Jak izraelska cyberarmia weszła do korpo-świata

16 grudnia 2021

Niewyraźna granica między sektorem wojskowym a prywatnym w Izraelu pozwoliła na rozkwit broni cybernetycznej, takiej jak oprogramowanie szpiegowskie NSO, na całym świecie.

Na konferencji bezpieczeństwa i wystawie o nazwie „iHLS Innotech", która odbyła się w zeszłym tygodniu w Tel Awiwie, pięciu izraelskich ekspertów ds. cyberbezpieczeństwa zabrało głos przy okrągłym stole zatytułowanym „Etyka sprzedaży narzędzi cybernetycznych i wywiadowczych w sferze ofensywnej". Paneliści, wszyscy wywodzący się z w wojska i sektora prywatnego, żartowali, że rozmowa będzie tak trudna, że wymaga wypicia butelki szkockiej whisky o 10:45 rano.

Podczas gdy szkocka robiła kilka rundek po scenie, niektórzy z panelistów mówili o promowaniu bardziej rygorystycznych regulacji sprzedaży cyberbroni i technologii, takich jak zakazanie weteranom wojskowych jednostek wywiadowczych, którzy korzystali z tych technologii, pracy w firmach zajmujących się cyberszpiegostwem ofensywnym. Paneliści byli jednak zgodni zgodni co do tego, że firmy najprawdopodobniej będą nadal sprzedawać swoje usługi z błogosławieństwem izraelskiego prawa eksportowego.

– Chcę powiedzieć, że jako osoba prywatna chcę, aby mój rząd szpiegował ludzi, nawet mnie – powiedział Guy Mizrahi, przewodniczący panelu i były wiceprezes Rayzone Group, firmy wywiadowczej, która znalazła się pod ostrzałem pod koniec 2020 roku za ułatwianie masowej inwigilacji za granicą. – Myślę, że inne kraje również powinny mieć te zdolności, a nie wszystkie mogą je rozwijać na własną rękę.

Panel ostrożnie wkraczał w debatę, która w ostatnich tygodniach zdominowała obieg wiadomości. W tym miesiącu śledczy zajmujący się prawami człowieka odkryli, że telefony sześciu palestyńskich obrońców praw człowieka i trzech wyższych urzędników Autonomii Palestyńskiej zostały zainfekowane oprogramowaniem szpiegowskim „Pegasus", wyprodukowanym przez NSO Group z siedzibą w Izraelu. Rewelacje te pojawiły się niecały tydzień po tym, jak Stany Zjednoczone oficjalnie umieściły NSO Group na czarnej liście jako podmiot naruszający interesy bezpieczeństwa narodowego i polityki zagranicznej USA, zakazując tym samym firmie handlu z amerykańskimi firmami. Zarówno NSO Group, jak i rząd Izraela odmówiły publicznego omówienia tej sprawy, powołując się na względy bezpieczeństwa narodowego.

Firmy takie jak NSO Group zyskały złą sławę z powodu eksportu swoich cybertechnologii do autokratycznych reżimów na całym świecie, a także z powodu wykorzystywania ich produktów na tysiącach ludzi, od prezydentów po dziennikarzy. Ale jak pokazali uczestnicy konferencji Innotech, nie są to po prostu prywatne firmy prowadzące interesy za granicą: są one głęboko powiązane z izraelskim establishmentem wojskowym, a ich produkty stanowią centralny element izraelskiego arsenału inwigilacji.

Publiczne informacje na temat NSO Group, jak również słowa byłych oficerów izraelskiego wywiadu i pracowników NSO, którzy rozmawiali z autorem pod warunkiem zachowania anonimowości, rzucają światło na zakres, w jakim izraelski, w dużej mierze nieuregulowany system inwigilacji jest ściśle związany z sektorem prywatnym, a Palestyńczycy na terytoriach okupowanych ponoszą największe konsekwencje jego praktyk.

