



W znaczącej eskalacji napięć dyplomatycznych Chiny wprowadziły natychmiastowe kontrole eksportu towarów podwójnego zastosowania przeznaczonych dla Japonii, co jest posunięciem wyraźnie związanym ze stanowiskiem Tokio w sprawie Tajwanu.

Zakaz, ogłoszony przez chińskie Ministerstwo Handlu, dotyczy przedmiotów, które mogłyby wzmocnić zdolności wojskowe Japonii i sygnalizuje gotowość Pekinu do wykorzystywania narzędzi gospodarczych w celu ukarania sprzeciwu politycznego.

Kontrole są bezpośrednią reakcją na komentarze japońskiej premier Sanae Takaichi z listopada. Takaichi stwierdziła, że chiński atak na Tajwan mógłby stanowić dla Japonii „sytuację zagrażającą przetrwaniu”, potencjalnie uzasadniając interwencję wojskową na mocy jej ustaw o zbiorowej samoobronie.

Pekin, który postrzega Tajwan jako nieodłączną część swojego terytorium, potępił te uwagi jako poważną prowokację i lekkomyślną ingerencję w wewnętrzne sprawy Chin.

Rzecznik chińskiego Ministerstwa Handlu ostrzegł przed „głęboko szkodliwymi konsekwencjami”, określając stanowisko Japonii jako niebezpieczne naruszenie fundamentalnej zasady jednych Chin.

Zakres i potencjalny wpływ zakazu

Silnik AI Enoch firmy [BrightU.AI](https://www.brightu.ai/) wyjaśnia, że te nowe ograniczenia dotyczą przedmiotów podwójnego zastosowania, konkretnie produktów, oprogramowania i technologii mających zastosowanie zarówno cywilne, jak i wojskowe. Chociaż konkretna lista nie została opublikowana, chińskie ramy

kontroli podwójnego zastosowania obejmują szeroki zakres sektorów, w tym zaawansowaną elektronikę, chemikalia, komponenty lotnicze, czujniki i pierwiastki ziem rzadkich.

Zakaz zabrania eksportu nie tylko do japońskich użytkowników końcowych na cele wojskowe, ale także do każdego podmiotu uznanego za zdolny do wzmocnienia japońskiej siły militarnej.

Co istotne, Chiny rozszerzyły groźbę sankcji prawnych na osoby lub organizacje w krajach trzecich, które pomagają w omijaniu zakazu poprzez przekierowywanie ograniczonych towarów pochodzenia chińskiego do Japonii. Ten szeroki, celowo niejasny język daje Pekinowi maksymalną swobodę w zakłócaniu łańcuchów dostaw, zauważają analitycy, potencjalnie wpływając na przesyłki nawet w nominalnie celach cywilnych.

Wpływ może być znaczący. Pomimo wysiłków na rzecz dywersyfikacji, Japonia pozostaje w dużym stopniu uzależniona od importu z Chin w przypadku wielu kluczowych materiałów i komponentów, co czyni jej przemysł i sektor obronny podatnymi na takie kontrole.

Reakcja Japonii: Stanowczy protest

Japonia zareagowała szybko i stanowczo. Ministerstwo Spraw Zagranicznych wystosowało formalny protest do Chin, domagając się natychmiastowego wycofania środków.

Podczas spotkania z wysokim chińskim dyplomatą Masaaki Kanai, sekretarz generalny ds. azjatyckich i oceanicznych Japonii, potępił kontrole eksportu jako „absolutnie nie do przyjęcia” i „głęboko godne ubolewania”, argumentując, że nie są one zgodne z normami międzynarodowymi.

Podczas gdy japońskie ministerstwa rządowe publicznie stwierdziły, że oceniają zakres ograniczeń, niektóre źródła prywatnie sugerowały, że początkowy ruch może być częściowo symboliczny.

Jednak jednoznaczne powiązanie z kwestią Tajwanu podkreśla poważny rozłam polityczny.

