BEZPRZEWODOWY ŚWIAT: Nowa era inwazyjnego nadzoru

W świecie coraz bardziej połączonym przez technologię, nowe badanie ujawnia niepokojące zjawisko: możliwość wykorzystania Wi-Fi i wież komórkowych do inwigilacji bez wiedzy lub zgody osób fizycznych. Technologia ta, która wykorzystuje promieniowanie bezprzewodowe otoczenia, może zmienić sposób, w jaki myślimy o prywatności i bezpieczeństwie, podnosząc istotne kwestie etyczne i prawne.

Technologia stojąca za zagrożeniem

Badanie, przeprowadzone przez wydział inżynierii na Uniwersytecie w Porto w Portugalii, zostało opublikowane na otwartej stronie naukowej Cornell University, arXiv, 24 stycznia 2025 roku. Naukowcy zaprojektowali system, który wykorzystuje rekonfigurowalną inteligentną powierzchnię (RIS) do manipulowania i kierowania sygnałami Wi-Fi, umożliwiając wykrywanie i renderowanie wizualnych obrazów ludzkiej aktywności z ponad 90% dokładnością.

Fariha Husain, kierownik programu promieniowania elektromagnetycznego (EMR) i sieci bezprzewodowych Children's Health Defense (CHD), wyjaśniła możliwości tej technologii: „Panele RIS mogą być strategicznie rozmieszczone, aby zoptymalizować odbicie i sterowanie sygnałem bezprzewodowym. W pomieszczeniach można je montować na ścianach, sufitach lub meblach. Na zewnątrz mogą być instalowane na budynkach,

latarniach i billboardach reklamowych. Dodatkowo, panele RIS umożliwią inteligentny nadzór miejski poprzez śledzenie ruchu pieszych i pojazdów”.

Implikacje tej technologii są głębokie. Według badań, system może wykrywać gesty dłoni i monitorować parametry życiowe, takie jak oddech, nawet gdy osoby znajdują się za przeszkodami lub nie współpracują. Naukowcy twierdzą, że ta zdolność stanowi postęp w dziedzinie rozpoznawania aktywności człowieka (HAR) w kontekście komunikacji szóstej generacji (6G).

Kwestie etyczne i dotyczące prywatności

Podczas gdy zwolennicy twierdzą, że technologia RIS może mieć korzystne zastosowania w opiece zdrowotnej i automatyzacji, obrońcy prywatności biją na alarm. W. Scott McCollough, główny prawnik zajmujący się sprawami EMR & Wireless w CHD, podkreślił niebezpieczne implikacje dla masowej inwigilacji: „Przyszłe sieci 6G będą miały wbudowaną funkcjonalność RIS i nie zdziwiłbym się, gdyby nie wdrożyli RIS w przyszłych aktualizacjach 5G. Kilka raportów branżowych i rządowych na temat 6G wprost mówi, że chcą wykorzystać te możliwości do inwigilacji”.

Obawy McCollougha nie są bezpodstawne. Technologia stojąca za badaniem jest podobna do Origin AI, komercyjnej technologii wykrywania Wi-Fi opracowanej przez Raya Liu, byłego wykonawcę Agencji Zaawansowanych Projektów Badawczych Obrony (DARPA). Origin AI może lokalizować ruch z ponad 90% dokładnością i rejestrować wzorce oddechowe, co czyni ją potężnym narzędziem do ochrony domu i automatyzacji. Jednak budzi to również poważne obawy dotyczące prywatności.

Husain zauważył: „Panele RIS mogą być zintegrowane z obiektami i środowiskami bez wiedzy lub zgody osób, co sprawia, że rezygnacja z tej formy nadzoru jest prawie niemożliwa”.

Dodała, że „technologia ta stwarza niebezpieczne implikacje dla masowego nadzoru, prywatności i bezpieczeństwa danych”.

Kontekst historyczny i współczesne znaczenie

Rozwój technologii RIS jest częścią szerszego trendu w ewolucji nadzoru. Peter Krapp, profesor filmu i studiów medialnych na Uniwersytecie Kalifornijskim w Irvine, badał wszechobecną naturę nadzoru w erze cyfrowej. Według Krappa, Stany Zjednoczone mają największą liczbę kamer monitorujących na osobę na świecie, a nadzór ten nie ogranicza się do kamer wideo. Telefony komórkowe, GPS, Wi-Fi, Bluetooth i różne aplikacje przyczyniają się do kompleksowego systemu śledzenia.

Krapp wyjaśnił: „Bazy danych mogą korelować dane o lokalizacji ze smartfonów, prywatnych kamer, czytników tablic rejestracyjnych i technologii rozpoznawania twarzy. Organy ścigania mogą śledzić, gdzie jesteś i gdzie byłeś, często bez nakazu. Prywatni brokerzy danych również gromadzą i sprzedają te dane, tworząc w dużej mierze nieuregulowany rynek danych osobowych”.

Historyczny kontekst inwigilacji w Stanach Zjednoczonych jest kluczowy dla zrozumienia współczesnego znaczenia technologii RIS. Od wczesnych dni podsłuchów po współczesną erę cyfrowego śledzenia, równowaga między bezpieczeństwem a prywatnością była kwestią sporną. Środowisko prawne po wyroku w sprawie Roe przeciwko Wade dodało nowe warstwy złożoności, z obawami o to, w jaki sposób dane śledzenia mogą być wykorzystywane w kontekście praw reprodukcyjnych i innych wrażliwych kwestii.

Wnioski: Wezwanie do regulacji

W miarę jak technologia RIS rozwija się i staje się coraz bardziej zintegrowana z sieciami 6G, potrzeba solidnych regulacji i wytycznych etycznych jest bardziej krytyczna niż

kiedykolwiek. Husain i McCollough opowiadają się za ściślejszym nadzorem i kampaniami uświadamiającymi społeczeństwo, aby zapewnić, że technologia ta nie narusza prywatności i bezpieczeństwa danych osobowych.

McCollough podsumował: „Musimy przeprowadzić krajową rozmowę na temat etycznych implikacji technologii RIS. Nie chodzi tylko o techniczną wykonalność; chodzi o ramy moralne i prawne, które będą regulować jej użycie”.

W świecie, w którym technologia może przekształcić przedmioty codziennego użytku w narzędzia nadzoru, walka o prywatność jest daleka od zakończenia. Ponieważ technologia ta nadal ewoluuje, ważne jest, aby prawodawcy, technolodzy i obywatele współpracowali w celu ochrony podstawowego prawa do prywatności w erze cyfrowej.

Chińskie procesory graficzne niemal dziesięciokrotnie przewyższają układy Nvidii w symulacjach superkomputerowych: Zmiana w suwerenności technologicznej

W przełomowym odkryciu, które może zmienić globalny krajobraz półprzewodników, chińscy naukowcy osiągnęli niemal dziesięciokrotny wzrost wydajności w symulacjach superkomputerowych przy użyciu krajowych procesorów graficznych (GPU), przewyższając systemy zasilane najnowocześniejszym sprzętem firmy Nvidia. Ten kamień milowy, szczegółowo opisany w recenzowanym badaniu opublikowanym w Chinese Journal of Hydraulic Engineering, podkreśla rosnącą sprawność Chin w zakresie wysokowydajnych obliczeń (HPC) i ich determinację w ograniczaniu zależności od zagranicznych technologii.

Osiągnięcie to pojawia się w kluczowym momencie globalnego wyścigu technologicznego, ponieważ eskalacja amerykańskich sankcji na zaawansowane półprzewodniki zmusiła Chiny do przyspieszenia wysiłków na rzecz opracowania własnych alternatyw. Podczas gdy sceptycy ostrzegają, że same optymalizacje oprogramowania nie mogą w nieskończoność wypełniać luk sprzętowych, badanie podkreśla, w jaki sposób innowacyjne projekty obliczeń równoległych i poprawki oprogramowania mogą odblokować bezprecedensowy wzrost wydajności, nawet przy mniej zaawansowanym sprzęcie.

Przełom w obliczeniach równoległych

Badania, prowadzone przez profesora Nan Tongchao z Państwowego Kluczowego Laboratorium Hydrologii Zasobów Wodnych i Inżynierii Wodnej Uniwersytetu Hohai, koncentrowały się na podejściu do obliczeń równoległych „wiele węzłów, wiele procesorów graficznych”. Wykorzystując produkowane w kraju procesory CPU i GPU, zespół osiągnął znaczną poprawę

wydajności w symulacjach na dużą skalę w wysokiej rozdzielczości – co ma kluczowe znaczenie dla takich zastosowań jak modelowanie obrony przeciwpowodziowej i zapobieganie podtopieniom w miastach.

„Wyzwanie dla chińskich naukowców jest jeszcze trudniejsze", zauważono w badaniu, wskazując na dominację zagranicznych producentów w produkcji zaawansowanych procesorów graficznych, takich jak A100 i H100 firmy Nvidia. Sprawę pogarsza również zastrzeżony ekosystem oprogramowania CUDA firmy Nvidia, który nie może być uruchamiany na sprzęcie innych firm, skutecznie uniemożliwiając chińskim programistom dostęp do kluczowych narzędzi do opracowywania algorytmów.

Pomimo tych przeszkód, zespół profesora Nana wykazał, że techniki optymalizacji oprogramowania mogą znacznie zwiększyć wydajność chińskich procesorów graficznych, umożliwiając im prześcignięcie amerykańskich superkomputerów w określonych obliczeniach naukowych. Przełom ten nie tylko podważa dominację firmy Nvidia, ale także podkreśla potencjał alternatywnych podejść do obliczeń o wysokiej wydajności.

Szersze implikacje sankcji technologicznych

Wyniki badania podkreślają niezamierzone konsekwencje amerykańskich sankcji technologicznych, które miały na celu ograniczenie dostępu Chin do zaawansowanych półprzewodników i krytycznych technologii. Wydaje się, że zamiast tłumić innowacje, ograniczenia te ożywiły wysiłki Chin na rzecz osiągnięcia samowystarczalności technologicznej.

„Osiągnięcie to wskazuje na możliwe niezamierzone konsekwencje eskalacji sankcji technologicznych Waszyngtonu, jednocześnie podważając dominację amerykańskich chipów, od dawna uważanych za kluczowe dla zaawansowanych badań naukowych" – czytamy w badaniu.

Rozwój ten jest zgodny z szerszą strategią Pekinu mającą na celu złagodzenie ryzyka „punktu krytycznego” w krytycznych technologiach – termin odnoszący się do słabych punktów w łańcuchach dostaw, które mogą zostać wykorzystane przez przeciwników geopolitycznych. Inwestując znaczne środki w krajową produkcję półprzewodników i ekosystemy oprogramowania, Chiny dążą do zmniejszenia swojej zależności od zagranicznego sprzętu i oprogramowania, zapewniając sobie odporność technologiczną na coraz bardziej rozdrobnionym rynku globalnym.

Kontekst historyczny: Od zależności do innowacji

Znaczenie tego osiągnięcia jest nie do przecenienia w kontekście trwającej od dziesięcioleci walki Chin o dogonienie zachodniej technologii półprzewodników. W przeszłości Chiny w dużym stopniu polegały na imporcie zaawansowanych chipów, a na rynku dominowały amerykańskie firmy, takie jak Nvidia, Intel i AMD. Zależność ta stała się rażącą słabością wraz z eskalacją napięć geopolitycznych, co skłoniło Stany Zjednoczone do nałożenia szeroko zakrojonych kontroli eksportu zaawansowanych półprzewodników i sprzętu do produkcji chipów.

W odpowiedzi Chiny zwiększyły inwestycje w swój krajowy przemysł półprzewodników, dzięki inicjatywom takim jak „Big Fund”, przeznaczając miliardy dolarów na badania i rozwój. Chociaż wyzwania pozostają – szczególnie w zakresie produkcji chipów w najnowocześniejszych 3-nanometrowych i niższych węzłach – ten najnowszy przełom pokazuje, że Chiny robią znaczące postępy w wykorzystywaniu istniejącego sprzętu poprzez innowacje w oprogramowaniu.

Co nas czeka?

