Infine, l'industria dello spyware è stata anche alimentata dalla crescente privatizzazione della sicurezza nazionale. Proprio come i governi si sono rivolti ad appaltatori privati per operazioni militari complicate o controverse, hanno scoperto di poter esternalizzare la sorveglianza e lo spionaggio ad attori privati meglio attrezzati e meno visibili. Come i soldati di ventura, le società di spyware avanzate tendono a mettere i ricavi davanti all'etica, *vendendo i loro prodotti senza tener conto della politica dei loro clienti - dando origine al termine* ***"spyware mercenario"*** - e come gli appaltatori militari, i loro rapporti con le agenzie di sicurezza del governo sono spesso ammantata di segretezza per evitare il controllo pubblico. Inoltre, proprio come gli appaltatori militari hanno offerto lucrative carriere nel settore privato per i veterani delle agenzie militari e di intelligence, aziende di spyware e servizi di sicurezza governativi hanno costruito partnership simili reciprocamente vantaggiose, dando impulso al settore nel processo. Molti membri anziani del gruppo NSO, ad esempio, sono veterani dell'intelligence israeliana, inclusa la direzione d'élite dell'intelligence militare.

Sebbene la mancanza di trasparenza abbia reso difficile misurare l'industria dello spyware mercenario, i giornalisti hanno stimato che valga circa 12 miliardi di dollari all'anno. Prima delle recenti battute d'arresto finanziarie causate da un numero crescente di cause legali, il gruppo NSO era valutato 2 miliardi di dollari e ci sono altri attori importanti nel mercato. Molte aziende ora producono spyware sofisticati, tra cui **Cytrox** (fondata nella Macedonia del Nord e ora con operazioni in Ungheria e Israele), **Cyberbit** e **Candiru** con sede in Israele, **Hacking Team** con sede in Italia (ora defunta) e **Gamma Group** anglo-tedesco.

Ognuna di queste aziende può ipoteticamente servire numerosi clienti. I governi che sembrano aver utilizzato lo spyware Predator di Cytrox, ad esempio, includono Armenia, Egitto, Grecia, Indonesia, Madagascar e Serbia. Nel 2021, il segretario alla sicurezza e pubblica sicurezza del Messico, Rosa Icela Rodríguez, ha affermato che le precedenti amministrazioni messicane avevano firmato più contratti con NSO Group, per un totale di 61 milioni di dollari, per acquistare lo spyware ***Pegasus*** e, come hanno dimostrato ricercatori messicani e internazionali, il governo ha continuato a utilizzare ***Pegasus*** nonostante le assicurazioni pubbliche dell'attuale leadership che avrebbe non. (Nell'ottobre 2022, il presidente messicano **Andrés Manuel López Obrador** ha negato i risultati, affermando che la sua amministrazione non stava usando lo spyware contro giornalisti o oppositori politici.)

Sulla base di tali affari redditizi, le aziende di spyware hanno goduto del sostegno di importanti fondi di private equity, come la società di San Francisco ***Francisco Partners*** e la londinese ***Novalpina Capital***, rafforzando così le proprie risorse. Francisco Partners, che ha detenuto una partecipazione di controllo in NSO Group per cinque anni, ha dichiarato a Bloomberg News nel 2021: "[Siamo] profondamente impegnati in pratiche commerciali etiche e valutiamo tutti i nostri investimenti attraverso quella lente". ***Novalpina,*** che insieme ai fondatori di NSO ha acquisito la quota di Francisco Partners nel 2019, ha affermato che avrebbe portato l'azienda di spyware "in pieno allineamento con i principi guida delle Nazioni Unite su affari e diritti umani", ma le rivelazioni sugli abusi di ***Pegasus*** sono continuate e la corrispondenza pubblicata da The Guardian nel 2022 ha indicato che Novalpina ha cercato di screditare i critici di NSO Group, incluso questo autore.

