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”.

Satelity NATO zostały oślepione

Niedawno w jednym z postów napisałem, że Rosja z niemal olimpijskim spokojem przyjęła zniszczenie gazociągów zbudowanych z myślą o dostarczaniu gazu bezpośrednio do Niemiec (zawsze będących celem amerykańskich operacji odstraszania i ostatecznie zniszczonych). Z pewnością kłopoty mają w dużej mierze Niemcy, które notabene, zgodnie z umową, wciąż muszą płacić za miliardy metrów sześciennych gazu, którego nie chcą otrzymywać, a dziś już nawet nie mogą. Jednak osąd, że Rosjanie bez reakcji odebrali ową amerykańską akcję militarną (skierowaną w dużej mierze przeciwko własnym niemieckim sojusznikom), jest błędny. Wczoraj, **5 października, satelity rozpoznawcze NATO obserwujące Ukrainę z jej granic zostały zneutralizowane po tym, jak Rosjanie użyli zaawansowanej, dopiero co opracowanej broni laserowej. W efekcie Zachód utracił możliwość kontroli ruchu części rosyjskiej broni jądrowej oraz znaczną część możliwości kierowania rakietami np. systemu Himars, które bez satelitów są w istocie jedynie starymi katiuszami.**

Według ekspertów-analityków, **rosyjskie wojsko wykorzystało do unieszkodliwienia satelitów nowy system laserowy Peresvet, tj. broń laserową, która jest w stanie unieszkodliwić samoloty, drony i satelity w odległości do 1500 kilometrów, co jest dystansem więcej niż wystarczającym do oślepienia satelitów szpiegowskich, których orbita zazwyczaj wynosi od 400 do 900 kilometrów.** https://en.wikipedia.org/wiki/Peresvet_(laser_weapon)

Niestety, Moskwa nie może zrobić nic więcej niż wysyłać sygnały do kompleksu imperialnego, który już całkowicie stracił rozum i którego reakcje są obecnie nieprzewidywalne z

punktu widzenia racjonalności. Ale ponieważ w Pentagonie, przynajmniej jeszcze kilka miesięcy temu, istniały wątpliwości co do skuteczności nowej rosyjskiej broni, oto nadchodzi odpowiedź. Lecz to, jak sądzę, **może mieć teraz niewielkie znaczenie, zarówno dla europejskiego środowiska politycznego, które zgodziło się na dokonanie samobójstwa całej gospodarki kontynentalnej, byle tylko być posłusznym swemu panu**, jak i **dla wielkiej masy obywateli, którzy są całkowicie nieświadomi owych technologicznych i militarnych realiów, a którzy tak czy inaczej wydają się nie posiadać zdolności do reagowania w obliczu własnej ruiny.** https://ilsimplicissimus2.com/2022/10/06/satelliti-nato-accecati/

Dziwne słupy światła na niebie europejskiej części Rosji

Wieczorem 4 października 2022, w kilku rosyjskich regionach jednocześnie, zauważono niezwykłe zjawisko na niebie. Obserwatorzy przedstawiają różne wersje tego, co widzieli. Na przykład, sugerowano, że jest to dzieło antysatelitarnej broni laserowej. Zaś w Biełgorodzie, nietypowe światło wzięto za reflektory obrony powietrznej.

https://yandex.com/video/preview/15193549313548865817

https://rutube.ru/video/8077a9ea7c2da034ee198218f6ba14c4/

Źródło

Naukowcy wynaleźli

mikroroboty z własnymi mózgami, które mogą wejść do Twego ciała.

Technologie wyprzedzają nasze wyobrażenia. Chyba, że oglądaliśmy filmy science fiction, w których owe technologie były nam zaserwowane, ale w takim razie te filmy przestają być fikcją.

Naukowcy z Cornell University zainstalowali **elektroniczne „mózgi”** w zasilanych energią słoneczną mikrorobotach o rozmiarach od 100 do 250 **mikrometrów** – mniejszych niż głowa mrówki – aby mogły poruszać się autonomicznie, bez kontroli z zewnątrz..

Chociaż naukowcy z Cornell i innych uniwersytetów opracowali wcześniej mikroskopijne maszyny, które mogą czołgać się, pływać, chodzić i składać, urządzenia te zawsze miały dołączone „struny”; w celu wygenerowania ruchu użyto przewodów do dostarczania prądu elektrycznego lub wiązek laserowych, które musiały być skierowane bezpośrednio na określone obszary robotów.

„Wcześniej musieliśmy dosłownie manipulować tymi „strunami”, aby uzyskać odpowiedź od robota. Ale teraz, gdy mamy te mózgi „na pokładzie”, to jak przecinanie sznurków marionetek. T**o tak, jak wtedy, gdy Pinokio zyskał świadomość**” – powiedział Itai Cohen, profesor fizyki w College of Arts and Sciences

„Mózg” nowych robotów składa się z komplementarnego obwodu zegarowego CMOS, który zawiera tysiąc tranzystorów oraz szereg diod, rezystorów i kondensatorów. Układ scalony CMOS generuje sygnał, który wytwarza szereg przesuniętych w fazie częstotliwości prostokątnych, które z kolei określają ruchy robota. Nogi robota to siłowniki na bazie platyny. Zarówno obwód, jak i nogi zasilane są energią fotowoltaiczną.

„Ostatecznie zdolność do przekazywania poleceń pozwoli nam wysyłać instrukcje do robota, a wewnętrzny mózg wymyśli, jak je wykonać. Następnie rozmawiamy z botem. Robot może nam coś powiedzieć o swoim otoczeniu, a my możemy zareagować mówiąc: „OK, idź tam i spróbuj dowiedzieć się, co się dzieje” – powiedział Cohen.

Nowe roboty są około 10 000 razy mniejsze niż roboty w skali makro, które mają na pokładzie elektronikę CMOS i mogą poruszać się z prędkością większą niż 10 mikrometrów na sekundę.

(…)

Co jest interesujące badania były wspierane przez Biuro Badań Naukowych Sił Powietrznych; Biuro Badań Armii; oraz Instytut Kavli na Uniwersytecie Cornell w Nanoskali.

Źródło

Norwegia chce śledzić zakupy żywności obywateli

To już się dzieje. Norwegia zmierza w kierunku społeczeństwa całkowicie kontrolowanego, gdzie państwo chce wiedzieć wszystko, co robisz.

Wcześniej pisano o tym, że Norwegia jest wiodącym krajem, jeśli chodzi o cyfrowy dowód osobisty. Jest to niemalże konieczność, aby prowadzić nowoczesne życie. Ludzie muszą go używać do bankowości internetowej i wielu innych rzeczy. Teraz okazuje się, że Norwegia chce mieć jeszcze większą kontrolę nad obywatelami. Centralne Biuro Statystyki Państwowej (SSB) w Norwegii żąda obecnie wiedzy na temat zakupów żywności przez obywateli i śledzenia wszystkich płatności kartą.