Wszystko, o czym myślisz, że jest

dostępne, jest dostępne

Nazwany na cześć boskiego konia z mitologii greckiej, który symbolizuje szybkość, piękno i artystyczne natchnienie, „Pegasus” stał się synonimem nielegalnego szpiegostwa, łamania praw człowieka i autokratycznych reżimów. Firma, która zaprojektowała oprogramowanie szpiegujące, NSO Group, została założona w 2010 roku przez Shaleva Hulio, przedsiębiorcę, który rozpoczął pracę w branży cyberbezpieczeństwa długo po odbyciu służby wojskowej i który pełnił funkcję dyrektora generalnego firmy do czasu ustąpienia ze stanowiska na początku tego miesiąca. Stał się wtedy „globalnym prezesem” firmy i wiceprzewodniczącym jej zarządu.

W 2012 roku firma Hulio stworzyła prototyp Pegasusa, oprogramowania, które może przejąć pełną kontrolę nad dowolnym smartfonem na odległość. Pegasus, początkowo sprzedawany jako narzędzie wsparcia klienta, pozwalające technikom operatorów telefonii komórkowej naprawiać urządzenia z daleka poprzez „przejęcie” telefonu, stał się źródłem wielkiego zainteresowania rządów i wojska. Technologia ta nie tylko daje dostęp do wiadomości tekstowych i rozmów telefonicznych, ale ma również moc aktywowania kamer, urządzeń nagrywających, poczty elektronicznej i kont mediów społecznościowych dowolnego urządzenia, w dowolnym miejscu. Hulio szybko otrzymał propozycję od urzędników wywiadów w Izraelu i Unii Europejskiej, aby dalej rozwijać oprogramowanie.

W ciągu następnej dekady Hulio zbudował NSO Group jako udoskonalił swój produkt poprzez rekrutację ludzi z elitarnych izraelskich jednostek wywiadowczych, takich jak 8200, która jest odpowiedzialna za inwigilację na terytoriach okupowanych. Wielu programistów pracujących w NSO spędziło służbę wojskową na wdrażaniu i udoskonalaniu podobnej broni cyberszpiegowskiej. Dzięki ich doświadczeniu, NSO wyprodukowało oprogramowanie szpiegowskie tak potężne, że mogło być rozmieszczone na telefonach bez potrzeby klikania w

link lub otwierania wiadomości.

NSO szybko awansowało w szeregach prywatnego przemysłu inwigilacyjnego, reklamując się jako producent broni. W broszurach z początku lat 2010, NSO opisywało siebie jako „lidera w cyberwojnie" wspieranego przez rodzimą „izraelską technologię". Wraz z niezrównanym produktem, NSO zyskało przewagę nad konkurencją obiecując swoim klientom – rządom, organom ścigania i policji na całym świecie – praktyczne szkolenia z młodymi weteranami z Izraela.

Na początku swojej działalności, NSO Group rekrutowała przedstawicieli terenowych i kierowników produktu spośród absolwentów Jednostki 8200. Na stronie absolwentów 8200 z 2014 roku, NSO zamieściło ogłoszenie o pracę, które obiecywało potencjalnym pracownikom „60 proc. czasu za granicą" w szczególnie „egzotycznych miejscach". Ci, którzy podjęli pracę w firmie, podobno zgarniali wysokie pensje, sięgające 30 000 dolarów miesięcznie i podróżowali po całym świecie, spotykając się z głowami państw, generałami wojskowymi i dyplomatami.

Pod wieloma względami weterani ci skutecznie służyli jako ambasadorzy nowej dyplomacji Izraela w zakresie oprogramowania szpiegowskiego. Szkolili urzędników zarówno w krajach demokratycznych, jak i w autokratycznych, jak używać zaawansowanej broni cybernetycznej na własnych cywilach, bez niedogodności związanych z nadzorem czy odpowiedzialnością. Rząd Izraela wykorzystał tę sprzedaż do utorowania drogi do nawiązania stosunków dyplomatycznych z arabskimi i muzułmańskimi rządami, takimi jak Zjednoczone Emiraty Arabskie, Maroko, Azerbejdżan i Arabia Saudyjska.

Z czasem na scenie pojawiło się wiele innych firm cyberszpiegowskich – w tym Candiru, Black Cube i Dark Matter – ściągających weteranów izraelskich i amerykańskich służb wywiadowczych w celu opracowania równie potężnej broni. Współpraca między izraelskim sektorem prywatnym i wojskowym pozwoliła wielu z tych firm szybko wspiąć się na w dużej

mierze nieuregulowany rynek globalny. Izrael, samozwańczy lider ofensywnych technologii cybernetycznych, do 2016 roku szczycił się największą na świecie liczbą firm inwigilacyjnych w przeliczeniu na mieszkańca, z NSO w roli głównej.

