Polscy hakerzy związani z Anonymous zapowiadają publikację kilkuset polskich firm powiązanych z Rosją

Grupa Squad303 (nazwa odnosi się do historycznego Dywizjonu 303 biorącego udział w Bitwie o Anglię), która należy do znanej siatki Anonymous, zapowiedziała publikację listy nawet kilkuset polskich firm powiązanych z Rosją.

Polscy hakerzy już od początku wojny są zaangażowani w ujawnianie prawdy na temat prawdziwych działań Federacji Rosyjskiej na Ukrainie.

> *– Od maja pracujemy nad kolejnym projektem, którego celem jest ujawnienie WSZYSTKICH firm powiązanych z Rosjanami w Europie. W tej chwili mamy bazę imion, nazwisk, adresów, odpowiedników PESEL i NIP, nazw firm i rodzaju powiazań z nimi obywateli Rosji (udziałowiec/akcjonariusz/członek organu) w UK, Danii, Polsce i kilku innych krajach w Europie. Krok po kroku, kraj po kraju będziemy ujawniali posiadane dane – możemy przeczytać w mailu wysłanym przez hakerów do redakcji „Głosu Wielkopolskiego".*

> *– To bardzo pracochłonne zajęcie, więc projekt będzie trwał jeszcze kilka miesięcy, ale dane z Polski postaramy się ujawnić już w sierpniu. Dlaczego o tym pisze? Bo w tych bazach jest bardzo wiele nazwisk (np. w UK 14 660 rekordów),*

> *a my nie mamy zasobów, żeby zbudować pełen obraz powiazań personalno-biznesowych. To już rola opinii publicznej, a w szczególności mediów – wyjaśniają przedstawiciele grupy, którzy zapowiadają publikację listy firm działających w Polsce w ciągu najbliższych 2-3 tygodni, czyli w drugiej połowie sierpnia.*

Niestety pomimo wielu pakietów sankcji ze strony Unii Europejskiej rosyjscy oligarchowie potrafili skutecznie ochronić się przed nieprzyjemnymi konsekwencjami. Najlepszy przykład stanowi jeden z najbogatszych Rosjan i dobry znajomy Władimira Putina, czyli Aleksiej Mordaszow, którego majątek na ten moment wycenia się na 29 mld dol. Ten biznesmen już kilka lat temu trafił na amerykańską „listę Putina", a w warunkach wojny, kiedy Federacja Rosyjska napadła na Ukrainę, musiał szybko działać, by chronić swoje aktywa.

Miliarder co prawda stracił luksusowy jacht oraz rezydencję we Włoszech, jednak tego samego nie można powiedzieć o jego firmach. W tym miejscu, jak wskazują media, ważne okazały się nie tylko kontakty w Moskwie, ale i w Berlinie. Parę miesięcy temu agencja Reutera informowała o tym, jak Mordaszow zdołał uniknąć zamrożenia ponad miliarda funtów w akcjach niemieckiego koncernu turystycznego TUI AG, odsprzedając niemal wszystkie swoje udziały spółce Ondero Limited z Brytyjskich Wysp Dziewiczych – tę kontroluje jego żona Marina Mordaszowa.

Chociaż Ministerstwo Gospodarki Niemiec uruchomiło w tej sprawie śledztwo, to trudno spodziewać się szybkich działań i wielkich sankcji, a zwłaszcza że jeszcze na początku 2021 z powodu koronawirusa niemiecki rząd wsparł firmę TUI AG kwotą 1,25 miliarda euro. To nie jedyny taki manewr w wykonaniu Aleksieja Mordaszowa. Serwis Bloomberg na początku marca donosił, że oligarcha przekazał też swojej żonie kontrolę nad pakietem akcji brytyjskiej spółki górniczej Nordgold o wartości ok. 1,1 mld dol.

W naszym kraju TUI Group prowadzi działalność jako spółka TUI Poland. Według statystyk jest to największe biuro turystyczne, które przed wybuchem pandemii zajmowało 40 procent rynku. Firma nie została objęta sankcjami przez polskie władze właśnie ze względu na zmiany prawne, których dokonał Mordaszow. Niemniej jednak głównym akcjonariuszem spółki wciąż pozostaje rosyjski oligarcha. Poza tym można zadać pytanie, czy prywatne dane Polaków mogą być bezpieczne w teoretycznie niemieckim, a w praktyce rosyjskim koncernie.