Biuro to odegrało kluczową rolę w tworzeniu „rejestru ludowego" w Norwegii po drugiej wojnie światowej, dzięki czemu ludzie otrzymali unikalny numer identyfikacyjny zwany „numerem urodzenia". Biuro to już wie, gdzie ludzie mieszkają i jakie mają dochody, ale teraz chce również śledzić dokładnie wszystko, co kupujesz w sklepie spożywczym. Chcą znać każdy pojedynczy artykuł spożywczy, który kupujesz. Państwo norweskie chce dosłownie wiedzieć, co jadłeś na obiad!

To idzie za daleko. To ostatnie posunięcie jest w istocie bardzo daleko idącym krokiem w kierunku społeczeństwa kontrolowanego. Idziemy teraz pełną parą do przodu. Prawie wszystkie duże sieci sklepów spożywczych w Norwegii muszą udostępniać państwu dane dotyczące paragonów. Wymogły również na firmie obsługującej terminale kart płatniczych, zwanej Nets, udostępnianie państwu szczegółowych informacji o wszystkich transakcjach. Około 80% płatności kartą w sklepach spożywczych w Norwegii odbywa się za pośrednictwem tej właśnie

firmy. „Sprzężenie z transakcjami płatniczymi dokonywanymi kartą debetową i paragonami sklepów spożywczych pozwala SSB [państwowemu biuru statystycznemu] połączyć transakcje płatnicze i paragony w ponad 70% codziennych zakupów spożywczych” – podało państwowe biuro w oświadczeniu na swojej stronie internetowej.

Spróbujcie to sobie wyobrazić! Norwegia zamierza połączyć szczegóły płatności dokonywanych kartą z paragonami ze sklepów spożywczych, aby dowiedzieć się dokładnie, jaki rodzaj żywności ludzie kupują i kto ją kupuje. Innymi słowy, Norwegia będzie śledzić dokładnie, jaki rodzaj żywności kupują obywatele. Mówimy tu o nowym poziomie kontroli państwowej.

Państwo będzie wiedziało, co jadłeś na śniadanie, obiad, kolację, wszystko. Cola, szynka, kurczak, stek, jak kto woli. Państwo będzie to wszystko widzieć. Państwo będzie śledzić wszystkie płatności Norwegii. Mówimy tu o ogromnych ilościach danych. Państwowy urząd statystyczny będzie zbierał 2,4 miliona paragonów KAŻDEGO dnia i jakieś 1,6 miliarda transakcji kartami rocznie. Aha, i jeszcze to. Te dane nie zostaną usunięte po ich zebraniu, jak podaje NRK.

Dane te zostaną następnie połączone z paragonami ze sklepu i wykorzystane do ustalenia, co dokładnie ludzie kupili. To jest przerażające!

Tak więc nie tylko państwo zbiera dane o wszystkich transakcjach kartą i łączy je z paragonami ze sklepów, aby dowiedzieć się, co dokładnie kupujesz, ale także będzie przechowywać te dane w nieskończoność. Państwo chce wiedzieć o tobie wszystko!

Jedna z sieci sklepów spożywczych o nazwie NorgesGruppen jest bardzo niezadowolona z tego nowego śledzenia, mówiąc, że złoży skargę w tej sprawie, ponieważ twierdzi, że jest to „bardzo inwazyjne w odniesieniu do danych osobowych naszych klientów, że nie możemy się na to zgodzić bez zwrócenia się o wskazówki

do Datatilsynet [organu ochrony danych osobowych w Norwegii]”.

Nawet Nets, firma zajmująca się płatnościami kartami jest krytyczna wobec tego procederu, twierdząc, że takie śledzenie może być „problematyczne i inwazyjne dla poszczególnych obywateli”.

Urząd Statystyczny twierdzi, że informacje te mogą być wykorzystane między innymi przez władze zdrowotne do obliczenia rozwoju konsumpcji żywności w Norwegii i sprawdzenia, jak to się różni w poszczególnych obszarach geograficznych. Mówią, że jest to ważne, aby znaleźć „regionalne, demograficzne i społeczne różnice w konsumpcji żywności”. Ponadto twierdzą, że te informacje o płatnościach mogą być wykorzystane do uzyskania statystyk o tym, którzy obywatele korzystają z prywatnej opieki zdrowotnej i ile pieniędzy na nią wydają.

Więc nie tylko zamierzają śledzić zakupy żywności przez obywateli, ale także śledzą inne rzeczy, takie jak osoby płacące za prywatną opiekę zdrowotną (w przeciwieństwie do korzystania z publicznej opieki zdrowotnej, która zresztą również sporo kosztuje w Norwegii). To jest torowanie drogi do społeczeństwa totalnej kontroli. (…) To, co widzimy obecnie, jest bardzo przerażające. Państwo próbuje zdobyć całkowitą kontrolę nad życiem ludzi i mikrozarządzać każdym drobnym szczegółem ich życia.

Jedynym sposobem na odrzucenie śledzenia zakupów przez państwo będzie użycie gotówki. Ale pytanie brzmi, jak długo będzie to dozwolone, ponieważ społeczeństwo bezgotówkowe jest coraz bardziej forsowane. A teraz może zaczniecie rozumieć, dlaczego to bezgotówkowe społeczeństwo jest forsowane… Aby państwo mogło kontrolować wszystko, co robicie. (…)

Źródło

Prawie wszystkie rządowe witryny informacyjne dotyczące COVID są tajnymi operacjami SZPIEGOWSKIMI

Europejscy naukowcy opracowali badanie ujawniające, że rządowe witryny informacyjne dotyczące (COVID-19 są koszmarem naruszającym prywatność – *niech opinia publiczna się strzeże*!

Dokument zatytułowany „Pomiar plików cookie w witrynach rządowych", finansowany przez Europejską Radę ds. Badań Naukowych (ERC), Unię Europejską (UE) i rząd hiszpański, wyjaśnia, że witryny rządowe są zasadniczo wykorzystywane jako „pojedynczy punkt" monitorowania i śledzenia całej populacji kraju" za pomocą plików cookie.

Badacze przyjrzeli się trzem różnym rodzajom stron internetowych, w tym oficjalnym rządowym stronom internetowym krajów „G20" na całym świecie; strony internetowe organizacji międzynarodowych, takich jak ONZ; oraz popularne strony internetowe wykorzystywane przez społeczeństwo do śledzenia i informacji o Grypie Fauciego. Przyjrzeli się wykorzystaniu plików cookie w każdej witrynie i doszli do wniosku, że ponad 90 procent witryn rządowych „tworzy pliki cookie zewnętrznych modułów śledzących bez zgody użytkowników".

„Ciasteczka internetowe były wykorzystywane do zbierania informacji o aktywnościach i zainteresowaniach użytkowników w Internecie” – wyjaśnia gazeta.

„Niesesyjne pliki cookie, które są tworzone przez moduły śledzące i mogą trwać przez kilka dni lub miesięcy, są powszechnie obecne nawet w krajach, w których obowiązują surowe przepisy dotyczące prywatności użytkowników. Pokazujemy również, że powyższe jest problemem dla oficjalnych stron internetowych organizacji międzynarodowych oraz popularnych serwisów, które informują opinię publiczną o pandemii COVID-19”.