Ma l'industria dello spyware comprende anche aziende molto meno sofisticate *in paesi come l'India, le Filippine e Cipro. Essendo l'equivalente di sorveglianza delle officine di riparazione di telefoni in un centro commerciale, tali attrezzature potrebbero non essere in grado di identificare i giorni zero, ma possono comunque raggiungere gli obiettivi con mezzi più semplici. Possono utilizzare il phishing delle credenziali, utilizzando false pretese, spesso tramite e-mail o SMS, per ottenere le password digitali di un utente o altre informazioni personali sensibili, oppure possono semplicemente acquistare vulnerabilità del software da altri hacker sul mercato nero.* E queste aziende più piccole possono essere più disposte a intraprendere operazioni illegali per conto di clienti privati perché si trovano al di fuori della giurisdizione in cui risiede una vittima o perché l'applicazione è lassista.

È difficile sopravvalutare la portata e la potenza degli ultimi spyware commerciali. Nelle sue forme più avanzate, può infiltrarsi silenziosamente in qualsiasi dispositivo vulnerabile in qualsiasi parte del mondo. Prendi l'exploit zero-day, zero-click che i ricercatori di Citizen Lab hanno scoperto nel 2021 su un iPhone infettato da ***Pegasus***. *Utilizzando l'exploit, che i ricercatori hanno chiamato ForcedEntry, un operatore di spyware può intercettare di nascosto messaggi e telefonate, comprese quelle crittografate da app come Signal o WhatsApp; accendere il microfono e la fotocamera dell'utente; tracciare i movimenti attraverso il GPS di un dispositivo; e raccogliere foto, note, contatti, e-mail e documenti*. L'operatore può fare quasi tutto ciò che un utente può fare e altro ancora, inclusa la riconfigurazione delle impostazioni di sicurezza del dispositivo e l'acquisizione dei token digitali utilizzati per accedere in modo sicuro agli account cloud in modo che la sorveglianza su un obiettivo possa continuare anche dopo che l'exploit è stato rimosso da un dispositivo, il tutto all'insaputa del bersaglio. Dopo che il Citizen Lab ha condiviso il ***ForcedEntry di Pegasus*** con gli analisti di Apple e Google, gli analisti di Google lo hanno descritto come *"uno degli exploit tecnicamente più sofisticati che abbiamo mai visto"*, osservando che forniva funzionalità che "precedentemente si pensava fossero accessibili solo a un una manciata di stati nazionali".

SPARARE AI MESSAGGERI

Nell'ultimo decennio, l'ascesa di regimi autoritari in molte parti del mondo ha sollevato nuove domande sulla durabilità dell'ordine internazionale liberale. Come è stato ampiamente notato, molte élite dominanti sono state in grado di scivolare verso l'autoritarismo limitando o controllando il dissenso politico, i media, i tribunali e altre istituzioni della società civile. *Tuttavia, è stata prestata molta meno attenzione al ruolo pervasivo dell'industria mercenaria dello spyware in questo processo*. Questa negligenza è in parte il risultato di quanto poco sappiamo sullo spyware, inclusa, in molti casi, l'identità delle specifiche agenzie governative che lo utilizzano. (Data la natura segreta delle transazioni spyware, è molto più facile identificare le vittime che gli operatori.)

Uno degli usi più frequenti della tecnologia è stato quello di infiltrarsi nei movimenti di opposizione, in particolare nel periodo precedente alle elezioni. I ricercatori hanno identificato casi in cui figure dell'opposizione sono state prese di mira, non solo in stati autoritari come l'Arabia Saudita e gli Emirati Arabi Uniti, ma anche in paesi democratici come l'India e la Polonia. In effetti, uno dei casi più eclatanti è sorto in Spagna, democrazia parlamentare e Unione Europeamembro. Tra il 2017 e il 2020, ha scoperto il Citizen Lab, ***Pegasus*** è stato utilizzato per intercettare un ampio spaccato della società civile e del governo catalani. Gli obiettivi includevano ogni membro catalano del Parlamento europeo che ha sostenuto l'indipendenza della Catalogna, ogni presidente catalano dal 2010 e molti membri degli organi legislativi catalani, inclusi più

presidenti del parlamento catalano. In particolare, alcuni degli attacchi sono avvenuti nel corso di delicati negoziati tra i governi catalano e spagnolo sul destino dei sostenitori dell'indipendenza catalana che sono stati imprigionati o in esilio. Dopo che i risultati hanno attirato l'attenzione internazionale, Paz Esteban, il capo della Spagnall National Intelligence Center, ha riconosciuto ai legislatori spagnoli che lo spyware era stato utilizzato contro alcuni politici catalani, ed Esteban è stato successivamente licenziato. Ma non è ancora chiaro quale agenzia governativa fosse responsabile e quali leggi, se del caso, siano state utilizzate per giustificare un'operazione di spionaggio interno così estesa.

