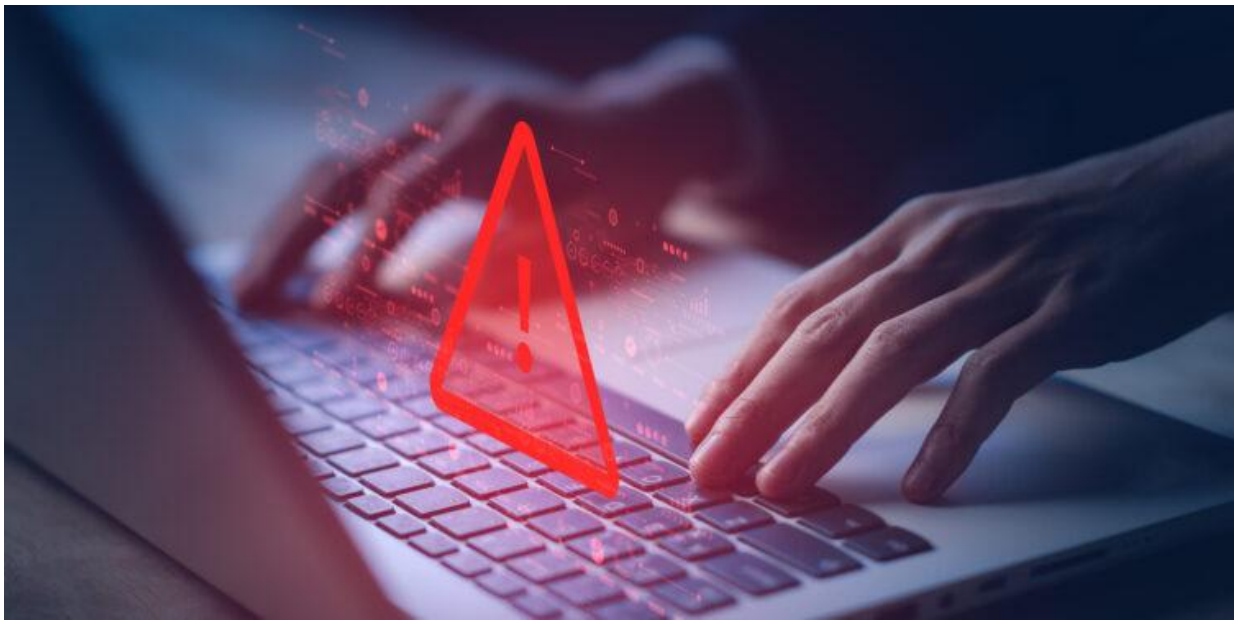
THE DAILY SCEPTIC
QUESTION EVERYTHING. STAY SANE. LIVE FREE.

Jak stworzyć Internet wolny od cenzury?

Autor Dr R P
16 sierpnia 2025 13:00



Liczba rejestracji VPN gwałtownie wzrosła w zeszłym miesiącu, przy czym niektórzy dostawcy odnotowali wzrost o 1400%, a VPN dla telefonów komórkowych zajęły najwyższe miejsca w sklepach z aplikacjami, ponieważ brytyjska opinia publiczna okazała pogardę dla nowego reżimu cenzury Internetu brytyjskiego rządu. Chociaż ustawa o bezpieczeństwie w Internecie została przegłosowana przez poprzedni, rzekomo konserwatywny rząd, jej główne symptomy pojawiły się w lipcu tego roku. Firmy zajmujące się mediami społecznościowymi zaczęły oznaczać wiekiem różne treści, z których wiele było całkowicie nieszkodliwych lub miało istotne znaczenie polityczne, w niebezpiecznym potencjalnym prekursorze cyfrowego systemu identyfikacji. Przypomnijmy, że obecny rząd prowadzi konsultacje w sprawie cyfrowego ID, których termin upływa 21 sierpnia. Brytyjczycy, nie chcąc tego, rzucili się do kupowania VPN.