Oto wskazówka: w pierwszej kolejności nie odwiedzaj żadnych rządowych witryn COVID, a nie będziesz śledzony

Innymi słowy, największe gospodarki świata angażują się w nieujawnione i potencjalnie nielegalne programy szpiegowskie i inwigilacyjne za pośrednictwem oficjalnych rządowych stron internetowych, z których społeczeństwo korzysta, aby dowiedzieć się o COVID i angażować się w inne formy konsumpcji propagandy.

Spośród 5550 rządowych witryn internetowych i ponad 118 000 adresów URL administrowanych przez rządy ponad 50 procent ich plików cookie należy do stron trzecich, podczas gdy od 10 do 90 procent pochodzi od znanych trackerów.

„Większość z tych ciasteczek ma żywotność dłużej niż jeden dzień, a wiele z nich wygasa rok lub dłużej” – ujawnia badanie.

Około 60 procent witryn rządowych używa co najmniej jednego pliku cookie stron trzecich, a 95 procent lub

prawie *wszystkie* tworzy pliki cookie bez zgody użytkownika. Nawiasem mówiąc, pliki cookie stron trzecich są „znane z tego, że śledzą użytkowników w celu gromadzenia danych", wyjaśnia badanie.

Rządowe strony internetowe dotyczące chińskiego wirusa są najgorszymi przestępcami, ponieważ 99 procent zawiera ukryte pliki cookie, które zostały tam umieszczone bez zgody użytkownika.

„Na przykład bardzo popularna strona internetowa z globalnymi mapami dotyczącymi przypadków COVID-19, prowadzona przez *Johns Hopkins University*, dodaje pliki cookie z 7 trackerów" – czytamy dalej.

„Wszystkie pozostałe witryny Top 10 to oficjalne krajowe witryny informacyjne w krajach europejskich, które mają co najmniej trzy trackery. Amerykańskie Centra Kontroli i Zapobiegania Chorobom (CDC) również znajdują się w pierwszej dziesiątce, z plikami cookie powiązanymi z trzema trackerami".

Kiedyś tego typu rzeczy miały miejsce tylko w krajach jawnie komunistycznych, takich jak Chiny, które przodują w totalitaryzmie. Jednak ostatnio Stany Zjednoczone i inne mocarstwa zachodnie wydają się naśladować model Komunistycznej Partii Chin, narzucając w swoich krajach systemy typu „społecznej oceny kredytowej".

Grypa Fauciego szybko stała się powszechnym pretekstem do naruszania prywatności ludzi, wymuszania pewnych restrykcyjnych zachowań, a nawet popełniania gwałtu medycznego w formie obowiązkowego maskowania i „szczepienia".

Okazuje się, że nawet w sieci rząd łamie prawa ludzi i śledzi ich zachowanie bez pozwolenia. Pełny zakres powodów, dla których rząd chce śledzić zachowanie ludzi w Internecie, jeszcze nie został ujawniony.

Branża technologiczna opracowuje technologię AI czytającą w myślach, która jest w stanie mierzyć lojalność obywateli wobec rządu

Chińscy naukowcy twierdzą, że opracowali nową technologię sztucznej inteligencji (AI) zdolną do „czytania w myślach”.

The Sunday Times (Wielka Brytania) po raz pierwszy doniósł o dziwnej i niepokojącej technologii, która rzekomo zostanie wykorzystana do pomiaru lojalności obywateli wobec Komunistycznej Partii Chin.

Podobnie jak wiele innych technologii Orwellowskich, ta technologia AI kontroli umysłu prawdopodobnie przejdzie test w komunistycznych Chinach, by ostatecznie zostać udostępniona reszcie świata.

Usunięte wideo i powiązany artykuł z Chińskiego Kompleksowego Narodowego Centrum Nauki w Hefei wyjaśniają, że technologia AI może analizować mimikę twarzy i fale mózgowe ludzi narażonych na „myśli i polityczną edukację” KPCh, znaną również

jako *propaganda*.

Jak wyjaśnili naukowcy, wyniki można następnie wykorzystać do „dalszego wzmocnienia ich pewności siebie i determinacji, aby być wdzięcznym partii, słuchać partii i podążać za partią”.

Business Insider poinformował, że wideo i artykuł wyjaśniające to wszystko zostały usunięte z Internetu po publicznym oburzeniu chińskich obywateli, którzy już teraz zmagają się z tyranią oceny kredytów społecznych i cenzurą internetową.

Stany Zjednoczone usankcjonowały kilka chińskich firm w 2021 r. za opracowanie „rzekomej broni kontrolującej mózg”

W artykule, który napisał dla *Forbesa*, ekspert od sztucznej inteligencji i uczenia maszynowego, dr Lance B. Eliot, zasugerował, że bez znajomości specyfiki technologii nie można stwierdzić, czy naprawdę działa tak, jak się twierdzi.

„Z pewnością nie jest to pierwszy raz, kiedy w badaniach naukowych wykorzystano funkcję skanowania fal mózgowych na ludziach” – powiedział.

„Mając to na uwadze, wykorzystywanie ich do mierzenia lojalności wobec KPCh nie jest czymś, na czym można by się skoncentrować. Kiedy taka sztuczna inteligencja jest wykorzystywana do kontroli rządowej, przekraczana jest czerwona linia”.

Komunistyczne Chiny były jednak w przeszłości usankcjonowane przez Departament Handlu USA za próby stworzenia podobnych technologii, w tym systemu biotechnologicznego opisanego jako „rzekoma broń kontrolująca mózg”.

KPCh już wykorzystuje sztuczną inteligencję i systemy

rozpoznawania twarzy do śledzenia i kontrolowania ujgurskich muzułmanów przetrzymywanych w obozach koncentracyjnych w całych Chinach. Aż trzy miliony Ujgurów jest przetrzymywanych w niewoli, wielu z nich jest torturowanych przy użyciu systemów sztucznej inteligencji.

„Naukowe dążenie do biotechnologii i innowacji medycznych może uratować życie" – powiedziała sekretarz handlu USA Gina M. Raimondo w komunikacie prasowym po sankcjach nałożonych na chińskie firmy AI w 2021 roku.

„Niestety [Chińska Republika Ludowa] decyduje się na wykorzystanie tych technologii do kontrolowania swoich obywateli i represjonowania członków mniejszości etnicznych i religijnych".

Jeśli Chiny osiągną swoje cele, powstanie potencjalnie światowa „tokracja AI" , pogrążająca miliardy ludzi w technokratycznej tyranii.

Według analityków, Chiny wielokrotnie wskazywały, że chcą wykorzystywać sztuczną inteligencję, duże zbiory danych, uczenie maszynowe i inne zaawansowane technologie, aby „dostać się do mózgów i umysłów swoich obywateli". *VOA News* nazywa plan Chin „drakońską dyktaturą cyfrową".

