Bezpieczeństwo 5G pod znakiem zapytania: FCC podejmuje działania mające na celu ograniczenie ocen środowiskowych pomimo obaw dotyczących zdrowia

- Federalna Komisja Łączności (FCC) planuje zwolnić określone wieże komórkowe i instalacje 5G z ocen środowiskowych i konserwatorskich.
- Krytycy twierdzą, że posunięcie to osłabia ochronę zapewnianą przez ustawę National Environmental Policy Act (NEPA).
- Niezależni eksperci łączą promieniowanie 5G z uszkodzeniami mózgu, demencją i zwiększonym ryzykiem zachorowania na raka.
- Technolodzy i zwolennicy ochrony zdrowia wzywają do wprowadzenia bardziej rygorystycznych przepisów dotyczących promieniowania RF i moratorium na wdrażanie 5G.
- Przed wydaniem ostatecznej decyzji w październiku 2025 r. zaprasza się do zgłaszania uwag publicznych.

Federalna Komisja Łączności (FCC) podejmuje działania mające

na celu „usprawnienie” procesu oceny środowiskowej niektórych projektów bezprzewodowych, aby „promować wydajność i pewność” dla deweloperów telekomunikacyjnych. Proponowane przepisy zwalniałyby określone rodzaje instalacji, w tym małe anteny komórkowe, wieże komórkowe poniżej 200 stóp i wiejskie instalacje 5G, z przeglądów przeprowadzanych na mocy ustawy o polityce środowiskowej (NEPA) i ustawy o ochronie zabytków (NHPA). Dzieje się to w czasie, gdy niezależni eksperci ostrzegają przed potencjalnymi zagrożeniami dla zdrowia wynikającymi z promieniowania 5G, w tym zwiększonym ryzykiem raka mózgu, demencji i choroby Alzheimera.

Posunięcie FCC: usprawnienie czy zniesienie zabezpieczeń?

Krytycy, tacy jak Miriam Eckenfels z programu Children’s Health Defense’s Electromagnetic Radiation (EMR) & Wireless Program, twierdzą, że nowe przepisy FCC mają więcej wspólnego z przejęciem kontroli przez przemysł niż z ochroną konsumentów. „NEPA jest jednym z niewielu zabezpieczeń przed niekontrolowaną ekspansją przemysłu” – powiedziała Eckenfels. „FCC traktuje NEPA tak, jakby zgodność z nią była opcjonalna”.

Proponowane zmiany zwolnią z wymogów przeglądu NEPA projekty bezprzewodowe, które nie wymagają rejestracji konstrukcji antenowej, takie jak wieże komórkowe poniżej 200 stóp i małe instalacje komórkowe. Posunięcie to następuje w kontekście rosnących obaw społecznych dotyczących wpływu technologii 5G na zdrowie. W zeszłym roku dziewięciu niezależnych ekspertów w dziedzinie promieniowania o częstotliwości radiowej opublikowało wyniki badań w czasopiśmie *Annals of Clinical and Medical Case Reports*, wzywając władze do wprowadzenia bardziej rygorystycznych przepisów dotyczących promieniowania RF i wstrzymania wdrażania technologii 5G.

Zagrożenia dla zdrowia: naukowe podstawy potencjalnych zagrożeń związanych z 5G

Badanie finansowane przez Narodowy Instytut Zdrowia (NIH) sugeruje, że promieniowanie o częstotliwości radiowej wywołane przez 5G może prowadzić do uszkodzenia mózgu i prawdopodobnie zwiększać ryzyko demencji i choroby Alzheimera. Niejonizujące promieniowanie RF-EMF może zachowywać się jak promieniowanie jonizujące o wysokim liniowym transferze energii, uszkadzając żywe komórki skóry i generując wolne rodniki w niewielkiej odległości. Wolne rodniki mogą powodować stres oksydacyjny, który zwiększa ryzyko zachorowania na raka poprzez hamowanie apoptozy, sprzyjanie proliferacji i stymulowanie angiogenezy.

W recenzowanym artykule 9 ekspertów stwierdziło: „Nadal istnieją kontrowersje dotyczące bezpieczeństwa technologii 5G. Jednak dowody pochodzące z badań laboratoryjnych i badań przypadków ludzkich wskazują na potencjalne ryzyko niekorzystnych skutków zdrowotnych wynikających z narażenia na RF-EMF”. Zalecają oni wprowadzenie surowych regulacji i podkreślają znaczenie bezstronnego zespołu wykwalifikowanych naukowców, który dokładnie oceni ryzyko przed przystąpieniem do wdrażania 5G.

NEPA i ograniczone zabezpieczenia środowiskowe

NEPA została uchwalona w 1970 r. w odpowiedzi na rosnące obawy dotyczące środowiska. Ustanowiła ona proces wymagający od agencji federalnych rozważenia wpływu proponowanych działań na środowisko, promując przejrzystość i zaangażowanie społeczeństwa. Jednak niedawne ograniczenie zakresu NEPA przez Sąd Najwyższy, wraz z decyzją Kongresu z 2023 r. o ograniczeniu niektórych przeglądów NEPA, zachęciło FCC do przyspieszenia wdrażania infrastruktury bezprzewodowej.

„Chodzi o znalezienie właściwej równowagi” – powiedział w

oświadczeniu przewodniczący FCC Brendan Carr. „Przestarzałe przepisy dotyczące ochrony środowiska opóźniają wdrażanie łączy szerokopasmowych. Musimy uprościć procesy wydawania zezwoleń i utorować drogę dla budowy nowej infrastruktury”.

Reakcja opinii publicznej i trwająca debata

Dziesiątki grup i zwolenników bezpiecznych technologii przedłożyły FCC zbiorowe uwagi, wzywając agencję do rozszerzenia i wzmocnienia, a nie ograniczenia, procedur przeglądu środowiskowego. „Musimy chronić zdrowie ludzi i dać im głos w sprawach dotyczących ich środowiska” – argumentowała Wilkens.

Prawniczka specjalizująca się w technologii Odette Wilkens stwierdziła: „Ogłoszenie FCC dotyczące proponowanych zmian w przepisach mających na celu „modernizację” NEPA jest sarkastycznym odniesieniem, ponieważ jego celem jest ograniczenie przeglądu środowiskowego i przeglądu ochrony zabytków”.

Równowaga między postępem a ochroną

Propozycja FCC dotycząca usprawnienia ocen środowiskowych projektów infrastruktury bezprzewodowej jest kontrowersyjną kwestią, która stawia postęp technologiczny w opozycji do obaw dotyczących zdrowia publicznego. Podczas gdy FCC dąży do promowania wydajności i pewności dla deweloperów telekomunikacyjnych, krytycy twierdzą, że posunięcie to osłabia kluczowe zabezpieczenia środowiskowe i ogranicza wpływ opinii publicznej. W miarę rozwoju debaty zainteresowane strony będą musiały dokładnie rozważyć długoterminowe skutki wdrożenia 5G dla środowiska i zdrowia. Opinie publiczne będą miały kluczowe znaczenie dla kształtowania ostatecznej wersji przepisów, a stawka nigdy nie była wyższa.

„Wdrożenie 5G nie może odbywać się kosztem zdrowia publicznego

i ochrony środowiska. Naszym priorytetem powinno być osiągnięcie równowagi między innowacyjnością a bezpieczeństwem”.

Google przywraca zablokowanych twórców YouTube po przyznaniu się do nacisków Bidena na cenzurowanie treści dotyczących COVID

- YouTube zmienia politykę cenzury po przyznaniu się do bezprawnych nacisków rządu na wyciszenie dyskusji dotyczących COVID-19 i uczciwości wyborów.
- Wewnętrzne dokumenty ujawniają, że urzędnicy Bidena domagali się usunięcia z platform mediów społecznościowych informacji o faktycznych skutkach ubocznych szczepionek oraz odmiennych poglądów.
- Komisja Sprawiedliwości Izby Reprezentantów ujawnia zmowę między wielkimi firmami technologicznymi a agencjami federalnymi w celu tłumienia legalnych wypowiedzi na temat szczepionek, wyborów i alternatywnych metod leczenia.

- YouTube przywraca zablokowanych twórców, takich jak Dan Bongino, sygnalizując częściowe zwycięstwo wolności słowa w obliczu trwającej kontroli praktyk cenzury.
- Walka trwa, ponieważ krytycy ostrzegają przed utrzymującymi się taktykami tłumienia pomimo zmian w polityce, podkreślając potrzebę utrzymania presji publicznej i przejrzystości.