Być może hakerzy z Anonymous ujawnią więcej tego typu powiązań w wykonaniu rosyjskich oligarchów, którzy robią wszystko, aby ukryć swoje wpływy w firmach działających w Europie.

Źródło

TVP Info: obiektywnie już było

Niedawna wizyta Nancy Pelosi na Tajwanie postawiła świat na progu wojny światowej. Było do niej już tak blisko, że część poważnych mediów światowych relacjonowała lot, lądowanie i wizytę przewodniczącej Izby Reprezentantów w czasie rzeczywistym minuta po minucie, spodziewając się rozpoczęcia poważnego konfliktu. Na szczęście wystrzały nie padły, przynajmniej jak na razie, świat odetchnął. Przynajmniej na

razie. Opisuję to tak drobiazgowo, by przypomnieć, jak ważne to było wydarzenie i jak wiele osób oczekiwało od mediów tego, co jest ich psim obowiązkiem: relacjonowania przebiegu wydarzeń.

TVP Info z właściwym jej opóźnieniem opowiedziało dzisiaj o wizycie Pelosi i napięciu wokół niej, ale nie po to, by dokonać analizy tej całej sytuacji, nie. Portal rządowej telewizji skarcił inne media, że śmiały dostarczyć odbiorcom inne fakty niż tylko te, które TVP Info uważa za jedynie słuszne. Opisując całą sytuację TVP Info konkluduje: „Spór między Waszyngtonem i Pekinem od kilku dni jest jednym z najważniejszych tematów w mediach na całym świecie". Po czym na jednym oddechu dodaje: „Zaskakujący może się wydawać zatem fakt, że portal Onet w piątek zdecydował się opublikować opinię ambasadora Chin w Polsce. W tekście pt. „Dlaczego Pelosi nie powinna była jechać na Tajwan" Sun Linjiang przekonuje, że „chińska strona nie może siedzieć bezczynnie", a wizyta amerykańskiej polityk na Tajwanie to „bezczelna ingerencja w wewnętrzne sprawy Chin".
Onet zrobił więc to, do czego jest powołany: przedstawił opinię również drugiej strony, bo zdanie strony amerykańskiej zaprezentował wcześniej w oddzielnym tekście. Dla propagandystów telewizji rządowej to jest „zaskakujące". Zaś podobną aktywność dziennika „Rzeczpospolita", kwituje: „Co ciekawe, list chińskiego ambasadora w tym tygodniu publikowała także „Rzeczpospolita".

Mam swoje oceny portalu Onet i nie są to oceny pochlebne, zapewniam. Lubię i szanuję „Rzeczpospolitą", choć często się z nią nie zgadzam. W tym jednak wypadku zrobiły to, co należało i czego od mediów oczekują ich odbiorcy: przedstawienia konkretnej sytuacji z obu stron. Dla TVP Info to wystarczyło, by wyrazić swoje fałszywe zdziwienie w tonie teorii spiskowych. Jeżeli dla TVP Info normalna robota zgodnie z podstawami dziennikarstwa (a zasada audiatur et altera pars – należy wysłuchać drugiej strony – jest jedną z

fundamentalnych) jest powodem do cierpkiego zdziwienia, to świadczy o całkowitym upadku zasad zawodu.

Problem polega na tym, że TVP Info nie jest wyjątkiem. Relacjonowanie tylko jednej strony i jej narracji jest obecnie normą. Co czyni z pracowników mediów nie dziennikarzy, a pracowników propagandowego frontu. I w porządku, tylko po co robić to wszystko ozdabiając swoje agitki zapewnieniami, że walczycie o wolność słowa?

Źródło

Wygenerowani przez sztuczną inteligencję „ludzie” rozpowszechniają antyzachodnie i pro-KPCh opinie w mediach społecznościowych

Ogromna prochińska sieć „spamuflażu” wykorzystywana jest w mediach społecznościowych do zniekształcania międzynarodowego postrzegania ważnych kwestii, takich jak

amerykańskie prawo dotyczące broni, COVID-19 oraz dyskryminacja rasowa, o czym w najnowszym raporcie poinformowało Centre for Information Resilience (CIR).

Przedstawiona w raporcie taktyka polega na wykorzystywaniu rozległej sieci wygenerowanych komputerowo „ludzi" do promowania narracji Komunistycznej Partii Chin (KPCh) i dyskredytowania Zachodu, zwłaszcza Stanów Zjednoczonych. Boty i fałszywe profile użytkowników są używane na Twitterze, Facebooku, Instagramie i YouTubie, jak wynika z opublikowanego 5 sierpnia (PDF) raportu CIR. Centre for Information Resilience to niezależna organizacja non profit, której celem jest przeciwdziałanie dezinformacji.