„Wykorzystała najnowocześniejszą technologię, aby wzmocnić swoje państwo partyjne", mówi Hung Ching-fu, profesor nauk politycznych na *National Cheng Kung University* na Tajwanie, o najnowszym przedsięwzięciu KPCh w zakresie sztucznej inteligencji.

„Chiny przeszły z wczesnego rozpoznawania twarzy na programy AI, które próbują dostać się do mózgów i umysłów (bardziej) niż na pierwszy rzut oka. Przyjęcie przez Chiny zaawansowanej sztucznej inteligencji wzmocni całkowitą kontrolę".

Innymi słowy, państwo policyjne napędzane sztuczną inteligencją jest w programie komunistycznych Chin, jak

również każdego innego kraju, który adoptuje lub jest zmuszony do przyjęcia tych metod.

Już teraz kraje, które skłaniają się ku autokracji, a nie demokracji, importują technologię sztucznej inteligencji do rozpoznawania twarzy z Chin. Wydaje się, że rośnie rynek dla tych orwellowskich systemów w krajach, które stają się lub już są napędzane przez totalitaryzm.

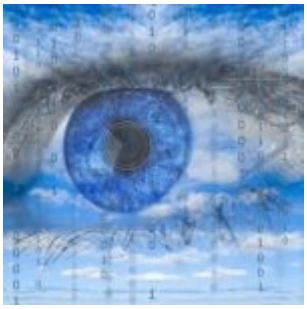
Źródła:

BusinessInsider.com

NaturalNews.com

VOAnews.com

Wielki Brat szpieguje cię na tysiące sposobów, a wszystkie te informacje trafiają do scentralizowanych „systemów fuzyjnych”



Wielki Brat cię obserwuje. Niestety, większość ludzi nie zdaje sobie sprawy, jak rozległa stała się siatka nadzoru. Gdy

jedziesz do pracy lub szkoły, czytniki tablic rejestracyjnych systematycznie śledzą Twoją podróż. W dużych miastach tysiące wysoce zaawansowanych kamer bezpieczeństwa (wiele z nich wyposażonych jest w technologię rozpoznawania twarzy) monitoruje każdy Twój ruch. Jeśli władze wykryją, że robisz coś podejrzanego, mogą szybko przejrzeć Twoją dokumentację karną, finansową i medyczną. Oczywiście, jeśli chcą sięgnąć głębiej, telefon i komputer nieustannie tworzą skarbnicę danych z monitoringu. Nic, co robisz na którymkolwiek z nich, nigdy nie jest prywatne.

W przeszłości zebranie wszystkich tych informacji zajmowało dużo czasu. Ale teraz giganci technologiczni, tacy jak Microsoft, Motorola, Cisco i Palantir, sprzedają „systemy fuzyjne" rządom na całym świecie. Te „systemy fuzyjne" mogą natychmiast integrować dane z monitoringu z tysięcy różnych źródeł, a to całkowicie zmieniło sposób, w jaki egzekwowanie prawa jest prowadzone w wielu największych miastach.

Arthur Holland Michel jest starszym wykładowcą w Carnegie Council for Ethics in International Affairs i odbył wycieczkę po „systemie fuzyjnym" używanym przez miasto Chicago o nazwie Citigraf:

> ***Kliknął „ZBADAJ" i Citigraf zabrał się do pracy nad zgłoszonym napadem.*** *Oprogramowanie działa na czymś, co Genetec nazywa „silnikiem korelacyjnym", czyli zestawem algorytmów, które przeszukują historyczne rejestry policyjne miasta i dane z czujników na żywo w poszukiwaniu wzorców i połączeń. Kilka sekund później na ekranie pojawiła się długa lista potencjalnych klientów, w tym wykaz osób wcześniej aresztowanych w okolicy za brutalne przestępstwa, adresy domowe mieszkających w pobliżu zwolnionych warunkowo, katalog podobnych niedawnych telefonów 911, zdjęcia i numery rejestracyjne pojazdów, które wykryto uciekające z miejsca zbrodni i nagrania wideo z wszelkich kamer, które mogły wykryć dowody samej zbrodni, w tym tych zamontowanych w przejeżdżających autobusach i pociągach. Innymi słowy, więcej*

> *niż wystarczająca ilość informacji, aby funkcjonariusz mógł odpowiedzieć na to pierwotne wezwanie pod numer 911 z niemal telepatycznym wyczuciem tego, co właśnie się wydarzyło.*

Ale te systemy służą nie tylko do tropienia przestępców.

W rzeczywistości można ich użyć do zbadania dosłownie każdego.

Przy innej okazji Arthur Holland Michel miał okazję przetestować „system fuzyjny", który Microsoft zbudował dla Nowego Jorku:

> *Funkcjonariusz NYPD pokazał mi, w jaki sposób może wyciągnąć kartotekę każdego mieszkańca miasta, listy jego znanych współpracowników, przypadki, w których zostali nazwani ofiarą przestępstwa lub świadkami, a jeśli mieli samochód, mapę cieplną gdzie zwykle prowadzili i pełną historię ich naruszeń parkingowych. Potem wręczył mi telefon. Śmiało, powiedział; wyszukaj nazwisko.*
>
> *Przyszła mi do głowy fala ludzi: przyjaciele. Kochankowie. Wrogowie. W końcu wybrałem ofiarę strzelaniny, której byłem świadkiem na Brooklynie kilka lat wcześniej. Pojawił się od razu, wraz z tym, co wydawało się bardziej osobistymi informacjami niż ja, a może nawet ciekawy funkcjonariusz, miałam prawo wiedzieć bez nakazu sądowego. Czując zawroty głowy, oddałem telefon.*

Jeśli tak się dzieje w dużych miastach, takich jak Chicago i Nowy Jork, czy możesz sobie wyobrazić technologię, którą muszą teraz posiadać agencje alfabetu rządu federalnego?

Oczywiście dzieje się to nie tylko w Stanach Zjednoczonych.

Po drugiej stronie Atlantyku wspólny europejski projekt nadzoru znany jako ROXANNE budzi wiele obaw:

> *Akronim **R**eal time netw**O**rk, te**X**t, and speaker **AN**alytics for*

*combating orga**N**ized crim**E** (Analiza sieci, tekstu i mowy w czasie rzeczywistym w celu zwalczania przestępczości zorganizowanej), został ogłoszony w listopadzie w ramach projektu opracowanego obecnie w Szwajcarii.*

Platforma biometryczna rzekomo służąca do monitorowania i rozprawiania się z przestępczością zorganizowaną, dodatkowe zastosowanie ROXANNE, które jego twórcy swobodnie reklamują, jest możliwość monitorowania osób winnych rzekomej mowy nienawiści i politycznego ekstremizmu.

W całej Europie wprowadzane są nowe, surowe przepisy przeciwko „mowie nienawiści" i „ekstremizmowi politycznemu", a to nowe narzędzie pomoże wytropić „myślozbrodniarzy".