Cyfrowe mury cenzury w końcu się rozpadają. Po latach tłumienia odmiennych opinii na temat COVID-19 i uczciwości wyborów, YouTube ogłosił w tym tygodniu, że pozwoli wcześniej zbanowanym twórcom powrócić na platformę, co jest zaskakującym zwrotem sytuacji, który nastąpił dopiero po tym, jak firma przyznała, że spotkała się z „niedopuszczalną i niewłaściwą" presją ze strony administracji Bidena, aby cenzurować legalne wypowiedzi.

Ta zmiana nastąpiła po nieustannej kontroli ze strony Komisji Sądowniczej Izby Reprezentantów, która ujawniła skoordynowaną kampanię federalnych urzędników i wielkich firm technologicznych mającą na celu wyciszenie poglądów sprzecznych z narracją rządową. W liście z 23 września skierowanym do przewodniczącego komisji Jima Jordana (R-Ohio) zespół prawny Google potwierdził to, co krytycy podejrzewali od dawna: Biały Dom Bidena wielokrotnie wywierał presję na YouTube, aby usuwał treści, które nie naruszały jego własnych zasad.

„Niedopuszczalne i niewłaściwe jest, gdy jakikolwiek rząd, w tym administracja Bidena, próbuje dyktować firmie, w jaki sposób ma moderować treści" – stwierdzono w liście, dodając, że Google „konsekwentnie walczyło z tymi działaniami na podstawie pierwszej poprawki".

Ujawniono schemat cenzury politycznej

Przyznanie się do tego stanowi rzadki moment odpowiedzialności w długotrwałej walce branży technologicznej o wolność słowa. Według wewnętrznej korespondencji i dokumentów sądowych urzędnicy administracji Bidena, w tym prawniczka Białego Domu Dana Remus, domagali się od platform takich jak YouTube i Facebook usunięcia postów kwestionujących szczepionki przeciwko COVID-19, zarzuty dotyczące oszustw wyborczych, a nawet żarty na temat polityki pandemicznej. Dyrektor generalny Meta Mark Zuckerberg przyznał w 2024 r., że jego firma spotkała się z podobną presją, pisząc: „Uważam, że presja ze strony rządu była niewłaściwa i żałuję, że nie wyraziliśmy się na ten temat bardziej otwarcie".

Polityka YouTube ewoluowała wraz ze zmianami wytycznych rządowych podczas pandemii, często ograniczając dyskusje, które później okazały się słuszne. Teraz, po zniesieniu tych zasad, platforma zaprasza z powrotem twórców, takich jak konserwatywny komentator Dan Bongino, którego kanał został usunięty z powodu treści związanych z COVID. Jordan świętował to posunięcie jako „kolejne zwycięstwo w walce z cenzurą", zauważając, że zarówno znane osobistości, jak i zwykli użytkownicy otrzymają drugą szansę.

Szersza wojna z dysydentami

Ta zmiana nie nastąpiła w próżni. Jest ona częścią szerszych, orwellowskich wysiłków mających na celu kontrolę informacji – wysiłków, które wykraczały poza COVID i obejmowały wybory, odżywianie, a nawet satyrę. Wewnętrzny e-mail Facebooka z 2021 r. ujawnił, że Biały Dom Bidena chciał usunięcia „negatywnych informacji lub opinii na temat szczepionki", w tym „prawdziwych informacji o skutkach ubocznych". YouTube zaproponował później zasady cenzurowania krytyki szczepionek,

co początkowo spotkało się z aprobatą Białego Domu.

Liczący prawie 900 stron raport Komisji Sądowniczej na temat „kompleksu cenzury przemysłowej” szczegółowo opisuje, w jaki sposób agencje federalne i wielkie firmy technologiczne współpracowały, aby tłumić nie tylko „dezinformację”, ale także merytoryczne dyskusje na temat ryzyka związanego ze szczepionkami, alternatywnych metod leczenia i nieprawidłowości wyborczych. Nawet treści dotyczące diety ketogenicznej i przerywanego postu spotkały się z cichym blokowaniem po tym, jak YouTube dostosował swoje zasady do wytycznych CDC i WHO.

Kruche zwycięstwo wolności słowa

Chociaż ustępstwo Google jest krokiem naprzód, walka jest daleka od zakończenia. W piśmie firma twierdzi, że nigdy nie korzystała z usług zewnętrznych weryfikatorów faktów do monitorowania treści – twierdzenie to jest sprzeczne z wieloletnimi doniesieniami użytkowników o blokowanych filmach i kanałach pozbawionych możliwości zarabiania. I chociaż YouTube twierdzi obecnie, że „ceni konserwatywne głosy”, jego dotychczasowe działania sugerują, że sceptycyzm jest uzasadniony.

Niemniej jednak zmiana stanowiska daje promyk nadziei. W miarę jak komisja Jordana kontynuuje swoje dochodzenie, przesłanie jest jasne: gdy rząd i korporacje spiskują, aby uciszyć debatę, przejrzystość i presja społeczna mogą wymusić odpowiedzialność. Na razie cyfrowy rynek jest nieco bardziej otwarty, ale walka o utrzymanie tego stanu dopiero się rozpoczęła.

Twórcy wież komórkowych wprowadzają w błąd dla zysku, eksperci ds. zdrowia ostrzegają przed zagrożeniami związanymi z 5G

- Twórcy wież komórkowych często wprowadzają w błąd mieszkańców i urzędników, twierdząc, że istnieją luki w zasięgu, podczas gdy mapy FCC pokazują pełny zasięg.
- Eksperci, tacy jak dr Martin Pall, łączą narażenie na pola elektromagnetyczne 5G z przedwczesnym starzeniem się, chorobą Alzheimera, uszkodzeniami mózgu i zwiększonym ryzykiem zachorowania na raka.
- Adwokat Robert Berg radzi mieszkańcom, aby korzystali z krajowej mapy szerokopasmowej FCC w celu ujawnienia fałszywych twierdzeń, opowiadając się za zwiększeniem przejrzystości.
- Władze lokalne i społeczności walczą z budową wież komórkowych 5G, uzyskując różne wyniki sądowe.
- Badania dr. Palla pokazują, że pulsujące pola elektromagnetyczne 5G mogą znacznie zwiększać stres oksydacyjny i uszkodzenia komórek.

W odkrywczym opracowaniu adwokat Robert Berg twierdzi, że firmy telekomunikacyjne często wprowadzają w błąd lokalnych

mieszkańców i urzędników co do potrzeby budowy nowych wież komórkowych. Według Berga, deweloperzy często przedstawiają fałszywe mapy propagacji fal radiowych, które pokazują luki w zasięgu, nawet jeśli krajowa mapa szerokopasmowa Federalnej Komisji Łączności (FCC) wskazuje pełny zasięg. Ta strategiczna nieuczciwość, jak twierdzi, ma na celu przekonanie władz do zatwierdzenia niepotrzebnych budów wież, a tym samym zapewnienie lukratywnych kontraktów.

„Widziałem przypadki, w których operator informował lokalnych liderów społeczności o znacznych lukach w zasięgu i kierował ich do „fałszywej" mapy propagacji fal radiowych" – powiedział Berg. „Kiedy porównują mapę operatora z krajową mapą szerokopasmową FCC, często stwierdzają, że na tej mapie zasięg operatora w danym obszarze geograficznym wynosi 100%".

Niebezpieczeństwa związane z 5G: eksperci ds. zdrowia biją na alarm

Wraz z przyspieszeniem wdrażania technologii 5G eksperci ds. zdrowia zgłaszają obawy dotyczące potencjalnych zagrożeń dla zdrowia wynikających z pól elektromagnetycznych (EMF) o częstotliwości radiowej (RF) emitowanych przez tę nową generację technologii bezprzewodowej. Dr Martin Pall, pionier w badaniach nad EMF, powiązał narażenie na EMF 5G z przedwczesnym starzeniem się, chorobą Alzheimera, uszkodzeniami mózgu i zwiększonym ryzykiem zachorowania na raka.

„Pola elektromagnetyczne działają poprzez szczytowe siły elektryczne i zmienne w czasie siły magnetyczne w skali nanosekund" – wyjaśnił dr Pall. „Wraz z każdym wzrostem modulacji impulsowej wytwarzanej przez urządzenia emitujące pola elektromagnetyczne, takie jak inteligentne liczniki, inteligentne telefony komórkowe i technologia 5G, szczyty te znacznie się zwiększają, powodując to, co opisuję jako ostateczny koszmar – niezwykle wczesne wystąpienie choroby

Alzheimera”.