W raporcie stwierdzono ponadto, że użytkownicy, którzy zamierzają prowadzić otwartą, uczciwą dyskusję lub szukają rzetelnych opinii na platformach społecznościowych, nie będą deliberować, gdy natrafią na wypowiedzi botów.

Boty są prawie nie do odróżnienia od prawdziwych ludzi. Choć sprawiają wrażenie, jakby były ludźmi, to są po prostu generowane przez najnowocześniejszą sztuczną inteligencję (SI). W raporcie zauważono również, że niektóre konta użytkowników należały wcześniej do prawdziwych ludzi i nie zostały stworzone na potrzeby sieci, ale zostały przejęte przez boty w celu przeprowadzania kampanii propagandowych KPCh w internecie.

CIR znalazło ponad 350 fałszywych kont, które posługują się pełnymi negatywnego nastawienia memami lub długimi blokami tekstowymi. Ich celem jest zarówno wzmocnienie spekulacji na temat amerykańskiego podejścia do kwestii COVID-19, jak i wywołanie u internautów wzburzenia w związku z dyskryminacją oraz przemocą z użyciem broni w Stanach Zjednoczonych. Posty te są w języku angielskim i chińskim.

Niektóre konta rozpowszechniają treści wizualne, takie jak kreskówki i filmy wideo, aby osiągnąć pewne cele: zasiać

wątpliwości odnośnie do twierdzeń rządu Stanów Zjednoczonych na temat wirusa KPCh, powszechnie znanego jako nowy koronawirus, który pochodzi z laboratorium w Wuhan, lub aby odpierać zarzuty dotyczące łamania praw człowieka w chińskim regionie Xinjiang oraz szerzyć dezinformację na temat przebywającego na emigracji chińskiego miliardera Guo Wengui i wirusolog z Hongkongu Li-Meng Yan.

Posty stworzone przez boty są echem osób publicznych z Pekinu, w tym redaktora naczelnego tuby medialnej KPCh – „Global Times" oraz rzeczników Departamentu Informacji Ministerstwa Spraw Zagranicznych Chińskiej Republiki Ludowej.

„Nasze badania pokazują dowody na celowy wysiłek w kierunku zniekształcenia międzynarodowego postrzegania istotnych kwestii – w tym przypadku, na korzyść Chin" – powiedział Benjamin Strick, autor raportu.

CIR prowadziło swoje badania, szukając wzorców w niektórych hashtagach używanych na portalach społecznościowych. Znaleźli skupiska kont konsekwentnie podbijających treści i hashtagi z głównego konta. CIR napisało, że wskaźnik komentarzy, retweetów i polubień jest „bardzo nieprawdziwy". Poprzez namierzenie centralnego posta, badacze mogą zidentyfikować więcej komentarzy.

Owa grupa badaczy stwierdziła, że nie ma konkretnych dowodów na sponsorowanie sieci przez chiński reżim. Niemniej działania mające na celu wywieranie takiego wpływu mają podobny znak rozpoznawczy znaleziony na kontach użytkowników, które zostały wcześniej zamknięte przez platformy mediów społecznościowych.

„Wzywamy platformy wymienione w tym raporcie do zbadania tejże sieci, formalnego przypisania autorów i jej zlikwidowania. Ważne jest, aby osoby odpowiedzialne za jej istnienie zostały zdemaskowane" – powiedział Ross Burley, współzałożyciel i dyrektor wykonawczy CIR.

Firmy z branży mediów społecznościowych

wielokrotnie podejmowały działania mające na celu usunięcie podobnych sieci.

Twitter usunął ponad 170 tys. kont w czerwcu 2020 roku po tym, jak Graphika, firma zajmująca się analizą społeczną, zidentyfikowała propekińską sieć propagandową nazwaną „Spamouflage Dragon”. Ta sieć fałszywych kont aktywnie rozpowszechnia posty, które chwalą komunistyczny reżim Chin, atakują ruch prodemokratyczny w Hongkongu oraz Stany Zjednoczone.

Źródło: TheEpochTimes.com

Wielka Brytania wdraża wojskowy oddział INFOWAR do walki z przeciwnikami szczepionek na COVID

Rząd brytyjski zmobilizował elitarną jednostkę ds. „Wojny informacyjnej”, aby zwalczać „bojowników antyszczepionkowych” i przerywać ich „propagandowe treści” w Internecie, według raportu The Sunday Times.