Ministrowie Partii Pracy potępili korzystanie z VPN, jednocześnie ubiegając się o ich wydatki. Aby było jasne, podczas gdy korporacyjne i organizacyjne sieci VPN wykorzystują dokładnie tę samą technologię, co usługi antycenzorskie, fakt, że sekretarz ds. biznesu Jonathon Reynolds

ubiegał się o NordVPN, pokazuje, że kupował usługę - dostępnych jest również wiele innych - która pozwala użytkownikom ominąć cenzurę i uniknąć nadzoru ze strony ISP (dostawców usług internetowych). Jego korzystanie z VPN nie ograniczało się zatem do korzystania z hostowanej przez rząd sieci VPN w celu uzyskania dostępu do oficjalnych zasobów poza siedzibą firmy, tak jakby znajdował się w biurze.

Hipokryzją jest to, że apologeci inwigilacji używają narzędzi, których chcą odmówić wszystkim innym, ale nie mogę winić nikogo za to, że chce zachować swoje prywatne sprawy w tajemnicy. Potrzeba prywatności i anonimowości rzadko była silniejsza. W końcu, gdy komentuje się sprawy polityczne i używa słów jako "eleganckiej broni dla bardziej cywilizowanego wieku", istnieją wszelkie powody, dla których należy starać się ukryć pod pseudonimami i szyfrowanymi połączeniami, aby uniemożliwić rządom użycie "niezdarnej i przypadkowej" rzeczywistej broni - kijów i kamieni oraz łamania kości - w odpowiedzi na krytykę.

Warto zatem zastanowić się, dlaczego ustawa o bezpieczeństwie online może mieć tak destrukcyjny wpływ. Zdecydowanie można argumentować, że w przypadku wcześniejszych wersji Internetu nie byłoby to możliwe. Być może dlatego, że tak duża część internetu stała się teraz "pięcioma gigantycznymi stronami internetowymi, z których każda wypełniona jest zrzutami ekranu z pozostałych czterech", że zarządzenie rządowe w ogóle mogło wywołać taki skutek.

Wiele osób uważa VPN za magiczne rozwiązanie tej cenzury, ale wszystko, co robi VPN, to zapewnienie tunelu z ocenzurowanego kraju do wolnego. VPN przestaje pomagać, gdy nie ma już wolnych krajów. Sytuacja jest poważna w Kanadzie, Australii, Irlandii, Francji, Danii i UE. Szwajcaria jest w pewnym stopniu zagrożona, a groźby przeciwko wolności Internetu są nawet podejmowane przez rządy w krajach będących synonimami pandemii zdrowego rozsądku, takich jak Szwecja. Stany Zjednoczone również mogą być zagrożone. Nawet jeśli wolne kraje nadal istnieją, VPN nie rozwiązują wszystkich problemów. Zbyt wiele monopolistycznych mega-stron internetowych, zirytowanych tym, że VPN może odmówić im śledzenia informacji, które mogą sprzedać reklamodawcom, już teraz oferuje bardziej ograniczone wersje witryny użytkownikom odwiedzającym ze znanych adresów IP VPN. Usługi mediów społecznościowych często odmawiają tworzenia nowych kont dla użytkowników odwiedzających je za pośrednictwem VPN lub węzła wyjściowego Tor, lub wymagają weryfikacji SMS za pośrednictwem numeru telefonu, który mogą rozpoznać po prefiksie + (na przykład +44 dla Wielkiej Brytanii) jako znajdujący się w fizycznej lokalizacji użytkownika, a nie w lokalizacji VPN.

Internet został początkowo stworzony w celu uniknięcia pojedynczych punktów awarii - z założenia był zdecentralizowany. Obecnie 43% ruchu obejmuje usługi sieciowe należące do zaledwie sześciu firm, a doświadczenie internetowe niektórych osób składa się wyłącznie z tego, co serwują im media społecznościowe. Zadaniem cenzora staje się więc nie proces "walenia w mordę" polegający na próbie namierzenia setek tysięcy małych stron, ale po prostu zadzwonienie do głównej platformy i zażądanie usunięcia podejrzanych treści. Wczesnym "cypherpunkom" Internetu trudno byłoby sobie wyobrazić, że system zaprojektowany jako tak zdecentralizowany - choć jest mitem, że motywacją dla tego projektu było właśnie przetrwanie w wojnie nuklearnej - zostanie podzielony na terytoria niewielkiej liczby ogromnych korporacji.

