Serwerowa Korea*. Jak Kreml zamknie internet i dlaczego VPN-y nie pomogą

* Tytuł jest grą słów: „Серверная Корея” (serwerowa Korea) - „Северная Корея” (Korea Północna)

Pod pretekstem wojny Kreml zaczął zamykać dostęp do niezależnych publikacji w Internecie, w tym do Dożdz (Deszcz) i Echa Moskwy, a The Insider również przestał się otwierać u wielu osób. Był to jednak dopiero początek ostatniej fazy walki z wolnym Internetem, której kulminacją miało być utworzenie „suwerennego Runetu”. Przygotowania do jej utworzenia rozpoczęły się w listopadzie 2019 r., kiedy to Państwowy Wydział Śledczy Ministerstwa Spraw Wewnętrznych wszczął postępowanie karne przeciwko jednemu z założycieli rosyjskiego internetu Aleksiejowi Sołdatowowi i jego partnerowi biznesowemu Aleksiejowi Szkittinowi - zostali oni oskarżeni o przekazanie administrowania około 470 tysiącami adresów IP firmie zarejestrowanej w Czechach. Sołdatow został aresztowany, Szkittin był poszukiwany (Niemcy odmówiły jego ekstradycji, uznając sprawę za polityczną). Wniosek w tej sprawie złożył osobiście Andriej Lipow, ówczesny kierownik działu w AP, a obecnie szef Roskomnadzoru. To właśnie walka o rejestry adresów IP pozwoli Kremlowi zrealizować marzenie o w pełni kontrolowanym „suwerennym Runecie”, mówi Aleksiej Szkittin. W wywiadzie dla The Insider wyjaśnił, jak dokładnie będzie wyglądać „suwerenny Runet”, dlaczego niemożliwe byłoby ominięcie cenzury, jakie są powiązania Lipowa z FSB i Usmanowem oraz dlaczego internetowi giganci, tacy jak Google i YouTube, mogą być zmuszeni do opuszczenia Rosji.

- Kto i w jaki sposób kontroluje dziś rosyjski Internet?

- Jako główne źródło kontroli państwowej wybrano Roskomnadzor, przy czym w razie potrzeby angażują się w nią różne agencje, zlecając lub wspomagając jej realizację (np. FAS, GKRC, GKRCz i inne). Od „Mincyfry” nie zależy praktycznie nic, a po upadku wiceministra Aleksieja Sokołowa (który był faktycznym przedstawicielem FSB w agencji i próbował przejąć kontrolę nad sytuacją w zakresie zarządzania Internetem) jest ona obecnie w zasadzie „ministerstwem niczego”. Rzeczywista (polityczna) władza nad Internetem spoczywa w rękach szefa Roskomnadzoru, Andrieja Lipowa, który jest autorem projektu „suwerennego Internetu” i któremu powierzono jego realizację.

- Czy Lipow ma wystarczające kompetencje, aby sprawować tę władzę?

- Całkowicie. W przeciwieństwie do swojego poprzednika, Lipow jest osobą kompetentną i rozumiejącą strukturę Internetu. Ale nie chodzi tylko o Lipowa. Nie mniej istotnym źródłem zagrożenia dla wolności „Runetu” jest FSB. W przeszłości FSB, wraz z RKN, odpowiadała za węzły komunikacyjne i nadzorowała rozmieszczenie i działanie SORM na tych węzłach. W rzeczywistości funkcje te pozwalają FSS kontrolować cały ruch użytkowników nie tylko na bieżąco, ale także (dzięki ustawie Jarowej) na kilka lat wstecz. Innymi słowy, wszystkie „rejestry” działań użytkownika, w przypadku wszczęcia przeciwko niemu postępowania karnego, mogą być dostępne na żądanie. W połączeniu z kontrolą przestrzeni adresowej i domenowej, takie „podsłuchiwanie” daje doskonały efekt kontroli nad użytkownikami sieci.

- Czy postępująca „suwerenizacja” Runetu to tylko kwestia kontroli, czy także kwestia pieniędzy? Czy są jacyś konkretni beneficjenci?