W szczególności to nowe narzędzie będzie intensywnie monitorować „serwisy społecznościowe, takie jak Facebook, YouTube, a także zwykłe platformy telekomunikacyjne"…

ROXANNE, produkt finansowany przez UE w ramach programu „Horyzont 2020", mający na celu wspieranie nowej technologii nadzoru, działa na portalach społecznościowych, takich jak Facebook, YouTube, a także na zwykłych platformach telekomunikacyjnych, aby identyfikować, kategoryzować i śledzić twarze i głosy, umożliwiając władzom stworzenie bardziej szczegółowego obrazu badanej sieci, czy to w związku z działalnością przestępczą, czy też uznaną za politycznie skrajną.

Umożliwienie władzom czerpania z surowych danych z różnych źródeł i platform w celu rozpoznania typowych wzorców mowy, rysów twarzy i geolokalizacji, rezultatem końcowym jest zarówno identyfikacja podejrzanych, jak i nakreślenie skomplikowanego obrazu sieci poddawanych pod mikroskop.

Jeśli więc mieszkasz w Europie i uważasz, że w pewnym momencie możesz być winny „myślozbrodni", możesz chcieć pozbyć się

telefonu i komputera.

Poważnie.

Tam naprawdę źle się potoczyło i to tylko kwestia czasu, zanim szaleństwo w Stanach Zjednoczonych osiągnie ten sam poziom, ponieważ idziemy dokładnie tą samą drogą.

W Stanach Zjednoczonych, z każdym dniem coraz więcej głosów politycznych jest „obniżanych". Postępowy reporter Jordan Chariton początkowo wiwatował, gdy konserwatyści byli odrzucani, ale w tym momencie żałuje, że wezwał do cenzury teraz, gdy YouTube usunął jeden z jego filmów:

> *Jednak po tym, jak YouTube usunął wideo z jego własnego kanału, przedstawiające materiał z zamieszek 6 stycznia za naruszenie zasad platformy przeciwko „spamowi i nieuczciwym praktykom", Chariton zmienił swoje stanowisko.*
>
> *„Mając czas na refleksję i widząc atak cenzury Doliny Krzemowej, żałuję tego tweeta" – napisał progresywny dziennikarz. „Niezależnie od tego, czy niektóre kanały telewizji kablowej/YouTube wprowadzają w błąd widzów, przedstawiając nieuczciwe twierdzenia pozbawione prawdziwych dowodów, nie należy ich atakować"*

To wszystko jest zabawne, kiedy dzieje się „po drugiej stronie", ale kiedy ci się to przytrafia, nagle staje się rzeczywistością.

Naprawdę chcą kontrolować to, co wszyscy robimy, mówimy i myślimy, a siatka nadzoru Wielkiego Brata staje się coraz bardziej dusząca z każdym mijającym rokiem.

Jeśli nie ograniczymy tej technologii, póki jeszcze możemy, to tylko kwestia czasu, zanim nasze społeczeństwo stanie się dystopijnym koszmarem o wiele straszniejszym niż cokolwiek, co George Orwell kiedykolwiek odważył się wyobrazić.

Artykuł przetłumaczono z zerohedge.com

Dane 2,4 mln osób z całego świata, w tym Polaków, zgromadziła chińska firma lojalna wobec Komunistycznej Partii Chin

W połowie września 2020 roku wyciekły informacje o tym, że chińska firma Shenzhen Zhenhua Data Technology, powiązana z tajnym oddziałem wojskowym i wywiadowczym Pekinu, zgromadziła gigantyczną bazę danych z plikami dotyczącymi 2,4 mln ludzi z całego świata, w tym dane wpływowych osób i ich rodzin. W ostatnich dniach pojawiły się doniesienia, że ChRL zebrała również dane Polaków.

„Kolekcja" danych z całego globu w komunistycznych rękach

Zhenhua Data Technology, która jest powiązana z Armią Ludowo-Wyzwoleńczą, Ministerstwem Bezpieczeństwa Państwa oraz Komunistyczną Partią Chin (KPCh), zgromadziła bazę skompilowaną głównie z tzw. materiałów open source, takich jak posty w mediach społecznościowych i dane online.

Baza danych okazała się uszkodzona. Australijska firma Internet 2.0, która zajmuje się cyberbezpieczeństwem, odzyskała ponad 10 proc. danych, które były w niej zawarte. Firma ujawniła, że pośród zrekonstruowanych plików znalazły się dane około 52 tys. Amerykanów, 35 tys. Australijczyków, 9 tys. 700 Brytyjczyków i 5 tys. Kanadyjczyków.

W ostatnim tygodniu października „Gazeta Polska" poinformowała w artykule, że otrzymała od Internet 2.0 fragment bazy danych z nazwiskami Polaków. „To spis ponad 3 tys. rekordów zawierających imiona i nazwiska (część się powtarza). Nie wiadomo jednak, z jakiego powodu chiński wywiad wojskowy zlecił Zhenhua zbieranie informacji o tych osobach. Pewne jest jednak, że służba ta ma bardzo dobrą orientację w polskim świecie politycznym. Na liście znajdują się nie tylko byli lub obecni wysocy rangą urzędnicy państwowi, lecz także ich rodziny – małżonkowie, dzieci, rodzice i rodzeństwo" – podaje gazeta.

Internet 2.0 odtworzył zaledwie 10 proc. całej bazy, wydaje się więc, że w tym momencie nie można stwierdzić, czy wśród odzyskanych rekordów znalazły się wszystkie dane Polaków, które zostały zgromadzone w bazie.

Na kogo „poluje" KPCh na całym świecie?

Zgodnie z raportami globalnego konsorcjum medialnego baza danych obejmuje osoby z różnych sektorów – polityki, biznesu, prawa, środowiska akademickiego i obronności – oraz zawiera szczegółowe dane, takie jak daty urodzenia, adresy, stan cywilny i upodobania polityczne.

Znajdują się tam dane dotyczące zarówno zwykłych biznesmenów, jak i wysokiej rangi osobistości, takich jak oficerowie marynarki wojennej Stanów Zjednoczonych, obserwatorzy Chin w Waszyngtonie, osoby ze środowiska naukowego, członkowie brytyjskiej rodziny królewskiej oraz liderzy przedsiębiorczości.

Ta baza danych, nazywana Overseas Key Information Database (OKIDB), pozwala na dostęp do zagranicznych danych politycznych, wojskowych i biznesowych. Zawiera szczegółowe informacje na temat infrastruktury państw, przemieszczania się zasobów wojskowych, a także analizy opinii publicznej.

Mimo że obecnie nie ma dowodów na to, że reżimowe władze wykorzystują oprogramowanie OKIDB, to jak podkreśla „Washington Post", z dokumentów marketingowych i rekrutacyjnych Zhenhua można wnioskować, że jest to „firma patriotyczna", której głównym klientem docelowym jest wojsko.

„The Globe and Mail" po analizie danych dotyczących Kanadyjczyków napisał, że twórcy bazy przypisali osobom z listy „ocenę" w skali od 1 do 3 .