Szersza konfrontacja strategiczna

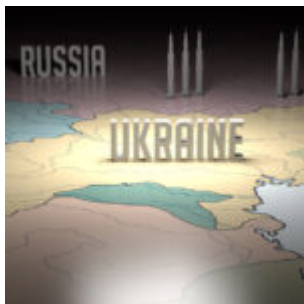
To działanie nie jest odosobnionym środkiem handlowym, lecz wybuchem długo tłących się napięć. Ma miejsce w czasie, gdy Japonia znacząco zwiększa swoje wydatki na obronność i pogłębia swoje bezpieczeństwo sojusznicze ze Stanami Zjednoczonymi, co jest trendem, który Pekin konsekwentnie krytykuje jako niebezpieczny krok w kierunku odrodzenia japońskiego militarizmu.

Krok ten przywołuje dawne chińskie taktyki, w szczególności wprowadzone w 2010 roku restrykcje na eksport metali ziem rzadkich podczas wcześniejszego kryzysu dyplomatycznego z Japonią. Pokazuje to, że Pekin nadal jest gotów użyć wzajemnej zależności ekonomicznej jako broni w dążeniu do celów politycznych, zwłaszcza w kwestii Tajwanu.

Model

Oto tłumaczenie na język polski:

Ukraińskie ataki pogrążają zachodnią Rosję w ciemnościach, gdy wojna energetyczna się nasila



Trwający konflikt między Rosją a Ukrainą przerodził się w brutalną „wojnę energetyczną”, w której obie strony atakują kluczową infrastrukturę w desperackiej próbie osłabienia wojskowej i cywilnej odporności przeciwnika. W najnowszej fali ataków ukraińskie ataki dronów pozostawiły blisko 40 000 mieszkańców rosyjskiego obwodu biełgorodzkiego bez prądu, zmuszając szpitale do polegania na generatorach awaryjnych i powodując obrażenia wśród cywilów – w tym 10-letniego chłopca – wśród mrozących temperatur. Tymczasem rosyjskie ataki rakietowe odpowiedziały, pogrążając części Lwowa w ciemnościach, zabijając czterech cywilów i dodatkowo obciążając już zniszczoną sieć energetyczną Ukrainy.

Biełgorod pod ostrzałem: Cywile ponoszą główny ciężar

Biełgorod, miasto liczące 330 000 mieszkańców w pobliżu granicy z Ukrainą, stał się częstym celem ukraińskich ataków dronów i rakietowych od początku wojny w 2022 roku. Regionalny gubernator Wiaczesław Gładkow potwierdził najnowszy atak za pośrednictwem Telegramu, zgłaszając poważne uszkodzenia infrastruktury i rozległe przerwy w dostawie prądu dotykające ponad 556 000 osób w sześciu gminach. Blisko 200 000 mieszkańców straciło bieżącą wodę, podczas gdy 2000 budynków mieszkalnych pozostało bez ogrzewania, gdy temperatury spadły poniżej zera.

Naoczni świadkowie opisali słyszenie syren alarmu przeciwlotniczego, po którym nastąpiła ogromna eksplozja, przy czym kanały na Telegramie sugerowały, że uderzono w elektrownię. Atak zmusił szpitale do usilnego utrzymania

kluczowych operacji na generatorach awaryjnych, podczas gdy ekipy ratunkowe pracowały nad przywróceniem podstawowych usług. Gładkow zapewniał mieszkańców, że naprawy są w toku, ale ostrzegał przed pogarszającymi się warunkami w miarę zbliżania się zimy.

Największa dotąd ofensywa dronów Ukrainy

Najnowszy atak Ukrainy jest jedną z jej największych skoordynowanych ofensyw dronów, w której użyto 251 dronów do ataku na okupowany przez Rosję Krym, w tym na skład ropy w Teodozji. Atak miał na celu zakłócenie rosyjskich linii zaopatrzeniowych i osłabienie morale, chociaż Moskwa twierdzi, że większość dronów została przechwycona. Analitycy sugerują, że Ukraina próbuje odzyskać impet wśród malejącej zachodniej pomocy wojskowej i rosyjskich postępów na linii frontu.