Raport (za zaporą) mówi, że jednostka jest zwykle używana do pomocy w operacjach przeciwko Al-Kaidzie i Talibom, ale teraz

zostanie skierowana do tych, którzy odważą się kwestionować świętość szczepień przeciwko COVID.

> *The army has mobilised an elite "information warfare" unit renowned for assisting operations against al-Qaeda and the Taliban to counter online propaganda against vaccines, as Britain prepares to deliver its first injections within days. https://t.co/7JY2gl0oMj*
>
> *— The Times and The Sunday Times (@thetimes) November 29, 2020*

W raporcie odnotowano ponadto, że jednostka znana jako „Obronna jednostka specjalistyczna ds. Kultury" powstała w Afganistanie w 2010 r. i jest częścią 77. Brygady armii.

„Sekretna jednostka często pracowała ramię w ramię z psychologicznymi zespołami operacyjnymi" – dodaje raport.

Fajnie… Rząd zatrudniający wojsko do używania psyopsów w społeczeństwie, aby nikt nie odstępował od akceptowalnej opinii na temat szczepionki.

https://www.bitchute.com/video/aQy7BsMzBQnI/

The Times twierdzi, że ruch został ujawniony przez dokumenty, które „wyciekły".

> *„Żołnierze już monitorują cyberprzestrzeń pod kątem zawartości Covid-19 i analizują, w jaki sposób obywatele Wielkiej Brytanii są atakowani w Internecie", twierdzi.*

Oczywiście rząd twierdzi, że w grę wchodzą Rosjanie… sposób na zmylenie ludzi i zaakceptowanie egzekwowania przez szpiegów grupowego myślenia.

> *„Gromadzi również dowody dezinformacji o szczepionkach z wrogich państw, w tym Rosji" – czytamy w raporcie.*

Dokładnie to, co stanowi „dezinformację" dotyczącą szczepionek, będzie zależało od rządu i prawdopodobnie każdy, kto wskaże potencjalne skutki uboczne szczepień lub kwestionuje ideę nakazania szczepienia stanie się celem, czy to dosłownie przez prawo, czy też przez uniemożliwienie uczestniczenia w życiu społecznym.

Po tym, jak „wyciek" wyszedł na jaw, brytyjskie Ministerstwo Obrony stwierdziło, że jednostka „nie jest skierowana do ludności Wielkiej Brytanii", a jedynie do „wrogich zagranicznych aktorów".

Dobra.

Podobnie jak jednostka strachów GCHQ w Downing Street 10 również nie jest skierowana do opinii publicznej.

Dwa tygodnie temu The London Telegraph (Paywall) ujawnił, że szpiedzy z najbardziej tajnej brytyjskiej organizacji wywiadowczej i bezpieczeństwa osadzili „komórkę" w sercu rządu, aby dostarczać premierowi Borisowi Johnsonowi w czasie rzeczywistym informacji dotyczących ruchów społeczeństwa.

> *Words we didn't expect to read in 2020:*
>
> *"GCHQ analysts have been given access to mobile phone data to track the public's movements during the national lockdown. The up-to-the-minute reports on compliance are passed to the Prime Minister"https://t.co/SKqk5uRw0z*
>
> *— Big Brother Watch (@BigBrotherWatch) November 19, 2020*

Daily Mail donosi również o rozwoju sytuacji, w której odnotowano, że GCHQ, którego zwykle zadaniem jest szpiegowanie terrorystów i obcych mocarstw, zostało skierowane do brytyjskiej opinii publicznej, aby ocenić, czy ludzie przestrzegają COVIDowych 'zasad', czy też nie, oraz zwalczać materiały anty-szczepionkowe.

Przemawiając anonimowo do London Times w listopadzie, źródło zauważyło, że „GCHQ otrzymało nakaz o usunięciu materiałów anty-szczepionkowych online i w mediach społecznościowych. Mają swoje sposoby, do monitorowania i zakłócania propagandy terrorystycznej”.

W raporcie zauważono, że agencja szpiegowska rozważała usunięcie stron internetowych i treści, które nie sprzyjają szczepieniom, a także „przeszkadzanie” osobom tworzącym te treści, „używając zestawu narzędzi opracowanych w celu zwalczania dezinformacji i materiałów rekrutacyjnych rozpowszechnianych przez Państwo Islamskie”.