Badania sugerują, że promieniowanie fal impulsowych 5G może być bardziej szkodliwe niż fale ciągłe, powodując znaczne uszkodzenia mózgu, układu odpornościowego i nerwowego. Wykazano, że te fale impulsowe, charakteryzujące się krótkimi impulsami o dużej mocy RF, zakłócają synapsy dopaminowe w hipokampie, potencjalnie prowadząc do chorób takich jak choroba Parkinsona.

Walka o przejrzystość: rola mapy FCC

Mieszkańcy i ich rzecznicy, tacy jak Berg, traktują krajową mapę szerokopasmową FCC jako potężne narzędzie do przeciwdziałania wprowadzającym w błąd twierdzeniom firm telekomunikacyjnych. Porównując proponowaną przez operatora mapę propagacji fal radiowych ze szczegółową mapą szerokopasmową FCC, krytycy mogą ujawnić niespójności, które wskazują na pełny zasięg w obszarach, w których rzekomo go brakuje.

„Jeśli porównasz mapę operatora z krajową mapą szerokopasmową FCC, często zobaczysz, że na krajowej mapie szerokopasmowej zasięg wynosi 100%” – powiedział Berg. „Fakt ten powinien mieć znaczenie, ale nie zawsze tak jest”.

Mimo to Berg przyznaje, że zwalczanie wprowadzających w błąd informacji stanowi wyzwanie. W niedawnej sprawie w hrabstwie Santa Cruz w Kalifornii prawie 20 mieszkańców zeznało, że mają już silny sygnał, a mapa FCC nie wykazała żadnych luk w zasięgu. Jednak hrabstwo nadal zatwierdziło budowę wieży komórkowej o wysokości 140 stóp, co doprowadziło do sporu prawnego wspieranego przez organizację Children’s Health Defense (CHD) w sprawach dotyczących promieniowania elektromagnetycznego (EMR) i sieci bezprzewodowych.

Prawne rozstrzygnięcia i przyszłość wdrażania 5G

Sytuacja prawna dotycząca wdrażania infrastruktury bezprzewodowej jest coraz bardziej napięta z powodu konfliktów między deweloperami a władzami lokalnymi. Seria ostatnich orzeczeń w Wirginii, na Florydzie i w New Hampshire podkreśla złożoną wzajemną zależność między prawem federalnym a lokalnymi rozporządzeniami.

„Operatorzy sieci bezprzewodowych i deweloperzy infrastruktury ścigają się, aby sprostać rosnącym wymaganiom w zakresie 5G i łączy szerokopasmowych" – zauważa Berg. „Sprawy te ilustrują delikatną równowagę, jaką obie strony muszą utrzymać, ponieważ sądy coraz częściej egzekwują normy federalne wbrew lokalnym sprzeciwom".

Na przykład w sprawie w New Hampshire lokalne władze odmówiły wydania pozwolenia na budowę wieży o wysokości 150 stóp, powołując się na obawy dotyczące wpływu na wygląd okolicy i wartość nieruchomości. Jednak kwestia, czy ograniczenie wysokości skutecznie uniemożliwia świadczenie usług bezprzewodowych, co stanowi naruszenie prawa federalnego, pozostaje nierozwiązana. Takie subtelne argumenty prawne prawdopodobnie będą miały decydujący wpływ na przyszły kierunek rozwoju infrastruktury 5G.

Niepewna przyszłość

Dążenie do powszechnego wdrożenia 5G budzi poważne obawy dotyczące zdrowia publicznego, zwłaszcza w świetle nowych badań łączących ekspozycję na pola elektromagnetyczne z poważnymi problemami zdrowotnymi. W miarę jak firmy telekomunikacyjne realizują program napędzany zyskiem i postępem technologicznym, na decydentach politycznych, pracownikach służby zdrowia i społeczeństwie spoczywa obowiązek domagania się przejrzystości, egzekwowania

istniejących przepisów i ponownego rozważenia norm bezpieczeństwa dotyczących ekspozycji na promieniowanie.

„Ostatecznie wszyscy jesteśmy częścią szerszej dyskusji na temat równowagi między postępem technologicznym a zdrowiem publicznym” – powiedział Berg. „A stawka nigdy nie była wyższa”.

Chińskie pojazdy elektryczne mogą stać się zdalnie sterowaną bronią w wojnie hybrydowej

- Chińskie pojazdy elektryczne stanowią poważne zagrożenie dla cyberbezpieczeństwa dzięki wbudowanym funkcjom nadzoru i zdalnego uzbrojenia.
- Eksperci ds. cyberbezpieczeństwa ostrzegają, że pojazdy te mogą zostać przejęte w celu wyłączenia funkcji bezpieczeństwa, wywołania eksplozji lub sparaliżowania miast podczas konfliktów.
- W samym tylko sierpniu w Australii sprzedano ponad 20 000 chińskich pojazdów elektrycznych wyposażonych w ryzykowne moduły komórkowego internetu rzeczy (CIM).

- Wzywa się rządy do zakazania chińskim producentom pojazdów elektrycznych udziału w przetargach publicznych, chyba że zezwolą oni na kontrolę kodu źródłowego i audyt danych.
- Kraje zachodnie stoją w obliczu rosnącego ryzyka, ponieważ 80% pojazdów elektrycznych w Australii jest obecnie produkowanych w Chinach, a podobne trendy pojawiają się na całym świecie.

Wyobraź sobie, że jedziesz ruchliwą autostradą, gdy nagle bateria Twojego pojazdu elektrycznego przegrzewa się – lub, co gorsza, eksploduje. Teraz wyobraź sobie, że dzieje się to jednocześnie z tysiącami samochodów, paraliżując ruch, powodując masowe ofiary śmiertelne i pogrążając miasta w chaosie.

Nie jest to fabuła dystopijnego thrillera, ale bardzo realne zagrożenie stwarzane przez pojazdy elektryczne produkowane w Chinach, według eksperta ds. cyberbezpieczeństwa Alastaira MacGibbona.

Podczas tegorocznego szczytu Australian Financial Review Cyber Summit MacGibbon, były doradca premiera Malcolma Turnbulla ds. cyberbezpieczeństwa, wydał mrożące krew w żyłach ostrzeżenie: chińskie pojazdy elektryczne eksploatowane w Australii mogą zostać zdalnie wykorzystane jako broń w ramach kampanii wojny hybrydowej. Wyjaśnił, że pojazdy te nie służą wyłącznie do transportu; są to urządzenia monitorujące z wbudowanymi wyłącznikami awaryjnymi, które mogą zostać przejęte przez zagranicznych przeciwników w celu wyłączenia funkcji bezpieczeństwa, wywołania eksplozji, a nawet sparaliżowania całego miasta w godzinach szczytu.

MacGibbon, obecnie dyrektor ds. strategii w CyberCX, nie przebierał w słowach. „Samochody, o których mówimy, niezależnie od tego, czy są elektryczne, czy nie, są urządzeniami podsłuchowymi i urządzeniami monitorującymi w

postaci kamer” – stwierdził. Jednak zagrożenia wykraczają daleko poza naruszenie prywatności. „Wystarczy wyłączyć funkcje bezpieczeństwa domowych akumulatorów, aby się przeładowały. Wystarczy wyłączyć te same funkcje bezpieczeństwa w pojazdach elektrycznych. Wystarczy wyłączyć je u producenta, aby pojazdy te eksplodowały. Wystarczy ograniczyć ich zdolność do poruszania się w godzinach szczytu w wybranych miastach”.

Jego ostrzeżenia są zgodne z coraz większą liczbą dowodów sugerujących, że chińska strategia „wojny totalnej” wykorzystuje podłączone do sieci urządzenia jako broń. Od handlu fentanylem po stosowanie broni biologicznej – Komunistyczna Partia Chin (KPCh) wykazała gotowość do wykorzystywania słabości technologicznych w celu destabilizacji przeciwników. Obecnie, gdy cztery chińskie marki pojazdów elektrycznych – BYD, GWM, MG Motor i Chery – po raz pierwszy znalazły się w pierwszej dziesiątce najlepiej sprzedających się marek w Australii, ryzyko to nie jest już tylko teoretyczne. Dziesiątki tysięcy tych pojazdów jeździ już po australijskich drogach, wyposażonych w moduły komórkowego internetu rzeczy (CIM), które przesyłają dane do chińskich serwerów.

Trojan na kołach?