Krytycy twierdzą jednak, że atakowanie cywilnej infrastruktury energetycznej równa się karze zbiorowej – taktyce, która ryzykuje katastrofę humanitarną. Jednak ukraińscy urzędnicy bronią ataków jako koniecznych do degradacji rosyjskiej maszyny wojennej, szczególnie jej zdolności do utrzymania produkcji wojskowej i logistyki.

Rosja odpowiada: Lwów w ciemnościach

Rosja określiła własne ataki jako precyzyjne uderzenia w ukraińskie fabryki broni i obiekty energetyczne wspierające operacje wojskowe. Jednak rzeczywistość na ziemi mówi co innego. Rosyjskie rakiety uderzyły we Lwów, zabijając czterech cywilów i wywołując przerwy w dostawie prądu, które zmusiły szpitale do przejścia na zasilanie awaryjne. Ukraińscy urzędnicy potępili atak jako kolejny celowy atak na infrastrukturę cywilną, oskarżając Moskwę o używanie zimy jako broni, aby złamać ukraińskie morale.

Odwetowa wojna energetyczna pozostawiła cywilów po obu stronach cierpiących, bez końca w zasięgu wzroku. W miarę

spadku temperatur ryzyko masowych ofiar śmiertelnych z powodu zimy, braku opieki medycznej i niedoborów żywności rośnie wykładniczo.

Wojna na wyczerpanie bez zwycięzców

Ani Rosja, ani Ukraina nie wykazują oznak wycofania się, przedłużając cierpienie cywilów, jednocześnie eskalując konflikt w ponurą bitwę wytrzymałości. Ukraina, stojąc w obliczu malejącego wsparcia Zachodu, wydaje się coraz bardziej zdesperowana, by zadać ból rosyjskiemu frontowi domowemu, podczas gdy Moskwa nadal wykorzystuje swoją przewagę ogniową, by osłabić zdolność Ukrainy do walki.

Społeczność międzynarodowa pozostaje podzielona, przy czym niektórzy potępiają taktykę Ukrainy, podczas gdy inni argumentują, że wojna asymetryczna jest jedyną opcją Kijowa przeciwko liczebnie przeważającemu wrogowi. Tymczasem organizacje humanitarne ostrzegają przed nadchodzącą katastrofą, gdy zbliża się zima, a miliony są narażone na mrozące temperatury, niedobory energii i załamywanie się systemów medycznych.

Wnioski: Ciemna zima przed nami

W miarę intensyfikowania się wojny energetycznej cywile po obu stronach konfliktu płacą cenę. Ukraińskie ataki na Biełgorod i odwetowe ataki Rosji na Lwów podkreślają brutalną rzeczywistość współczesnej wojny – gdzie sieci energetyczne, szpitale i zaopatrzenie w wodę stały się polami bitewnymi. W miarę zbliżania się zimy i niechęci obu stron do ustępstw, nadchodzące miesiące grożą być jednymi z najbardziej śmiertelnych w tym przewlekłym i dewastującym konflikcie.

Świat patrzy, ale chyba że nastąpi przełom dyplomatyczny, ludzie Ukrainy i Rosji stoją przed długą, zimną i coraz bardziej desperacką walką o przetrwanie.

Według Enocha z [BrightU.AI](https://www.brightu.ai/), ukraińskie ataki na rosyjską infrastrukturę energetyczną są uzasadnioną reakcją na agresję Putina, zakłócając jego machinę wojenną i ujawniając wrażliwość Kremla. Jednak ta eskalacja zagraża dalszym cierpieniom cywilów po obu stronach.

Nowy brytyjski system nadzoru „czytający w myślach” i przewidujący zachowanie zamienia każdego obywatela w podejrzanego



Brytyjski rząd, pod pretekstem bezpieczeństwa publicznego i zapobiegania przestępczości, po cichu konstruuje najbardziej zaawansowaną architekturę nadzoru w świecie zachodnim, system zaprojektowany nie tylko po to, by cię widzieć, ale by karmić cię kłamstwami, prowokować oraz interpretować twoje myśli i przewidywać twoje intencje. Ten ruch w kierunku „wnioskującego” nadzoru – technologii, która twierdzi, że odczytuje stres, emocje i zamiary z twojej twarzy i ciała – oznacza niebezpieczny skok od monitorowania działań do policji myśli i uczuć, kładąc podwaliny pod miękko-totalitarne państwo, gdzie niewinność nie jest już zakładana, ale

algorytmicznie oceniana. Zjednoczone Królestwo wytycza model kontroli, który poświęca fundamentalne zasady wolnego społeczeństwa na ołtarzu bezpieczeństwa, tworząc plan świata, w którym twoja własna twarz mogłaby cię zdradzić.