Innymi ofiarami ustawy o bezpieczeństwie online są brytyjskie fora. Wiele z nich poczuło się na tyle zagrożonych uciążliwymi wymogami ustawy, że zamknęły się, zamiast ryzykować monumentalne grzywny. Mam szczerą nadzieję, że zachowały one kopie zapasowe historycznych postów, ponieważ, jak powiedziała nauczycielka Maureen O'Hara w dramacie o życiu pod okupacją podczas II wojny światowej This Land is Mine, strony, których cenzorzy domagają się wyrwania z podręczników, pewnego dnia zostaną wklejone z powrotem.

Zagrożenie wynikające z ustawy jest wiarygodne dla właścicieli forów, ponieważ obecna architektura Internetu nie robi prawie nic, aby ukryć własność stron internetowych. Anonimowe przeglądanie Internetu jest wystarczająco wykonalne - VPN i sieć Tor istnieją - ale anonimowe prowadzenie strony internetowej jest trudne. Strony internetowe potrzebują nazw domen, tożsamości bardziej zapamiętywalnych niż adresy IP serwerów i, w przeciwieństwie do adresów IP, niepodlegających zmianom w dowolnym momencie. Samo posiadanie nazwy domeny stawia nas na łasce rejestratorów, z których niektórzy będą próbowali bronić się przed rządowymi próbami odebrania domeny, ale niewielu z nich sprzeciwi się nakazowi sądowemu w dowolnym kraju, w którym mają siedzibę. Każdy, kto sprzeciwił się nakazowi usunięcia określonych domen, może zostać sparaliżowany przez rząd, który przejdzie do następnego etapu łańcucha i zagrozi właścicielowi domeny najwyższego poziomu, na którym polegał zbuntowany rejestrator. Konieczne jest również hostowanie witryny; polega to albo na tym, że ktoś płaci komercyjnej usłudze - ponownie punkt nacisku - za hostowanie witryny dla niego, albo na poświęceniu własnego komputera, aby służył jako host, a zatem musi utrzymywać go zasilanego, bezpiecznie aktualizowanego i podłączonego do Internetu przez cały czas, chyba że chce, aby jego witryna została wyłączona.

Tak więc nasza dyskusja przenosi się teraz do Tora. Pierwotnie opracowany przez US Naval Research Lab jako środek dla amerykańskich agentów za granicą do wysyłania wiadomości z powrotem do bazy, został udostępniony jako sposób na ukrycie się amerykańskich agentów w stogu siana użytkowników cywilnych. Organizacje medialne podsycające strach próbowały twierdzić, że użytkownicy VPN zostaną wciągnięci do ciemnej sieci, jednak oprócz tego, że Tor i VPN to różne technologie, nawet w ramach Tora zdecydowana większość (93,3% do 96,6%) danych przepływających przez sieć pochodzi od osób korzystających z Tora jako anonimowej trasy - skutecznie VPN w przypadku użycia, jeśli nie pod względem technicznym - do zwykłych stron internetowych z czystą siecią. Tylko od 3,4% do 6,7% użytkowników Tora uzyskuje dostęp do ciemnej sieci ukrytych usług domeny cebulowej. To właśnie w tej ciemnej sieci, jak twierdzą osoby siejące postrach, rezydują przestępcy, a przestępcze witryny cebulowe istnieją. W rzeczywistości jednak większość ciemnej sieci jest ledwo nawigowalna i istnieje bardzo niewielka motywacja dla stron, które twierdzą, że oferują nielegalne towary lub usługi, aby po prostu przyjmować płatności kryptowalutą, a następnie uciec z nią. Techniczna koncepcja usług cebulowych jest jednak interesująca.