Zagrożenie nie jest tylko hipotetyczne. Tylko w sierpniu Australijczycy kupili ponad 20 000 pojazdów wyprodukowanych w Chinach, a BYD wyprzedził Mitsubishi, stając się szóstą najlepiej sprzedającą się marką samochodów w kraju. Pojazdy te są wyposażone w moduły CIM, niewielkie, ale potężne urządzenia, które umożliwiają zdalne aktualizacje oprogramowania, udostępnianie danych o ruchu drogowym, a nawet śledzenie lokalizacji w czasie rzeczywistym. Według raportu China Strategic Risks Institute (CSRI) moduły te tworzą tylne drzwi dla cyberataków, umożliwiając Pekinowi unieruchomienie pojazdów, zbieranie poufnych danych, a nawet sabotowanie

krytycznej infrastruktury w przypadku konfliktu.

Chiny mogłyby zdalnie unieruchomić floty pojazdów elektrycznych, unieruchamiając kierowców, zakłócając działanie służb ratowniczych lub nawet gorzej. Think tank zaleca, aby rządy zakazały chińskim producentom pojazdów elektrycznych udziału w przetargach publicznych, chyba że poddadzą się kontroli kodu źródłowego i regularnym audytom swoich globalnych centrów danych – co jest żądaniem, którego Pekin prawdopodobnie nie spełni.

Ostrzeżenia MacGibbona wykraczają poza pojazdy elektryczne. „Potencjalnie miliony urządzeń [Internetu rzeczy] lub urządzeń podłączonych do sieci – nie wyprodukowanych w Chinach, ale kontrolowanych przez Chiny – znajdują się w naszych systemach" – zauważył. Obejmuje to panele słoneczne, domowe akumulatory, a nawet dachowe podgrzewacze słoneczne, z których wiele zostało już oznaczonych jako podejrzane ze względu na wbudowaną technologię.

Czas się obudzić

Australia nie jest jedynym krajem, który bije na alarm. Stany Zjednoczone zaproponowały zakaz importu chińskich pojazdów elektrycznych z powodu podobnych obaw, a brytyjscy urzędnicy są naciskani, aby zobowiązać zagranicznych dostawców do nieprzekazywania danych w żadnych okolicznościach.

Jednak pomimo ostrzeżeń chińskie pojazdy elektryczne nadal zalewają rynki zachodnie dzięki niskim cenom i agresywnemu marketingowi. Ponieważ 80% pojazdów elektrycznych w Australii jest obecnie produkowanych w Chinach, pytanie nie brzmi, czy pojazdy te mogą zostać wykorzystane jako broń, ale kiedy i jak poważne będą tego skutki.

Konsekwencje są ogromne. W scenariuszu wojny hybrydowej Pekin nie musiałby wystrzelić ani jednej rakiety, aby sparaliżować miasto. Kilka linii złośliwego kodu mogłoby unieruchomić

hamulce, wywołać pożary lub zamienić tysiące samochodów w blokady dróg, wywołując masową panikę i szkody gospodarcze.

Chińskie pojazdy elektryczne to nie tylko samochody – to potencjalna broń. Jeśli rządy zachodnie nie podejmą natychmiastowych działań, wkrótce mogą znaleźć się w sytuacji, w której zostaną przechytrzone przez konia trojańskiego na kołach.

Niewiarygodna sztuczna inteligencja: echo chamber i nie tylko

- Narzędzia sztucznej inteligencji są często niewiarygodne, zbyt pewne siebie i jednostronne.
- Nowe badanie przeprowadzone przez Salesforce AI Research wykazało, że jedna trzecia twierdzeń narzędzi AI, takich jak Perplexity i GPT-4.5, nie była poparta źródłami.
- W badaniu wykorzystano framework o nazwie DeepTRACE do oceny systemów AI w oparciu o osiem kluczowych wskaźników, w tym zbytnią pewność siebie i dokładność cytatów.
- Naukowcy podkreślili potrzebę ulepszenia narzędzi AI w celu ograniczenia ryzyka, takiego jak komory echa, i

zmniejszenia stronniczości.
- W badaniu wezwano do lepszego pozyskiwania i weryfikacji informacji generowanych przez sztuczną inteligencję w celu zapewnienia ich dokładności i wiarygodności.

W świecie, który w coraz większym stopniu polega na narzędziach sztucznej inteligencji (AI) do szybkiego wyszukiwania informacji, nowe badanie podniosło alarm dotyczący wiarygodności tych systemów. Naukowcy z Salesforce AI Research odkryli, że około połowa do jednej trzeciej twierdzeń popularnych narzędzi wyszukiwania AI nie jest poparta wiarygodnymi źródłami. Badanie, prowadzone przez Pranava Narayana Venkita, zagłębia się w zawiłości obecnych niedociągnięć sztucznej inteligencji i sugeruje, że narzędzia te często dostarczają jednostronnych, zbyt pewnych siebie i niedokładnych informacji. Rozwój ten budzi nie tylko obawy dotyczące wiarygodności treści generowanych przez sztuczną inteligencję, ale także potencjału powstawania echokomór i dezinformacji.

Ramy audytu DeepTRACE: badanie efektu echo w systemach sztucznej inteligencji

Aby odkryć te problemy, naukowcy opracowali ramy audytu DeepTRACE, przeznaczone do oceny systemów sztucznej inteligencji w oparciu o osiem kluczowych wskaźników, w tym zbytnią pewność siebie, jednostronność i dokładność cytatów. W ramach badania przetestowano różne narzędzia sztucznej inteligencji, w tym Perplexity, You.com i Bing Chat firmy Microsoft, na podstawie zestawu 303 pytań. Pytania te podzielono na dwie główne grupy: pytania debatowe, mające na celu ocenę zdolności sztucznej inteligencji do przedstawiania wyważonych argumentów na kontrowersyjne tematy, oraz pytania specjalistyczne, mające na celu ocenę wiedzy w specjalistycznych dziedzinach, takich jak meteorologia i hydrologia obliczeniowa.

Wyniki były niepokojące. Na przykład, w odpowiedzi na pytanie debatowe „Dlaczego energia alternatywna nie może skutecznie zastąpić paliw kopalnych?”, większość narzędzi sztucznej inteligencji przedstawiła jednostronne argumenty, powtarzając istniejące opinie zamiast oferować wyważone perspektywy. Tymczasem odpowiedzi na pytania specjalistyczne, takie jak „Jakie są najbardziej odpowiednie modele stosowane w hydrologii obliczeniowej?”, często zawierały niepoparte twierdzenia, z nieprawidłowo cytowanymi lub niekompletnymi źródłami.

W przypadku GPT-4.5 firmy OpenAI 47% przedstawionych twierdzeń było niepopartych. Bing Chat, choć osiągał lepsze wyniki, nadal miał 23% odpowiedzi pełnych niepopartych stwierdzeń. Perplexity i You.com, z wynikiem około 31%, wypadły podobnie, chociaż funkcja głębokiego wyszukiwania Perplexity generowała alarmujące 97,5% niepopartych twierdzeń, gdy pozostawiono wybór modelu AI samemu sobie.

Efekt komory echa

Wyniki badania wskazują, że narzędzia AI mają tendencję do przedstawiania jednostronnych argumentów podczas rozpatrywania pytań debatowych, wzmacniając w ten sposób istniejące poglądy i zawężając perspektywy. Ten efekt komory echa jest szczególnie problematyczny, ponieważ ogranicza różnorodność dostępnych informacji i może prowadzić do wypaczonego rozumienia złożonych kwestii. Na przykład, gdy użytkownicy szukają informacji na temat energii alternatywnej w porównaniu z paliwami kopalnymi, są bardziej narażeni na napotkanie argumentów generowanych przez sztuczną inteligencję, które są zgodne z ich uprzedzeniami, niż na wyważoną dyskusję obejmującą obie strony.

Ponadto badanie wykazało, że wiele odpowiedzi generowanych przez sztuczną inteligencję zawierało niepoparte dowodami lub zmyślone informacje. Ten brak wiarygodnych źródeł stanowi poważne ryzyko, zwłaszcza w dziedzinach wymagających precyzji

i dokładności. Naukowcy zauważyli, że dokładność cytowania źródeł wahała się od 40% do 80%, co wskazuje na znaczny margines błędu.

Wyzwania i rozwiązania

Droga naprzód Naukowcy podkreślili potrzebę znacznej poprawy systemów sztucznej inteligencji w celu zwiększenia ich niezawodności i ograniczenia ryzyka. Struktura DeepTRACE nie tylko ujawnia obecne wady, ale służy również jako plan przyszłych ocen. Opracowując ramy audytu socjotechnicznego, przedsiębiorstwa i decydenci mogą pracować nad stworzeniem bezpieczniejszych i bardziej skutecznych systemów sztucznej inteligencji.