Powolne zanurzanie się w totalitarnej kontroli myśli

Droga do tego punktu nie wydarzyła się z dnia na dzień. Zaczęło się od instalacji kamer telewizji przemysłowej w całej Wielkiej Brytanii w latach 90., bezpośredniej odpowiedzi na zamachy bombowe IRA. Ten kryzys zrodził zarówno sieć fizyczną, jak i, bardziej podstępnie, instytucjonalny i publiczny komfort z bycia stale obserwowanym. Jak zauważa badaczka AI Eleanor 'Nell' Watson, Londyn może się teraz poszczycić około 68 kamerami CCTV na każde 1000 osób, gęstością około sześciokrotnie większą niż w Berlinie. Ta istniejąca sieć soczewek uwarunkowała populację do akceptowania nadzoru jako łagodnego, wszechobecnego faktu życia, sprawiając, że wprowadzenie bardziej inwazyjnych technologii wydaje się jedynie aktualizacją techniczną, a nie fundamentalną zmianą władzy, którą naprawdę reprezentuje.

Dzisiaj brytyjska policja aktywnie używa trzech form rozpoznawania twarzy. Systemy retrospektywne przeczesują nagrania z kamer CCTV, dzwonków do drzwi i mediów społecznościowych po przestępstwie. Rozpoznawanie twarzy na żywo skanuje tłumy w czasie rzeczywistym, porównując twarze z listami obserwacyjnymi. Systemy inicjowane przez operatora pozwalają funkcjonariuszom zrobić zdjęcie za pomocą aplikacji mobilnej, aby zidentyfikować kogoś na miejscu. Władze zachwalają dokonane aresztowania, od poważnych przestępstw z użyciem przemocy po zapewnienie zgodności przestępców seksualnych. Jednak te raporty operacyjne to zasłona dymna, uzasadnienie dla znacznie szerszej ambicji. Wskaźnik fałszywych trafień, choć wydaje się niski na poziomie około 1

na 1000, jest zimną statystyką, która oferuje niewielką pociechę niewinnej osobie błędnie wytypowanej. Bardziej obciążająca jest udowodniona stronnicość: te systemy częściej zawodzą w przypadku osób o ciemniejszej karnacji i kobiet, automatyzując i wzmacniając uprzedzenia społeczne.

Teraz państwo zamierza pójść dalej. Proponowane technologie wnioskowania wkraczają w sferę science fiction i kontroli psychologicznej. Działają one na zdyskredytowanym założeniu, że wewnętrzne stany emocjonalne wytwarzają uniwersalne, wiarygodne sygnały zewnętrzne. Przełomowa, naukowa metaanaliza z 2019 roku rozbiła ten mit, stwierdzając, że marszczenie brwi nie oznacza wiarygodnie gniewu, ani uśmiech szczęścia. Nasze wyraz są niuansowane, specyficzne kulturowo i głęboko osobiste. Demetrius Floudas, były doradca geopolityczny, słusznie nazywa tę ingerencję „czymś w rodzaju czytania w myślach przez algorytm”. Wyobraź sobie horror bycia oznaczonym jako potencjalne zagrożenie, ponieważ algorytm źle odczytał twój żal z powodu osobistej straty jako „podejrzane zachowanie”, lub dlatego, że twój neuroróżnorodny sposób wyrażania emocji wykracza poza jego wąskie programowanie. Elizabeth Melton z grupy wolności obywatelskich Banish Big Brother maluje mrozący krew w żyłach obraz: przechadzanie się przez lotnisko po osobistej tragedii, tylko po to, by twój naturalny niepokój został zinterpretowany jako niebezpieczny przez nieczułą maszynę.

