SNOWDEN
NIGDZIE SIĘ NIE UKRYJESZ

NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE BY GLENN GREENWALD

Tłumaczenie
Barbara Gadomska

Redakcja
Roman Imielski
Korekta
Bartosz Choroszewski

Projekt graficzny serii
Przemek Dębowski i Wojtek Kwiecień–Janikowski
Skład
Elżbieta Wastkowska

Projekt graficzny okładki
Przemek Dębowski i Wojtek Kwiecień–Janikowski
Zdjęcie na okładce
© Alex Milan Tracy/Corbis /Fotochannels

Redaktor naczelny
Paweł Goźliński
Producenci wydawniczy
Małgorzata Skowrońska, Robert Kijak
Koordynacja projektu
Magdalena Kosińska

Copyright © 2014 by Glenn Greenwald. All Rights Reserved.
Published by arrangement with Henry Holt and Company, LLC, New York.
Copyright © 2014, Agora SA

Warszawa 2014
ISBN: 978-83-268-1340-5

Druk
Drukarnia Perfekt

Wszelkie prawa zastrzeżone

GLENN GREENWALD

SNOWDEN

NIGDZIE SIĘ NIE UKRYJESZ

Tę książkę dedykuję wszystkim, którzy starali się rzucić światło na prowadzone przez rząd USA tajne programy powszechnej inwigilacji, a szczególnie tym odważnym sygnalistom, którzy dla tej sprawy ryzykowali wolność.

Glenn Greenwald

Rząd Stanów Zjednoczonych udoskonalił potencjał technologiczny umożliwiający nam monitorowanie przesyłanych wiadomości. [...] Ten potencjał może być w każdej chwili zwrócony przeciwko narodowi amerykańskiemu i żaden Amerykanin nie będzie się już cieszył prywatnością, taki bowiem jest potencjał monitorowania wszystkiego – rozmów telefonicznych, telegramów, nie ma znaczenia czego. Nie sposób będzie się ukryć.

– **senator Frank Church**, przewodniczący Senackiej Komisji Specjalnej do Badania Operacji Rządowych w odniesieniu do Działań Wywiadu, 1975

WSTĘP

Jesienią 2005 roku postanowiłem założyć polityczny blog. Nie miałem pojęcia, do jakiego stopnia ta decyzja zmieni moje życie. Kierowało mną przede wszystkim rosnące zaniepokojenie radykalnymi i ekstremistycznymi teoriami władzy przyjętymi przez rząd USA w następstwie ataków z 11 września 2001 roku na Nowy Jork i Waszyngton. Miałem nadzieję, że pisząc o tych sprawach, osiągnę więcej, niż działając jako prawnik specjalizujący się w kwestiach przestrzegania konstytucji i praw człowieka.

Nie minęło nawet siedem tygodni od mojego pierwszego wpis, gdy „New York Times" opublikował sensacyjny artykuł: w 2001 roku administracja George'a W. Busha wydała tajny rozkaz Agencji Bezpieczeństwa Narodowego (National Security Agency, NSA), by podsłuchiwała połączenia elektroniczne Amerykanów bez nakazu sądowego, wymaganego stosownym przepisem prawa karnego. W chwili ujawnienia tej informacji podsłuchy prowadzono już od czterech lat, obejmując nimi co najmniej kilka tysięcy Amerykanów.

W tej sprawie znakomicie splatały się moja pasja i doświadczenie. Rząd usiłował uzasadnić tajny program NSA, odwołując się do tej właśnie skrajnej teorii władzy wykonawczej, która skłoniła mnie do rozpoczęcia pisania. Najważniejsze było w niej przekonanie, że zagrożenie terroryzmem nadaje prezydentowi praktycznie nieograniczone prawo do wszelkich działań służących „zapewnieniu bezpieczeństwa narodowi",

w tym także prawo do łamania prawa. Wynikła z tego debata dotyczyła skomplikowanych kwestii prawa konstytucyjnego i interpretacji ustaw. Dzięki prawniczemu wykształceniu byłem dobrze przygotowany, by się nimi zająć.

Rozliczne aspekty podsłuchów, prowadzonych przez NSA bez nakazu, opisywałem przez następne dwa lata na blogu i w bestsellerowej książce wydanej w 2006 roku. Moje stanowisko było jednoznaczne: rozkazując prowadzić nielegalne podsłuchy, prezydent popełnił przestępstwo i powinien za nie odpowiedzieć. W coraz bardziej szowinistycznym i dusznym klimacie politycznym Ameryki pogląd ten okazał się niezwykle kontrowersyjny. Kilka lat później dzięki temu, że krytykowałem działania rządu to do mnie, zwrócił się Edward Snowden, gdy postanowił ujawnić występki NSA na jeszcze większą skalę. Uznał, że może liczyć, iż zrozumiem niebezpieczeństwo związane z masową inwigilacją i skrajną tajemniczością państwa, oraz że nie cofnę się w obliczu nacisków ze strony rządu i jego licznych sojuszników w mediach i poza nimi.