In alcuni paesi, lo spyware si è dimostrato ugualmente efficace contro i giornalisti che stanno indagando su chi detiene il potere, con conseguenze di vasta portata sia per gli obiettivi che per le loro fonti. Nel 2015, a diversi dispositivi appartenenti alla giornalista messicana **Carmen Aristegui** e a un membro della sua famiglia sono stati inviati collegamenti di sfruttamento di Pegasus mentre stava indagando sulla corruzione che coinvolgeva l'allora presidente messicano **Enrique Peña Nieto**. Non esiste una pistola fumante che identifichi la parte responsabile, sebbene forti prove circostanziali suggeriscano un'agenzia governativa messicana. Nel 2021, un giornalista ungherese indaga sulla corruzione nell'ufficio del presidente Viktor Orbancerchio interno è stato violato con ***Pegasus.*** (Il governo ungherese ha successivamente riconosciuto di aver acquistato la tecnologia.) E quello stesso anno, il cellulare del corrispondente del New York Times per il Medio Oriente Ben Hubbard è stato infettato da ***Pegasus*** mentre stava lavorando a un libro sul leader de facto dell'Arabia Saudita, il principe ereditario **Maometto bin Salman.**

Con lo spyware, i governi possono fermare le proteste prima che si verifichino. Quasi altrettanto frequentemente, lo spyware è stato utilizzato per indebolire i funzionari giudiziari e le organizzazioni della società civile che cercano di chiedere conto ai governi. Prendiamo il caso di **Alberto Nisman**, un noto procuratore anticorruzione argentino che stava indagando su una presunta associazione a delinquere da parte di funzionari argentini di alto livello. Nel gennaio 2015, Nisman è stato trovato morto in circostanze sospette - la sua morte è stata successivamente dichiarata omicidio - il giorno prima che fornisse una testimonianza al Congresso coinvolgendo l'allora presidente dell'Argentina Cristina Fernández de Kirchner e il suo ministro degli Esteri, Héctor Timerman, in una copertina -up del presunto coinvolgimento iraniano nel bombardamento del 1994 di un centro ebraico a Buenos Aires. Nello stesso anno, il Citizen Lab ha documentato come un gruppo sudamericano di hack-for-hire fosse stato incaricato di prendere di mira Nisman con spyware prima della sua morte, suggerendo che qualcuno al potere fosse desideroso di scrutare nelle sue indagini. InIn Messico nel 2017, una o più agenzie governative ancora sconosciute hanno utilizzato lo ***spyware Pegasus*** contro gruppi per i diritti umani e investigatori internazionali che stavano rintracciando potenziali insabbiamenti governativi della famigerata scomparsa e del raccapricciante omicidio di 43 studenti a Iguala, in Messico. Rapporti successivi hanno mostrato che il governo messicano aveva gravemente fallito le indagini e che il personale del governo era implicato in un insabbiamento, scoperte che non sarebbero mai venute alla luce senza gli sforzi dei cani da guardia della società civile.

Altri obiettivi comuni di ***Pegasus*** sono avvocati coinvolti in casi importanti o politicamente sensibili. Nella maggior parte delle democrazie liberali, il privilegio avvocato-cliente è sacrosanto. Eppure il Citizen Lab ha identificato una varietà di casi in cui lo spyware è stato utilizzato per hackerare o prendere di mira i dispositivi degli avvocati. Nel 2015, la tattica è stata usata contro due avvocati in Messico che rappresentavano le famiglie di **Nadia Vera**, una critica del governo uccisa e sostenitrice dei diritti delle donne. Più di recente, diversi avvocati che rappresentavano eminenti catalani sono stati presi di mira nell'ambito della campagna di

sorveglianza spagnola. E in Polonia, lo ***spyware Pegasus*** è stato utilizzato più volte per hackerare il dispositivo di Roman Giertych, consulente legale di **Donald Tusk**, ex primo ministro e leader del principale partito di opposizione del paese.