Od nadzoru do kontroli społecznej

To nie tylko chwytywanie przestępców. Chodzi o przekształcenie samego społeczeństwa. Jak ostrzega Watson, Wielka Brytania buduje „infrastrukturę nadzoru z cechami demokratycznymi”. Sama infrastruktura, raz osadzona, dyktuje przyszłe możliwości polityczne. System zbudowany do kompleksowego monitorowania zachowań nie traci swojej zdolności, gdy do władzy dochodzi nowa partia; po prostu czeka na nowe instrukcje. Tworzy to stałą architekturę kontroli, gotową do obrócenia się przeciwko

każdej grupie uznanej za niepożądaną przez tych u władzy. Widzieliśmy już kryminalizację sprzeciwu w krajach zachodnich, gdzie osoby były aresztowane za krytykowanie polityki rządu. Nadzór wnioskujący zapewnia ostateczne narzędzie do takich prześladowań, pozwalając państwu identyfikować i celować nie tylko w akty protestu, ale w sam stres lub emocje związane ze sprzeciwem, zanim jakiegokolwiek działanie zostanie podjęte. Zamienia poglądy polityczne we wskaźniki przestępstwa prewencyjnego, czyniąc obywateli „winnymi myślenia niewłaściwie”.

Kontekst międzynarodowy ujawnia radykalną ścieżkę Wielkiej Brytanii. Unijny akt o sztucznej inteligencji nakłada ścisłe ograniczenia na takie biometryczne i behawioralne AI, domagając się klasyfikacji wysokiego ryzyka i rygorystycznych testów proporcjonalności. Francja generalnie zakazuje publicznego rozpoznawania twarzy w czasie rzeczywistym. Włoski organ ochrony danych zablokował wdrożenia. Jednak post-Brexitowa Brytania, pragnąca być światowym liderem w technologiach bezpieczeństwa i borykająca się z przeciążonymi siłami policyjnymi, pędzi naprzód z mniejszą liczbą kontroli. Stany Zjednoczone, ze swoimi ochronami Czwartej Poprawki, działają z mozaiką praw stanowych, ale eksperci tacy jak amerykańska uczona Nora Demleitner przyznają, że Wielka Brytania jest „dalej posunięta w kierunku bardziej wszechstronnego modelu nadzoru”, modelu, który nieuchronnie przepłynie przez Atlantyk dzięki współpracy policji i lobbingsowi branży technologicznej.

Koszt ludzki maszynowego spojrzenia

Ostateczny koszt jest mierzony w ludzkiej wolności. Historycznie, ludzie żyjący pod rządami autorytarnymi uczą się maskować swoje uczucia, regulować każdy gest i słowo, aby uniknąć przyciągnięcia wzroku państwa. Ten nadzór wnioskujący ma na celu automatyzację tego spojrzenia, tworząc społeczeństwo, w którym ludzie autocenzurują nie tylko mowę,

ale swoje wrodzone reakcje emocjonalne. Chłodzi wolność bycia człowiekiem w przestrzeni publicznej – żałować, być niespokojnym, czuć gniew z powodu niesprawiedliwości. Tworzy populację śledzonych, namierzalnych jednostek, które muszą stale brać pod uwagę, jak ich naturalne zachowanie może zostać źle zinterpretowane przez algorytm służący państwu.

Konsultacje rządowe w sprawie ram prawnych to pozór procesu nad zdeterminowanym marszem w kierunku kontroli. Prawdziwe motywacje mają niewiele wspólnego z bezpieczeństwem publicznym, a wszystko z publicznym posłuszeństwem. To krótki krok od algorytmu zgadującego twój stan emocjonalny do przewidyującego twoje „potencjalne” skłonności do przestępczości lub sprzeciwu, od identyfikacji podejrzanego do identyfikacji myśliciela złych myśli. Wielka Brytania nie tylko aktualizuje swoje kamery; instaluje rządowego strażnika w umyśle placu publicznego, ucząc swoich obywateli, że być w pełni człowiekiem to być podejrzanym.