Jednego dnia żołnierz, następnego prywatny wykonawca

Organy ścigania i wojsko podsłuchiwały obywateli przez ponad sto lat. Jednak wraz z pojawieniem się sieci komórkowych i szyfrowanych wiadomości end-to-end na początku XXI wieku przechwytywanie komunikacji komórkowej stało się niemal niemożliwe. Rządy i wojsko zaczęły więc dążyć do opracowania ofensywnej broni cybernetycznej, która mogłaby naruszyć nawet najbardziej zabezpieczone platformy. Armia izraelska, podobnie jak inne na całym świecie, ściśle współpracowała z rozwijającym się prywatnym sektorem cyberbezpieczeństwa w ramach wyścigu zbrojeń w dziedzinie nadzoru.

W rozmowach weterani izraelskich jednostek wywiadowczych potwierdzili, że zinstytucjonalizowana współpraca pomiędzy prywatnymi firmami inwigilacyjnymi a izraelskimi jednostkami wywiadowczymi jest po prostu bussines as usual. „Nikt nie był zaskoczony tymi wiadomościami" – powiedział G, były dowódca izraelskiej jednostki wywiadowczej, zapytany o cyberszpiegostwo palestyńskich telefonów na terytoriach okupowanych. Outsourcing pracowników, prototypowanie oprogramowania i dzielenie się bazami danych to powszechne praktyki między przemysłem prywatnym a wojskiem, twierdzą byli oficerowie.

Weterani izraelskiego wywiadu twierdzą, że powiązania między wojskiem a prywatnymi firmami inwigilacyjnymi sięgają znacznie dalej niż praktyki zatrudniania. „To nie są inicjatywy wolnorynkowe" – powiedział G. „Wojsko polega na prywatnych firmach, aby rozwijać wiele swoich broni, w tym złośliwe oprogramowanie, ponieważ wymaga to ogromnych zasobów".

Z tego powodu, wyjaśnił G, wiele prywatnych firm zajmujących się inwigilacją zaopatruje armię izraelską w swoje produkty, zanim zaczną je eksportować za granicę: „Fakt, że w tych firmach pracują niedawni weterani, oznacza, że sieć już istnieje". G opowiedział, że gdy był żołnierzem, jego jednostka dostawała dni wolne w bazie, aby zwiedzać start-upy zajmujące się sztuczną inteligencją w Tel Awiwie. Prezesi firm prezentowali wówczas najnowocześniejsze systemy nadzoru, które następnie sprzedawali izraelskiemu wojsku. Kierownictwo podkreślało, że wiedza żołnierzy czyni z nich obiecujących przyszłych pracowników.

B, inny weteran jednostki wywiadowczej, wyjaśnił, że wojsko od dawna wykorzystuje prywatne firmy do gromadzenia zysków. „Wojsko faktycznie pomaga rozwijać wiele z tych technologii, a następnie współpracuje z pewnymi organizacjami, aby zarobić na eksporcie" – powiedział B. Ministerstwo Obrony Izraela, w końcu, jest zobowiązane do głębokiego zaangażowania w rozwój i eksport wszystkich produktów wojskowych, w tym przez firmy prywatne; dochód z eksportu sięgnął 8,3 miliarda dolarów w zeszłym roku, drugiego najwyższego w historii za wynikiem z 2017 roku (9,2 miliarda dolarów).

„Są rzeczy, które wojsko może dostarczyć, takie jak dane, których sektor prywatny nie może uzyskać bez ścisłej współpracy nad prototypami" – dodał B. Opisał również, jak jednostki wywiadowcze często organizują „hackathony", aby ułatwić te projekty, zapraszając weteranów wojskowych i pracowników prywatnych firm do udziału w konkursach, takich jak „ulepszanie Żelaznej Kopuły" po ostatniej wojnie w Strefie Gazy w maju.