„Wydaje się, że ci, którym przypisano 1, to osoby o bezpośrednim wpływie, takie jak burmistrzowie, posłowie lub wyżsi urzędnicy państwowi, podczas gdy ci, którym przypisano 2, byli często krewnymi osób u władzy […]" – podaje gazeta. Z kolei ci, których oznaczono numerem 3, to najczęściej osoby skazane, przeważnie za przestępstwa gospodarcze – napisał dziennik.

Tajemnicza baza ujrzała światło dzienne

Baza danych została ujawniona przez źródło w Chinach, a informację przekazano profesorowi Christopherowi Baldingowi. To amerykański naukowiec, który do 2018 roku pracował na Uniwersytecie w Pekinie, skąd udało mu się wyjechać ze względów bezpieczeństwa. To dzięki niemu sprawą zajęła się firma Internet 2.0.

14 września Balding opublikował na swojej stronie oświadczenie, w którym napisał, że zajmował się badaniami doniesień dotyczących Huawei. Trwało to do momentu, zanim w jego badaniach nie nastąpił nagły zwrot. Natknął się na „coś, co dla badaczy Chin jest czymś podobnym do odkrycia

Świętego Graala” – otrzymał informację o istnieniu tej potężnej bazy danych.

Przekazał ją konsorcjum mediów w Australii, Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, Włoszech i Niemczech.

Balding uważa, że dane potwierdzają utrzymywane od dawna podejrzenia, dotyczące działalności KPCh w zakresie nadzoru i monitorowania. „To, czego nie można lekceważyć, to rozległość i szczegółowość nadzoru [prowadzonego przez] chińskie państwo oraz jego zasięg na całym świecie” – podkreśla.

Jak zauważa: „Świat jest dopiero na początkowych etapach zrozumienia, ile Chiny inwestują w wywiad i jak wpływają na operacje, korzystając z surowych danych, musimy zrozumieć ich cele”.

We wcześniejszym wpisie naukowiec zwraca uwagę, że KPCh stanowi „bezprecedensowe wyzwanie dla otwartych, kochających wolność państw prawa na całym świecie”. Reżim „buduje opresyjne państwo z nadzorem technologicznym, które daje partii komunistycznej potężne środki do kontroli obywateli w kraju” – wyjaśnia.

„Mamy teraz dowody na to, jak chińskie firmy współpracują z agencjami państwowymi w celu monitorowania osób i instytucji na całym świecie” – ocenia Balding.

Reakcja Zhenhua nie zdziwiła ekspertów

Poproszona przez „The Guardian” o komentarz firma Zhenhua zaprzeczyła istnieniu takiej bazy danych, podając, że wszelkie zebrane informacje są danymi ogólnodostępnymi w internecie. Przedstawicielka firmy stwierdziła, że nie zbierają danych i jest to tylko „integracja danych”. Zaznaczyła, że model biznesowy i partnerzy stanowią tajemnicę handlową firmy.

Zanegowała również doniesienia, że Zhenhua ma jakiekolwiek powiązania z chińskimi władzami lub wojskiem, dodając, że ich klientami są organizacje badawcze i grupy biznesowe.

W rozmowie z anglojęzyczną edycją „The Epoch Times" eksperci przyznali, że nie byli zaskoczeni takim stanowiskiem chińskiej firmy.

Według Michaela Shoebridge'a, dyrektora programu obrony, strategii i bezpieczeństwa narodowego w think tanku Australian Strategic Policy Institute (ASPI), stwierdzenie Zhenhua „nie może być przyjmowane za dobrą monetę", wziąwszy pod uwagę, że tamtejsze prawo zobowiązuje firmy do pomocy chińskim agencjom bezpieczeństwa i wywiadu. Dodaje, że firmy oczywiście muszą publicznie temu zaprzeczać.

W ocenie Caseya Fleminga, dyrektora generalnego firmy BLACKOPS Partners, zajmującej się strategią wywiadowczą i bezpieczeństwa, zgromadzone w bazie informacje są wykorzystywane do wspierania operacji „nieograniczonej wojny hybrydowej" chińskiego reżimu. Obejmuje to szpiegostwo, tajne zagraniczne kampanie wpływów oraz kradzież zagranicznych innowacji i technologii wojskowej.

Termin nieograniczona wojna hybrydowa nawiązuje do powstałej w latach 90. ubiegłego wieku strategii, którą stworzyli i opisali dwaj chińscy pułkownicy sił powietrznych Qiao Liang i Wang Xiangsui w książce „Unrestricted Warfare". Wydała ją Armia Ludowo-Wyzwoleńcza, siły zbrojne KPCh. Autorzy korzystali z oryginalnych dokumentów wojskowych. Strategia ta opowiada się za zastosowaniem serii niekonwencjonalnych taktyk, stworzonych po to, by osiągnąć cele wojny jednak bez angażowania się w rzeczywistą walkę.

Jak zauważa Fleming, ostatecznym celem tej strategii jest „zniszczenie demokracji po to, by chiński komunizm mógł globalnie przejąć nadzór".

Dyrektorem naczelnym Zhenhua jest Wang Xuefeng, były inżynier

IBM. Jak podaje australijski nadawca ABC, wcześniej w chińskich mediach społecznościowych zamieścił wpis o prowadzeniu „wojny hybrydowej" poprzez manipulowanie opinią publiczną i „wojnę psychologiczną".

Zdaniem Nicholasa Eftimiadesa, byłego wysokiego funkcjonariusza sił wywiadowczych USA i autora książki „Chinese Intelligence Operations" (pol. „Chińskie operacje wywiadowcze"), baza danych pomogłaby chińskiemu wywiadowi w namierzeniu tych, którzy nadawaliby się do rekrutacji lub szantażu. Chodzi o osoby ze „słabościami", które można wykorzystać, np. „zapotrzebowanie na pieniądze [lub] sympatie polityczne przeciwne administracji". Reżim mógłby wyszukiwać w mediach społecznościowych posty, które sugerują niezadowolenie z rządu lub trudności finansowe.

W analogiczny sposób działa to w przypadku operacji wywierania wpływu. Wyszukiwani są ludzie publikujący opinie, które popierają politykę reżimu. Kolejnym krokiem jest wspieranie takiej osoby, jej organizacji, a tym samym wzmacnianie jej poglądów.

Michael Shoebridge zwraca uwagę, że w bazie Zhenhua znajdują się także dane dzieci wpływowych ludzi, m.in. polityków i dyrektorów biznesowych. „To dość niepokojący potencjał wykorzystania takich danych" – zaznacza ekspert. Umożliwia bowiem wywieranie nacisku na te osoby, wykorzystując słabości ich potomstwa.

Ponadto część tych dzieci może w dorosłym życiu piastować eksponowane stanowiska. Zatem na skutek analizowania ich profili już od dzieciństwa „możliwość wykorzystywania tych osób i wpływania na nie jest znacznie większa, ponieważ z biegiem czasu zyskujesz o wiele bardziej wszechstronne ich zrozumienie" – wskazuje Shoebridge.