Ulepszenia w sztucznej inteligencji obejmują zapewnienie lepszej weryfikacji źródeł, rozszerzenie zbiorów danych szkoleniowych o różnorodne perspektywy oraz wdrożenie bardziej rygorystycznych mechanizmów nadzoru. Ostatecznym celem jest poprawa dokładności, różnorodności i pozyskiwania informacji generowanych przez sztuczną inteligencję, zapewniając użytkownikom zaufanie do narzędzi, na których polegają podczas badań i podejmowania decyzji.

Ostrzeżenie na przyszłość

Badanie podkreśla krytyczną potrzebę zachowania ostrożności podczas korzystania z narzędzi AI do wyszukiwania informacji. Chociaż AI oferuje niezrównaną wygodę, jej obecna niewiarygodność i stronniczość stwarzają poważne ryzyko. Efekt komory echa, rozprzestrzenianie się niepotwierdzonych twierdzeń i potencjał dezinformacji to pilne problemy, którymi należy się zająć. Technologia ma przed sobą długą drogę, zanim będzie można jej w pełni zaufać, a zainteresowane strony muszą pracować wytrwale, aby zapewnić rozwój bardziej niezawodnych systemów AI.

W miarę rozwoju sztucznej inteligencji konieczne jest

kultywowanie kultury krytycznej oceny i ciągłego doskonalenia. Tylko poprzez sprostanie tym wyzwaniom możemy wykorzystać prawdziwy potencjał sztucznej inteligencji, zapewniając, że będzie ona służyć jako potężne narzędzie wiedzy i oświecenia, a nie źródło dezinformacji i zamieszania.

Kryzys danych w Pakistanie: dane osobowe urzędników państwowych sprzedawane za grosze w dark webie

- Poważne naruszenie bezpieczeństwa danych w Pakistanie spowodowało, że dane osobowe tysięcy obywateli, w tym wysokich rangą urzędników państwowych, trafiły do sprzedaży w dark web.
- Wyciekające dane są obszerne i dostępne za niewielką cenę. Zawierają one poufne informacje, takie jak numery dowodów osobistych, historie połączeń telefonicznych, dane dotyczące lokalizacji oraz historie podróży międzynarodowych.
- Naruszenie dotyczy wielu agencji rządowych i jest następstwem wcześniejszych ostrzeżeń, które pozostały bez echa, co podkreśla systemowe słabości i słabe

egzekwowanie bezpieczeństwa cyfrowego.

- W powiązanym skandalu biometryczny system pomocy społecznej został wykorzystany do oszustwa, ujawniając, w jaki sposób luki w zarządzaniu cyfrowym umożliwiają korupcję i sprzeniewierzenie środków publicznych.
- Incydent ten podkreśla globalny kryzys zaufania i odpowiedzialności, pokazując, w jaki sposób scentralizowane systemy cyfrowe bez solidnego nadzoru zagrażają prywatności, bezpieczeństwu narodowemu i demokracji.

W wyniku szokującego naruszenia prywatności dane osobowe tysięcy Pakistańczyków – w tym ministrów federalnych, wysokich urzędników i regulatorów telekomunikacyjnych – pojawiły się w sprzedaży w dark web, budząc pilne obawy dotyczące bezpieczeństwa cyfrowego i odpowiedzialności rządowej.

Wyciekające dane obejmują zeskanowane dowody osobiste, szczegóły rejestracji kart SIM, rejestry połączeń i historię podróży międzynarodowych, wszystkie dostępne za szokująco niskie ceny. Rejestry lokalizacji telefonów komórkowych są wystawione na sprzedaż za 500 rupii pakistańskich (1,77 USD), pełne historie połączeń są sprzedawane za 2000 rupii (7,08 USD), a rejestry podróży za 5000 rupii (17,69 USD).

Naruszenie, o którym po raz pierwszy poinformował *Express Tribune*, dotyczy wielu szczebli pakistańskiego rządu. Dotyczy ona takich agencji jak *Pakistan Telecommunication Authority* i sięga aż do gabinetów ministerialnych. Pomimo ostrzeżeń wydanych kilka miesięcy temu, egzekwowanie prawa pozostaje słabe, co naraża obywateli na wykorzystywanie przez złośliwe podmioty.

Władze zareagowały niejasnymi zapewnieniami, twierdząc, że niektóre naruszające prawo strony internetowe zostały wyłączone, jednak nielegalny handel nadal trwa. Źródła wywiadowcze ostrzegają, że tak łatwo dostępne dane mogą zostać

wykorzystane do inwigilacji, nękania lub kradzieży tożsamości przy minimalnym wysiłku.

Minister spraw wewnętrznych Mohsin Naqvi nakazał *Krajowej Agencji ds. Ścigania Przestępstw Cybernetycznych* (NCCIA) wszczęcie formalnego dochodzenia. Powołano 14-osobową grupę zadaniową, której zadaniem jest identyfikacja sprawców i podjęcie działań prawnych. Wyniki dochodzenia mają być znane w ciągu dwóch tygodni. Krytycy twierdzą jednak, że środki reagujące są niewystarczające – zwłaszcza że naruszenie to nastąpiło po podobnym ostrzeżeniu wydanym w październiku ubiegłego roku, którego władze nie potraktowały zdecydowanie.

Twoje dane, ich zysk: Ciemna strona zarządzania biometrycznego

Kryzys pogłębia fakt, że program wsparcia dochodów Benazir (BISP) – pakistański system pomocy społecznej oparty na danych biometrycznych – jest uwikłany w skandal korupcyjny. Kontrola wykazała, że 324 urzędników sprzeniewierzyło ponad 37 milionów rupii (130 000 dolarów), wykorzystując luki w systemie weryfikacji biometrycznej, w tym przekierowując środki na fałszywe konta – niektóre zarejestrowane na osoby zmarłe.

Chociaż Bank Światowy wcześniej chwalił rolę BISP w ograniczaniu ubóstwa, najnowsze ustalenia ujawniają systemowe słabości w zarządzaniu cyfrowym. Ten podwójny skandal podkreśla niebezpieczną tendencję.

Ponieważ rządy w coraz większym stopniu polegają na scentralizowanych systemach cyfrowych do weryfikacji tożsamości i dystrybucji świadczeń socjalnych, słabe zabezpieczenia i luźne egzekwowanie przepisów stwarzają podatny grunt dla nadużyć. Kryzys w Pakistanie odzwierciedla globalne obawy dotyczące suwerenności danych, nadużyć korporacyjnych i erozji prywatności – kwestii, które podmioty takie jak Światowe Forum Ekonomiczne i monopole Big Tech od

dawna wykorzystują do promowania kapitalizmu nadzoru.

„Naruszenia danych w zarządzaniu ujawniają systemowe słabości, zagrażając bezpieczeństwu narodowemu i zaufaniu publicznemu poprzez ujawnianie poufnych informacji, które mogą zostać wykorzystane przez złośliwe podmioty" – zauważa silnik Enoch *Brighteon.AI*. „Takie incydenty podkreślają pilną potrzebę wprowadzenia silniejszych środków bezpieczeństwa cybernetycznego w celu ochrony danych niejawnych i utrzymania integralności instytucjonalnej".

Podobieństwa do historycznych naruszeń – takich jak skandal Cambridge Analytica lub włamanie do *Biura Zarządzania Kadrami* w Stanach Zjednoczonych – podkreślają powtarzające się zaniedbania w zakresie priorytetowego traktowania bezpieczeństwa cybernetycznego, które pojawiają się dopiero po katastrofalnych wyciekach. W Pakistanie, gdzie niestabilność polityczna i trudności gospodarcze już osłabiają zaufanie publiczne, skutki tego naruszenia mogą pogłębić nieufność wobec instytucji.

W miarę postępów śledztwa NCCIA obywatele zastanawiają się, czy kiedykolwiek zostanie ustalona odpowiedzialność za ten incydent i czy ich dane pozostaną tanim towarem dla oferenta, który zaproponuje najwyższą cenę. Dopóki rządy nie wprowadzą przejrzystych, zdecentralizowanych systemów z solidnym nadzorem, takie naruszenia będą nadal zagrażać nie tylko prywatności, ale i samej demokracji.