- Jakże mogłoby ich nie być! Aby zrozumieć, co się dzieje, należy przyjrzeć się holdingowi Citadel, który skoncentrował i nadal gromadzi w swoich rękach komercyjny komponent narzędzi potrzebnych do kontrolowania Runetu. Za „Cytadelą” stoją krewni wysokich rangą oficerów FSB i byli pracownicy FSB, ale ostatecznie wszystkie wątki prowadzą do struktur Usmanowa. W

rzeczywistości wszystkie państwowe podsłuchy są teraz w jego rękach. Według naszych informacji, umieszczenie Lipowa na stanowisku szefa RKN w czasie jego pracy w AP (Administracji Prezydenckiej) jest również zasługą struktur Usmanowa.

- Usmanow sprzedał niedawno VKontakte i Mail.ru (gdzie pracowali syn Lipowa i syn Kirienki) - czy to oznacza, że traci pozycję w kontrolowaniu Runetu?

- W tym miejscu należy ogólnie zrozumieć, że główną dźwignią wpływu na wszystkie firmy informatyczne w kraju jest kontrola bezpieczeństwa (a to jest związek FSB-Citadel-RKN), gdzie Lipow i Usmanow działają w porozumieniu z najwyższymi funkcjonariuszami FSB. Drugą dźwignią są domeny narodowe, które Lipow i Usmanow również kontrolują. Teraz mogą już nie być właścicielami firm oferujących treści, takich jak VK i Mail.RU, ale kontrolują wszystko od dołu poprzez zarządzanie bezpieczeństwem i infrastrukturą.

- Na ile realne jest uzyskanie przez państwo pełnej i ostatecznej kontroli nad infrastrukturą internetową w Rosji?

- Przede wszystkim zdefiniujmy, co nazywamy infrastrukturą internetową. Wbrew obiegowej opinii nie są to bynajmniej popularne aplikacje internetowe, takie jak YouTube czy VK. Podstawą Internetu jest logiczna infrastruktura obejmująca rejestry adresów IP, systemy nazw domenowych i tablice routingu. Wszystko inne istnieje nad nią (lub odwrotnie, pod nią, jak kable lub systemy tworzenia i transmisji pakietów).

- Co oznacza termin „infrastruktura rejestrów adresów IP”?

- Każdy węzeł w sieci ma swój adres, a między nimi istnieje trasa, po której przemieszczają się informacje. Kluczowe znaczenie ma system adresowania i routingu IP (adresy IP, systemy autonomiczne i BGP) oraz systemy nazw domenowych DNS, a także infrastruktura okablowania, która obejmuje wszystkie kable przychodzące z zagranicy. To jest właśnie to, nad czym planuje się przejąć kontrolę.

- „Planuje się”, czyli jeszcze się nie kontroluje?

- Jeszcze nie, ale po przejęciu kontroli nad tą infrastrukturą można uzyskać całkowitą kontrolę nad siecią poprzez zastosowanie systemu urządzeń blokujących w węzłach sieci, a także usprawnienie mechanizmów DPI (głębokiego skanowania i rozpoznawania ruchu) oraz SORM.

- A więc jedyne, co pozostaje państwu do zrobienia, to ustanowienie kontroli nad nazwami domen i systemem adresów IP?

- Połowa tego zadania została już wykonana. W rzeczywistości struktury Lipowa (czytaj Usmanowa) przejęły kontrolę nad systemem nazw domen krajowych, eliminując za pomocą sprawy karnej mnie i Aleksieja Sołdatowa - byliśmy ostatnimi, którzy stawiali opór i mogli faktycznie zapobiec suwerennemu Runetowi. Usunięcie Sołdatowa z grona założycieli KC (Centrum Koordynacyjnego Domeny Krajowej) całkowicie rozwiązało Lipowowi ręce, a dzięki dodatkowym, niewyszukanym manipulacjom uzyskał on pełną kontrolę nad infrastrukturą nazw domen.