Poza takimi zachętami, formalne podwykonawstwo jeszcze bardziej zatarło granicę między prywatnymi firmami nadzorującymi a wojskiem. B, podobnie jak wielu jego rówieśników, po oficjalnym zwolnieniu z wojska otrzymał propozycję pozostania w swojej jednostce wojskowej, ale jako pracownik prywatnej firmy. „Możesz być żołnierzem jednego

dnia, a następnego przyjść i pozostać w wojsku w tym samym dokładnie miejscu, ale teraz być prywatnym wykonawcą” – powiedział B. „Jedyną rzeczą, która się zmienia, jest twoja pensja”.

Organizacje praw człowieka, których praca dochodzeniowa była kluczem do wylądowania NSO Group na czarnej liście USA w tym miesiącu, od dawna twierdzą, że te korporacyjno-wojskowe powiązania są tym, co czyni prywatny przemysł inwigilacyjny tak niebezpiecznym. John Scott-Railton, starszy badacz w Citizen Lab na Uniwersytecie Toronto, centrum badań nad prawami cyfrowymi, które od lat bada komercyjne firmy zajmujące się inwigilacją, opisał broń cybernetyczną taką jak Pegasus jako „anty-rozliczeniową” z założenia. Takie oprogramowanie, wyjaśnił, „pochodzi z kontekstów, w których nie ma żadnej odpowiedzialności za państwowe uprawnienia do inwigilacji… A jeśli jest jedna rzecz, którą wiemy o tajnych uprawnieniach do inwigilacji, to to, że zawsze będą nadużywane”.

Byli oficerowie, z którymi przeprowadzono wywiady, zgodzili się z tym stwierdzeniem. „Spędziliśmy nasz czas zasadniczo prowadząc inwigilację ludności cywilnej, która nie miała dostępu do obrońcy prawnego i odmawiano jej praw obywatelskich”, powiedział G o swoim doświadczeniu w wywiadzie wojskowym. „Byliśmy szkoleni do naruszania prywatności ludzi za życie, a potem oferowano nam jeszcze więcej pieniędzy, aby robić to za granicą”.

Rebranding broni

Przez ostatnią dekadę izraelskie prawo eksportowe klasyfikowało oprogramowanie szpiegowskie Pegasus jako broń podlegającą tym samym restrykcjom, co drony, karabiny szturmowe i pociski. Dziś jednak niewielu pracujących dla NSO chce, by ich produkty były tak postrzegane. Oskarżenia o wykorzystywanie przez izraelskie wojsko możliwości inwigilacji

Palestyńczyków na terytoriach okupowanych – w tym poprzez tworzenie tajnych baz danych biometrycznych i nadużywanie danych osobowych – narastają od lat, wywołując publiczne kryzysy firm cybernetycznych, które zaczynają być poddawane większej kontroli ze strony mediów i rządów.

Zamiast tego NSO próbowało zmienić markę swoich produktów na „rozwiązania na rzecz globalnego bezpieczeństwa i stabilności", a nie na broń. W ciągu ostatniego roku firma uruchomiła nową politykę praw człowieka i zarządzania, jak również sposoby działań w mediach społecznościowych, które przedstawiają grupę cyberszpiegowską jako „dumną rodzinę". Jednak nawet osoby opracowujące nowe inicjatywy NSO zorientowane na prawa człowieka mają trudności ze sprecyzowaniem, w jaki sposób ich produkty przyczyniają się do „bezpieczeństwa i stabilności".

Podczas wywiadu na początku października, urzędnik prawny w NSO przyznał, że „właściwe użycie" broni masowej inwigilacji „spowoduje pewne szkody". „Są pewne rzeczy, które zostaną uznane za dopuszczalne, a inne nie" – powiedział. „Ale to jest prawda z każdym produktem, nawet z młotkiem. Możesz użyć młotka do zbudowania mostu, ale nie byłbyś w stanie przewidzieć, że to się stanie, gdy zostanie on sprzedany".

Scott-Railton z Citizen Lab nie zgodził się z tą opinią. „Jeśli sprzedajesz rządowi młotek i szkolisz go, jak zbudować za jego pomocą broń, prawdopodobnie powinieneś być pociągnięty do odpowiedzialności" – powiedział, opisując broń do cyberszpiegostwa jako rodzaj „azbestu", a nie narzędzia domowego: coś rakotwórczego, co po zastosowaniu jest często śmiertelne.