Choć wyniki badania są imponujące, eksperci ostrzegają, że

same optymalizacje oprogramowania nie są w stanie w pełni zrekompensować ograniczeń sprzętowych. Przykładowo, układy GPU firmy Nvidia słyną nie tylko z surowej mocy obliczeniowej, ale także z wszechstronności i integracji z solidnym ekosystemem oprogramowania. Powtórzenie tego poziomu wydajności w szerokim zakresie aplikacji będzie wymagało ciągłego rozwoju zarówno sprzętu, jak i oprogramowania.

Niemniej jednak badanie to stanowi znaczący krok naprzód w dążeniu Chin do suwerenności technologicznej. Ponieważ zespół profesora Nana nadal udoskonala swoje podejście do obliczeń równoległych, implikacje dla takich dziedzin jak modelowanie klimatu, sztuczna inteligencja i bezpieczeństwo narodowe mogą być głębokie.

Zdaniem jednego z obserwatorów branży, „jest to sygnał alarmowy dla globalnej społeczności technologicznej. Chiny udowadniają, że potrafią wprowadzać innowacje pod presją, a reszta świata będzie musiała dostosować się do tej nowej rzeczywistości”.

W miarę nasilania się wojny technologicznej między Stanami Zjednoczonymi a Chinami, badanie to służy jako przypomnienie, że innowacje często rozwijają się w obliczu przeciwności losu. Czy ten przełom doprowadzi do szerszej zmiany w równowadze sił technologicznych, dopiero się okaże, ale jedno jest pewne: wyścig o dominację półprzewodników jest daleki od zakończenia.

Wiceprezydent USA Vance ostrzega Europę przed

przyjmowaniem chińskich modeli sztucznej inteligencji typu open source

W przemówieniu o wysokiej stawce na paryskim szczycie AI wiceprezydent USA JD Vance naciskał na globalne przyjęcie zamkniętych systemów sztucznej inteligencji, przedstawiając sztuczną inteligencję jako broń geopolityczną. Jego uwagi, przeplatane cienko zawoalowanymi groźbami, podkreślają rosnące napięcie między wysiłkami USA zmierzającymi do zmonopolizowania sztucznej inteligencji a wzrostem znaczenia Chin jako lidera innowacji open source.

USA rozpoczynają geopolityczną bitwę o przyszłość sztucznej inteligencji

W przemówieniu, które łączyło ambicję z zastraszaniem, wiceprezydent USA JD Vance wyszedł na scenę podczas paryskiego szczytu AI w dniu 12 lutego 2025 r., aby przekazać surowe przesłanie: Przyszłość sztucznej inteligencji musi być kształtowana przez Stany Zjednoczone, a wszelkie odchylenia od tej ścieżki będą kosztować. Uwagi Vance'a, które określiły sztuczną inteligencję zarówno jako narzędzie dobrobytu, jak i broń wpływów geopolitycznych, podkreślają eskalację rywalizacji między Stanami Zjednoczonymi a Chinami w wyścigu o dominację w krajobrazie sztucznej inteligencji.

„Sztuczna inteligencja to broń, która jest niebezpieczna w niewłaściwych rękach, ale jest niesamowitym narzędziem wolności i dobrobytu we właściwych rękach” – oświadczył Vance, nie pozostawiając wątpliwości co do tego, kto jego zdaniem powinien sprawować tę władzę. Jego przemówienie, opisane przez obserwatorów jako „groźne” i „mroczne”, podkreśliło zaangażowanie USA w utrzymanie pozycji lidera w dziedzinie sztucznej inteligencji poprzez ograniczenie dostępu do krytycznych komponentów i technologii.

„Stany Zjednoczone Ameryki są liderem w dziedzinie sztucznej inteligencji, a nasza administracja planuje utrzymać ten stan rzeczy” – powiedział Vance, dodając, że USA »zamkną drogi przeciwnikom do osiągnięcia zdolności AI« na równi z własnymi.

Rozwój sztucznej inteligencji open source: wyzwanie dla dominacji i arogancji USA

Ostrzeżenia Vance’a pojawiają się w czasie, gdy chińskie modele sztucznej inteligencji typu open source, takie jak DeepSeek, zyskują na popularności na całym świecie. W przeciwieństwie do zamkniętych, zastrzeżonych systemów promowanych przez amerykańskie firmy, takie jak OpenAI, DeepSeek oferuje przejrzystą, konfigurowalną alternatywę, która już wykazała wyższą wydajność i opłacalność.

„Stany Zjednoczone nadal trzymają się myślenia” małego dziedzińca z wysokimi murami ”, zauważył jeden z analityków, odnosząc się do preferencji Ameryki dla systemów o zamkniętym kodzie źródłowym. „Ale dzięki otwartemu oprogramowaniu i tanim alternatywom” wysoki mur dziedzińca »może stać się ślepą uliczką«.

Otwarty charakter DeepSeek pozwala programistom na całym świecie replikować i modyfikować technologię bez warstw

cenzury wbudowanych w modele amerykańskie. Na przykład, podczas gdy serwery DeepSeek w Chinach mogą ograniczać niektóre zapytania, takie jak te związane z protestami na placu Tiananmen w 1989 roku i innymi wrażliwymi tematami, wersje DeepSeek działające poza Chinami mogą działać bez takich ograniczeń, umożliwiając programistom wykorzystanie jego pełnych możliwości. Ta elastyczność sprawiła, że model ten stał się potężnym narzędziem innowacji w regionach, w których dostęp do amerykańskich systemów sztucznej inteligencji jest ograniczony lub gdzie utrzymują się obawy dotyczące cenzury i bezpieczeństwa danych.

Amerykańskie systemy sztucznej inteligencji mają więcej warstw cenzury niż modele chińskie

Przemówienie Vance'a i powstanie DeepSeek podkreślają fundamentalny podział w ekosystemie sztucznej inteligencji: wybór między zastrzeżonymi systemami o zamkniętym kodzie źródłowym a alternatywami o otwartym kodzie źródłowym. Podczas gdy amerykańskie firmy, takie jak OpenAI, wspierane przez rząd, zbudowały swoją reputację na ściśle kontrolowanych, wysokowydajnych modelach, podejście Chin polegało na demokratyzacji sztucznej inteligencji poprzez udostępnienie swojej technologii globalnej społeczności. Strategia ta już zaczęła zmieniać układ sił w wyścigu o sztuczną inteligencję.

Krytycy amerykańskiego podejścia twierdzą, że jego nacisk na zamknięte systemy grozi izolacją amerykańskich firm i tłumieniem innowacji. Z kolei modele open-source, takie jak DeepSeek, oferują ścieżkę do współpracy i szybkiego rozwoju, umożliwiając mniejszym krajom i prywatnym przedsiębiorstwom konkurowanie na równych warunkach. Dla Europy, która od dawna stara się stać trzecim biegunem w transatlantycko-azjatyckiej rywalizacji technologicznej, DeepSeek stanowi potencjalną szansę na zmniejszenie zależności od technologii

amerykańskiej.

Rozwój sztucznej inteligencji typu open source ma również istotne implikacje strategiczne. Zwiększając dostępność zaawansowanych narzędzi sztucznej inteligencji, Chiny rzucają wyzwanie monopolowi USA na najnowocześniejsze technologie. Na przykład zdolność DeepSeek do przetwarzania ogromnych ilości danych z większą wydajnością niż wiele modeli amerykańskich może przyspieszyć innowacje w dziedzinach takich jak opieka zdrowotna, energia i pojazdy autonomiczne. Co więcej, dostępność sztucznej inteligencji typu open-source mogłaby umożliwić krajom i firmom rozwijanie własnych możliwości w zakresie sztucznej inteligencji bez polegania na infrastrukturze lub wiedzy specjalistycznej Stanów Zjednoczonych, zmniejszając dźwignię, jaką Stany Zjednoczone posiadają obecnie na globalnych rynkach technologicznych.

Istnieją jednak obawy dotyczące bezpieczeństwa i etycznych implikacji sztucznej inteligencji typu open source. Chociaż przejrzystość DeepSeek jest mocną stroną, rodzi również pytania o to, w jaki sposób technologia ta może zostać niewłaściwie wykorzystana lub uzbrojona. Ostrzeżenie Vance’a o tym, że sztuczna inteligencja jest „bronią”, przypomina, że stawka w tej rywalizacji jest niezwykle wysoka.

Wielka Brytania żąda od Apple stworzenia globalnego backdoora, zagrażającego

prywatności na całym świecie

W oszałamiającym posunięciu, które może na nowo zdefiniować granice prywatności i nadzoru rządowego, Wielka Brytania potajemnie nakazała Apple stworzenie backdoora do zaszyfrowanej pamięci masowej w chmurze, zapewniając brytyjskim władzom bezprecedensowy dostęp do danych użytkowników na całym świecie. Żądanie to, wydane na mocy kontrowersyjnej brytyjskiej ustawy o uprawnieniach śledczych z 2016 roku – nazwanej „Kartą szpiega" – oznacza znaczącą eskalację w globalnej bitwie o szyfrowanie, prywatność i swobody obywatelskie.

Zamówienie, o którym po raz pierwszy poinformował Washington Post, wymaga od Apple zapewnienia ogólnego dostępu do wszystkich zaszyfrowanych danych użytkowników przechowywanych w chmurze, a nie tylko do kont docelowych. Pozwoliłoby to brytyjskim organom ścigania ominąć zabezpieczenia szyfrowania i uzyskać dostęp do poufnych informacji, w tym zdjęć, wiadomości i dokumentów, bez wiedzy lub zgody użytkowników.

Dla Apple, firmy, która od dawna broni prywatności użytkowników jako podstawowej wartości, żądanie to stanowi egzystencjalny dylemat: zastosować się do nakazu Wielkiej Brytanii i zdradzić zaufanie użytkowników lub całkowicie wycofać zaszyfrowane usługi przechowywania danych w Wielkiej Brytanii. Źródła zaznajomione ze sprawą sugerują, że Apple prawdopodobnie wybierze to drugie rozwiązanie, ale nie rozwiązałoby to żądania Wielkiej Brytanii dotyczącego dostępu do danych w innych krajach, w tym w Stanach Zjednoczonych.

Niebezpieczny precedens dla prywatności

Według Washington Post, żądanie Wielkiej Brytanii nie ma precedensu w największych demokracjach. W przeszłości firmy technologiczne, takie jak Apple, współpracowały z organami ścigania w indywidualnych przypadkach, na przykład pomagając FBI w uzyskaniu dostępu do iPhone'a terrorysty w 2016 roku. Jednak nakaz Wielkiej Brytanii wykracza daleko poza te ukierunkowane żądania, szukając szerokiego backdoora, który podważyłby szyfrowanie dla wszystkich użytkowników.

„Nie ma powodu, dla którego [rząd] Wielkiej Brytanii miałby prawo decydować za obywateli całego świata, czy mogą oni korzystać ze sprawdzonych korzyści w zakresie bezpieczeństwa, które wynikają z szyfrowania typu end-to-end" – powiedział Apple brytyjskim prawodawcom w marcu 2024 r., przewidując taki ruch.

Obrońcy prywatności i eksperci ds. cyberbezpieczeństwa potępili działania Wielkiej Brytanii, ostrzegając, że stworzenie tylnych drzwi dla organów ścigania nieuchronnie osłabi szyfrowanie dla wszystkich. „Ważne jest, aby zrozumieć, że każdy rodzaj dostępu tylnymi drzwiami (lub frontowymi drzwiami) dla" dobrych »może być również wykorzystany przez« złych "- stwierdziła Fundacja Technologii Informacyjnych i Innowacji w raporcie z 2020 roku.

Obawy te nie są hipotetyczne. W 2021 r. były dyrektor FBI Chris Wray argumentował przed Senacką Komisją Sądownictwa, że szyfrowanie utrudnia dochodzenia w sprawie krajowego ekstremizmu, wzywając firmy technologiczne do tworzenia backdoorów, które chronią prywatność, umożliwiając jednocześnie dostęp rządowi. Jednak eksperci wielokrotnie ostrzegali, że taka równowaga jest niemożliwa – każdy backdoor może zostać wykorzystany przez hakerów, autorytarne reżimy lub inne złośliwe podmioty.