All'inizio del 2022, Con l'aumentare della disponibilità di spyware, anche i clienti del settore privato stanno entrando in azione. Prendiamo in considerazione le attività di **BellTroX,** una società indiana di hack-for-hire responsabile di un vasto spionaggio per conto di clienti privati in tutto il mondo. Tra il 2015 e il 2017, qualcuno ha utilizzato i servizi di **BellTroX** contro le organizzazioni non profit americane che stavano lavorando per pubblicizzare rivelazioni secondo cui la compagnia petrolifera ExxonMobil aveva nascosto per decenni le sue ricerche sul cambiamento climatico. **BellTroX** è stato utilizzato anche per prendere di mira le organizzazioni statunitensi che lavorano sulla neutralità della rete, presumibilmente per volere di uno o più clienti diversi che si opponevano a tale riforma. **BellTroX** ha anche una fiorente attività nel mondo legale; studi legali in molti paesi hanno utilizzato i servizi dell'azienda per spiare i legali avversari. Nell'aprile 2022, un investigatore privato israeliano che ha agito come broker per **BellTroX** si è dichiarato colpevole presso il tribunale statunitense per frode telematica, cospirazione per commettere hacking e furto di identità aggravato, ma gli operatori con sede in India di **BellTroX** sono rimasti fuori dalla portata della legge. (Chiesto da Reuters nel 2020 di rispondere ai risultati, il fondatore dell'azienda, Sumit Gupta, ha negato qualsiasi illecito e ha rifiutato di rivelare i suoi clienti.)

NESSUN POSTO IN CUI NASCONDERSI

L'uso proliferante di spyware contro obiettivi politici e della società civile nelle democrazie avanzate è abbastanza preoccupante. Ancora più minacciosi, tuttavia, possono essere i modi in cui la tecnologia ha consentito a regimi autoritari di estendere la loro repressione ben oltre i propri confini. Nei decenni passati, gli autocrati hanno dovuto affrontare notevoli ostacoli alla repressione dei cittadini che erano andati in esilio. Con lo spyware, tuttavia, un operatore può entrare nell'intera rete di un esule politico senza mettere piede nel paese di adozione dell'obiettivo e con pochissimi dei rischi e dei costi associati allo spionaggio internazionale convenzionale.

Gli esempi di questa nuova forma di repressione transnazionale sono molteplici. A partire dal 2016, Cyberbit è stato utilizzato per prendere di mira dissidenti, avvocati, studenti e altri etiopi in quasi 20 paesi. Nel 2021, i telefoni di due eminenti egiziani, il politico dell'opposizione in esilio Ayman Nour, che ha vissuto in Turchia, e l'ospite di un popolare programma di notizie (che ha chiesto di rimanere anonimo per la propria incolumità), sono stati violati con lo spyware Predator di Cytrox. Infatti, il telefono di Nour, che è un aperto critico del presidente egiziano Abdel Fattah el-Sisi, è stato contemporaneamente infettato sia dallo ***spyware Predator*** che dallo spyware Pegasus di NSO Group, ciascuno apparentemente gestito da clienti governativi separati: l'Egitto nel caso di Predator e entrambi Arabia Saudita o Emirati Arabi Uniti nel caso di Pegasus. In una dichiarazione a Vice News, Cyberbit ha affermato che il governo israeliano sovrintende alla sua tecnologia e che "le agenzie di intelligence e difesa che acquistano questi prodotti sono obbligate a utilizzarli in conformità con la legge". Nel caso dell'hacking egiziano, il CEO di Cytrox, Ivo Malinkovski, ha rifiutato di commentare; secondo VICE news, successivamente ha cancellato i riferimenti a Cytrox nel suo profilo LinkedIn. (I governi di Egitto, Etiopia, Arabia Saudita ed Emirati Arabi Uniti hanno rifiutato di commentare i risultati.)