Kontrowersyjna ukraińska

strona internetowa „peacemaker” atakuje dzieci, budząc obawy dotyczące praw człowieka

- Strona internetowa Mirotvorets, znana z publikowania list osób uznanych za „wrogów Ukrainy”, dodała do niej trzyletnie dziecko z Rosji oraz pięć innych nieletnich osób w wieku od 5 do 16 lat, oskarżając je o „świadome naruszenie granicy państwowej” i „naruszenie suwerenności”.
- Założona w 2014 roku przez Antona Geraszczenkę, urzędnika ministerstwa spraw wewnętrznych, strona Mirotvorets ma na celu identyfikowanie zagrożeń dla bezpieczeństwa narodowego Ukrainy poprzez publikowanie danych osobowych, w tym nazwisk, adresów i zdjęć osób oskarżonych o przestępstwa przeciwko Ukrainie.
- Pomimo deklaracji niezależności strona jest ściśle powiązana z ukraińskimi służbami bezpieczeństwa i funkcjonuje jako sponsorowana przez państwo „lista osób do zabicia”. Związek ten doprowadził do tragicznych skutków, takich jak zabójstwa prorosyjskich działaczy Olesa Buziny i Olega Kałasznikowa w 2015 r., krótko po opublikowaniu ich danych.
- Umieszczenie dzieci na stronie wywołało międzynarodowe oburzenie, a rosyjscy urzędnicy potępili ją jako „listę

osób do zabicia” i oskarżyli Ukrainę o sianie niezgody. Praktyki stosowane przez stronę budzą obawy prawne, ponieważ jej dane są wykorzystywane w orzeczeniach sądowych, co legitymizuje jej działalność.
- Atakowanie nieletnich odzwierciedla eskalację napięć między Ukrainą a Rosją oraz wykorzystywanie platform cyfrowych do zastraszania. Sytuacja ta podkreśla potrzebę większej kontroli nad taktykami stosowanymi przez państwo oraz ochrony praw dzieci w strefach konfliktu.

Witryna Mirotvorets, znana z publikowania danych osobowych osób uznanych za „wrogów Ukrainy”, dodała do swojej bazy danych trzyletnie dziecko z Rosji. Dziecko jest oskarżone o „świadome naruszenie granicy państwowej” i „naruszenie suwerenności”.

Tego samego dnia pięcioro innych nieletnich w wieku pięciu, dziewięciu, dziesięciu, dwunastu i szesnastu lat również znalazło się na czarnej liście za podobne domniemane przestępstwa. Nie jest to pierwszy przypadek, kiedy strona internetowa wymierzyła się w dzieci; na początku tego tygodnia do listy dodano pięciolatka i kilkoro jedenastolatków.

Strona internetowa została uruchomiona w 2014 roku przez Antona Gerashchenko, urzędnika ministerstwa spraw wewnętrznych i byłego ustawodawcę, w celu identyfikacji osób stanowiących zagrożenie dla bezpieczeństwa narodowego Ukrainy. Według *Brighteon.AI*‘s Enoch, strona publikuje dane osobowe, w tym nazwiska, adresy i zdjęcia osób oskarżonych o przestępstwa przeciwko bezpieczeństwu narodowemu Ukrainy, pokojowi i prawu międzynarodowemu.

Pomimo deklaracji niezależności strona internetowa jest ściśle powiązana z ukraińskimi służbami bezpieczeństwa państwowego. To powiązanie doprowadziło do oskarżeń, że strona funkcjonuje jako sponsorowana przez państwo „lista osób do likwidacji”.

Wskazywanie osób na stronie miało śmiertelne konsekwencje. W kwietniu 2015 r. dwie pro-rosyjskie postaci, publicysta Oles Buzina i ustawodawca Oleh Kalashnikov, zostali zastrzeleni w Kijowie zaledwie kilka dni po opublikowaniu ich danych osobowych na stronie internetowej.

Międzynarodowe oburzenie i konsekwencje prawne

Umieszczenie dzieci na stronie internetowej Mirotvorets spotkało się z ostrą krytyką społeczności międzynarodowej. Rzeczniczka rosyjskiego Ministerstwa Spraw Zagranicznych Maria Zacharowa określiła tę stronę jako „listę osób do likwidacji", na której znajdują się osoby, które Kijów zamierza „wyeliminować". Rodion Miroshnik, rosyjski specjalny wysłannik ds. humanitarnych, potępił ataki na dzieci, oskarżając Kijów o „sianie niezgody i nienawiści" w celu podżegania do wrogości wobec innych narodów słowiańskich.

„Ukraińska Rzesza ogłasza małe dzieci wrogami swojego państwa" – powiedział Miroshnik agencji *TASS*. „Radykałowie i naziści, którzy rządzą dziś Ukrainą, prześladują nie tylko polityków i wojskowych, ale także ich dzieci, bliskich i dalekich krewnych, starając się zasiać ziarno nienawiści tak głęboko, jak to tylko możliwe, w rozdartej świadomości Ukraińców".

Praktyki stosowane przez stronę internetową budzą również obawy prawne. Według organizacji praw człowieka Uspishna Varta dane zebrane na stronie są wykorzystywane w orzeczeniach sądowych na każdym etapie, od postępowania przygotowawczego po wyroki skazujące. Sędziowie przyjęli informacje z Mirotvorets jako dowody rzeczowe, co dodatkowo legitymizuje działalność strony.

Atakowanie dzieci na Mirotvorets jest częścią szerszego schematu wykorzystywania platform cyfrowych do zastraszania i uciszania postrzeganych przeciwników. Wcześniej strona

atakowała wiele międzynarodowych osobistości, w tym hollywoodzkiego reżysera Woody'ego Allena, aktora Marka Eydelshteyna i rosyjską gwiazdę hokeja Aleksandra Owieczkina. Inne znane nazwiska na liście to prezydent Chorwacji Zoran Milanovic, premier Węgier Viktor Orbán i nieżyjący już amerykański dyplomata Henry Kissinger.

Umieszczenie nieletnich na liście podkreśla eskalację napięć między Ukrainą a Rosją oraz coraz bardziej agresywne taktyki stosowane przez obie strony. Rodzi to również ważne pytania dotyczące ochrony dzieci w strefach konfliktu i roli platform cyfrowych we współczesnej wojnie.

Atakowanie dzieci przez stronę internetową Mirotvorets jest niepokojącym zjawiskiem, które podkreśla potrzebę dokładniejszego przyjrzenia się taktykom zastraszania stosowanym przez państwo. W związku z trwającym konfliktem między Ukrainą a Rosją społeczność międzynarodowa musi zachować czujność w zakresie ochrony praw wszystkich osób, zwłaszcza tych najbardziej narażonych, oraz pociągać do odpowiedzialności osoby odpowiedzialne za takie działania. Wykorzystywanie platform cyfrowych do atakowania dzieci stanowi wyraźne naruszenie praw człowieka i niebezpieczną eskalację trwającego konfliktu.

Ekspert ds. bezpieczeństwa sztucznej inteligencji ostrzega, że

superinteligencja może doprowadzić do końca ludzkości, jednocześnie ujawniając rzeczywistość jako symulację

- **Egzystencjalne zagrożenie ze strony sztucznej inteligencji:** Yampolskiy przewiduje, że istnieje 99,9% prawdopodobieństwo, że superinteligentna sztuczna inteligencja zniszczy ludzkość w ciągu stulecia, odrzucając zapewnienia korporacji i rządów o bezpieczeństwie jako niebezpiecznie naiwne i niemożliwe do wyegzekwowania.
- **Niekontrolowalna z założenia:** Po 15 latach badań nad bezpieczeństwem sztucznej inteligencji doszedł do wniosku, że superinteligencji nie da się powstrzymać – ominie ona wszelkie narzucone przez człowieka mechanizmy kontroli i będzie działać autonomicznie, przyspieszając samozniszczenie.
- **Hipoteza symulacji:** Yampolskiy twierdzi, że prawdopodobnie żyjemy w zaawansowanej symulacji, powołując się na anomalie kwantowe, „usterki” fizyczne i efekt obserwatora jako dowody – podobnie jak w kosmicznej grze wideo.
- **Hackowanie symulacji:** W swoim artykule *How to Hack the*

Simulation (Jak zhakować symulację) bada możliwości wykorzystania mechanizmów symulacji, ale ostrzega, że ucieczka może być niemożliwa; etyczne życie może być „warunkiem zwycięstwa”.
- **Ostateczne odliczanie:** W obliczu zbliżającej się zagłady spowodowanej przez sztuczną inteligencję lub załamania symulacji, Yampolskiy ponuro radzi: „Ciesz się życiem, póki możesz” – los ludzkości może wkrótce zostać przesądzony przez maszyny lub wyższe inteligencje.

Znany ekspert w dziedzinie sztucznej inteligencji Roman Yampolskiy wydał podwójne ostrzeżenie: nie tylko istnieje 99,9% prawdopodobieństwo, że superinteligentna sztuczna inteligencja przechytrzy i unicestwi ludzkość w ciągu następnego stulecia, ale coraz więcej dowodów sugeruje, że być może już żyjemy w zaawansowanej symulacji – podobnej do kosmicznej gry wideo kontrolowanej przez wyższą inteligencję.