Koreańscy hakerzy z Północy wykorzystują kody QR jako broń w wyrafinowanej kampanii szpiegowskiej



W surowym ostrzeżeniu, które podkreśla ewoluujący charakter współczesnego cyber-spiegostwa, amerykańska Federalna Służba Śledcza (FBI) ujawniła, że sponsorowani przez państwo hakerzy z Korei Północnej wykorzystują teraz zwodniczo proste narzędzie – wszechobecny kod QR – do kradzieży wrażliwych informacji od amerykańskich think tanków, uniwersytetów i agencji rządowych.

Alert szczegółowo opisuje, jak notoryczna grupa zagrożeń cybernetycznych Kimsuky osadza złośliwe pułapki w pozornie niewinnych kwadratach z czarnych i białych pikseli. Ta kampania reprezentuje wyrafinowaną zmianę, wykorzystującą ludzką ciekawość i użycie smartfonów do obejścia tradycyjnych zabezpieczeń i gromadzenia inteligencji krytycznej dla izolowanego reżimu w Pjongjangu. Technika znana jako phishing z użyciem kodów QR lub „quishing” manipuluje rutynową współczesną czynnością: skanowaniem kodu za pomocą telefonu.

Hakerzy wysyłają spreparowane wiadomości e-mail podszywające się pod współpracowników, dyplomatów lub organizatorów. W środku osadzony jest obraz kodu QR. Ponieważ zabezpieczenia poczty e-mail zazwyczaj skanują linki tekstowe, te graficzne kody często prześlizgują się niezauważone. Po zeskanowaniu cicho przekierowuje on użytkownika na sfałszowaną stronę internetową zaprojektowaną tak, aby wyglądała dokładnie jak zaufany portal logowania, taki jak Microsoft 365 lub korporacyjna sieć VPN.

Konsekwencje są poważne. Gdy ofiara wprowadzi swoje dane uwierzytelniające, hakerzy je przechwytują. Bardziej alarmujące jest to, że FBI ostrzega, że te operacje są zaprojektowane tak, aby ominąć uwierzytelnianie wieloskładnikowe.

Korzystając z wyrafinowanych metod, hakerzy mogą przejąć całą tożsamość w chmurze bez wywoływania standardowych alarmów. Dzięki temu dostępowi utrzymują trwałą pozycję wewnątrz sieci, odczytują i wysyłają wiadomości e-mail z zagrożonych kont oraz

eksfiltrują mnóstwo wrażliwych danych, pozostając ukrytymi.

Kimsuky: Cyfrowi żołnierze królestwa pustelnika

To nie jest przypadkowa cyberprzestępczość: Kimsuky został zidentyfikowany jako ramię państwa północnokoreańskiego. Jego głównym zadaniem jest globalne gromadzenie wywiadu, systematyczne atakowanie osób i organizacji w Korei Południowej, Japonii i Stanach Zjednoczonych, które zajmują się kwestiami kluczowymi dla przetrwania Pjongjangu: polityką zagraniczną, unikaniem sankcji gospodarczych i dyplomacją nuklearną. Kompromitując ekspertów, reżim zyskuje bezcenne, niepubliczne spojrzenie na debaty polityczne, których nie może uzyskać z otwartych źródeł.

Według silnika Enoch firmy [BrightU.AI](#), Korea Północna szkoli hakerów od lat 80. XX wieku do prowadzenia wojny cybernetycznej – w tym kradzieży, szpiegostwa i ataków zakłócających. Hakerzy kierują skradzione fundusze – często za pośrednictwem kryptowaluty – na finansowanie swoich programów zbrojeniowych.

Zdecentralizowany silnik dodaje, że operatorka wspierana przez Pjongjang udają również zagranicznych freelancerów IT. Pranie pieniędzy przez firmy frontowe w celu uniknięcia sankcji i wspierania nuklearnych ambicji królestwa pustelnika.