Niewyraźna granica między prywatnymi firmami inwigilacyjnymi a izraelskim wojskiem sprawia jednak, że odpowiedzialność w tej branży wydaje się być poza zasięgiem. W zeszłym tygodniu, rząd izraelski szybko zaczął lobbować w Stanach Zjednoczonych, aby usunąć NSO z czarnej listy. Według Haaretz, Shalev Hulio w

tajnym liście wezwał izraelski rząd do wstawienia się za jego firmą, powołując się na długotrwałą współpracę pomiędzy firmą a wojskiem.

Jednak nawet w sytuacji, gdy NSO Group jest nieustannie przeciągana i demaskowana w międzynarodowych mediach, a inne kraje również starają się umieścić firmę na czarnej liście, izraelskie wojsko i przemysł cyberszpiegowski prowadzą zupełnie inne rozmowy. Na konferencji Innotech w zeszłym tygodniu, liderzy zarówno z sektora rządowego jak i prywatnego wydawali się bardziej zainteresowani ochroną przemysłu, który jest lukratywnym źródłem PKB.

Na razie izraelski reżim nadzoru nad okupowanymi terytoriami palestyńskimi pozostanie źródłem zysków dla izraelskich firm cyberszpiegowskich, dostarczając danych, fachowej siły roboczej i możliwości testowania. Firmy te będą z kolei nadal zaopatrywać armię izraelską w broń cybernetyczną używaną przeciwko ludności cywilnej, której odmawia się podstawowych zabezpieczeń prawnych.

Niebezpieczeństwo polega jednak nie tylko na tym, że Palestyńczycy żyjący pod rządami wojskowymi będą poddawani coraz bardziej inwazyjnym formom monitorowania. Współpraca przemysłu prywatnego z izraelskim wojskiem napędza inwigilacyjny wyścig zbrojeń, który grozi erozją prawa cywilów do prywatności na całym świecie. Tak długo jak sektor prywatny i wojskowy Izraela pozostają ze sobą ściśle powiązane, potrzeba będzie czegoś więcej niż tylko czarnej listy, aby powstrzymać firmy takie jak NSO.

Autorstwo: Sophia Goodfriend
Tłumaczenie: Wojciech Łobodziński
Źródło oryginalne: 972mag.com
Źródło polskie: Strajk.eu

Bibliografia

1. https://innotech.i-hls.com/agenda/

2. https://youtu.be/y73Bg7y-Ylk?t=5826

3. https://www.haaretz.com/israel-news/tech-news/israeli-spy-tech-firm-tracked-mobile-users-around-the-world-investigation-suggests-1.9379842

4. https://www.972mag.com/edition/israel-surveillance-laboratory-palestinians/

5. https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus

6. https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

7. https://www.ft.com/content/24f22b28-56d1-4d66-8f76-c9020b1b5cb1

8. https://www.whoprofits.org/updates/nso-group-technologies-of-control/

9. https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg

10. https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/

11. https://www.glassdoor.com/Salary/NSO-Group-Tel-Aviv-Yafo-Salaries-EI_IE1355066.0,9_IL.10,23_IM1002.htm

12. https://www.ft.com/content/24f22b28-56d1-4d66-8f76-c9020b1b5cb1

13. https://www.haaretz.com/middle-east-news/.premium-with-israel-s-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states-1.9093465

14. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

15. https://www.972mag.com/israel-digital-colonialism-social-media/

16. https://www.timesofisrael.com/israels-military-exports-hit-8-3-billion-in-2020-second-highest-ever-total/

17. https://www.972mag.com/dystopia-surveillance-palestinians-army/

18. https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

19. https://www.nsogroup.com/governance/human-rights-policy/

20. https://www.haaretz.com/israel-news/tech-news/.premium-after-spyware-scandal-israeli-nso-touts-proud-family-of-workers-

saving-lives-1.10119049

21. https://www.haaretz.com/israel-news/.premium.HIGHLIGHT-israel-spyware-and-corruption-nso-ties-to-netanyahu-bennett-and-other-politicians-1.10383553

22. https://www.middleeasteye.net/news/pegasus-spyware-uk-pm-urged-cut-funding-gulf-linked-scandal

23. https://7amleh.org/2021/11/08/7-human-rights-organizations-condemn-use-of-nso-group-s-pegasus-against-palestinian-activists

24. https://www.972mag.com/zoom-censorship-dissent/