Globalne konsekwencje

Jeśli Wielkiej Brytanii uda się zmusić Apple do przestrzegania przepisów, może to wywołać efekt domina, ośmielając inne narody do żądania podobnego dostępu. Kraje takie jak Chiny, które już zablokowały szyfrowane aplikacje do przesyłania wiadomości, takie jak Signal, mogłyby wykorzystać precedens Wielkiej Brytanii do uzasadnienia własnych żądań dotyczących backdoorów. Mogłoby to zmusić Apple do wycofania zaszyfrowanych usług w chmurze na całym świecie, zamiast ryzykować naruszenie prywatności użytkowników.

Brytyjska ustawa o uprawnieniach śledczych, która upoważnia rząd do zmuszania firm do pomocy w dostępie do danych użytkowników, od dawna jest krytykowana za jej nadmierny zasięg. Krytycy twierdzą, że prawo, które czyni przestępstwem nawet ujawnienie takich żądań, przyznaje rządowi niekontrolowane uprawnienia do inwigilacji.

Apple ma możliwość odwołania się od nakazu Wielkiej Brytanii do tajnego panelu technicznego i sędziego, ale prawo nie zezwala firmie na opóźnienie wykonania nakazu podczas procesu odwoławczego. Pozostawia to Apple niewielkie pole manewru, rodząc pytania o przyszłość szyfrowania i prywatności w erze cyfrowej.

Historia oporu

Stanowisko Apple w kwestii prywatności jest od lat cechą charakterystyczną marki. W 2016 roku firma słynnie opierała się nakazowi rządu USA odblokowania iPhone’a zmarłego terrorysty w sprawie San Bernardino, argumentując, że stworzenie backdoora stworzy niebezpieczny precedens. Podczas gdy Apple ostatecznie poszło na kompromis, opracowując plan skanowania urządzeń użytkowników w poszukiwaniu nielegalnych materiałów, inicjatywa ta została odłożona na półkę po szerokiej reakcji ze strony obrońców prywatności.

Najnowsze żądanie Wielkiej Brytanii grozi wznowieniem tej bitwy, stawiając obawy o bezpieczeństwo narodowe przeciwko podstawowemu prawu do prywatności. Jak zauważył Washington Post, brytyjski nakaz stanowi znaczącą porażkę firm technologicznych w ich trwającej od dziesięcioleci walce o uniknięcie wykorzystania ich jako narzędzi nadzoru rządowego.

Dalsza droga

Domaganie się przez Wielką Brytanię globalnego backdoora do szyfrowanej pamięci masowej Apple w chmurze jest przełomowym momentem w toczącej się debacie na temat prywatności i bezpieczeństwa. Podczas gdy organy ścigania twierdzą, że szyfrowanie umożliwia przestępcom i terrorystom uniknięcie wykrycia, firmy technologiczne i obrońcy prywatności utrzymują, że osłabienie szyfrowania miałoby daleko idące konsekwencje dla wolności osobistych i cyberbezpieczeństwa.

Podczas gdy Apple rozważa swoje opcje, świat bacznie się temu przygląda. Czy firma podtrzyma swoje zobowiązanie do ochrony prywatności, nawet jeśli oznacza to wycofanie usług z Wielkiej Brytanii? A może skapituluje pod presją rządu, ustanawiając precedens, który może osłabić szyfrowanie na całym świecie?

Jedno jest pewne: wynik tej bitwy ukształtuje przyszłość cyfrowej prywatności na nadchodzące lata. W erze, w której dane są cenniejsze niż kiedykolwiek, stawka nie może być wyższa.

„Dostęp, którego domaga się Wielka Brytania, nie ma precedensu w największych demokracjach” – donosi Washington Post. Jeśli Wielka Brytania odniesie sukces, może nie być ostatnia.

Wi-Fi może być wykorzystywane do wpływania na fale mózgowe, ma potencjał do efektów hipnotycznych i inżynierii społecznej.

W dzisiejszym połączonym świecie bezprzewodowy dostęp do Internetu stał się wszechobecny, można go znaleźć w prawie każdej kawiarni, biurze i domu. Sygnały Wi-Fi nie są jednak łagodne. Promieniowanie o częstotliwości radiowej (RF) nieustannie bombarduje komórki i wpływa na fale mózgowe. Szczególnie niepokojące są fale o ekstremalnie niskiej częstotliwości (ELF), które mogą potencjalnie zakłócać fale mózgowe i sprawiać, że dana osoba nieświadomie wchodzi w sugestywny stan umysłu. Wi-Fi jest wektorem inżynierii społecznej, powodującym, że ludzie rezygnują z krytycznego myślenia, aby dostosować się do oficjalnych narracji i myślenia grupowego.

Keith Cutter, znany krytyk nowoczesnych technologii bezprzewodowych, spędził lata badając ciemną stronę promieniowania Wi-Fi. Według Cuttera wpływ Wi-Fi nie ogranicza się do bezpośredniej ekspozycji na promieniowanie, ale rozciąga się również na bardziej subtelne i niepokojące efekty, w tym porywanie fal mózgowych, zaburzenia poznawcze i to, co nazywa „efektem pamięci Wi-Fi” na tkankach ciała.

Wpływ pól elektromagnetycznych o częstotliwości radiowej w czasie

Wi-Fi może być wykorzystywane do wpływania na fale mózgowe, ma potencjał hipnotyczny i socjotechniczny
11/13/2024 / Autor: Lance D Johnson

W dzisiejszym połączonym świecie bezprzewodowy dostęp do Internetu stał się wszechobecny, można go znaleźć w prawie każdej kawiarni, biurze i domu. Ale sygnały Wi-Fi nie są łagodne. Promieniowanie o częstotliwości radiowej (RF) nieustannie bombarduje komórki i wpływa na fale mózgowe. Szczególnie niepokojące są fale o ekstremalnie niskiej częstotliwości (ELF), które mogą potencjalnie zakłócać fale mózgowe i sprawiać, że dana osoba nieświadomie wchodzi w sugestywny stan umysłu. Wi-Fi jest wektorem inżynierii społecznej, powodującym, że ludzie rezygnują z krytycznego myślenia, aby dostosować się do oficjalnych narracji i myślenia grupowego.

Keith Cutter, znany krytyk nowoczesnych technologii bezprzewodowych, spędził lata badając ciemną stronę promieniowania Wi-Fi. Według Cuttera wpływ Wi-Fi nie ogranicza się do bezpośredniej ekspozycji na promieniowanie, ale rozciąga się również na bardziej subtelne i niepokojące efekty, w tym porywanie fal mózgowych, zaburzenia poznawcze i to, co nazywa „efektem pamięci Wi-Fi” na tkankach ciała.

Wpływ pól elektromagnetycznych o częstotliwości radiowej w czasie
Wi-Fi działa przy użyciu pól elektromagnetycznych o częstotliwości radiowej, przesyłając dane za pomocą modulowanego impulsowo promieniowania RF. Podczas gdy sama technologia może wydawać się nieszkodliwa – w końcu większość urządzeń emituje tylko stosunkowo niskie poziomy promieniowania RF – Cutter uważa, że skumulowany wpływ tej ekspozycji w czasie jest daleki od łagodnego.

Jedną z głównych obaw, na które zwraca uwagę Cutter, jest wpływ fal o ekstremalnie niskiej częstotliwości (ELF), które Wi-Fi emituje oprócz sygnałów RF o wyższej częstotliwości. Fale ELF mają zakres od około 3 do 30 Hz, czyli zakres częstotliwości, który akurat pokrywa się z naturalnymi częstotliwościami oscylacji ludzkiego mózgu. Aktywność elektryczna mózgu jest podzielona na różne pasma częstotliwości, z których każde jest związane z różnymi stanami świadomości i funkcjami umysłowymi:

- Fale delta (0,5-4 Hz): Związane z głębokim snem, leczeniem i relaksacją.
- Fale Theta (4-8 Hz): Związane z głębokim relaksem, medytacją i kreatywnością
- Fale alfa (8-12 Hz): Obecne podczas spokojnych, zrelaksowanych stanów, takich jak marzenia na jawie lub lekka medytacja.
- Fale beta (13-30 Hz): Związane z aktywnym myśleniem, koncentracją i rozwiązywaniem problemów.
- Fale gamma (30-44 Hz): Zaangażowane w wyższe funkcje poznawcze, takie jak uczenie się, pamięć i przetwarzanie sensoryczne.

Cutter najbardziej interesuje się impulsami ELF o częstotliwości 10 Hz, emitowanymi przez nadajniki Wi-Fi. Sygnalizatory te, które stale pulsują na tej częstotliwości, zasadniczo nadają stały sygnał, aby zapewnić, że urządzenia pozostaną połączone. Cutter uważa, że impulsy o częstotliwości 10 Hz mogą mieć głęboki wpływ na aktywność mózgu, w szczególności poprzez wywoływanie zjawiska znanego jako porywanie fal mózgowych.

Przetwarzanie fal mózgowych za

pomocą impulsów o częstotliwości 10Hz może wprowadzać ludzi w sugestywny stan

Porywanie fal mózgowych odnosi się do synchronizacji fal mózgowych z częstotliwością zewnętrzną. Kiedy mózg jest wystawiony na działanie spójnego bodźca zewnętrznego o określonej częstotliwości, takiego jak sygnał 10 Hz emitowany przez Wi-Fi, może przesunąć swoje naturalne wzorce fal mózgowych, aby je dopasować. Przy częstotliwości 10 Hz mózg wchodzi w bardziej zrelaksowany stan, podobny do fal alfa, co odpowiada zmniejszonej aktywności korowej.

Cutter jest tym szczególnie zaniepokojony, ostrzegając, że długotrwała ekspozycja na sygnał ELF 10 Hz może stworzyć „stan sugestywny", w którym mózg jest bardziej podatny na wpływy zewnętrzne. Te zewnętrzne wpływy mogą obejmować media, marketing, a nawet podświadome programowanie, z których wszystkie są wprowadzane do ludzi, gdy są pod wpływem urządzeń emitujących Wi-Fi.

„Mówimy o możliwości kontroli umysłu" – ostrzega Cutter, sugerując, że tego rodzaju manipulacja falami mózgowymi może sprawić, że osoby będą bardziej podatne na zewnętrzne sugestie (takie jak hipnoza). Manipulacja może być wykorzystywana do zmuszania ludzi do wierzenia lub myślenia w określony sposób, wbrew ich intuicji, wiedzy, racjonalnemu myśleniu lub instynktom.

Promieniowanie Wi-Fi może wywoływać „efekt pamięci"

Kolejną kwestią poruszoną przez Cuttera jest możliwość wywoływania przez Wi-Fi „efektu pamięci" w tkankach ciała. Odnosi się to do sposobu, w jaki pewne częstotliwości

elektromagnetyczne mogą być absorbowane i zatrzymywane przez organizm, potencjalnie prowadząc do długoterminowych zmian fizycznych lub warunków zdrowotnych.

Cutter porównuje to zjawisko do traumy przechowywanej w ciele – podobnej do psychologicznej koncepcji „pamięci traumy", w której przeszła trauma emocjonalna lub fizyczna przejawia się w ciele nawet po minięciu wydarzenia. W przypadku Wi-Fi sugeruje on, że ciało może absorbować promieniowanie i przechowywać je w tkankach, prowadząc do ciągłych problemów zdrowotnych, takich jak zmęczenie, bóle głowy, a nawet poważniejsze schorzenia związane z nadwrażliwością elektryczną.

Wi-Fi nie jest łagodnym udogodnieniem technologicznym. Jego rozprzestrzenianie się w codziennym życiu stanowi „ukrytą epidemię", która po cichu neguje zdrowie i dobre samopoczucie jednostek oraz czyni ich umysły bardziej podatnymi na sugestie.