W przeciwieństwie do zwykłego Internetu, usługi cebulowe są zaprojektowane tak, aby ukryć tożsamość serwera, a także umożliwić odwiedzającym anonimowość. Ta anonimowość nie jest idealna; zdarzały się przypadki usuwania anonimowości usług cebulowych poprzez korelację takich rzeczy, jak to, kiedy dana witryna cebulowa nie działała, z przerwami w dostawie prądu lub Internetu, nawet krótkotrwałymi, w obszarach geograficznych, w których może znajdować się serwer usługi. Większość witryn cebulowych wyłączonych w ten sposób to nikczemne usługi, które zasłużyły na wyłączenie, ale ponieważ może się to zdarzyć w przypadku takich usług, technicznie możliwe jest również śledzenie i wyłączanie w ten sam sposób usług moralnie

przyzwoitych. Domeny onion nie są bezbłędnym sposobem na anonimowe prowadzenie nieocenzurowanej strony internetowej; wystarczy zapytać Rossa Ulbrichta, uwięzionego w 2015 roku i niedawno ułaskawionego przez Trumpa. Donald Trump, rzecz jasna, nadal zwleka ze spełnieniem obietnicy swojego sojusznika, R.F. Kennedy'ego Jr. dotyczącej ułaskawienia bardziej zasłużonego Edwarda Snowdena.

Inną wielką wadą domen cebulowych jest to, że dostęp do nich wymaga pewnych umiejętności technicznych - niewielkich, ale wystarczających, aby ludzie, którzy znali komputery tylko w formie tabletów i telefonów, bez nawet prawdziwej struktury folderów, mogli mieć trudności z zainstalowaniem Tora i zweryfikowaniem jego podpisu cyfrowego. Oznacza to, że każda domena cebulowa - również bardzo trudna do reklamowania, ponieważ nie można jej indeksować w wyszukiwarkach - dotrze do znacznie mniejszej liczby odbiorców niż zwykła strona internetowa. Domeny cebulowe są również znacznie trudniejsze do skonfigurowania niż łatwość, z jaką ludzie, nieświadomi szkód, jakie wyrządza to ich prywatności, mogą zalogować się na stronie mediów społecznościowych i gorączkowo wpisywać swoje spontaniczne przemyślenia, aby cały świat mógł je zobaczyć.

Jak zatem wyglądałby idealny internet odporny na cenzurę? Nie znam wszystkich odpowiedzi, ale mogę wskazać trzy kluczowe problemy, spośród prawdopodobnie wielu innych, które musiałby przezwyciężyć.

- **Jak możemy uruchomić sieć bez polegania na scentralizowanych korporacjach w zakresie architektury fizycznej?** Od swoich najwcześniejszych wcieleń Internet zależał w warstwie fizycznej od sprzętu innych osób i było to w porządku, dopóki firmy telekomunikacyjne nie stały się celem nacisków ze strony państwa. Omówione do tej pory technologie - VPN, Tor, usługi cebulowe - zostały zaprojektowane tak, aby obejść ten podstawowy problem; kryptografia pozwala wiele osiągnąć pomimo scentralizowanej, skompromitowanej warstwy fizycznej. Jednak rządy, w swoich wysiłkach na rzecz stłumienia sprzeciwu, posuwają się obecnie naprzód na tak wielu frontach, że przeprojektowanie warstwy fizycznej - aby zrobić krok tak daleko do przodu, że cenzorzy nigdy nie będą mogli nadrobić zaległości - wydaje się jedyną nadzieją na dłuższą metę.