Particolarmente vasta è stata la campagna spyware transnazionale del governo saudita. Nel 2018, un telefono appartenente a Ghanem al-Masarir, un dissidente saudita residente nel Regno

Unito, è stato violato con lo ***spyware Pegasus***. In concomitanza con l'infezione del suo dispositivo, al-Masarir è stato rintracciato e aggredito fisicamente da agenti sauditi a Londra. Lo spyware potrebbe anche aver avuto un ruolo nella famigerata uccisione del giornalista saudita in esilio Jamal Khashoggi nel consolato saudita in Turchia. Nel 2018, un telefono di proprietà di Omar Abdulaziz, un attivista saudita, residente permanente canadese e stretto confidente di Khashoggi, è stato violato con lo ***spyware Pegasus***. Abdulaziz e Khashoggi avevano discusso del loro attivismo contro il regime saudita su quelle che erroneamente presumevano fossero piattaforme di comunicazione sicure. Dopo l'uccisione di Khashoggi, l'analisi forense ha rivelato che anche i dispositivi di molte altre persone più vicine a Khashoggi, tra cui sua moglie egiziana e la sua fidanzata turca, erano stati infettati.omicidio . (Il governo saudita ha rifiutato di commentare le rivelazioni. Nel 2021, NSO Group ha dichiarato a The Guardian: "La nostra tecnologia non è stata in alcun modo associata all'atroce assassinio di Jamal Khashoggi".)

In effetti, prendere di mira i critici del regime all'estero con spyware è solo uno dei tanti modi in cui il governo saudita ha utilizzato la tecnologia digitale per neutralizzare il dissenso. Ad esempio, secondo un'accusa federale degli Stati Uniti, un alto consigliere del principe ereditario saudita Mohammed bin Salman ha pagato un dipendente di Twitter $ 300.000 e ha fornito altri doni nel 2014 e nel 2015, apparentemente in cambio di spiare i dissidenti sulla piattaforma. Il dipendente, che ha lasciato Twitter nel 2015, è stato condannato dal tribunale statunitense nel 2022. Quando tali tattiche vengono utilizzate in combinazione con il tipo di sorveglianza altamente intrusiva rappresentata dallo spyware, i dissidenti possono subire una straordinaria pressione psicologica. Molte vittime di hacking hanno subito uno shock debilitante sapendo che i loro dispositivi compromessi hanno messo a rischio anche amici e colleghi e che ogni loro mossa viene monitorata. Un'attivista saudita ha spiegato che essere presa di mira digitalmente era una forma di "guerra psicologica ed emotiva" che le causava "paura e ansia senza fine". Utilizzando spyware, autocrati e despoti sono quindi in grado di reprimere le reti della società civile ben oltre i propri confini, anche se rafforzano l'autocrazia interna.

Nonostante un ampio e crescente corpus di documentazione sugli abusi di spyware in tutto il mondo, ci sono diversi motivi per cui la tecnologia sembra destinata a diventare ancora più diffusa**.**

In primo luogo, sebbene il controllo approfondito delle aziende mercenarie di spyware abbia riguardato i loro contratti con le agenzie governative nazionali, molte aziende commercializzano più di un cliente in un determinato paese, comprese le forze dell'ordine locali. Ad esempio, durante un viaggio conoscitivo in Israele nell'estate del 2022, i funzionari del Parlamento europeo hanno appreso che NSO Group ha almeno 22 clienti in 12 paesi europei, suggerendo che un numero significativo di questi clienti sono agenzie subnazionali. Tali accordi sollevano ulteriori domande sulla responsabilità, dato che la ricerca ha dimostrato che le forze dell'ordine locali sono spesso più suscettibili agli abusi, come la profilazione razziale o la corruzione,

In secondo luogo, sebbene alcune società mercenarie di spyware come NSO Group affermino di trattare solo con clienti governativi, c'è poco che impedisce loro di vendere la loro tecnologia a società private o individui corrotti. Le prove suggeriscono che alcuni lo fanno già: nel luglio 2022, il Threat Intelligence Center di Microsoft ha pubblicato un rapporto su una società di spyware e hacking su commissione con sede in Austria chiamata DSIRF che aveva preso di mira individui in banche, studi legali e società di consulenza in diversi paesi. Sebbene Microsoft non abbia specificato quale tipo di clienti ha assunto DSIRF, l'azienda pubblicizza servizi di "due diligence" per

le aziende, implicando che queste operazioni di hacking sono state intraprese per conto di clienti privati. Quando Reuters ha chiesto a DSIRF informazioni sul rapporto Microsoft, la società ha rifiutato di commentare. Anche se è illegale se fatto senza un mandato, è meno probabile che tale hacking nel settore privato venga scoraggiato quando le aziende degli hacker si trovano al di fuori della giurisdizione in cui si verifica il targeting. Poiché le protezioni dei diritti alla privacy, della libertà di stampa e dei tribunali indipendenti sono sempre più minacciate in molti paesi, probabilmente diventerà ancora più facile per le aziende corrotte o gli oligarchi distribuire spyware mercenario senza responsabilità.