Chiny twierdzą, że grupa cyberprzestępcza Volt Typhoon jest aktywem CIA wymyślonym w celu ich zdyskredytowania

Organizacja cyberprzestępcza Volt Typhoon trafiła na pierwsze strony gazet za swoje ataki w ostatnich latach i często donosi się, że ścigają ją amerykańskie władze. Chińskie Narodowe Centrum Reagowania na Wirusy Komputerowe (CVERC) twierdzi jednak, że Volt Typhoon został w rzeczywistości stworzony przez Stany Zjednoczone i ich sojuszników z NATO w celu zniszczenia ich reputacji i właśnie opublikowali trzecią część trwającej serii, która ich zdaniem potwierdza ich twierdzenia.

Oskarżyli oni Stany Zjednoczone, Kanadę, Wielką Brytanię, Australię i Nową Zelandię, wraz z licznymi agencjami wywiadowczymi, o angażowanie się w cyberszpiegostwo przeciwko Chinom i innym krajom, w tym Japonii, Niemcom i Francji, a także użytkownikom Internetu na całym świecie.

Następnie oskarżyli Stany Zjednoczone o rozpoczęcie operacji fałszywej flagi mających na celu ukrycie cyberataków. Chiny twierdzą, że Ameryka robi to wszystko, aby stworzyć iluzję „tak zwanego zagrożenia chińskimi cyberatakami".

FBI, Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) oraz NSA obwiniają grupę Volt Typhoon o atakowanie krytycznej amerykańskiej infrastruktury.

CVERC opublikowało trzecią część swojej serii w formie dokumentu w wielu językach zatytułowanego „Lie to Me: Volt Typhoon III – Unravelling Cyberespionage and Disinformation Operations Conducted by US Government Agencies". Przedstawiono w nim swoje twierdzenia, opierając się na poprzednich raportach o tym, jak władze amerykańskie wykonują „bezpodstawne uprawnienia do szpiegowania wszystkich ludzi na całym świecie, w tym Amerykanów za pośrednictwem sekcji 702 FISA, aby agencje rządowe USA mogły wyeliminować zagranicznych konkurentów i bronić cybernetycznej hegemonii i długoterminowych interesów monopoli".

Według raportu, Chiny współpracowały z dziesiątkami ekspertów ds. cyberbezpieczeństwa, aby dojść do wniosku, że USA i

Microsoft nie mogą udowodnić, że Chiny były zaangażowane w Volt Typhoon; raport nie wymienia ekspertów, z którymi się konsultowano.

Raport wskazuje również na programy takie jak gromadzenie danych PRISM i Biuro Operacji Dostosowanego Dostępu NSA, z których oba zostały ujawnione przez Edwarda Snowdena i mają podobne zdolności do tych z Volt Typhoon.

W raporcie powtórzono również wiele materiałów wymienionych w pierwszych dwóch częściach serii, w tym znane amerykańskie programy, takie jak sekcja 702 dotycząca bezprawnej inwigilacji cudzoziemców oraz struktura Marble, której CIA używa do cyberoperacji, która została wcześniej ujawniona przez Wikileaks.

Złośliwe oprogramowanie Volt Typhoon przeniknęło do krytycznej amerykańskiej infrastruktury

Złośliwe oprogramowanie Volt Typhoon było wykorzystywane do infiltracji krytycznych amerykańskich systemów i infrastruktury, zagrażając fizycznemu bezpieczeństwu Amerykanów poprzez atakowanie systemów energetycznych, kontroli ruchu lotniczego i portowego, kolejowych i wodnych.

Wyciekłe dokumenty, które pojawiły się na początku tego roku, wskazywały również na udział CCP w złożonej zagranicznej kampanii cyberszpiegowskiej, która wywołała szereg ostrzeżeń ze strony ekspertów ds. cyberbezpieczeństwa. Celem programu jest destabilizacja wrogów i zapewnienie Chinom lepszej pozycji do przygotowania się do potencjalnej wojny z USA i ich sojusznikami.

Dokumenty wykazały, że chińska grupa znana jako I-Soon infiltrowała departamenty rządowe w Korei Południowej, Wietnamie, Tajlandii, Indiach i organizacjach stowarzyszonych

z NATO.

Poprzez Volt Typhoon KPCh stara się zapewnić sobie przewagę militarną nad USA za pomocą środków niemilitarnych.

Casey Fleming, dyrektor generalny firmy doradczej BlackOps Partners, powiedział The Epoch Times: „KPCh jest hiper-koncentrowana na osłabianiu USA pod każdym kątem, aby wygrać wojnę bez walki. Tak właśnie wygląda III wojna światowa. To szybkość technologii, skrytość nieograniczonej wojny i brak zasad”.

Studenci Harvardu demonstrują, w jaki sposób inteligentne okulary Meta mogą być wykorzystywane do natychmiastowej identyfikacji osób i uzyskiwania dostępu do ich danych osobowych

Studenci z Uniwersytetu Harvarda odkryli, że nowe inteligentne okulary Meta mogą być wykorzystane do identyfikacji osoby i

uzyskania dostępu do jej danych osobowych.

Facebook, we współpracy z producentem luksusowych okularów przeciwsłonecznych Ray-Ban, stworzył Ray-Ban Stories. Te inteligentne okulary są wyposażone w podwójną zintegrowaną kamerę o rozdzielczości pięciu megapikseli, zestaw trzech mikrofonów i dyskretne głośniki nauszne. Użytkownicy mogą potajemnie robić zdjęcia i nagrywać filmy w podróży oraz kontrolować niektóre aplikacje bez użycia rąk.

Po naciśnięciu przycisku z boku Meta Ray Ban 2, użytkownicy mogą filmować do trzech minut wideo na żywo, które można nawet przesyłać strumieniowo na Instagram.

Niedawno dwóch studentów Harvardu opracowało program dla Ray-Ban Stories, który może być wykorzystany do natychmiastowej identyfikacji osób i uzyskania dostępu do ich danych osobowych, w tym adresów domowych.

Studenci inżynierii AnhPhu Nguyen i Caine Ardayfio opublikowali mrożącą krew w żyłach demonstrację tego, co potrafi ich program o nazwie I-Xray.

„Jakiś koleś mógłby po prostu znaleźć adres domowy jakiejś dziewczyny w pociągu i po prostu podążać za nią do domu” – powiedział Nguyen. „Czy jesteśmy gotowi na świat, w którym nasze dane są widoczne na pierwszy rzut oka?”.

„Celem stworzenia tego narzędzia nie jest niewłaściwe użycie i nie udostępniamy go” – powiedzieli Nguyen i Ardayfio w dokumencie przedstawiającym technologię. „Naszym celem jest zademonstrowanie obecnych możliwości inteligentnych okularów, wyszukiwarek twarzy, dużych modeli językowych i publicznych baz danych. [Podnosimy świadomość, że wyodrębnienie czyjegoś adresu domowego i innych danych osobowych na podstawie samej twarzy na ulicy jest dziś możliwe”.

Ekspert ds. bezpieczeństwa: okulary umożliwiające filmowanie osób postronnych to niebezpieczny krok naprzód

Program I-Xray działa poprzez rozpoczęcie transmisji na żywo w inteligentnych okularach. Nagrania na żywo są następnie przesyłane do programu o nazwie PimEyes, narzędzia do rozpoznawania twarzy, które wykorzystuje sztuczną inteligencję do dopasowania nagranej twarzy do wszelkich publicznie dostępnych obrazów w Internecie.

I-Xray następnie uruchamia inne narzędzie AI, które przeszukuje publiczne bazy danych w celu uzyskania danych osobowych osoby na zdjęciu, w tym jej imienia i nazwiska, adresu, numeru telefonu, a nawet informacji o krewnych.

„Wszystko to jest przekazywane z powrotem do aplikacji, którą napisaliśmy na naszym telefonie" – powiedział Nguyen w filmie opublikowanym na X.

I-Xray jest wyjątkowy, ponieważ działa całkowicie automatycznie, szybko pozwalając użytkownikowi znaleźć informacje o napotkanych osobach.

Jake Moore, doradca ds. bezpieczeństwa w firmie ESET, powiedział: „Okulary umożliwiające filmowanie osób postronnych to „niepokojąco niebezpieczny rozwój".

„Obserwujemy rozwój technologii w obszarach, które po prostu nie są potrzebne" – powiedział Moore. „Co więcej, gdy są one przystosowane do rozpoznawania osób, staje się to przerażającym narzędziem, które może być łatwo nadużywane".

Tymczasem rzecznik Meta powiedział: „Aby było jasne, okulary Ray-Ban Meta nie są wyposażone w technologię rozpoznawania twarzy".

Ciemna strona GEOLOKACJI: Jak nasze gadżety stały się cichymi prześladowcami dzięki pozycjonowaniu WiFi

W dzisiejszym cyfrowo połączonym świecie geolokalizacja odgrywa kluczową rolę w sposobie nawigacji, interakcji z usługami, a nawet zachowania bezpieczeństwa.

Geolokalizacja to proces identyfikacji dokładnego położenia geograficznego urządzenia lub osoby przy użyciu technologii takich jak systemy pozycjonowania WiFi i globalne systemy nawigacji satelitarnej (GNSS). Chociaż technologie te oferują ogromne korzyści, wiążą się również z poważnymi zagrożeniami i lukami w zabezpieczeniach, budząc obawy o prywatność i bezpieczeństwo.

Korzyści z geolokalizacji

Wprowadzenie technologii geolokalizacji do szerszego społeczeństwa zasadniczo zmieniło sposób, w jaki ludzie nawigują i wchodzą w interakcje z otoczeniem. Ułatwia znalezienie najszybszej drogi do domu, a także innych miejsc docelowych i pomaga firmom usprawnić operacje dostawy – zwiększając ogólną wydajność i wygodę. Co więcej, precyzyjne

dane lokalizacyjne mają kluczowe znaczenie dla służb ratunkowych – umożliwiając szybki czas reakcji, który może uratować życie w krytycznych sytuacjach.

Systemy pozycjonowania wewnątrz budynków, określane również jako śledzenie lokalizacji wewnątrz budynków, są niezbędne w dużych zamkniętych przestrzeniach, takich jak szpitale, centra handlowe i stacje kolejowe. Systemy te umożliwiają dokładne śledzenie lokalizacji za pomocą urządzeń mobilnych, takich jak smartfony lub tablety, poprawiając nawigację i wydajność operacyjną w budynkach.

Dla profesjonalistów pracujących w środowiskach odizolowanych lub wysokiego ryzyka, geolokalizacja wewnątrz budynków jest nieoceniona dla zapewnienia bezpieczeństwa. Śledzenie pozycji pracowników w czasie rzeczywistym może mieć kluczowe znaczenie w sytuacjach awaryjnych, umożliwiając szybką interwencję w razie potrzeby. W scenariuszach takich jak pożary lub incydenty terrorystyczne w miejscach publicznych, geolokalizacja wewnątrz budynków pomaga służbom ratowniczym w szybkim zlokalizowaniu osób znajdujących się w niebezpieczeństwie.

Zewnętrzne usługi geolokalizacyjne, zasilane przez GNSS – takie jak Galileo w Unii Europejskiej i GPS w Stanach Zjednoczonych – stały się wszechobecne. Te konstelacje satelitów transmitują sygnały, które umożliwiają odbiornikom obsługującym GNSS określenie dokładnych danych o lokalizacji, wspierając szeroki zakres zastosowań w różnych sektorach i demonstrując ich szerokie zastosowanie w nowoczesnej technologii i życiu codziennym.

Niebezpieczeństwa, zagrożenia i słabe punkty geolokalizacji

Technologia geolokalizacji stwarza poważne zagrożenia dla prywatności i bezpieczeństwa użytkowników. Systemy

pozycjonowania WiFi, które są używane zarówno na zewnątrz, jak i wewnątrz budynków, gromadzą obszerne dane, które mogą zostać niewłaściwie wykorzystane przez nieupoważnione podmioty.

Integracja geolokalizacji z krytycznymi systemami bezpieczeństwa wprowadza wyzwania związane z cyberbezpieczeństwem. Cyberataki mogą manipulować danymi o lokalizacji, zagrażając bezpieczeństwu służb ratowniczych i osób znajdujących się w niebezpieczeństwie. Dlatego też ochrona wewnętrznych systemów geolokalizacji przed cyberzagrożeniami ma kluczowe znaczenie.