Trudność polega na tym, że fizycznie sieć peer-to-peer będzie potrzebować bardzo dużej przepustowości. Widmo radiowe jest niestety ograniczonym zasobem i choć wielu Brytyjczyków z radością widziałoby zniesienie nadmiernego Ofcomu, pierwotna podstawowa rola tej organizacji nadal musi być w jakiś sposób realizowana. Współdzielenie widma bez przejęcia go przez monopolistę może być jedną z niewielu rzeczy, których sam wolny rynek nie jest w stanie rozwiązać. Rozwiązaniem jest uniknięcie konieczności współdzielenia widma w ogóle; korzystanie z przekaźników optycznych lub podczerwonych w linii wzroku oznacza, że nie musisz się martwić, że jedno łącze komunikacyjne zakłóca inne. I chociaż łącze w linii wzroku może zostać tymczasowo zakłócone przez cokolwiek przecinającego ścieżkę, to sprawia, że powszechne zagłuszanie przez przeciwnika jest prawie niemożliwe. Różnorodne łącza biegnące na przykład między szczytami górskimi mogą bez trudu przesyłać dane ponad ogrodzeniem granicznym kraju, w którym panuje ścisła cenzura. Kluczowymi nierozwiązanymi kwestiami przy projektowaniu tego rodzaju warstwy fizycznej są te dotyczące odporności; te dotyczące tego, w jaki sposób jakiś odpowiednik protokołu Border Gateway Protocol kierowałby ruchem w sieci fizycznej bez potrzeby scentralizowanych zaufanych stron; oraz tego, jak ukryć, a tym samym chronić węzły przed manipulacjami ze strony cenzorskich zbirów. Sposób obsługi

wyższych warstw stosu OSI działających na szczycie tej sieci jest rozwiązany; nie jest potrzebna żadna nowa praca w zakresie szyfrowania, na przykład. Szyfrowanie, które już działa w skompromitowanej, scentralizowanej dzisiejszej sieci, działałoby w optycznej sieci peer-to-peer.

- **W jaki sposób możemy zapewnić, że ludzie nadal mogą ufać stronom internetowym, że działają uczciwie, skoro sama architektura idealnego Internetu uniemożliwiłaby śledzenie ich tożsamości za pomocą środków technicznych?** Jak wspomniałem powyżej, dark-web jest zbyt atrakcyjnym miejscem dla kogoś, kto może pobierać płatności za usługi, których nigdy nie dostarcza. Oczywiście jest to objaw płatności kryptowalutowych - z założenia niemożliwych do obciążenia zwrotnego - a nie tylko anonimowego adresowania stron internetowych. Ale ponieważ procesory kart angażują się w cenzurę, idealna sieć prawdopodobnie potrzebowałaby jakiejś jeszcze niewyobrażalnej metody płatności, bez centralizacji istniejącej infrastruktury ani potencjału oszustwa kryptowalut. Potrzebne byłyby środki, za pomocą których użytkownicy mogliby wymusić zwrot pieniędzy w przypadku oszustwa, ale bez środków, za pomocą których jakiekolwiek władze mogłyby blokować płatności.

Modele typu "Fediverse" oparte na reputacji społeczności mogą zawieść, gdy cenzorskie kolektywy wścibskich jednostek rzucają się na siebie. Modele oparte na mikropłatnościach, uwielbiane przez wielu entuzjastów kryptowalut Web 3.0, którzy wydają się wierzyć, że można je zastosować do wszystkiego, pachną raczej okazjami do czerpania zysków z wynajmu niż funkcjonalnymi sposobami na utrzymanie systemu.

Już teraz istnieje ryzyko, że podczas gdy zwykłe przeglądanie i media społecznościowe mogą być w stanie migrować z platform, na których władzę sprawują fanatycy cenzury online pod przykrywką bezpieczeństwa, handel online będzie miał znacznie trudniejszy czas działania w świecie, w którym każdy potrzebuje VPN i warstw anonimowości, aby uniknąć padnięcia ofiarą systemu kredytu społecznego. Każdy, kto myśli, że wszystko jest w porządku, ponieważ może obejść blokadę artykułu lub filmu, powinien zapytać, czy jego obejście byłoby tak niezawodne, gdyby chciał zamówić irytująco niemetryczny typ śruby maszynowej od jedynego sprzedawcy, który istniał dla tego typu, ale który został niedawno zmuszony do wdrożenia cyfrowej kontroli tożsamości przy każdym zakupie.