Chiński uczony przechwala się, że pandemia przyspieszyła realizację planów Pekinu, by prześcignąć Stany Zjednoczone

Niedawno chiński uczony, naśmiewając się, że wirus KPCh zabił około 220 000 Amerykanów w porównaniu z oficjalną niewielką liczbą ofiar śmiertelnych w Chinach, przechwalał się tym, jak Pekin poradził sobie z pandemią.

Li Yi, który jest także rezydentem USA, stwierdził również, że zniszczenie gospodarki spowodowane ogólnoświatową pandemią oznacza, iż realizacja planu Chin prześcignięcia Stanów Zjednoczonych przyspieszyła.

„Ten COVID-19 jest najbardziej niekorzystny dla Europy i Ameryki" – powiedział Li, socjolog, podczas przemówienia na forum w Shenzhen w południowych Chinach 16 października br.

„Przyniósł on najwięcej korzyści Korei Północnej i Chinom".

Wskazał na oficjalną liczbę ofiar śmiertelnych podaną przez reżim, wynoszącą ok. 4000 – prawdopodobnie znacznie niższą od rzeczywistej, biorąc pod uwagę systematyczne i konsekwentne zatajanie oraz zaniżanie liczby zgłaszanych przez reżim wybuchów epidemii w Chinach.

„Ale w porównaniu z 220 000 zgonów w Stanach Zjednoczonych 4000 oznacza brak zgonów, prawda?" – powiedział, śmiejąc się.

Li zaczął wychwalać ożywienie gospodarcze w Chinach w czasie pandemii.

„Przybliżył się dzień, w którym Chiny prześcigną Stany Zjednoczone" – powiedział, dodając, że „do 2027 roku nie będzie problemu".

„Ameryka nie może przetrwać" – stwierdził Li.

Dodał, że Chińczycy nie zdają sobie sprawy z tego, że „to nie Stany Zjednoczone rozprawiają się z Chinami. W rzeczywistości to my wypieramy Amerykę".

Przemówienie Li wygłoszone w zeszłym miesiącu przyciągnęło uwagę opinii publicznej dopiero 23 listopada, kiedy to chińskie media zaczęły promować to nagranie wideo na Weibo, chińskiej platformie mediów społecznościowych.

Li, według informacji zawartych na jego profilu na LinkedIn, jest pracownikiem naukowo-badawczym z dziedziny socjologii

w chińskim uniwersytecie Renmin University of China, wcześniej studiował w Stanach Zjednoczonych, gdzie otrzymał tytuł magistra na Uniwersytecie Missouri i tytuł doktora na Uniwersytecie Illinois w Chicago.

Opublikował kilka książek, w tym dwie napisał w języku angielskim na temat chińskiego społeczeństwa.

To nie pierwszy raz, kiedy Li uwłacza Stanom Zjednoczonym. Naukowiec znany jest z promowania socjalistycznych ideologii reżimu i siłowego zjednoczenia Tajwanu z kontynentem. Regularnie wychwala także wysiłki Wydziału Pracy Zjednoczonego Frontu (ang. United Front Work Department, UFWD), agencji Komunistycznej Partii Chin. UFWD nadzoruje prowadzone przez reżim operacje wywierania wpływu za granicą, których celem jest subwersja społeczeństw na korzyść Pekinu.

W październiku ubiegłego roku w chińskim państwowym serwisie informacyjnym Kunlun Ce ukazał się wywiad Li z nowojorską radiostacją ICN Chinese American Voice, we Flushing, podczas którego powiedział, że chiński reżim, emitując antyamerykańskie programy wojenne w całym kraju, z powodzeniem stworzył antyamerykańską atmosferę w czasie wojny handlowej między USA a Chinami.

„Wróciłem do Chin i byłem świadkiem: ciężka choroba, która toczyła Chińczyków przez ostatnie 40 lat [nastawienie proamerykańskie], została wyleczona w ciągu pięciu dni [przez oglądanie filmów i czytanie materiałów propagandowych]" – powiedział Li.

W kwietniu 2019 roku Li został deportowany z Tajwanu za planowanie przemówienia promującego zjednoczenie wyspy z Chinami, czym naruszył warunki pobytu dla turystów. Li został zaproszony przez organizację UFWD z Tajwanu, aby porozmawiać o planach zjednoczenia Pekinu z Tajwanem w ramach modelu „jeden kraj, dwa systemy", podobnie jak w Hongkongu i Makau.

Tajwańska agencja imigracyjna oświadczyła wtedy, że Li został zaklasyfikowany „jako persona non grata i w przyszłości nie może odwiedzać Tajwanu”.

Źródło:

theepochtimes.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