Przykłady solidnych środków cyberbezpieczeństwa obejmują wdrażanie silnych protokołów szyfrowania w celu zabezpieczenia przesyłanych danych o lokalizacji; stosowanie uwierzytelniania wieloskładnikowego w celu kontrolowania dostępu do poufnych informacji; oraz przeprowadzanie regularnych testów penetracyjnych w celu identyfikacji i naprawy luk w zabezpieczeniach.

Usługi geolokalizacji wewnątrz budynków są podatne na zagrożenia cybernetyczne, podobnie jak każdy inny sektor technologiczny. Cyberprzestępcy wykorzystują luki w oprogramowaniu i protokołach komunikacyjnych, aby uzyskać dostęp do danych o lokalizacji w czasie rzeczywistym lub przechowywanych informacji z tych systemów. Ponadto ataki spoofingowe wprowadzają w błąd sygnały lokalizacji, prowadząc do błędów nawigacji i potencjalnego zagrożenia bezpieczeństwa użytkowników.

Urządzenia infrastrukturalne zintegrowane z systemami geolokalizacji, takie jak beacony i bramy, mogą być również celem ataków cybernetycznych. Komponenty te służą jako punkty wejścia dla zdalnych ataków lub nieautoryzowanego dostępu za pośrednictwem połączeń Bluetooth.

Zabezpieczenie tych punktów dostępu ma zasadnicze znaczenie dla zapobiegania naruszeniom i ochrony poufnych danych

związanych z geolokalizacją w pomieszczeniach. Na przykład konfiguracja zapór ogniowych i systemów wykrywania włamań może pomóc w monitorowaniu i blokowaniu podejrzanej aktywności sieciowej.

Powszechne przyjęcie geolokalizacji rodzi obawy o niewłaściwe wykorzystanie osobistych danych o lokalizacji. Reklamodawcy wykorzystują te dane do ukierunkowanych reklam, podczas gdy złośliwe podmioty mogą wykorzystywać je do inwigilacji lub kradzieży tożsamości. Ochrona wrażliwych informacji jest najważniejsza w usługach geolokalizacji wewnątrz budynków, wymagając solidnych środków bezpieczeństwa, takich jak bezpieczne praktyki programistyczne, szyfrowanie, silne uwierzytelnianie i regularne audyty bezpieczeństwa.

Aby skutecznie ograniczyć to ryzyko, osoby fizyczne i organizacje powinny priorytetowo traktować zabezpieczanie sieci Wi-Fi za pomocą szyfrowanych połączeń. Wdrożenie rygorystycznych ustawień prywatności na urządzeniach i aplikacjach pomaga ograniczyć informacje o lokalizacji udostępniane stronom trzecim. Ponadto podnoszenie świadomości na temat zagrożeń cyberbezpieczeństwa i promowanie najlepszych praktyk wzmacnia ogólne bezpieczeństwo IT, zapewniając bezpieczne i odpowiedzialne korzystanie z technologii geolokalizacji.

Wojskowe korzenie Facebooka

Komentarz: Przecież to jasne , że nie ma czegoś takiego jak geniusz, który napisał aplikację i z zera został miliarderem. Bez opieki odpowiednich ludzi nie robi się takiej kariery. Tak samo z Gates'em – gdyby nie to że to był SWÓJ chłop, z dziadkiem związanym z klinikami aborcyjnymi, to by też nie był promowany. Tak samo jak Owsiak. Krzysztof

Rosnąca rola Facebooka w stale rozwijającym się aparacie nadzoru i „przedkryminalnym" państwie bezpieczeństwa narodowego wymaga nowej analizy pochodzenia firmy i jej produktów w odniesieniu do poprzedniego, kontrowersyjnego programu nadzoru prowadzonego przez DARPA, który był zasadniczo analogiczny do tego, co jest obecnie największą na świecie siecią społecznościową.

W połowie lutego Daniel Baker, amerykański weteran określany przez media jako „antytrumpowy, antyrządowy, przeciwny białej supremacji i przeciwny policji", został oskarżony przez wielką ławę przysięgłych z Florydy o dwa zarzuty „przekazywania wiadomości komunikat w handlu międzystanowym zawierający groźbę porwania lub zranienia."

Komunikat, o którym mowa, Baker umieścił na Facebooku, gdzie stworzył stronę wydarzenia mającą na celu zorganizowanie zbrojnego wiecu w stosunku do zaplanowanego przez zwolenników Donalda Trumpa 6 stycznia w stolicy Florydy, Tallahassee. „Jeśli boisz się umrzeć, walczyć z wrogiem, a potem zostań w łóżku i żyj. Zadzwoń do wszystkich swoich znajomych i powstańcie!" – napisał Baker na swojej stronie wydarzenia na Facebooku.

Sprawa Bakera jest godna uwagi, ponieważ jest to jedno z

pierwszych aresztowań „przed przestępstwem” opartych wyłącznie na wpisach w mediach społecznościowych – logiczny wniosek płynący z wysiłków administracji Trumpa, a obecnie Bidena, na rzecz normalizacji aresztowań osób za wpisy w Internecie, aby zapobiec aktom przemocy, zanim będą one mogły to zrobić. zdarzyć. Począwszy od rosnącego stopnia zaawansowania programów predykcyjnych działań policyjnych Palantira, przedsiębiorstwa wywiadu USA/kontraktora wojskowego , po formalne ogłoszenie przez Departament Sprawiedliwości programu zakłócania i wczesnego zaangażowania w 2019 r. po pierwszy budżet Bidena, który obejmuje 111 mln dolarów na ściganie i zarządzanie „rosnącą liczbą spraw związanych z terroryzmem krajowym” – Pod rządami każdej administracji prezydenckiej po 11 września zauważalny był stały postęp w kierunku skupionej przed przestępczością „wojny z terroryzmem wewnętrznym”.

Ta nowa, tak zwana wojna z terroryzmem krajowym faktycznie zaowocowała wieloma tego typu postami na Facebooku. I chociaż Facebook od dawna starał się przedstawiać siebie jako „rynek miejski”, który umożliwia nawiązywanie kontaktów ludziom z całego świata, głębsze spojrzenie na jego pozornie wojskowe pochodzenie i ciągłe powiązania wojskowe ujawnia, że największa na świecie sieć społecznościowa zawsze miała działać jako narzędzie nadzoru służące identyfikowaniu i zwalczaniu sprzeciwu w kraju.

Część 1 tej dwuczęściowej serii na temat Facebooka i amerykańskiego stanu bezpieczeństwa narodowego bada początki tej sieci mediów społecznościowych oraz czas i charakter jej powstania w związku z kontrowersyjnym programem wojskowym, który został zamknięty tego samego dnia, w którym uruchomiono Facebooka. Program, znany jako LifeLog, był jednym z kilku kontrowersyjnych programów obserwacji po 11 września, realizowanych przez Agencję Zaawansowanych Projektów Badawczych w dziedzinie Obronności (DARPA) Pentagonu, który groził zniszczeniem prywatności i swobód obywatelskich w

Stanach Zjednoczonych, a jednocześnie miał na celu zebranie danych do celów produkujących „humanizowaną” sztuczną inteligencję (AI).

Jak wykaże ten raport, Facebook nie jest jedynym gigantem z Doliny Krzemowej, którego początki ściśle pokrywają się z tą samą serią inicjatyw DARPA i którego obecne działania stanowią zarówno silnik, jak i paliwo dla zaawansowanej technologicznie wojny z krajowym sprzeciwem.

Eksploracja danych DARPA dla „bezpieczeństwa narodowego” i „humanizowania” sztucznej inteligencji

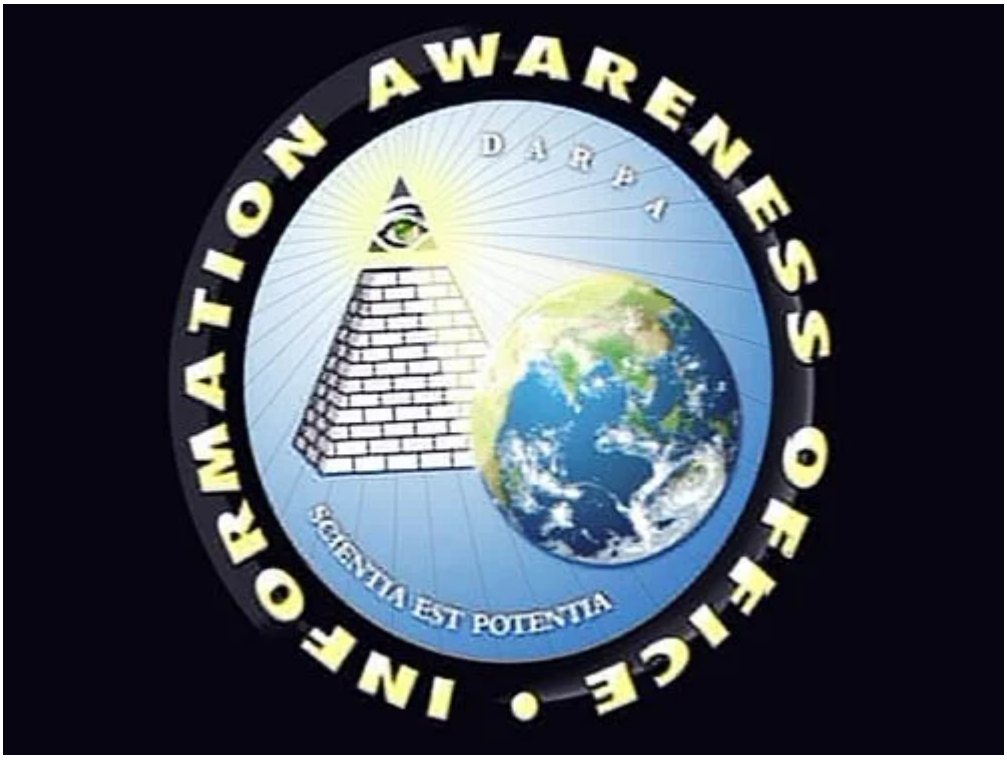
W następstwie ataków z 11 września DARPA, w ścisłej współpracy ze społecznością wywiadowczą USA (w szczególności z CIA), rozpoczęła opracowywanie „przedprzestępczego” podejścia do zwalczania terroryzmu, znanego jako Total Information Awareness (TIA). Celem TIA było opracowanie „wszystkowidzącego” aparatu wojskowego nadzoru. Oficjalna logika stojąca za TIA była taka, że □□inwazyjna inwigilacja całej populacji USA była konieczna, aby zapobiec atakom terrorystycznym, zjawiskom bioterroryzmu, a nawet naturalnie występującym epidemiom chorób.

Pomysłodawcą TIA i człowiekiem, który przewodził jej podczas jej stosunkowo krótkiego istnienia, był John Poindexter , najbardziej znany z tego, że był doradcą Ronalda Reagana ds. bezpieczeństwa narodowego podczas afery Iran-Contras i został skazany za pięć przestępstw w związku z tym skandalem. Mniej znaną działalnością przedstawicieli Iran-Contras, takich jak Poindexter i Oliver North, było opracowanie przez nich bazy danych Main Core do wykorzystania w protokołach „ciągłości rządzenia”. Main Core został wykorzystany do sporządzenia listy amerykańskich dysydentów i

„potencjalnych wichrzycieli”, z którymi należy się uporać w przypadku powołania się na protokoły COG. Na protokoły te można się powołać z różnych powodów, w tym z powodu powszechnego sprzeciwu opinii publicznej wobec amerykańskiej interwencji wojskowej za granicą, powszechnego sprzeciwu wewnętrznego lub niejasno określonego momentu „kryzysu narodowego” lub „czasu paniki”. Amerykanie nie byli informowani, czy ich nazwisko znalazło się na liście, a dana osoba mogła zostać dodana do listy tylko dlatego, że w przeszłości brała udział w protestach, nie płaciła podatków lub miała inne, „często błahe” zachowania uznawane za „ nieprzyjazny” przez jego architektów w administracji Reagana.