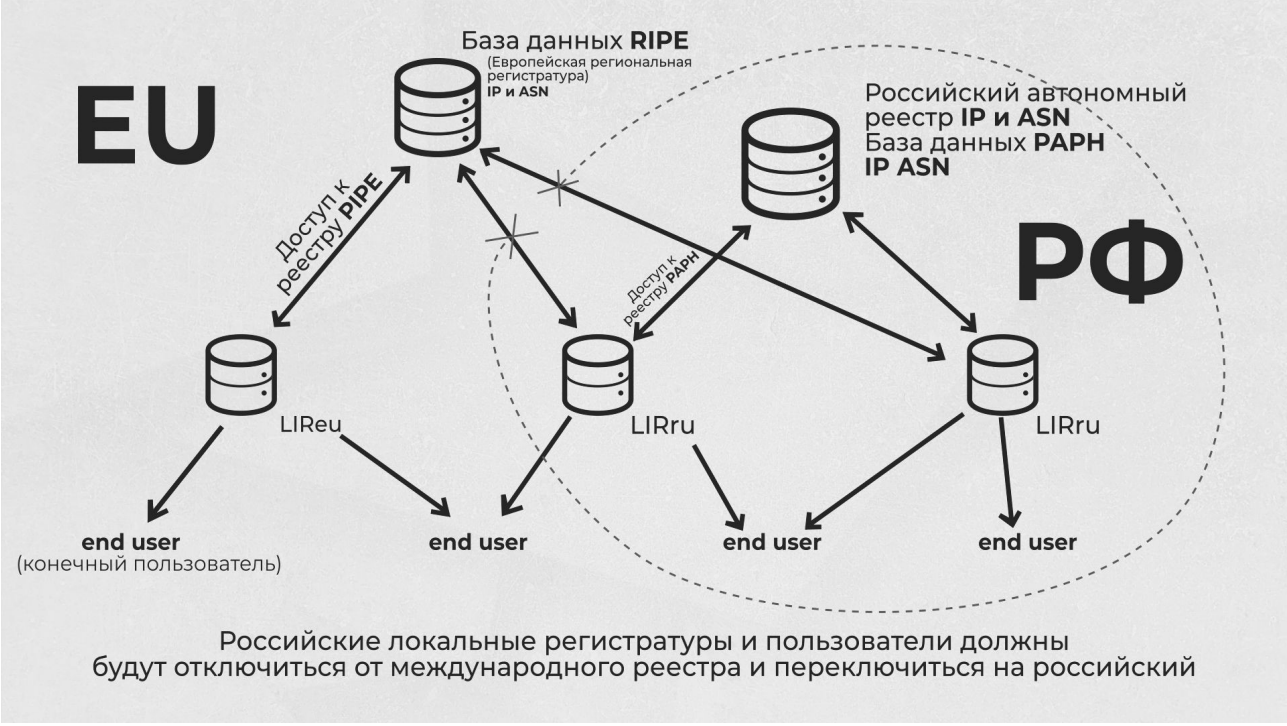
- Czy wojna może przyspieszyć realizację planów stworzenia suwerennego Runetu?

- Z pewnością, ale nie chodzi tu nawet o tworzenie, ale o stosowanie wcześniej przygotowanego schematu. Istnieje projekt RARN, który jest w rzeczywistości pełną kopią europejskiego rejestru adresów IP i jest powiązany z krajowym systemem nazw domen. Wszyscy operatorzy posiadający

systemy autonomiczne muszą być zarejestrowani na indywidualnym koncie w tym systemie i tylko tam mogą uzyskać przestrzeń adresową wymaganą dla węzłów sieci. 28 lutego Roskomnadzor wydał polecenie przygotowania wszystkich operatorów do przejścia na system RARN i zażądał uaktualnienia wszystkich dostępnych informacji. Na razie jest to kwestia tras BGP, które muszą pozostać pozostać w aktualnym stanie nawet w przypadku ich usunięcia lub zastąpienia przez regulatora lub inne siły. W następnej fazie planowane jest całkowite przejście do rejestru adresowego RARN i budowanie routingu już w oparciu o niego. Według posiadanych informacji, wyznaczony jest na to termin kilku tygodni.

- To będzie taka matrioszka, Internet w Internecie?

- Tak, suwerenny Runet byłby odizolowanym systemem z własnym systemem nazw domen i przestrzenią adresową, czyli swego rodzaju modelem dużego Internetu, wdrożonym odrębnie w kraju. Biorąc pod uwagę całkowitą kontrolę źródeł ruchu zagranicznego (nie na darmo pospieszono się z przerabianiem kabli wzdłuż granicy) i wdrożenie systemu głębokiego skanowania, zwykły użytkownik nie będzie miał swobodnego dostępu do globalnego Internetu ani możliwości tworzenia dowolnych zasobów niepożądanych przez władze wewnątrz kraju. Operatorzy dysponujący bezpośrednimi łączami kablowymi mogą zachować łączność ze światem zewnętrznym, ale są zobowiązani do zgłaszania takich połączeń do RKN i prawdopodobnie kanały te również znajdą się pod kontrolą RKN.