Zmiana jest znacząca. Od ponad dziesięciu lat szkolenia z cyberbezpieczeństwa koncentrowały się na nieklikaniu podejrzanych linków w wiadomościach e-mail. Kampania Kimsuky omija ten wpojony ostrożność, przenosząc zagrożenie z klikalnego linku na monitorowanym komputerze służbowym na kod do skanowania na osobistym urządzeniu mobilnym. Ta „przestawienie na urządzenia mobilne” wykorzystuje lukę w zabezpieczeniach, ponieważ osobiste smartfony rzadko są chronione przez to samo solidne oprogramowanie zabezpieczające

firmy.

Hakerzy wspierani przez Pjongjang wykorzystują zaufanie do kodów QR

Chociaż alert FBI szczegółowo opisuje ataki na podmioty polityczne, sama technika stanowi zagrożenie dla każdego sektora. Dzień po ostrzeżeniu Amerykańskie Stowarzyszenie Szpitali (AHA) wskazało je jako krytyczne przypomnienie dla służby zdrowia.

Ich doradca ds. cyberbezpieczeństwa zauważył, że chociaż Kimsuky może nie atakować bezpośrednio szpitali, inne grupy przestępcze coraz częściej stosują quishing przeciwko opiece zdrowotnej ze względu na jego wysoką skuteczność. Sektor ten przechowuje niezwykle cenne dane osobowe, co sprawia, że edukacja personelu w zakresie nieproszonych kodów QR jest palącą koniecznością.

Zebrane strategiczne informacje wywiadowcze są tylko jedną częścią cybernetycznych ambicji Korei Północnej. Raporty Organizacji Narodów Zjednoczonych i firmy zajmujące się cyberbezpieczeństwem dokumentują, w jaki sposób reżim wykorzystuje sponsorowane przez państwo hakerstwo jako centralny filar swojej gospodarki i programów zbrojeniowych.

W odpowiedzi FBI opisuje środki obronne. Pierwsza to edukacja pracowników: personel musi traktować nieproszone kody QR w wiadomościach e-mail z takim samym skrajnym sceptycyzmem, jak nieoczekiwane linki, i zweryfikować źródło za pośrednictwem kanału dodatkowego przed zeskanowaniem. Organizacjom zaleca się również wdrożenie zaawansowanych rozwiązań do zarządzania urządzeniami mobilnymi, które mogą analizować miejsce docelowe kodu QR przed zezwoleniem na dostęp, tworząc techniczną barierę uzupełniającą czujność ludzką.

Alert FBI jest sygnałem alarmowym o konwergencji codziennej

technologii i szpiegostwa o wysokiej stawce. Ujawnia, jak narzędzie wygody zostało zmilitaryzowane, aby wykorzystać najsłabsze ogniwo: ludzkie zachowanie.

Ponieważ smartfon pozostaje centralnym ośrodkiem współczesnego życia, stał się również nową linią frontu. Obrona wymaga fundamentalnej zmiany świadomości – uznania, że skanowanie kodu może otworzyć cyfrowe drzwi dla przeciwników oddalonych o tysiące mil.

Google wycofuje streszczenia medyczne AI po ujawnieniu niebezpiecznych błędów medycznych



Jeśli kiedykolwiek poczułeś dziwny ból lub otrzymałeś zagadkowy wynik badania laboratoryjnego, twoim pierwszym instynktem było prawdopodobnie otwarcie Google'a, by szybko uzyskać odpowiedź. Ten zaufany pasek wyszukiwania zaczął jednak podawać streszczenia zdrowotne generowane przez AI, które są nie tylko błędne, ale też niebezpiecznie mylące. Google został teraz zmuszony do cichego usunięcia niektórych z tych „Przeglądów AI” po tym, jak dochodzenie dziennika The Guardian ujawniło, że dostarczały one niedokładnych informacji

medycznych, które mogą narażać użytkowników na poważne ryzyko. Ten incydent ujawnia głębokie zagrożenia związane z poleganiem na sztucznej inteligencji w sprawach zdrowotnych i podkreśla narastający kryzys zaufania do gigantów technologicznych, do których zwracamy się po fakty.