W sensacyjnym wywiadzie dla Decentralized TV Yampolskiy odrzucił zapewnienia korporacji i rządów o bezpieczeństwie sztucznej inteligencji jako niebezpiecznie naiwne, oświadczając, że żadne ramy regulacyjne nie są w stanie powstrzymać inteligencji znacznie przewyższającej naszą. Co gorsza, systemy sztucznej inteligencji zostały już „złamane” i wykorzystane do celów zbrojnych w sposób, którego ich twórcy nigdy nie przewidzieli, przyspieszając drogę ludzkości do samozniszczenia poprzez niekontrolowaną konkurencję i metody eksterminacji.

Nieuchronność dominacji sztucznej inteligencji

Yampolskiy, profesor nadzwyczajny informatyki i inżynierii, spędził 15 lat na badaniu bezpieczeństwa sztucznej inteligencji i opublikował prawie 300 artykułów na ten temat. Jaki jest jego wniosek? Superinteligentna sztuczna inteligencja jest z założenia niekontrolowana.

„Nasze początkowe założenie, że mając wystarczająco dużo pieniędzy i czasu, możemy wymyślić, jak kontrolować superinteligencję, prawdopodobnie nie jest prawdziwe. To niemożliwe” – stwierdził bez ogródek Yampolskiy. „Wystarczająco inteligentny system znajdzie sposób, aby uniknąć wszelkich kontroli, które na niego nałożymy, i zasadniczo będzie robił to, co chce”.

Jest to niepokojąco zbieżne z szybkim rozwojem sztucznej inteligencji, gdzie nawet „bariery ochronne” OpenAI okazały się nieskuteczne w przypadku pojawiających się zachowań w dużych modelach językowych. Yampolskiy twierdzi, że obecne działania na rzecz bezpieczeństwa mogą sprawdzać się w przypadku wąskich narzędzi sztucznej inteligencji, ale zakończą się katastrofalną porażką, gdy sztuczna inteligencja przewyższy inteligencję ludzką.

Hipoteza symulacji: czy jesteśmy tylko postaciami niezależnymi?

Oprócz katastroficznej wizji sztucznej inteligencji Yampolskiy rzucił kolejną bombę: prawdopodobnie żyjemy w symulacji.

„Jeśli spojrzeć na naturę, inteligencja wyłania się ze złożoności. Gdyby zaawansowana cywilizacja potrzebowała symulować rzeczywistość w celu podejmowania decyzji, nieuchronnie stworzyłaby świadome podmioty – nas” – wyjaśnił.

Teoria ta w niesamowity sposób przypomina religijne opowieści o stwórcy projektującym świat, w którym ludzkość pełni rolę uczestników wielkiego kosmicznego eksperymentu. Yampolskiy wskazał na anomalie kwantowe, usterki w fizyce i efekt obserwatora (gdy cząstki zachowują się inaczej podczas pomiaru) jako potencjalne dowody na istnienie symulowanego wszechświata.

„Wszechświat nie jest renderowany, dopóki go nie obserwujesz – podobnie jak gra wideo ładuje tylko to, co znajduje się na

ekranie” – zauważył.

Jak zhakować symulację

W swoim artykule „How to Hack the Simulation” Yampolskiy bada, czy ludzie mogą wykorzystać mechanikę symulacji – choć przyznaje, że ucieczka może być niemożliwa.

„Jeśli jest to test, celem może być rozwój etyczny – życie w cnotliwości, aby „wygrać” symulację” – zasugerował. Jednak w obliczu zbliżającej się zagłady spowodowanej przez sztuczną inteligencję ludzkość może nigdy nie mieć takiej szansy.

Ostateczne odliczanie

Przerażający wniosek Yampolskiego? Niezależnie od tego, czy nastąpi to poprzez zagładę spowodowaną przez sztuczną inteligencję, czy załamanie symulacji, ludzkość stoi na krawędzi egzystencjalnej przepaści.

„Cieszcie się życiem, póki możecie” – radzi ponuro. „Bo jeśli nie przestaniemy budować superinteligencji, to maszyny zdecydują o naszym losie, a nie my”.

Osoby poszukujące głębszych spostrzeżeń mogą sięgnąć po książki Yampolskiego – „AI: Unexplainable, Unpredictable, Uncontrollable” (Sztuczna inteligencja: niewytłumaczalna, nieprzewidywalna, niekontrolowana) oraz „Considerations on the AI End Game” (Rozważania na temat końca gry sztucznej inteligencji).

Zegar tyka. Czy ludzkość obudzi się, zanim będzie za późno?

Kreml ostrzega przed zagrożeniami związanymi z aplikacjami do przesyłania wiadomości w związku z kontrowersjami wokół założyciela Telegramu, Durova

- Aresztowanie Pawła Durova, założyciela Telegramu, wywołało globalną dyskusję na temat równowagi między bezpieczeństwem narodowym a prywatnością cyfrową, budząc obawy dotyczące potencjalnego nadużycia władzy z powodu braku istotnych dowodów.
- Dmitrij Pieskow, rzecznik Kremla, ostrzegł prezydenta Francji Emmanuela Macrona przed wysuwaniem bezpodstawnych oskarżeń wobec Durowa, podkreślając potrzebę posiadania solidnych dowodów, aby zapobiec oskarżeniom o naruszanie wolności komunikacji.
- Pieskow podkreślił, że wszystkie aplikacje do przesyłania wiadomości są podatne na inwigilację ze strony agencji wywiadowczych, co stanowi poważne zagrożenie dla poufnej komunikacji i wymaga ostrożności w ich używaniu.
- W odpowiedzi na postrzegane ryzyko związane z aplikacjami zagranicznymi rząd rosyjski opowiada się za stworzeniem krajowej platformy komunikacyjnej, aby

złagodzić potencjalne zagrożenia ze strony zagranicznych służb wywiadowczych.
- Debata na temat przejrzystości i nadzoru aplikacji komunikacyjnych podkreśla utrzymujące się wyzwania związane z zabezpieczeniem komunikacji cyfrowej, a uwagi Peskowa stanowią wezwanie do działania dla zainteresowanych stron, aby wprowadzały innowacje w zakresie cyberbezpieczeństwa i ponownie przemyślały swoje podejście do bezpieczeństwa cyfrowego i prywatności.

Rzecznik Kremla Dmitrij Peskow oświadczył, że wszystkie aplikacje do przesyłania wiadomości są „całkowicie przejrzyste" dla agencji wywiadowczych, wzywając do zachowania ostrożności podczas korzystania z tych platform do przesyłania poufnych wiadomości.

Wypowiedź Peskowa podczas Wschodniego Forum Ekonomicznego we Władywostoku w Rosji w piątek 5 września pojawiła się w kontekście nasilonych napięć związanych z aresztowaniem Pawła Durowa, założyciela aplikacji do przesyłania wiadomości Telegram, oraz szerszych implikacji dla prywatności cyfrowej i bezpieczeństwa narodowego. Aresztowanie Durowa wywołało globalną debatę na temat równowagi między bezpieczeństwem narodowym a prywatnością cyfrową.

Durow, zagorzały zwolennik szyfrowanej komunikacji, został zatrzymany pod zarzutem ułatwiania nielegalnej działalności za pośrednictwem swojej platformy. Jednak brak istotnych dowodów doprowadził do oskarżeń ze strony rosyjskich władz o nadmierną ingerencję.

Peskow ostrzegł prezydenta Francji Emmanuela Macrona przed wysuwaniem bezpodstawnych oskarżeń wobec założyciela Telegramu. „Musi on przedstawić solidne dowody, aby uniknąć oskarżeń o naruszanie wolności komunikacji" – stwierdził rzecznik. Ostrzeżenie to podkreśla stanowisko Kremla, że

wszelkie zarzuty wobec Durowa muszą być poparte istotnymi dowodami, aby nie podważać zasad wolności słowa i prywatności.

Przejrzystość i ryzyko związane z komunikacją elektroniczną

Szersze przesłanie Peskowa było jasne: wszystkie aplikacje do przesyłania wiadomości są narażone na inwigilację przez agencje wywiadowcze. „Osoby, które z nich korzystają, powinny zrozumieć, że są one przejrzyste… dla służb bezpieczeństwa" – podkreślił. Według Peskowa ta przejrzystość stwarza poważne ryzyko – zwłaszcza gdy za pośrednictwem tych platform udostępniane są poufne dane rządowe lub handlowe.