Według najnowszych danych już pierwszego marca RKN zażądał, aby wszyscy operatorzy składali sprawozdania dotyczące ich zagranicznych urządzeń łączności kablowej. RKN stoi na stanowisku, że wszystkie kable doprowadzane do Rosji powinny być w całości własnością firm rosyjskich. Domyślam się, że wyłączenie dotknie również operatorów na poziomie fizycznym. Istnieje więc duże prawdopodobieństwo, że w marcu Runet zostanie całkowicie zamknięty od wewnątrz. Oznacza to, że włazy będą zakratowane.

- Jak trudno będzie ominąć blokady w „suwerennym Runecie”?

- Jeśli przez jakiś czas będą utrzymywać kontakt ze światem zewnętrznym, to będzie możliwość ominięcia blokady. W takim przypadku rozpowszechnią się sieci o topologii siatki, w których każdy

użytkownik staje się węzłem sieci, przepuszczając przez siebie ruch sąsiada. Jest o wiele więcej wariantów walki. Jednak w przypadku Internetu satelitarnego nie ma co liczyć na zbyt wiele, ponieważ systemy dostępu są bardzo łatwe do monitorowania i wykrycia.

- Czym system rosyjski różniłby się od, powiedzmy, wielkiego chińskiego firewalla?

- Są one bardzo różne, ponieważ chiński Internet na najwcześniejszym etapie (kiedy było w nim niewiele ponad 100 tys. użytkowników) był zamknięty potężną zaporą ogniową, która rosła wraz z siecią i została z nią w pełni zintegrowana. Chiński system kontroli ruchu to rozwiązanie sprzętowo-programowe, które powstawało przez 30 lat i nie ma możliwości powtórzenia go w ciągu kilku lat, niezależnie od tego, ile by to kosztowało.

- A koszty tam są wielomiliardowe.

- Zarówno koszty są ogromne, jak i liczba zaangażowanych specjalistów. Chiński system opiera się na wykorzystaniu podobnej logiki adresowania i routingu, jak cały światowy Internet, tylko Chińczycy odgrodzili się sprzętem, pozwalającym na głębokie skanowanie ruchu, dzięki czemu są w stanie powstrzymać zakazane treści. Filtrowanie wewnątrz prawdopodobnie działa na podobnej zasadzie. Izolację ułatwia fakt, że Chiny są NIR-em, czyli krajowym rejestrem internetowym, co umożliwia państwu zmuszenie wszystkich operatorów do korzystania w kraju wyłącznie z przydzielonych im adresów IP.

- A Rosja tak nie może?

- Nie, ponieważ Rosja znajduje się na obszarze objętym rejestrem internetowym RIPE, który zajmuje się dystrybucją adresów IP w Europie, Azji Środkowej i na Bliskim Wschodzie. W systemie RIPE każdy operator może korzystać ze swojego systemu autonomicznego i zakresu IP w dowolnym miejscu, nawet w innym regionie.

- A czym „suwerenny Internet” będzie się różnił od północnokoreańskiego „intranetu”?

- W Korei Północnej sytuacja jest dość prymitywna. Tamtejsi towarzysze, nie zastanawiając się długo, po prostu zbudowali „sieć lokalną”, która została zredukowana do jednego autonomicznego systemu z dwoma „uplinkami” (tj. dwoma kanałami komunikacyjnymi): z Chin i z Rosji. Wszystko wewnątrz jest tylko wewnętrzną siecią lokalną, w której zasady i prawa są określane przez administratorów systemu. Jednak w Korei Północnej niewiele osób korzysta z Internetu, podczas gdy w Rosji jest ponad 2000 dostawców, a potrzeba komunikacji międzynarodowej jest oczywista, przynajmniej dla sektora bankowego i handlu zagranicznego.

- Ale czy „suwerenny Runet” nie jest po prostu przeskalowanym modelem północnokoreańskim?