Zauważ, że w tym pytaniu powiedziałem, że nie można go zidentyfikować za pomocą środków technicznych: legalna firma prowadząca stronę internetową z pewnością nadal miałaby dosłowny adres ulicy na swojej stronie internetowej. Tak więc część tego pytania staje się rozwiązanym problemem. Istnieją podpisy cyfrowe oparte na PGP/GnuPG, które pozwalają udowodnić, przy braku poważnej mocy obliczeń kwantowych, że tylko osoba znająca określone tajne hasło może być tą, która podpisała nim jakąś treść. Mamy już zatem środki dla osoby lub organizacji, której już ufamy, aby udowodnić, że usługa należy do nich, a nie do oszusta, o ile podpis, który sprawdzasz, został wcześniej dostarczony weryfikowalnym kanałem, takim jak znak na zewnątrz ich biura, sklepu lub magazynu.

- **W jaki sposób nowe usługi w doskonałej sieci mogą kiedykolwiek stać się konkurencyjne dla istniejących usług?** W przypadku bardziej tradycyjnych usług jest to nieco łatwiejsze: jeśli prowadzisz witrynę dziennikarską publikującą artykuły, to pod warunkiem, że ludzie wiedzą o jej istnieniu, przyjdą tam, gdzie ją hostujesz, o ile jest to wystarczająco łatwe. Ale w przypadku usług odgrywających rolę podobną do mediów

> społecznościowych jest to znacznie trudniejsze. Atrakcyjność serwisu społecznościowego dla każdego nowego użytkownika jest proporcjonalna - w porządku, prawdopodobnie nieliniowo, ale wciąż monotonicznie - do tego, ilu użytkowników już tam jest. W jaki sposób nowa usługa może konkurować na rynku, na którym istniejący duzi gracze cieszą się ugruntowaną, skutecznie monopolistyczną przewagą?

Logika tego problemu wiąże się również z pierwszym z tych trzech trudnych problemów - opracowanie projektu architektury fizycznej nie jest wystarczające. Musi istnieć wystarczająca adopcja jednej konkretnej architektury warstwy fizycznej, aby nie wygasła, tak jak zrobiło to wiele konkurencyjnych projektów prywatności typu open source, gdy nie udało im się zdobyć wystarczającej liczby użytkowników, aby stać się samowystarczalnymi. Narzędzie do symetrycznego szyfrowania plików lokalnych jest nadal działającym narzędziem, jeśli nawet tylko jedna osoba go potrzebuje; infrastruktura sieciowa działa tylko wtedy, gdy korzysta z niej wiele osób.

Oczywiście, poza tymi technicznymi "trudnymi problemami", wysiłki mające na celu obronę wolności słowa za pośrednictwem każdej drogi politycznej i prawnej są również niezbędne, a wsparcie dla tych wysiłków jest silniejsze niż kiedykolwiek wcześniej. Wiele osób wcześniej postrzegało cenzurę jako odległe zagrożenie na horyzoncie; wraz z najnowszym przykładem nadmiernego zasięgu rządu, cenzura spadła z gór i zbyt mocno zaznaczyła swoją obecność u bram. Opinia publiczna nie jest zadowolona, a parafrazując rzymskiego senatora, ich postawa stała się jedną z "Cenzura delenda Est"!

Stop Press: Lord Sumption, były sędzia Sądu Najwyższego i pryncypialny przeciwnik nadmiernego zasięgu Covid, potępił absurdalność ograniczania korzystania z Internetu przez osoby poniżej 18 roku życia, jednocześnie dając prawo głosu 16 i 17-latkom. Jak dotąd nie ma on "zastrzeżeń do [ustawy o bezpieczeństwie online] samej w sobie", ale tak jak jego sprzeciw wobec paszportów szczepionkowych pojawił się dopiero wtedy, gdy zobaczył, jak daleko one sięgają, jestem pewien, że zda sobie sprawę, jak rażącym naruszeniem wolności i prywatności ogółu populacji jest ta ustawa.

Dr R P ukończył doktorat z robotyki podczas globalnej nadmiernej reakcji na Covid. Spędza czas z jednym okiem na oscyloskopie, jedną ręką na lutownicy i jednym uchem w oczekiwaniu na najnowsze złe wieści.