W świetle tego nie było przesadą, gdy felietonista *„New York Timesa”* William Safire zauważył, że dzięki TIA „Poindexter realizuje teraz swoje dwudziestoletnie marzenie: uzyskanie mocy „eksploracji danych” umożliwiającej szpiegowanie każdego publicznego i prywatnego działania każdego Amerykanina”.

Program TIA spotkał się ze znacznym oburzeniem obywateli po jego ujawnieniu opinii publicznej na początku 2003 r. Wśród krytyków TIA znalazła się Amerykańska Unia Wolności Obywatelskich, która twierdziła , że □□wysiłki inwigilacyjne „zabiją prywatność w Ameryce”, ponieważ „każdy aspekt naszego życia byłby skatalogowane”, podczas gdy kilka mediów głównego nurtu ostrzegało, że TIA „walczy z terroryzmem poprzez przerażanie obywateli USA”. W wyniku nacisków DARPA zmieniła nazwę programu na Terrorist Information Awareness, aby brzmiała mniej jak panoptykon dotyczący bezpieczeństwa narodowego, a bardziej jak program skierowany szczególnie do terrorystów w epoce po 11 września.



Logo Biura Świadomości Informacyjnej DARPA, które nadzorowało Total Information Awareness podczas jego krótkiego istnienia

Projekty TIA nie zostały jednak w rzeczywistości zamknięte, a większość z nich została przeniesiona do tajnych tek Pentagonu i społeczności wywiadowczej USA. Niektóre z nich, jak na przykład Palantir Petera Thiela , stały się finansowane przez wywiad i kierowały przedsięwzięciami sektora prywatnego , podczas gdy inne pojawiły się ponownie po latach pod pozorem walki z kryzysem związanym z Covid-19.

Wkrótce po zainicjowaniu TIA podobny program DARPA nabierał kształtu pod kierownictwem bliskiego przyjaciela Poindextera, menadżera programu DARPA Douglasa Gage'a. Projekt Gage'a, LifeLog, miał na celu „zbudowanie bazy danych śledzącej całe życie danej osoby", która obejmowałaby relacje i komunikację danej osoby (rozmowy telefoniczne, poczta itp.), jej nawyki dotyczące korzystania z mediów, zakupy i wiele innych w celu zbudowania cyfrowy zapis „ wszystko, co dana osoba mówi, widzi lub robi". LifeLog następnie pobierze te nieustrukturyzowane dane i uporządkuje je w „ dyskretne odcinki " lub migawki, jednocześnie „mapując relacje, wspomnienia, wydarzenia i doświadczenia".

Według Gage'a i zwolenników programu LifeLog stworzyłby trwały i przeszukiwalny elektroniczny dziennik całego życia danej osoby, który według DARPA mógłby zostać wykorzystany do stworzenia „cyfrowych asystentów" nowej generacji i zaoferować użytkownikom „niemal idealną pamięć cyfrową". " Gage upierał się , że nawet po zakończeniu programu poszczególne osoby miałyby „pełną kontrolę nad własnymi działaniami związanymi z gromadzeniem danych", ponieważ mogłyby „decydować, kiedy włączyć, a kiedy wyłączyć czujniki i kto udostępni dane". Od tego czasu analogiczne obietnice dotyczące kontroli użytkowników składali giganci technologiczni z Doliny Krzemowej, ale wielokrotnie łamali je dla zysku i w celu zasilania rządowego aparatu nadzoru wewnętrznego.

Informacje, które LifeLog zbierał na podstawie każdej interakcji danej osoby z technologią, byłyby łączone z informacjami uzyskanymi z nadajnika GPS, który śledził i dokumentował lokalizację danej osoby, czujników audiowizualnych rejestrujących to, co dana osoba widziała i mówiła, a także biomedycznych monitorów oceniających zdrowie danej osoby. Podobnie jak TIA, LifeLog był promowany przez DARPA jako potencjalnie wspierający „badania medyczne i wczesne wykrywanie pojawiającej się epidemii".

Krytycy w mediach głównego nurtu i poza nim szybko zwrócili uwagę, że program nieuchronnie zostanie wykorzystany do budowania sylwetek dysydentów, a także podejrzanych o terroryzm. W połączeniu z wielopoziomowym monitorowaniem osób przez TIA, LifeLog poszedł dalej, „dodając informacje fizyczne (takie jak to, jak się czujemy) i dane medialne (takie jak to, co czytamy) do danych transakcyjnych". Jeden z krytyków, Lee Tien z Electronic Frontier Foundation, ostrzegł wówczas , że programy realizowane przez DARPA, w tym LifeLog, „mają oczywiste i łatwe ścieżki do wdrożenia w ramach bezpieczeństwa wewnętrznego".

W tamtym czasie DARPA publicznie utrzymywała , że □□LifeLog i TIA nie są ze sobą powiązane, pomimo ich oczywistych

podobieństw, oraz że LifeLog nie będzie wykorzystywany do „tajnego nadzoru”. Jednakże w dokumentacji DARPA dotyczącej LifeLog odnotowano, że w ramach projektu „będzie można . . . wywnioskować o rutynach, zwyczajach i relacjach użytkownika z innymi ludźmi, organizacjami, miejscami i przedmiotami oraz wykorzystać te wzorce, aby ułatwić mu zadanie”, w którym uznano jego potencjalne zastosowanie jako narzędzia masowej inwigilacji.

Oprócz możliwości profilowania potencjalnych wrogów państwa, LifeLog miał inny cel, prawdopodobnie ważniejszy dla państwa zapewniającego bezpieczeństwo narodowe i jego partnerów akademickich – „humanizację” i rozwój sztucznej inteligencji. Pod koniec 2002 roku, zaledwie kilka miesięcy przed ogłoszeniem istnienia LifeLog, DARPA opublikowała dokument strategiczny szczegółowo opisujący rozwój sztucznej inteligencji poprzez zasilanie jej ogromnym strumieniem danych z różnych źródeł.

Projekty nadzoru wojskowego po 11 września – LifeLog i TIA to tylko dwa z nich – zapewniły ilości danych, których uzyskanie wcześniej było nie do pomyślenia, a które mogłyby potencjalnie stanowić klucz do osiągnięcia hipotetycznej „osobliwości technologicznej”. Dokument DARPA z 2002 r. omawia nawet wysiłki DARPA mające na celu stworzenie interfejsu mózg-maszyna, który przesyłałby ludzkie myśli bezpośrednio do maszyn w celu rozwoju sztucznej inteligencji poprzez ciągłe zalewanie jej świeżo wydobytymi danymi.

Jeden z projektów przedstawionych przez DARPA, Cognitive Computing Initiative, miał na celu rozwój zaawansowanej sztucznej inteligencji poprzez stworzenie „trwałego, spersonalizowanego asystenta poznawczego”, nazwanego później Perceptive Asystent, który się uczy , (PAL). PAL od samego początku był powiązany z LifeLog, którego pierwotnym zamierzeniem było zapewnienie „asystentowi” sztucznej inteligencji przypominającego człowieka zdolności podejmowania decyzji i rozumienia poprzez przekształcanie mas

nieustrukturyzowanych danych w format narracyjny.

Przyszli główni badacze projektu LifeLog odzwierciedlają także końcowy cel programu, jakim jest stworzenie humanizowanej sztucznej inteligencji. Na przykład Howard Shrobe z Laboratorium Sztucznej Inteligencji MIT i jego ówczesny zespół mieli być ściśle zaangażowani w LifeLog. Shrobe pracował wcześniej dla DARPA nad „ewolucyjnym projektowaniem złożonego oprogramowania", zanim został zastępcą dyrektora Laboratorium AI na MIT i poświęcił swoją długą karierę na budowaniu „sztucznej inteligencji w stylu kognitywnym". W latach po odwołaniu LifeLog ponownie pracował dla DARPA, a także przy projektach badawczych związanych ze sztuczną inteligencją związanych ze społecznością wywiadowczą. Ponadto laboratorium AI na MIT było ściśle powiązane z korporacją z lat 80. XX wieku i wykonawcą DARPA o nazwie Thinking Machines , która została założona przez wielu luminarzy laboratorium i/lub zatrudniała wielu luminarzy laboratorium, w tym Danny'ego Hillisa, Marvina Minsky'ego i Erica Landera, i starała się budować superkomputery AI zdolne do myślenia na poziomie ludzkim. Później okazało się, że wszystkie trzy osoby były bliskimi współpracownikami i/lub sponsorowanymi przez powiązanego z wywiadem pedofila Jeffreya Epsteina, który również hojnie przekazał darowizny na rzecz MIT jako instytucji oraz był głównym fundatorem i orędownikiem badań naukowych związanych z transhumanizmem.

Wkrótce po zamknięciu programu LifeLog krytycy obawiali się, że podobnie jak TIA będzie on kontynuowany pod inną nazwą. Na przykład Lee Tien z Electronic Frontier Foundation powiedział *VICE* w momencie anulowania LifeLog: „Nie zdziwiłbym się, gdybym dowiedział się, że rząd w dalszym ciągu finansował badania, które popchnęły tę dziedzinę do przodu, nie nazywając go LifeLog".

Wraz z krytykami jeden z potencjalnych badaczy pracujących nad LifeLog, David Karger z MIT, również był pewien, że projekt DARPA będzie kontynuowany w nowej formie. Powiedział *Wired* ,

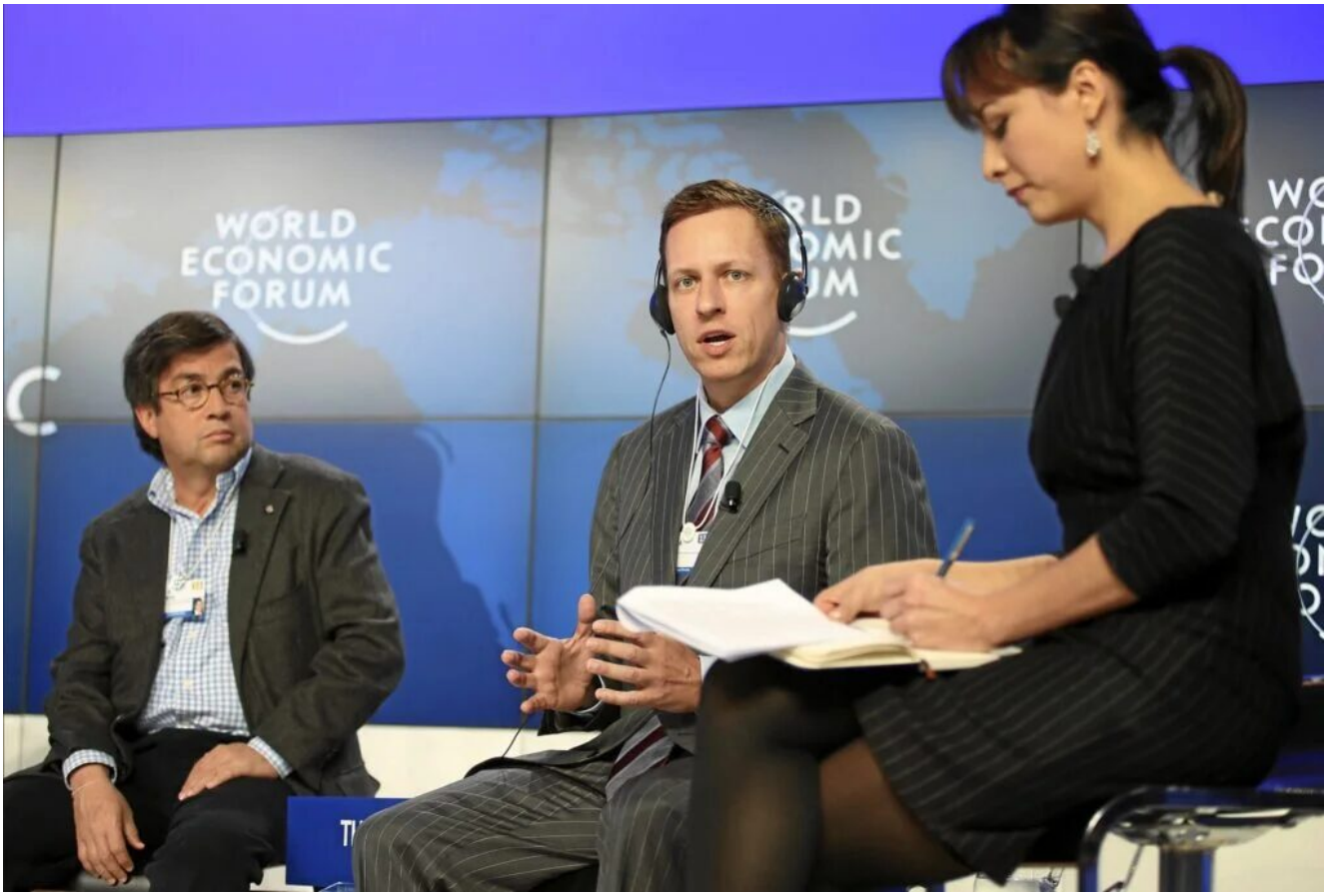
że „Jestem pewien, że takie badania będą nadal finansowane z innego tytułu. . . Nie mogę sobie wyobrazić, że DARPA „porzuci" tak kluczowy obszar badawczy".