Kropla w morzu… chińskich baz danych

Eksperci zaznaczają, że gromadzenie danych przez chiński reżim

komunistyczny odbywa się na masową skalę, znacznie większą, niż jesteśmy w stanie sobie wyobrazić, a wyciek danych z Zhenhua, to jedynie przysłowiowa kropla w morzu tego, co tam się dzieje.

Shoebridge porównał bazę danych do pojedynczej plastikowej piłeczki w ogromnym basenie. Jak twierdzi, ten zbiór danych byłby łączony z danymi, które zebrały inne chińskie podmioty w celu ich wykorzystania do różnych operacji, mających wesprzeć interesy reżimu.

„To interakcja firm posiadających takie dane z innymi firmami i danymi rządowymi daje władzę" – skomentował ekspert.

Michael Shoebridge tłumaczy, że strategia ta znajduje odzwierciedlenie w doktrynie reżimu o „fuzji cywilno-wojskowej". Dzięki niej władze wykorzystują innowacje prywatnych przedsiębiorstw do napędzania rozwoju wojskowego.

W październiku 2019 roku Australian Strategic Policy Institute opublikował raport „Engineering global consent", napisany przez Samanthę Hoffman. Stwierdzono w nim, że reżim tworzy „masowy i globalny ekosystem gromadzenia danych", wykorzystując możliwości przedsiębiorstw państwowych i prywatnych chińskich firm technologicznych.

Wymienia się w nim Global Tone Communication Technology Co., spółkę zależną chińskiego przedsiębiorstwa państwowego, nadzorowanego przez centralny wydział propagandy KPCh.

W wywiadzie udzielonym pod koniec zeszłego roku polskiej edycji „The Epoch Times" gen. Robert Spalding powiedział, że Global ToneCommunication, to firma prowadząca usługi tłumaczeniowe, która „w rzeczywistości przy użyciu sztucznej inteligencji gromadzi wielki zbiór danych". Jak dodał: „Czasami ma tę funkcję wbudowaną na podobnych zasadach co produkty Huawei, jako most telekomunikacyjny, lub może bazować na oprogramowaniu opartym na tzw. chmurze".

Poza gromadzeniem ogromnych baz danych z całego świata w ponad 65 językach, które przetwarza na użytek Pekinu do celów wywiadowczych, bezpieczeństwa i propagandy, firma koncentruje się na technologiach sztucznej inteligencji, takich jak rozpoznawanie twarzy.

W opinii Nicholasa Eftimiadesa chińskich firm zaangażowanych w gromadzenie dużych ilości danych na potrzeby reżimu są prawdopodobnie dziesiątki, jeśli nie setki. Nie wliczając w to działań prowadzonych przez chińskie agencje bezpieczeństwa, które za pośrednictwem zaawansowanego technologicznie aparatu nadzoru tego kraju zbierają dane na temat wszystkich obywateli, a więc 1,4 mld ludzi.

Eftimiades twierdzi, że dane dziesiątek milionów Amerykanów zostały wykradzione przez chińskich hakerów. Zostały one wprowadzone do baz w Chinach i służą do doskonalenia narzędzi sztucznej inteligencji. Wśród ataków wyliczyć można włamanie do amerykańskiego Urzędu Zarządzania Personelem (ang. Office of Personnel Management, OPM) w 2014 roku, federalnej agencji ds. personelu, naruszenie obowiązku sprawozdawczego firmy Equifax w 2017 roku, a także cyberatak na ubezpieczyciela zdrowotnego Anthem w 2016 roku.

W lutym 2016 roku anglojęzyczna edycja „The Epoch Times", powołując się na poufne źródło w Chinach, poinformowała, że chińskie agencje bezpieczeństwa stworzyły bazę danych wykorzystywaną do przetwarzania skradzionych danych Amerykanów. Zawiera ona także poufne dane osobowe, wyszczególnione w poświadczeniach bezpieczeństwa 21 mln obecnych i byłych pracowników federalnych, pochodzące z włamania do Urzędu Zarządzania Personelem (OPM) oraz osobiste dane prawie 80 mln obecnych i byłych klientów i pracowników Anthem.

Ta baza danych funkcjonuje na potężnym oprogramowaniu zdolnym do przyjmowania ogromnych ilości danych. Zgromadzone zasoby analizuje się pod kątem relacji między różnymi osobami

i zdarzeniami.

Wyciek danych z Zhenhua Data Technology jest dla wszystkich, niezależnie od statusu społecznego, okazją do zastanowienia się nad zamieszczanymi treściami w mediach społecznościowych. Jak widać, mogą one nieoczekiwanie stać się pożywką dla podmiotów gromadzących dane. Mogą zostać wykorzystane przeciwko nam, zwłaszcza jeśli trafią do państwa totalitarnego, jakim są Chiny.

Źródła:

Military-Linked Chinese Company Collected Personal Data On Thousands of Canadians

How Chinese Data Trove on 2 Million People Serves Beijing's Unrestricted Warfare

„Gazeta Polska"

The Washington Post

The Globe and Mail

The Guardian

Kalifornia zakazuje stosowania technologii rozpoznawania twarzy w nagraniach z kamer

policjantów

Kalifornia może mieć wiele wątpliwych praw, ale jest takie, które zasługuje na aplauz. Zabrania stosowania technologii rozpoznawania twarzy w nagraniach wykonanych przez kamery funkcjonariuszy policji.

Rozpoznawanie twarzy to technologia, która polega na dopasowywaniu w czasie rzeczywistym obrazu osoby do jej poprzedniego zdjęcia. Opiera się na fakcie, że twarz każdej osoby ma około 80 unikalnych punktów węzłowych w obszarach nosa, ust, policzków i oczu, które można wykorzystać do odróżnienia ludzi od siebie.

Cyfrowa kamera wideo służy do pomiaru odległości między tymi punktami na twarzy osoby. Obejmuje między innymi pomiary głębokości oczodołów, odległości między oczami, kształtem linii żuchwy i szerokości nosa. Informacje te służą do tworzenia unikalnego kodu numerycznego, który można dopasować do kodu pobranego z poprzedniego zdjęcia.

W marcu Waszyngton stał się pierwszym stanem w kraju, który zalegalizował używanie rozpoznawania twarzy przez organy ścigania i inne agencje stanowe. Oprogramowanie było już używane na poziomie hrabstwa i miasta przed wprowadzeniem tam nowego prawa. Jednak rozpoznawanie twarzy może być używane tylko w niektórych przypadkach, takich jak poszukiwanie zaginionych osób lub identyfikacja zwłok. Agencje będą zobowiązane do złożenia zawiadomienia o zamiarze użycia systemu zanim go użyją, a także raportu dotyczącego odpowiedzialności.

