Po spotkaniu u Rzecznika Praw Obywatelskich.

Odpowiedzi na pytania i prośby o fakty ze strony Fundacji Panoptykon.

> *(Teza) blokowanie jest: (i) nieskuteczne*

Tak. Dopóki jakaś treść jest w internecie udostępniona, nie da się jej zablokować. Skuteczna w 90% blokada wymagałby po pierwsze delegalizacji szyfrowania, po drugie analizowania każdego przesyłanego bajtu.

Nawet w przypadku zakazu szyfrowania oraz heurystycznej analizy każdego przesyłanego pakietu, treść może być udostępniana za pomocą technik steganograficznych. W trzyminutowym filmie z youtube można skutecznie ukryć kilkaset zdjęć dobrej jakości lub kilka sekund innego filmu. Więcej o steganografii: pobieżnie w wikipedii; Dokładniej a przystępnie: tutaj .

> *(Teza) blokowanie jest:* (ii) łatwe do obejścia.

Dopóki legalne jest posiadanie i kupowanie oprogramowania bez policyjnej koncesji, dopóty każdy, kto ma potrzebę ominięcia blokad a nie potrafi sam, będzie mógł skorzystać z darmowej lub płatnej pomocy.

Nawet gdy do zakazu szyfrowania i kontroli wszystkich pakietów dołożymy ~~chiński~~ europejski wielki internetowy mur, nie powstrzyma on znanych (i jeszcze nieznanych) metod ukrytej transmisji.
Na przykład ukrytej usługi tunelowania w ruchu DNS (strona w jęz angielskim, EN).
A tu szczegóły o ukrywaniu danych w powtórzonych pakietach.

> (Przykłady, że) *blokowanie jednego typu treści najprawdopodobniej doprowadzi z czasem do blokowania innych rodzajów treści/usług.*

Australia. Dostęp do gier online zablokowany. Mogą szkodzić dzieciom (EN).
Turcja. prof. Richard Dawkins zablokowany. Za głoszenie ateizmu (EN).

Przykład wycieku (do wikileaks) zawartości czarnych list Australii czy Danii pokazuje też, że teoretyczne możliwości odwoływania się są właśnie takie: teoretyczne. Strony dentystów i malarzy (pokojowych) trafiają na listę rzadko (ci akurat – gdyby wiedzieli – mogliby się bez ryzyka odwołać). Ale listy „pornografii do zablokowania" pełne są adresów stron z treścią legalną, acz kontrowersyjną. Blokowaną z powodu „pomyłki", „nietrafnej interpretacji" albo też z powodu „przypadkowego dopisania przez komputer" *(tłumaczenia cenzorów po wycieku do wikileaks)*. W przypadku Australii blokowane były np strony ruchu ProLife. W przypadku Danii blokowane były ponoć strony nawołujące do sądowej kontroli cenzorów.

W Polsce do takich „pomyłek" typowałbym jako pierwsze blogi homo-rodziców. Osoba myląca się przy dopisywaniu do listy nie ryzykuje niczym, natomiast osoba, która miałaby się odwoływać od skutków tej „pomyłki", ryzykuje bezpieczeństwem swoim i swoich bliskich.

> (...) *blokowanie treści najprawdopodobniej będzie używane jako środek zastępczy a nie uzupełniający identyfikowanie i ściganie sprawców przestępstw*.

Taka jest praktyka i – co gorsza – taka jest chyba intencja proponujących! Piszą oni wszak, że:

„*Lista blokowanych stron i usług musi być tajna, bo inaczej byłaby spisem złych treści do pobrania*".

W powyższym wyraża się ich założenie, że:

a) żadne działania w celu usunięcia treści podjęte nie będą.

b) nie ma technicznej możliwości całkowitego zablokowania dostępu do nieusuniętej treści.

Czy (i dlaczego) nie należy dopuszczać blokowania nawet jako rozwiązania doraźnego/tymczasowego (np. na kilka miesięcy, dopóki treść nie zostanie usunięta)?.

Ponieważ **blokowanie,** choćby tymczasowe, tylko na jeden dzień, **wymaga wdrożenia mechanizmów zaglądania do każdej paczki z danymi, które wysyłamy.** A jak już się zagląda, to i **retencja musi być.**

Rozwinięcie:, by w miarę skutecznie blokować, trzeba będzie zalegalizować masową kontrolę treści przesyłanych pakietów (DPI, deep packet inspection). Nie da się blokować bez dowiedzenia się wcześniej, po jaką stronę czy usługę obywatel chce sięgnąć. ISP będą więc zobowiązani do zaglądania w każdy pakiet danych, który wysyłamy. W tej chwili zaglądanie do treści korespondencji (transmisji) bez nakazu sądu lub prokuratora jest w Europie nielegalne. W imię „ochrony dzieci", ma się stać nie tylko legalne, ale ma stać się obowiązkiem każdego dostawcy internetu.

Następne będzie żądanie, by dane te podlegały retencji. Obecnie retencja obejmuje same adresy, a pod jednym adresem mogą być dostępne tysiące różnych domen (np www.site.com i poker.gambling.org). Kiedy ISP będą już zobligowani do odczytywania z pakietów dokładnego adresu URL, to wprowadzenie retencji danych o tym do jakiej dokładnie informacji obywatel uzyskał dostęp „*nie będzie powodowało skutków finansowych*" a także „*umożliwi policji skuteczniejszą walkę z terroryzmem i dziecięcą pornografią*".

Czy blokowanie stron – ze względów technicznych – musi działać jako „system wczesnego ostrzegania przestępców" (tj. czy można skutecznie ukryć przed administratorem strony fakt jej blokowania?).

Nie. Przed administratorem nie można ukryć faktu zablokowania strony.
Przed administratorem przestępczym tym bardziej ukryć blokady nie można: Przestępca będzie miał ustawione w różnych krajach automaty sprawdzające czy dostęp jest czy go brak.

„Ukryć" się da przed autorem czy autorką mało popularnego kontrowersyjnego bloga. Ci się dowiedzą, jak ktoś im powie. O ile się dowiedzą, bo „dobre blokowanie" zapewne odetnie ich od tych, którzy by im o tym mogli powiedzieć przez formularz na blogu.

Czy problem pojawiania się w spamie odnośników do treści z tzw. pornografią dziecięcą (a tym samym narażania użytkowników na przypadkowy, niechciany kontakt z takimi treściami) jest poważny i jak można go skutecznie rozwiązać.

Nie wiem. (Na prawie dwadzieścia lat) spamów z tytułem sugerującym dziecięcą pornografię widziałem kilka. Nie czytuję jednak spamu. Mało kto czyta spam, spam jest filtrowany na nasze życzenie przez nasze programy pocztowe.

W ogóle nie zdarzyło mi się *trafić* na taką pornografię – ale też nigdy nie szukałem jakiejkolwiek.

Natomiast mam informacje od osób używających (nadużywających?) płatnych stron dla dorosłych, że spotykali się tam z linkami do takich treści w ogłoszeniach wyskakujących ze stron z „twardą ale dorosłą" pornografią. Ogłoszenia znikały chwilę po ich zgłoszeniu administratorom (te strony mają przyciski „zgłoś").

Wojciech S. Czarnecki. <ohir AT fairbe.org>