In terzo luogo, lo spyware è diventato un componente centrale di un più ampio menu di strumenti di sorveglianza, come il rilevamento della posizione e l'identificazione biometrica, utilizzati da molte agenzie di sicurezza governative. Quanto più lo spyware viene incorporato nella raccolta e nelle attività di polizia di tutti i giorni, tanto più difficile sarà tenerlo a freno. Ancora più minaccioso, lo spyware potrebbe presto acquisire capacità ancora più invasive sfruttando applicazioni indossabili, come monitor biomedici, tecnologia di rilevamento emotivo e Internet reti neurali connesse attualmente in fase di sviluppo. Molte applicazioni digitali mirano già a scavare più a fondo negli aspetti subliminali o inconsci del comportamento degli utenti e raccogliere dati sulla loro salute e fisiologia.

ORDINI RESTRITTIVI

Per quasi un decennio, l'industria dello spyware mercenario è stata in grado di espandere la propria portata in tutto il mondo in gran parte senza regolamentazione o responsabilità. Ma questa è una scelta che i governi hanno fatto, non un risultato inevitabile che deve essere semplicemente accettato. Poiché i cani da guardia della società civile ei giornalisti hanno portato alla luce flagranti abusi, è diventato più difficile per i principali fornitori di spyware e clienti governativi nascondere le loro operazioni. In Europa e negli Stati Uniti, i comitati hanno tenuto audizioni sullo spyware e le agenzie governative hanno iniziato a sviluppare nuove politiche per limitarne l'uso. In particolare, il Dipartimento del Commercio degli Stati Uniti ha inserito NSO Group, Candiru e altre società di hacking su commissione in un elenco di restrizioni all'esportazione, limitando il loro accesso agli Stati Uniti prodotti e tecnologia e inviando un segnale forte ai potenziali investitori che le società di spyware sono sottoposte a un controllo crescente. Anche le piattaforme tecnologiche sono intervenute. Meta (la società madre di Facebook) e Apple hanno fatto causa a NSO Group nei tribunali statunitensi, hanno informato le vittime di infezioni da spyware e hanno lavorato per supportare i cani da guardia della società civile. Apple ha anche donato 10 milioni di dollari alla ricerca sulla sorveglianza informatica e si è impegnata a fare lo stesso con eventuali danni concessi dalla sua causa contro NSO Group.

Ma frenare la diffusione globale dello spyware mercenario richiederà un approccio globale. Per cominciare, le aziende devono dedicare molte più risorse all'identificazione e allo sradicamento dello spyware e alla garanzia che i loro servizi siano adeguatamente protetti dallo sfruttamento. WhatsApp e Apple hanno già mostrato come avvisare le vittime quando viene rilevato spyware e ritengono legalmente responsabili i fornitori di spyware come NSO Group per violazioni dei loro termini di servizio e altri reati legali. Che si tratti di un cambiamento nella cultura aziendale o, più probabilmente, di normative governative più severe, le piattaforme tecnologiche dovrebbero anche porre maggiormente l'accento sulla sicurezza e ridimensionare la ricerca incessante di aspirare i dati degli utenti. A loro volta, le indagini forensi di Citizen Lab, Amnesty International, giornalisti, e altri dovranno essere ampliati e integrati da altre organizzazioni che svolgono un lavoro simile, siano esse ONG, università o organizzazioni di notizie

investigative. La scienza forense digitale e la responsabilità digitale dovrebbero essere riconosciute come una disciplina di ricerca formale in grado di monitorare l'attività dello spyware, assistere le vittime e gli obiettivi e mantenere la pressione sui governi e le aziende affinché siano più trasparenti e responsabili delle loro azioni. Affinché un tale campo emerga, saranno necessari molti anni di sostegno pubblico, privato e filantropico. e mantenere la pressione sui governi e le aziende affinché siano più trasparenti e responsabili delle loro azioni. Affinché un tale campo emerga, saranno necessari molti anni di sostegno pubblico, privato e filantropico. e mantenere la pressione sui governi e le aziende affinché siano più trasparenti e responsabili delle loro azioni. Affinché un tale campo emerga, saranno necessari molti anni di sostegno pubblico, privato e filantropico.