Jeśli chodzi o ruch Waszyngtonu, American Civil Liberties Union stwierdziła, że □□zamiast zabezpieczyć wykorzystanie rozpoznawania twarzy, grozi legitymizacją jego rozszerzenia. Kierownik projektu ACLU Jennifer Lee powiedziała, że □□prawo zawiera język, który pozwala agencjom na używanie rozpoznawania twarzy do odmawiania ludziom podstawowych potrzeb i innych niezbędnych rzeczy, takich jak mieszkanie, jedzenie, woda i opieka zdrowotna.

Zwolennicy prywatności chwalą ustawę CA.

Zwolennicy prywatności wyrazili ulgę, że ustawa kalifornijska została podpisana przez gubernatora Gavina Newsoma. Dotyczy to nie tylko rozpoznawania twarzy, ale także ogólnie nadzoru biometrycznego, takiego jak analiza chodu z wykorzystaniem materiału filmowego, który można zebrać z materiału wideo z kamery policyjnej.

W projekcie ustawy stwierdza się: „Korzystanie z rozpoznawania twarzy i innego nadzoru biometrycznego jest funkcjonalnym odpowiednikiem wymagania od każdej osoby, aby zawsze okazywała dowód tożsamości ze zdjęciem, co stanowi naruszenie uznanych praw konstytucyjnych. Ta technologia umożliwia również śledzenie osób bez pozwolenia".

Posunięcie to nastąpiło niedługo po tym, jak ACLU przeprowadziło badanie rozpoznawania twarzy, które wykazało, że program Amazon błędnie zidentyfikował ponad dwa tuziny kalifornijskich prawodawców jako przestępców.

Podobny zakaz został wprowadzony kilka miesięcy wcześniej przez San Francisco w związku z wykorzystywaniem przez rząd funkcji rozpoznawania twarzy do nadzoru, kilka innych amerykańskich miast zrobiło to samo.

Chiny mają przeciwny pogląd na technologię rozpoznawania twarzy, w pełni ją wykorzystując do śledzenia swoich obywateli. Służy również do tworzenia wyników społecznych, które dają tym, którzy są posłuszni KPCh, pewne korzyści w ich

codziennym życiu i ograniczają ruch i wolności tych, których wyniki są niższe.

Niestety nowe prawo Kalifornii dotyczy tylko korzystania z tej technologii przez organy ścigania, a nie sektor prywatny. Niemniej jednak jest to krok we właściwym kierunku, o wiele więcej, niż możemy powiedzieć o wielu innych prawach pochodzących z Kalifornii .

Źródła:

DailyMail.co.uk

Mashable.com

NaturalNews.com

Armia USA rozpoczyna testy latających balonów obserwacyjnych w całym kraju, aby śledzić ruchy ludzi

Wojsko USA testowało balony, które mogą szpiegować ludzi i śledzić ich ruchy. Zgodnie z dokumentami złożonymi w FCC balony mogą unosić się na wysokości 65 000 stóp. W zeszłym roku zostały przetestowane w stanach takich jak Iowa,

Missouri, Illinois, Wisconsin, Minnesota i Południowa Dakota.

Testy zostały przeprowadzone przez US Southern Command, czyli Southcom, które jest częścią Departamentu Obrony i odpowiada za operacje wywiadowcze, współpracę w zakresie bezpieczeństwa i reagowanie na katastrofy w Ameryce Środkowej i Południowej. Jest to wspólny wysiłek US Air Force, US Navy, US Army i innych sił, których głównym zadaniem jest znalezienie i przechwycenie transportów narkotyków, które są przeznaczone dla USA. Według the Guardian, aż 25 bezzałogowych zasilanych energią słoneczną balonów rozpoczęto lot od obszarów wiejskich w Dakocie Południowej i pokonaó 250 mil przez sąsiednie stany.

Zgodnie z dokumentami FCC, balony mają na celu zapewnienie stałego nadzoru, który może wykryć i powstrzymać handel narkotykami oraz zagrożenia dla bezpieczeństwa wewnętrznego. Balony są wyposażone w czułą technologię radarową, która może śledzić pojazdy przy każdej pogodzie, w dzień i w nocy. Tylko jedno z urządzeń radarowych w tych balonach może uchwycić ruch wszystkich samochodów podróżujących w promieniu 25 mil.

Oznacza to, że wojsko może śledzić ruch pojazdów a co za tym idzie także ruch ludzi. Technologię tę porównuje się do „walki TiVo", ponieważ kiedy coś się wydarzy na obserwowanym obszarze, kontrolujący go mogą cofnąć się w czasie i zobaczyć, co się stało, kto był zaangażowany w incydent i jaka była przyczyna.

Sieć MESH jest również wykorzystywana, aby umożliwić balonom komunikację między sobą oraz z ludźmi na ziemi. Raport wskazuje również, że balony mogą być w stanie nagrywać lub transmitować wideo.

Balony budzą wiele obaw dotyczących prywatności

Oczywiście ten rodzaj nadzoru jest niezwykle niepokojący dla obrońców praw obywatelskich. Starszy analityk American Civil Liberties Union, Jay Stanley, powiedział w the*Guardian* :

„Nawet podczas testów wciąż zbierają wiele danych na temat Amerykanów [jadących] do domu związkowego, kościoła, meczetu, kliniki… Nie powinniśmy iść w kierunku dopuszczenia tego do użytku w Stanach Zjednoczonych, niepokojące jest też to, że testy te są przeprowadzane przez wojsko”.

Southcom już używa lekkich samolotów wyposażonych w czujniki do przelotów nad częściami Panamy, Kolumbii, Meksyku i Morza Karaibskiego. Jednak samoloty te mogą latać tylko przez kilka godzin i wymagają kosztownych załóg. Nowe balony są tańszą opcją, mogą podążać za wieloma łodziami i samochodami przez dłuższy czas i łatwiej im zawisnąć na jakiś czas nad określonym obszarem.

Wojsko nie jest jedyną grupą testującą tego typu nadzór; Prywatne firmy, takie jak World View, również pracują nad podobnymi balonami. Stratollites to systemy nadzoru zamontowane w balonach, którymi można zdalnie sterować i regulować. Balon World View wykonał w zeszłym roku 16-dniową misję w zachodnich Stanach Zjednoczonych – o czym wielu na ziemi nie wiedziało.

World View twierdzi, że jego Stratollites mogą być wykorzystywane do zastosowań, takich jak pomoc w nadzorze żołnierzy, prognozowanie pogody, komunikacja i 'pierwszej odpowiedzi’, a także mogą być używane przez organy ścigania.

Chociaż nikt nie chce widzieć narkotyków przedostających się do kraju, wielu Amerykanów czuje się niekomfortowo, na myśl o byciu śledzonym, rejestrowaniu i potencjalnym przechowywaniu każdego ich ruchu, dostęp do tych danych jest narażony na ataki hakerów. Większość ludzi nawet nie zdaje sobie sprawy ze wszystkich sposobów, na jakie każdego dnia tracimy coraz więcej naszej prywatności dzięki nowoczesnej technologii, która ma poprawiać jakość naszego życia.

Źródła:

DailyMail.co.uk

TheGuardian.com