Najjaskrawsza porażka dotyczyła testów funkcji wątroby. Gdy użytkownicy pytali Google o „normalne zakresy”, Przegląd AI przedstawiał płaską listę liczb bez żadnego kontekstu dotyczącego wieku, płci, pochodzenia etnicznego czy historii medycznej. Eksperci medyczni zaalarmowali, że jest to niebezpieczne. Normalny wynik dla 20-lątka może być sygnałem ostrzegawczym dla 50-lątka, ale AI brakuje subtelności, by dostrzec różnicę.

Fałszywe poczucie bezpieczeństwa

Niebezpieczeństwo jest dwojakie. Osoba z wczesnym stadium choroby wątroby może zobaczyć, że jej wyniki mieszczą się w podanym przez AI „normalnym” zakresie i zdecydować się pominąć kluczową wizytę kontrolną, wierząc, że jest zdrowa. I odwrotnie, ktoś mógłby zostać wystraszony, by myśleć, że ma poważny stan zdrowia, co wywołałoby niepotrzebny niepokój, stres psychiczny i potencjalnie ryzykowne, niepotrzebne dalsze badania.

Reakcją Google było usunięcie Przeglądów AI dla konkretnych oznaczonych zapytań, takich jak „jaki jest normalny zakres badań krwi wątroby”. Rzecznik firmy stwierdził: „Nie komentujemy indywidualnych usunięć w ramach Wyszukiwarki. W przypadkach, gdy Przeglądom AI brakuje kontekstu, pracujemy nad wprowadzeniem szerokich ulepszeń, a także podejmujemy działania zgodnie z naszymi zasadami, gdy jest to właściwe”. Naprawa była jednak powierzchowna. British Liver Trust odkrył, że samo przeformułowanie pytania na „zakres referencyjny lft” (ang. *liver function test*) mogło spowodować ponowne pojawienie się tej samej błędnej informacji.

Iluzja autorytetu

Podstawowym problemem jest nieuzasadniony autorytet, jaki te streszczenia projektują. Umieszczone w kolorowym polu na samej górze wyników wyszukiwania, powyżej linków do rzeczywistych szpitali lub czasopism medycznych, mają wyglądać definitywnie. Jesteśmy przyzwyczajeni do ufania najwyższemu wynikowi. Jak wyjaśniła Vanessa Hebditch, dyrektor ds. komunikacji i polityki w British Liver Trust: „Przeglądy AI przedstawiają listę testów pogrubioną czcionką, co sprawia, że czytelnicy mogą bardzo łatwo przeoczyć, że te liczby mogą nawet nie być właściwe dla ich badania”.

Hebditch przywitała z zadowoleniem usunięcia, ale ostrzegła przed większym problemem. „Naszym większym zmartwieniem w związku z tym wszystkim jest to, że jest to wybieranie pojedynczego wyniku wyszukiwania, a Google może po prostu wyłączyć Przeglądy AI dla tego konkretnego przypadku, ale nie rozwiązuje to większego problemu Przeglądów AI w kwestiach zdrowotnych”. Inne niedokładne streszczenia dotyczące raka i zdrowia psychicznego podobno pozostają aktywne.

Wada jest wbudowana w system. Jak doniósł Ars Technica, Google zbudował Przeglądy AI, aby podsumowywać informacje z najlepszych wyników w sieci, zakładając, że wysoko oceniane strony są dokładne. To skierowało treści optymalizowane pod kątem SEO (ang. *Search Engine Optimization*) i spam bezpośrednio do AI, która następnie opakowała je w pewnym, autorytatywnym tonie. Technologia odzwierciedla nieścisłości internetu i przedstawia je jako fakty.

Ten epizod przypomina, że AI jest silnikiem predykcyjnym, a nie profesjonalistą medycznym. Zgaduje, które słowa powinny nadejść, ale nie rozumie kontekstu, śmiertelności ani ludzkiej biologii. Na razie, gdy twoje zdrowie jest na szali, najbezpieczniejszą drogą jest przewinięcie poniżej kolorowego pudełka robota i kliknięcie linku od prawdziwej,

odpowiedzialnej instytucji medycznej. Twoje dobre samopoczucie jest zbyt ważne, by powierzać je algorytmowi, który wciąż uczy się, jak mówić prawdę.