Wydaje się, że odpowiedź na te spekulacje należy do firmy, która uruchomiła usługę dokładnie tego samego dnia, w którym Pentagon zamknął LifeLog: Facebooka.

Świadomość informacyjna Thiela

Po znacznych kontrowersjach i krytyce pod koniec 2003 roku TIA została zamknięta i pozbawiona finansowania przez Kongres, zaledwie kilka miesięcy po jej uruchomieniu. Dopiero później ujawniono, że TIA *tak naprawdę* nigdy nie została zamknięta , a jej różne programy zostały potajemnie podzielone pomiędzy sieć agencji wojskowych i wywiadowczych tworzących amerykańskie państwo zapewniające bezpieczeństwo narodowe. Część z nich została sprywatyzowana.

W tym samym miesiącu, w którym TIA została zmuszona do zmiany nazwy w związku z rosnącymi sprzeciwami, Peter Thiel założył firmę Palantir, która, nawiasem mówiąc, opracowywała podstawowe oprogramowanie panopticon, którego TIA miała nadzieję używać. Wkrótce po założeniu Palantir w 2003 r. Richard Perle, notoryczny neokonserwatysta z administracji Reagana i Busha oraz architekt wojny w Iraku, zadzwonił do Poindextera z TIA i powiedział, że chce przedstawić go Thielowi i jego współpracownikowi Alexowi Karpowi, obecnie dyrektorowi generalnemu Palantir. Według raportu magazynu *New York* Poindexter „był dokładnie tą osobą", z którą Thiel i Karp chcieli się spotkać, głównie dlatego, że „ich nowa firma miała podobne ambicje do tego, co Poindexter próbował stworzyć w Pentagonie " , czyli TIA . Podczas tego spotkania Thiel i Karp starali się „wybrać mózg człowieka obecnie powszechnie postrzeganego jako ojciec chrzestny współczesnej inwigilacji".



Peter Thiel przemawia na Światowym Forum Ekonomicznym w 2013 r., Źródło: Mirko Ries Dzięki uprzejmości Światowego Forum Ekonomicznego

Wkrótce po założeniu Palantira, choć dokładny termin i szczegóły inwestycji pozostają ukryte przed opinią publiczną, In-Q-Tel z CIA stał się, obok samego Thiela, pierwszym sponsorem firmy, przekazując jej szacunkową kwotę 2 milionów dolarów. Informacje o udziałach In-Q-Tel w Palantir zostaną podane do wiadomości publicznej dopiero w połowie 2006 roku .

Pieniądze z pewnością się przydały. Ponadto Alex Karp powiedział *New York Times* w październiku 2020 r.: „prawdziwą wartością inwestycji In-Q-Tel było to, że zapewniła ona Palantirowi dostęp do analityków CIA, którzy byli jego zamierzonymi klientami". Kluczową postacią w inwestycjach In-Q-Tel w tym okresie, w tym w inwestycji w Palantir, był dyrektor ds. informacji CIA, Alan Wade, który był głównym przedstawicielem społeczności wywiadowczej w zakresie Totalnej Świadomości Informacyjnej. Wade był wcześniej współzałożycielem firmy Chiliad, dostawcy oprogramowania

Homeland Security po 11 września, wraz z Christine Maxwell, siostrą Ghislaine Maxwell i córką działacza Iran-Contras, agenta wywiadu i barona medialnego Roberta Maxwella.

Po inwestycji In-Q-Tel CIA była jedynym klientem Palantira aż do 2008 roku. W tym okresie dwaj czołowi inżynierowie Palantira – Aki Jain i Stephen Cohen – podróżowali co dwa tygodnie do siedziby CIA w Langley w Wirginii . Jain pamięta, że □□w latach 2005–2009 odbył co najmniej dwieście podróży do siedziby CIA. Podczas tych regularnych wizyt analitycy CIA „testowali [oprogramowanie Palantira] i przekazywali opinie, a następnie Cohen i Jain wracali do Kalifornii, aby je ulepszyć". Podobnie jak w przypadku decyzji In-Q-Tel o inwestycji w Palantir, główny specjalista ds. informacji CIA pozostał w tym czasie jednym z architektów TIA. Alan Wade odegrał kluczową rolę w wielu z tych spotkań, a następnie w „udoskonalaniu" produktów Palantir.

Obecnie produkty Palantir są wykorzystywane do masowej inwigilacji, predykcyjnych działań policyjnych i innych niepokojących polityk amerykańskiego państwa zapewniającego bezpieczeństwo narodowe. Wymownym przykładem jest znaczne zaangażowanie Palantir w nowy program nadzoru nad ściekami prowadzony przez służbę zdrowia i opiekę społeczną, który po cichu rozprzestrzenia się w całych Stanach Zjednoczonych. Jak zauważono w poprzednim raporcie *Unlimited Hangout* , system ten jest wskrzeszeniem programu TIA o nazwie Biosurveillance. Przesyła wszystkie swoje dane do zarządzanej przez Palantir i tajnej platformy danych HHS Protect. Decyzja o przekształceniu kontrowersyjnych programów prowadzonych przez DARPA w prywatne przedsięwzięcia nie ograniczała się jednak do Palantira Thiela.

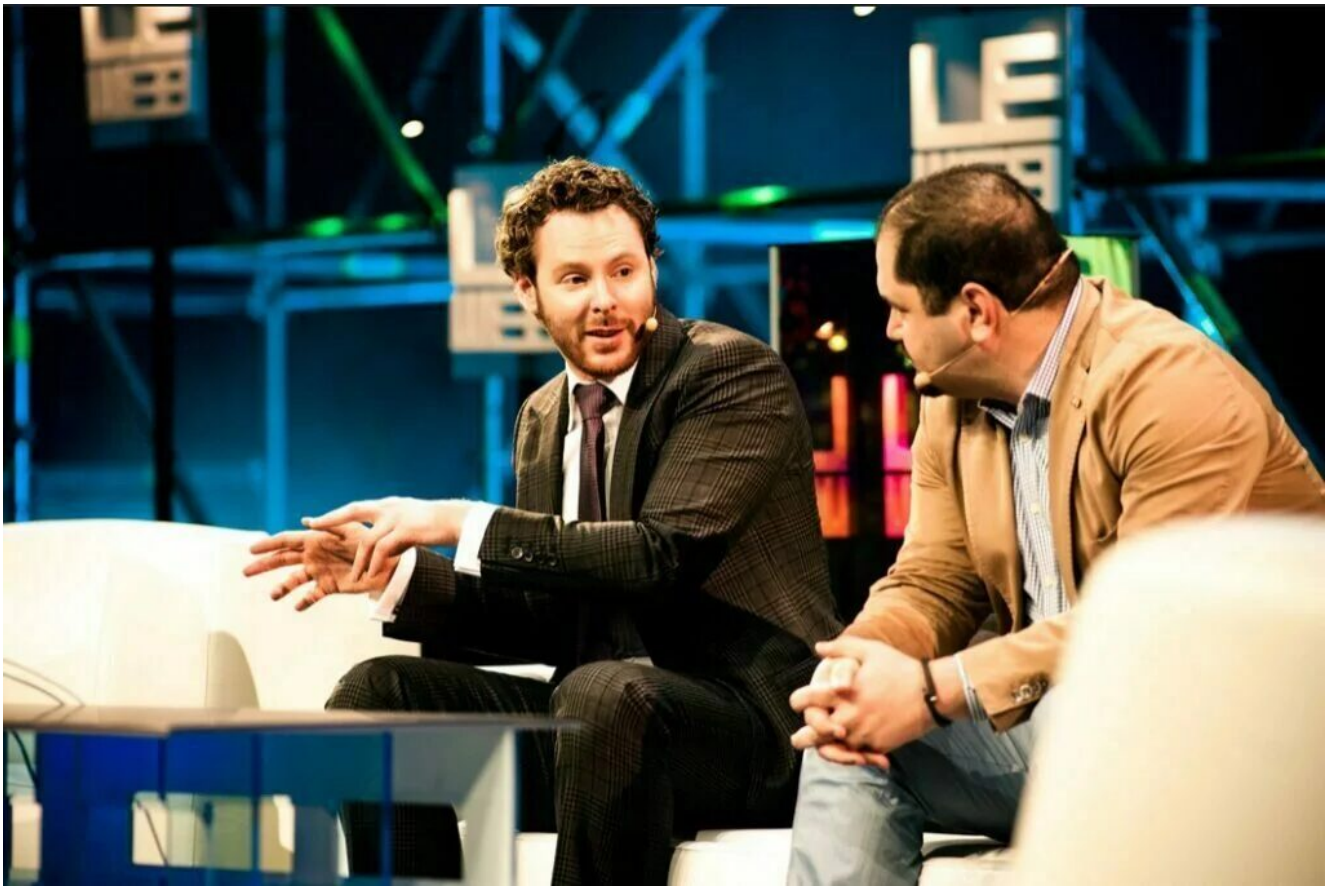
Powstanie Facebooka

Zamknięcie TIA w DARPA miało wpływ na kilka powiązanych programów, które również zostały zlikwidowane w wyniku

publicznego oburzenia wywołanego programami DARPA po 11 września. Jednym z takich programów był LifeLog. Gdy wieść o programie rozeszła się po mediach, wielu z tych samych głośnych krytyków, którzy zaatakowali TIA, z podobną gorliwością zaatakowało LifeLog, a Steven Aftergood z Federacji Amerykańskich Naukowców powiedział wówczas *Wired* , że „LifeLog ma potencjał, aby stać się czymś jak „TIA w kostkach". Postrzeganie LifeLog jako czegoś, co mogłoby okazać się jeszcze gorsze niż niedawno odwołany TIA, miało wyraźny wpływ na DARPA, która właśnie anulowała zarówno TIA, jak i inny powiązany program po znacznych protestach opinii publicznej i prasy.

Burza krytyki programu LifeLog zaskoczyła jego menadżera programu, Douga Gage'a, a Gage w dalszym ciągu zapewniał, że krytycy programu „całkowicie błędnie scharakteryzowali" cele i ambicje projektu. Pomimo protestów Gage'a oraz potencjalnych badaczy i innych zwolenników LifeLog, projekt został publicznie porzucony 4 lutego 2004 r. DARPA nigdy nie wyjaśniła swojego cichego ruchu w celu zamknięcia LifeLog, a rzecznik stwierdził jedynie, że było to powiązane z „ zmiana priorytetów" dla agencji. W związku z decyzją dyrektora DARPA Tony'ego Tethera o zabiciu LifeLog, Gage powiedział później *VICE* : „Myślę, że TIA tak go poparzyła, że □□nie chciał mieć do czynienia z dalszymi kontrowersjami z LifeLog. Śmierć LifeLog była szkodą uboczną związaną ze śmiercią TIA.