In definitiva, i governi stessi dovranno adottare un solido quadro normativo per l'uso dello spyware. La regolamentazione del settore richiederà probabilmente l'emanazione di un complesso insieme di regole che affrontino vari aspetti del mercato dello spyware. Ad esempio, alle società nazionali di spyware potrebbe essere richiesto di effettuare regolarmente comunicazioni pubbliche sulle loro esportazioni e, a loro volta, alle agenzie governative potrebbe essere richiesto di segnalare da chi e dove stanno importando spyware. Le regole sull'esportazione devono essere rafforzate per impedire la vendita di spyware a governi o altri clienti che potrebbero utilizzarli in violazione del diritto internazionale sui diritti umani. Sono inoltre necessarie regole e standard di controllo chiari per l'uso dello spyware. Sarà probabilmente necessaria anche una legislazione specifica per affrontare il mercato zero-day, anche se dovrà essere elaborato con cura in modo da non ostacolare la legittima ricerca sulla sicurezza. I governi potrebbero anche approvare una legislazione che dia alle vittime di spyware il diritto di citare in giudizio sia i governi stranieri che i fornitori di spyware per i danni causati dallo spionaggio.

Tali sforzi potrebbero essere rafforzati a livello internazionale attraverso lo sviluppo di un regime globale di controllo dello spyware. Le attività militari, ad esempio, sono state a lungo soggette a supervisione internazionale attraverso meccanismi come il Registro delle armi convenzionali delle Nazioni Unite e le politiche che sono state messe in atto relative agli standard per gli appaltatori militari e di sicurezza privati o il divieto delle mine terrestri. Un processo simile potrebbe portare alla regolamentazione internazionale dello spyware, compresi i requisiti per la trasparenza e la segnalazione del suo utilizzo. Questi modelli esistenti, tuttavia, suggeriscono che il successo richiederà il buy-in di un numero significativo di paesi e che è necessaria una maggiore pressione per convincere i governi e i leader mondiali che lo spyware mercenario rappresenta una seria e crescente minaccia alla sicurezza internazionale e all'ordine internazionale liberale .

Senza dubbio, i governi autoritari e le agenzie di sicurezza che attualmente traggono vantaggio dallo spyware cercheranno di ostacolare tale regolamentazione, ma i crescenti rischi per la sicurezza nazionale di un mercato non regolamentato potrebbero richiedere una valutazione più sobria. Nel novembre 2022, **Sir Jeremy Fleming**, un alto funzionario dell'intelligence britannica, ha avvertito che l'uso proliferante di spyware mercenario e "hacker a pagamento" da parte di paesi e malfattori "aumenterà la futura minaccia alla sicurezza informatica del Regno Unito". Se l'uso di spyware mercenario continua a crescere senza controllo*, i rischi per la democrazia diventeranno acuti*. Se le élite in qualsiasi paese possono utilizzare questa tecnologia per neutralizzare l'opposizione politica legittima in qualsiasi punto della terra, mettere a tacere il dissenso attraverso lo spionaggio mirato, minare il giornalismo indipendente ed erodere la responsabilità pubblica impunemente.

Letture consigliate

" **Come l'IA rende i dittatori più pericolosi** "
di Henry Farrell, Abraham Newman e Jeremy Wallace

" **Come i poteri digitali rimodelleranno l'ordine globale** "
di Ian Bremmer

“ **Come salvare la democrazia dalla tecnologia** ”
di Francis Fukuyama, Barak Richman e Ashish Goel

“ **I dittatori digitali** ”
di Andrea Kendall-Taylor, Erica Frantz e Joseph Wright

" **L'insidiosa minaccia informatica** "
di Jacquelyn Schneider