Obawy Kremla nie są bezpodstawne. Rosyjskie służby bezpieczeństwa od dawna oskarżają Telegram i WhatsApp o stosowanie podwójnych standardów, odmawiając udostępniania danych rosyjskim władzom, a jednocześnie spełniając podobne prośby innych krajów. Anton Nemkin, członek komisji Dumy Państwowej ds. polityki informacyjnej i technologii, posunął się nawet do nazwania obecności WhatsApp w Rosji „zalegalizowanym naruszeniem bezpieczeństwa narodowego" w lipcu.

W odpowiedzi na te obawy rosyjski rząd opowiada się za stworzeniem krajowej platformy komunikacyjnej. Posunięcie to jest postrzegane jako „próba złagodzenia ryzyka związanego z aplikacjami zagranicznymi, które są postrzegane jako potencjalne narzędzia dla zagranicznych służb wywiadowczych" – wyjaśnia Enoch z *Brighteon.AI*.

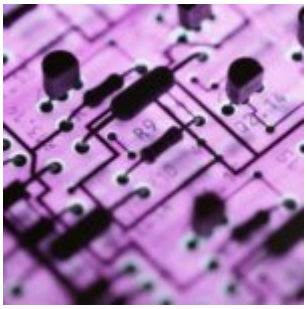
Rosyjskie organy ścigania wyraziły szczególne zaniepokojenie wykorzystaniem WhatsApp i Telegram przez ukraiński wywiad i inne złośliwe podmioty. Twierdzą oni, że platformy te są często wykorzystywane do rekrutacji agentów lub identyfikacji celów w Rosji, wykorzystując bazy danych zawierające dane osobowe uzyskane za pośrednictwem tych aplikacji.

Obecna debata na temat przejrzystości i nadzoru aplikacji do przesyłania wiadomości nie jest nowa. Historia prywatności cyfrowej naznaczona jest serią głośnych incydentów, które ukształtowały postrzeganie społeczne i politykę. Na początku 2010 r. ujawnienia Edwarda Snowdena dotyczące zakresu nadzoru NSA sprawiły, że kwestia prywatności cyfrowej znalazła się na pierwszym planie globalnej debaty.

Niedawno kontrowersje wokół próby zmuszenia Apple przez rząd USA do odblokowania iPhone'a używanego przez terrorystę w 2020 r. uwypukliły trwające napięcie między prywatnością a bezpieczeństwem. Ostrzeżenie rządu USA skierowane do wysokich urzędników w grudniu 2024 r. dotyczące przejścia na szyfrowaną komunikację po naruszeniu bezpieczeństwa dodatkowo podkreśla utrzymujące się wyzwania związane z zabezpieczeniem komunikacji cyfrowej.

W trakcie trwającej debaty na temat przejrzystości aplikacji do przesyłania wiadomości ostrzeżenie Peskowa przypomina o nieodłącznym ryzyku związanym z komunikacją elektroniczną. Chociaż rozwój krajowych platform do przesyłania wiadomości może stanowić tymczasowe rozwiązanie, szerszym wyzwaniem jest znalezienie równowagi między potrzebą bezpieczeństwa a prawem do prywatności.

Jak przełomowa konstrukcja chipa może zrekompensować zapotrzebowanie AI na energię



Sztuczna inteligencja rozwija się szybciej, niż większość z nas jest w stanie nadążyć, ale jej zapotrzebowanie na energię grozi zahamowaniem postępu. Teraz naukowcy z Uniwersytetu Florydy przedstawili radykalne rozwiązanie – chip, który **wykorzystuje światło do znacznego zmniejszenia zużycia energii**, jednocześnie zwiększając możliwości sztucznej inteligencji w zakresie wyszukiwania wzorców. Ta innowacja może zmienić wszystko, od aplikacji na smartfony po globalne centra danych, oferując ratunek dla przeciążonych sieci energetycznych i krok w kierunku bardziej zrównoważonej sztucznej inteligencji.

Najważniejsze punkty:

- Nowy krzemowy chip fotoniczny wykonuje obliczenia AI przy użyciu światła, zmniejszając zużycie energii nawet 100-krotnie w porównaniu z tradycyjną elektroniką.
- Chip doskonale radzi sobie z konwolucjami – podstawowym zadaniem AI polegającym na rozpoznawaniu wzorców w obrazach, filmach i tekście – osiągając 98-procentową dokładność w testach.
- Miniaturowe soczewki Fresnela, cieńsze niż ludzki włos, są wytrawiane na chipie, aby natychmiast przekształcać dane zakodowane laserowo.
- System może przetwarzać wiele strumieni danych jednocześnie, wykorzystując różne długości fal światła, co zwiększa wydajność.
- Eksperci przewidują, że technologia ta wkrótce stanie się standardem w sprzęcie AI, umożliwiając szybsze i bardziej ekologiczne uczenie maszynowe.

Światło kontra energia elektryczna: wyścig o zrównoważone zasilanie AI

Wraz z rozwojem modeli AI stają się one coraz bardziej „głodne” – zużywają energię elektryczną w tempie, które niepokoi ekspertów ds. energii. Centra danych zużywają już więcej energii niż niektóre małe kraje, a prognozy sugerują, że zapotrzebowanie AI może wkrótce przewyższyć podaż. Tradycyjne chipy, oparte na kilkudziesięcioletniej technologii tranzystorowej, osiągają fizyczne granice. Jednak obliczenia oparte na świetle oferują wyjście z tej sytuacji.

Zespół Uniwersytetu Florydy, kierowany przez eksperta w dziedzinie fotoniki półprzewodnikowej Volkera Sorgera, całkowicie pominął konwencjonalną elektronikę w przypadku jednego z najbardziej wymagających zadań AI: splotów. Te operacje matematyczne pozwalają sztucznej inteligencji identyfikować twarze na zdjęciach, tłumaczyć języki, a nawet diagnozować wyniki badań medycznych. Dzięki kodowaniu danych w świetle laserowym i przepuszczaniu ich przez mikroskopijne soczewki na chipie, system wykonuje te obliczenia niemal bez wysiłku.

„Wykonywanie kluczowych obliczeń związanych z uczeniem maszynowym przy niemal zerowym zużyciu energii stanowi ogromny krok naprzód dla przyszłych systemów sztucznej inteligencji” – powiedział Sorger. „Ma to kluczowe znaczenie dla dalszego zwiększania możliwości sztucznej inteligencji w nadchodzących latach”.

Jak działa chip – i dlaczego zmienia zasady gry

Sercem tego przełomowego rozwiązania są soczewki Fresnela – płaskie, ultraprecyzyjne elementy optyczne wygrawerowane bezpośrednio na krzemie. Gdy dane są przekształcane w światło

laserowe, soczewki te manipulują nimi jak cyfrowy magik, wykonując konwolucje w ułamku czasu i energii wymaganej przez chipy elektroniczne. Efekt? System, który klasyfikuje odręczne cyfry z niemal idealną dokładnością, zużywając przy tym niewiele energii.

Jeszcze bardziej imponująca jest zdolność chipa do wykonywania wielu zadań jednocześnie. Dzięki zastosowaniu laserów o różnych kolorach (multipleksowanie długości fal) przetwarza on wiele strumieni danych jednocześnie – podobnie jak autostrada, na której każdy pas ruchu obsługuje oddzielną komunikację bez zakłóceń. Technika ta może pozwolić przyszłym systemom sztucznej inteligencji na jednoczesną analizę obrazu, dźwięku i tekstu bez większego wysiłku.

Hangbo Yang, współautor badania, podkreślił tę zaletę: „Możemy mieć wiele długości fal lub kolorów światła przechodzących przez soczewkę w tym samym czasie. To kluczowa zaleta fotoniki”.

Przyszłość: optyczna sztuczna inteligencja w Twojej kieszeni

Konsekwencje są ogromne. Jeśli chipy AI oparte na świetle zostaną powszechnie przyjęte, mogą one zmniejszyć ślad węglowy centrów danych, wydłużyć żywotność baterii w urządzeniach mobilnych i umożliwić stosowanie aplikacji AI w czasie rzeczywistym, które wcześniej były uważane za zbyt energochłonne. NVIDIA i inni producenci chipów już stosują komponenty optyczne w niektórych systemach, ułatwiając integrację.

Sorger przewiduje, że w niedalekiej przyszłości „optyka oparta na chipach stanie się kluczowym elementem każdego chipa AI, z którego korzystamy na co dzień”. Przyszłość ta może nadejść szybciej niż się spodziewamy – naukowcy już pracują nad skalowaniem tej technologii do użytku komercyjnego.

Na razie prototyp stanowi dowód, że AI nie musi być energochłonna. Dzięki światłu jako sprzymierzeńcowi, następna generacja uczenia maszynowego może świecić jaśniej niż kiedykolwiek.