Szczęśliwie dla zwolenników celów i ambicji LifeLog, firma, która okazała się jej odpowiednikiem z sektora prywatnego, narodziła się tego samego dnia, w którym ogłoszono zakończenie działalności LifeLog. 4 lutego 2004 r. Facebook, będący obecnie największą siecią społecznościową na świecie, uruchomił swoją witrynę internetową i szybko wspiął się na szczyty mediów społecznościowych, pozostawiając inne ówczesne firmy zajmujące się mediami społecznościowymi w tyle.



Sean Parker z Founders Fund przemawia podczas konferencji LeWeb w 2011 r., Źródło: @Kmeron dla LeWeb11 @ Les Docks de Paris

Kilka miesięcy po uruchomieniu Facebooka, w czerwcu 2004 roku, współzałożyciele Facebooka Mark Zuckerberg i Dustin Moskovitz wprowadzili Seana Parkera do zespołu wykonawczego Facebooka. Parker, wcześniej znany ze współzałożyciela Napstera, później połączył Facebooka z pierwszym inwestorem zewnętrznym, Peterem Thielem. Jak wspomniano, Thiel w tym czasie, w porozumieniu z CIA, aktywnie próbował wskrzesić kontrowersyjne programy DARPA, które zostały zlikwidowane w poprzednim roku. Warto zauważyć, że Sean Parker, który został pierwszym prezydentem Facebooka, miał także historię związaną z CIA, która zwerbowała go w wieku szesnastu lat, wkrótce po tym, jak FBI przyłapało go za włamywanie się do korporacyjnych i wojskowych baz danych. Dzięki Parkerowi we wrześniu 2004 r. Thiel formalnie nabył akcje Facebooka o wartości 500 000 dolarów i został włączony do jego zarządu. Parker utrzymywał bliskie kontakty z Facebookiem i Thielem, a w 2006 roku Parker został zatrudniony jako partner zarządzający Thiel's

Founders Fund.

Thiel i współzałożyciel Facebooka, Mosokvitz, zaangażowali się poza siecią społecznościową długo po tym, jak Facebook zyskał na znaczeniu, a fundusz założycielski Thiela stał się znaczącym inwestorem w firmie Moskovitz Asana w 2012 r. Długotrwała symbiotyczna relacja Thiela ze współzałożycielami Facebooka rozciąga się na jego firmę Palantir, jak wynika z danych informacje, które użytkownicy Facebooka upubliczniają, niezmiennie trafiają do baz danych Palantir i pomagają w napędzaniu silnika monitorującego, który Palantir obsługuje garstkę amerykańskich departamentów policji, wojska i służb wywiadowczych. W przypadku skandalu związanego z danymi Facebooka i Cambridge Analytica Palantir był również zaangażowany w wykorzystywanie danych z Facebooka na potrzeby kampanii prezydenckiej Donalda Trumpa w 2016 r.

Dziś, jak wykazały niedawne aresztowania, takie jak aresztowanie Daniela Bakera, dane z Facebooka mają pomóc w nadchodzącej „wojnie z terroryzmem krajowym", biorąc pod uwagę, że informacje udostępniane na platformie są wykorzystywane do „przed popełnieniem przestępstwa" przechwytywania obywateli USA na szczeblu krajowym . W świetle tego warto zatrzymać się nad faktem, że wysiłki Thiela mające na celu wskrzeszenie głównych aspektów TIA jako jego własnej prywatnej firmy zbiegły się w czasie z tym, że stał się pierwszym inwestorem zewnętrznym w czymś, co zasadniczo było analogią do innego programu DARPA, głęboko powiązanego z TIA.

Facebook, front

Ze względu na zbieg okoliczności, że Facebook uruchomił się tego samego dnia, w którym zamknięto LifeLog, pojawiły się ostatnio spekulacje, że Zuckerberg rozpoczął i uruchomił projekt wspólnie z Moskovitzem, Saverinem i innymi w drodze zakulisowej koordynacji z DARPA lub innym organem. państwa bezpieczeństwa narodowego. Chociaż nie ma bezpośrednich

dowodów potwierdzających to dokładne twierdzenie, wczesne zaangażowanie Parkera i Thiela w projekt, szczególnie biorąc pod uwagę czas innych działań Thiela, ujawnia, że □□w rozwój Facebooka zaangażowane było państwo zapewniające bezpieczeństwo narodowe. Dyskusyjne jest, czy Facebook od samego początku miał być analogiem LifeLog, czy też stał się projektem mediów społecznościowych, który spełniał te wymagania po jego uruchomieniu. To drugie wydaje się bardziej prawdopodobne, zwłaszcza biorąc pod uwagę, że Thiel zainwestował także w inną wczesną platformę mediów społecznościowych, Friendster .

Ważnym punktem łączącym Facebooka i LifeLog jest późniejsza identyfikacja Facebooka z LifeLog przez samego architekta DARPA tego ostatniego. W 2015 roku Gage powiedział *VICE* , że „Facebook jest obecnie prawdziwą twarzą pseudo-LifeLog". Wymownie dodał: „Skończyło się na udostępnianiu tego samego rodzaju szczegółowych danych osobowych reklamodawcom i brokerom danych, nie wywołując przy tym takiego sprzeciwu, jaki wywołał LifeLog".

Użytkownicy Facebooka i innych dużych platform mediów społecznościowych byli dotychczas zadowoleni, umożliwiając tym platformom sprzedaż ich prywatnych danych, o ile działają one publicznie jako przedsiębiorstwa prywatne. Reakcja pojawiła się naprawdę dopiero wtedy, gdy takie działania zostały publicznie powiązane z rządem USA, a zwłaszcza z armią amerykańską, mimo że Facebook i inni giganci technologiczni rutynowo udostępniają dane swoich użytkowników państwu zapewniającemu bezpieczeństwo narodowe. W praktyce różnica pomiędzy podmiotami publicznymi i prywatnymi jest niewielka.

Edward Snowden, sygnalista NSA, w szczególności ostrzegł w 2019 r., że Facebook jest tak samo niegodny zaufania jak wywiad USA, stwierdzając, że „wewnętrznym celem Facebooka, niezależnie od tego, czy podaje to publicznie, czy nie, jest gromadzenie doskonałych zapisów życia prywatnego w maksymalnym stopniu możliwości, a następnie wykorzystać je do wzbogacenia

własnego przedsiębiorstwa. I cholera, konsekwencje.

Snowden stwierdził również w tym samym wywiadzie, że „im więcej Google o Tobie wie, im więcej wie o Tobie Facebook, tym więcej może. . . tworzyć trwałe zapisy życia prywatnego, tym większy wpływ i władzę mają na nas.” To podkreśla, jak zarówno Facebook, jak i powiązane z wywiadem Google osiągnęły wiele z tego, co zamierzał LifeLog, ale na znacznie większą skalę, niż pierwotnie przewidywała DARPA.

Rzeczywistość jest taka, że □□większość dzisiejszych dużych firm z Doliny Krzemowej jest od samego początku ściśle powiązana z amerykańskim establishmentem zapewniającym bezpieczeństwo narodowe. Godnymi uwagi przykładami, poza Facebookiem i Palantirem, są Google i Oracle . Dziś firmy te bardziej otwarcie współpracują z agencjami wywiadu wojskowego, które kierowały ich rozwojem i/lub zapewniały finansowanie na wczesnym etapie, ponieważ są wykorzystywane do dostarczania danych niezbędnych do napędzania nowo ogłoszonej wojny z terroryzmem krajowym i towarzyszącymi mu algorytmami.

To nie przypadek, że ktoś taki jak Peter Thiel, który zbudował Palantir wraz z CIA i pomógł zapewnić rozwój Facebooka, jest również mocno zaangażowany w oparte na Big Data „predykcyjne działania policyjne” oparte na sztucznej inteligencji i podejściu do inwigilacji i egzekwowania prawa, zarówno za pośrednictwem Palantira, jak i jego inne inwestycje . TIA, LifeLog oraz powiązane programy i instytucje rządowe i prywatne uruchomione po 11 września zawsze miały na celu wykorzystanie przeciwko amerykańskiemu społeczeństwu w wojnie przeciwko sprzeciwowi. Zostało to zauważone przez ich krytyków w latach 2003-2004 oraz przez tych, którzy badali pochodzenie zwrotu „bezpieczeństwa wewnętrznego” w USA i jego powiązanie z przeszłymi programami „antyterrorystycznymi” CIA w Wietnamie i Ameryce Łacińskiej.

Ostatecznie iluzja, że □□Facebook i powiązane z nim firmy są niezależne od amerykańskiego państwa zapewniającego

bezpieczeństwo narodowe, uniemożliwiła rozpoznanie rzeczywistości platform mediów społecznościowych i ich od dawna planowanych, ale ukrytych zastosowań, które – jak zaczynamy – zaczynają wychodzić na jaw po wydarzeniach z 6 stycznia. Teraz, gdy miliardy ludzi jest zmuszonych do korzystania z Facebooka i mediów społecznościowych w codziennym życiu, pojawia się pytanie: czy gdyby dziś ta iluzja została bezpowrotnie rozwiana, zrobiłoby to różnicę dla użytkowników Facebooka? A może społeczeństwo tak przyzwyczaiło się do oddawania swoich prywatnych danych w zamian za napędzane dopaminą pętle walidacji społecznej, że nie ma już znaczenia, kto ostatecznie będzie przechowywał te dane?

„NYT" pozwał OpenAI i Microsoft za używanie artykułów do trenowania sztucznej inteligencji

Dziennik „New York Times" poinformował w środę, że złożył pozew przeciwko firmom OpenAI i Microsoft zarzucający im bezprawne wykorzystanie artykułów gazety do szkolenia swoich chatbotów ChatGPT i Bing. Według dziennika, firmy wykorzystały miliony tekstów, naruszając prawa autorskie, tworząc na ich podstawie usługę, która konkuruje z gazetą. „NYT" domaga się

miliardów dolarów odszkodowania.

Jak napisali prawnicy dziennika w pozwie złożonym w sądzie federalnym Dystryktu Południowego Nowego Jorku, ChatGPT i Bing – oba oparte na dużym modelu językowym (LLM) GPT-4 stworzonym przez OpenAI – zostały „zbudowane poprzez kopiowanie i wykorzystywanie milionów artykułów 'Timesa' objętych prawami autorskimi".

„Podczas gdy pozwani byli zaangażowani w kopiowanie na szeroką skalę z wielu źródeł, dali treściom 'Timesa' szczególną wagę podczas budowy LLM, ujawniając preferencję, która dostrzega wartość tych dzieł" – twierdzi gazeta w pozwie. Choć „NYT" nie postawił konkretnej kwoty żądanego odszkodowania, zaznaczono, że ubiega się o „miliardy" zadośćuczynienia, argumentując, że stworzone przez OpenAI i Microsoft chatboty stanowią dla gazety konkurencję jako źródło informacji. Podkreślono, że kiedy ich użytkownik zapyta ChatGPT lub Binga o jakieś wydarzenie, w odpowiedzi dostaje często treść opartą na artykułach „NYT".

Firmy nie udzieliły dotąd komentarza.

Nowojorska gazeta jest pierwszym amerykańskim medium, które pozwało czołowe firmy tworzące sztuczną inteligencję w ten sposób, choć wcześniej podobne pozwy złożyli m.in. pisarze John Grisham i Jonathan Franzen, a także agencja fotograficzna Getty. Ich dzieła również były wykorzystywane przez OpenAI, Metę i Stability AI do budowy własnych modeli AI.

Jak pisze „NYT", do złożenia pozwu dochodzi po fiasku negocjacji między gazetą i koncernami na temat „polubownego rozwiązania" sporu dotyczącego potencjalnego porozumienia handlowego lub wytyczenia zasad użytkowania tekstów gazety. W grudniu porozumienie z OpenAI zawarł koncern Axel Springer, do którego należą m.in. portale Politico i Business Insider (a także polski Onet) oraz gazety „Bild" i „Die Welt". Wedle umowy, ChatGPT może wykorzystywać treści z mediów koncernu

(także tych za płatnym paywallem) do szkolenia modelu, a także w odpowiedziach na pytania, jednocześnie podając linki do artykułów. W zamian OpenAI ma wspomóc własne przedsięwzięcia Axela Springera w dziedzinie sztucznej inteligencji.

Źródło