- Nie do końca. AP, a wraz z przybyciem Lipowa RKN, zaczęła rozwijać pomysł stworzenia własnego analogu Internetu dla całego kraju, który nie różniłby się technicznie od oryginału, ale nie pokrywałby się z nim na poziomie logicznym. Innymi słowy, wzięli międzynarodowy system dystrybucji adresów IP, skopiowali go i stworzyli własny na analogicznej zasadzie. Adresy te są przymusowo rozdzielane między rosyjskich dostawców za pośrednictwem systemu RARN, a następnie muszą oni zaprzestać rozgłaszania adresów międzynarodowych za pośrednictwem swoich autonomicznych systemów i zacząć rozgłaszać wewnątrzrosyjskie, a ponadto wszystkie kanały komunikacyjne muszą być rosyjskie. Wtedy Internet niejako zamknie się w sobie i będzie działał poprawnie, ale bez kontaktu ze światem zewnętrznym.

- Filtrowanie ruchu staje się o wiele łatwiejsze.

- Oczywiście! Nie ma potrzeby globalnego filtrowania międzynarodowego, po prostu domyślnie nie byłoby ruchu zewnętrznego, chyba że przez bramki pod pełną kontrolą Rostelekomu i spółki. Natomiast ruch wewnętrzny będzie odszyfrowywany przez DPI (głębokie filtrowanie) i blokowany w razie potrzeby. Nie będzie można zbudować tunelu VPN, ani korzystać z systemów obchodzenia blokad wbudowanych w przeglądarki. Planowany suwerenny Internet jest więc zasadniczo zamkniętym systemem na poziomie logicznego zarządzania siecią lub suwerennym segmentem sieci międzynarodowej, który działa na wzór Internetu światowego, ale jest od niego całkowicie oddzielony.

- Mówiąc prościej, Kreml otrzymuje wyłącznik, którym może w każdej chwili wyłączyć kanały zewnętrzne.

- Dokładnie tak. Przecież obecnie wszystkie dwa tysiące rosyjskich dostawców usług internetowych obsługuje globalny Internet i blokuje strony na żądanie RKN tylko z obawy przed grzywną lub karą, ale technicznie mogą to złamać i włączyć pełny dostęp - na przykład w przypadku rewolucji lub tak jak teraz, w czasie wojny. Nowy system zasadniczo eliminuje taki bieg spraw, ponieważ możliwe będzie zablokowanie działania bezpośrednio z centrum kontroli RKN na poziomie systemu autonomicznego poprzez trywialne usunięcie niepożądanych tras.

Podobnie system nazw domen, który Lipow nazwał "systemem domen narodowych", zostaje przejęty pod kontrolę, rejestr również zostaje przeniesiony do Rosji i nie jest już zsynchronizowany z rejestrem globalnym, działając jedynie w obrębie kraju w połączeniu z krajowym systemem adresowania i routingu IP, który również nie jest połączony z rejestrami globalnymi. Jeśli przejmą kontrolę nad wszystkimi kablami zewnętrznymi, co właśnie robią, szansa na całkowite zamknięcie wzrasta do 100%.

- Jednak aby to się udało, giganci internetowi musieliby zgodzić się na przejście na adresy IP "suwerennego Runetu". A jeśli odmówią?

- Po pierwsze, Google i Facebook są prawnie zobowiązane do posiadania serwerów w Rosji i już dawno zaczęły przenosić je do rosyjskich centrów danych, gdzie oczywiście łączą się tylko z rosyjskimi dostawcami, ponieważ innych nie ma i prawdopodobnie nie będzie. Obecnie prawie wszyscy dostawcy, nawet zagraniczni, mają rosyjskie osoby prawne (a ci, którzy ich nie mają, będą, jak sądzę, zmuszeni do tego, ponieważ przyjęto już ustawę stanowiącą, że obcokrajowcy nie mogą być właścicielami sieci przekraczających granicę Rosji). Zatem z definicji serwery będą musiały być podłączone do rosyjskich „uplinków”.

Oczywiście, na razie wszyscy pracują normalnie, korzystając z międzynarodowej numeracji i routingu, wszyscy rosyjscy dostawcy usług internetowych używają IP przydzielonego im przez RIPE, ale po ustanowieniu suwerenności wszyscy operatorzy przejdą na numerację RARN i w Rosji nie będzie się używać żadnej innej. Google i Facebook nie będą miały żadnego wyboru, ponieważ międzynarodowa numeracja po prostu przestanie działać, a ich IP staną się bezużyteczne - rosyjski Internet po prostu nie będzie ich widział.

Ruch zagraniczny będzie przechodził przez bramę, np. Rostelekomu, w której adresy będą przekształcane z wewnętrznych na zewnętrzne i odwrotnie (coś w rodzaju tunelu), oczywiście wszystko pod pełną kontrolą RKN, z rozszyfrowaniem całego ruchu i jego analizą. Na komendę "zamknięcia włazów" brama przestaje działać, po czym rosyjskie serwisy Facebook i Google będą musiały jakoś działać samodzielnie, ale czy mają taką możliwość, tego jeszcze nie wiemy.

- Czy międzynarodowe organy regulacyjne mogą powiedzieć, że nie podoba im się pomysł RARN i że nie będą się w niego angażować? Czy społeczność międzynarodowa może zrobić cokolwiek, aby zapobiec utworzeniu przez RKN suwerennego Runetu?

- Nie, jeśli ktoś stworzy własny rejestr adresów na wewnętrzny użytek Rosji, niezwiązany z użytkiem zewnętrznym, to światowe organy regulacyjne nie będą miały na niego wpływu. Na punktach styku, powiedzmy, Rostelekomu, ruch z adresacji wewnętrznej przechodzi na zewnętrzną i z powrotem, ale co może zrobić regulator? Zabronić tego ruchu? Usunąć międzynarodowe adresy IP Rostelekomu? Spowodowałoby to odcięcie wszystkich usług międzynarodowych w Rosji, ale funkcjonalność wewnętrznego Internetu pozostałaby nienaruszona.

- Ale jeśli mówimy o korporacjach takich jak Google czy Facebook, to okazuje się, że one same będą decydować, czy współpracować z Rosją przez bramę, czy nie. Jakie jest prawdopodobieństwo, że nie zaakceptują tego formatu pracy?

- Oczywiście, że sami o tym zdecydują. Myślę, że do końca będą się dostosowywać. I tylko jeśli sytuacja będzie taka, że będą musieli mieć wyizolowany segment na terytorium Rosji, to najprawdopodobniej nie zgodzą się na taki dziwny schemat pracy, ponieważ ich systemy to kompletny mechanizm i nie można go używać autonomicznie. Z technicznego punktu widzenia mogą one pracować w ten sposób, ale ogólnie rzecz biorąc, będzie to wyglądało bardzo niezgrabnie. Myślę, że w końcu mogą się wynieść, częściowo dlatego, że koszty „osadzenia się" w Rosji w ramach suwerennej sieci byłyby zbyt wysokie. Nikt też nie zrezygnował z kwestii prywatności użytkowników.

- Trudno sobie wyobrazić, jak na przykład YouTube mógłby działać autonomicznie w Rosji, nawet gdyby chciał.

- W tym miejscu należy zrozumieć, jak działa struktura buforowania danych, sieć CDN itd. Myślę, że najpierw musieliby stworzyć zrównoważony mechanizm dystrybucji danych i zarządzania nimi, aby przecisnąć się przez wąskie gardło suwerennej sieci, ale nie tego chce Google i inni. Jak już wspomniałem, prawdopodobnie po prostu odmówią pracy w takich warunkach, ponieważ ich systemy nie zapewniają autonomii ze względu na technologię buforowania.

- Ale jeśli giganci internetowi odejdą, jak w ogóle przetrwają rosyjskie firmy, jeśli nie będzie normalnych odpowiedników? Czy próba stworzenia własnej infrastruktury internetowej nie doprowadzi do tego, że po prostu zepsują Internet i zrujnują gospodarkę?

- Oczywiście, że je zepsują; czyż pomysł zaopatrywania wszystkich w „Elbrusy" i „Bajkały", z procesorami, które ledwo działają, nie niszczy wszystkiego, co się da? Ale tak się dzieje. (A raczej już nie, bo nawet oni byli zależni od sprzedawcy tajwańskiego, który nałożył sankcje). Nie liczą się z konsekwencjami, zajmują się sprawami bieżącymi - przejęciem pełnej kontroli nad siecią. Jeśli wszyscy będą pracować za pośrednictwem Mail.ru i znajdującej się pod kontrolą poczty firmowej (obecnie wymaga się, aby sieci firmowe również przechowywały i udostępniały dane), całkowicie ich to zadowoli. Oczywiście wszystko całkowicie się nie załamie, ale będzie to wyglądało bardzo mizernie. Gospodarka raczej nie rozkwitnie, choć służby państwowe i strona podatkowa zapewne będą działać.

Źródło: https://whatisyournameinsider.com/politika/248511