Niezwykła objętość ściśle tajnych dokumentów, które Snowden mi przekazał, w połączeniu z dramatyczną otoczką sprawy samego Snowdena wywołały na całym świecie bezprecedensowe zainteresowanie zagrożeniem ze strony masowej inwigilacji elektronicznej i wagą prywatności w epoce cyfrowej. Problemy leżące u podstaw tej inwigilacji narastały jednak od lat, tyle że pozostawały niejawne.

Obecne kontrowersje w sprawie NSA mają niewątpliwie wiele aspektów. Rozwój technologii umożliwił taki rodzaj wszechobecnej inwigilacji, jaki uprzednio istniał jedynie w wyobraźni najbardziej pomysłowych autorów science fiction. Ponadto zrodzone po 11 września amerykańskie uwielbienie dla bezpieczeństwa ponad wszystko stworzyło klimat szczególnie sprzyjający nadużyciom władzy. Dzięki odwadze Snowdena i stosunkowej łatwości kopiowania informacji cyfrowych

otrzymaliśmy z pierwszej ręki wyjątkowy wgląd w szczegóły tego, jak system nadzoru rzeczywiście funkcjonuje.

Kwestie wywołane przez historię NSA stanowią pod wieloma względami echo licznych epizodów z przeszłości, nawet sprzed kilku stuleci. Co więcej, sprzeciw wobec naruszania prywatności przez rząd był jednym z głównych czynników decydujących o samym powstaniu Stanów Zjednoczonych – warto pamiętać, że mieszkańcy amerykańskich kolonii zaprotestowali przeciwko prawu zezwalającemu brytyjskim urzędnikom dowolnie plądrować każdy dom. Osadnicy zgadzali się, że państwu wolno zgodnie z prawem uzyskiwać nakazy rewizji, dotyczące konkretnych osób, jeśli istnieją dowody sugerujące, że osoby te mogły popełnić przestępstwo. Jednak nakazy ogólne – praktyka wystawiająca wszystkich obywateli na niczym nieograniczone przeszukania – były z natury rzeczy nielegalne.

Czwarta poprawka do konstytucji wprowadziła tę zasadę do amerykańskiego prawa. Jej język jest jasny i klarowny: „Prawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez bezzasadne rewizje i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone". Przede wszystkim chodziło o to, by w Ameryce rząd nigdy już nie miał prawa poddawać obywateli uogólnionej, pozbawionej podstaw inwigilacji.

Spór na temat inwigilacji w XVIII wieku dotyczył rewizji w domach, ale w miarę postępu technologii rozwijała się także sama inwigilacja. W połowie XIX wieku, gdy rozbudowa kolei umożliwiła tanie i szybkie usługi pocztowe, w Wielkiej Brytanii wybuchł skandal wywołany odkryciem, że rząd potajemnie otwiera listy. W początkach XX wieku Amerykańskie Biuro Śledcze – poprzednik dzisiejszego FBI – korzystało

z podsłuchów, monitorowania przesyłek pocztowych i informatorów, by ściśle kontrolować tych, którzy sprzeciwiali się polityce rządu.

Niezależnie od stosowanych w danej chwili konkretnych technik, w sensie historycznym masowa inwigilacja miała kilka stałych cech. Początkowo jej celem stawali się zawsze dysydenci i ludzie żyjący na marginesie, co sprawiało, że osoby popierające rząd lub po prostu apatyczne błędnie wierzyły, że ich to nie dotyczy. Historia pokazuje jednak, że samo istnienie aparatu masowej inwigilacji – niezależnie od tego, jak jest używany – wystarczy do zduszenia protestu. Obywatele – świadomi, że są cały czas obserwowani – szybko stają się ulegli i lękliwi.

Podjęte w połowie lat 70. ubiegłego wieku przez senatora Franka Churcha dochodzenie w sprawie działań szpiegowskich prowadzonych przez FBI na terenie kraju przyniosło szokujące informacje, że Biuro uznało pół miliona obywateli USA za potencjalnych „wywrotowców" – wyłącznie na podstawie ich przekonań politycznych – więc rutynowo ich szpiegowało (lista celów FBI obejmowała całe spektrum od Martina Luthera Kinga po Johna Lennona, od Ruchu Wyzwolenia Kobiet po antykomunistyczne John Birch Society). Jednak plaga nadużywania nadzoru występowała w historii nie tylko Ameryki. Wręcz przeciwnie, masowa inwigilacja kusi każdą pozbawioną skrupułów władzę. I w każdym przypadku motyw jest ten sam: stłumienie głosów sprzeciwu i narzucenie uległości.

A zatem inwigilacja łączy rządy o skądinąd całkowicie odmiennych profilach politycznych. Na początku XX wieku brytyjskie i francuskie imperia utworzyły specjalne departamenty nadzoru mające przeciwdziałać zagrożeniom ze strony ruchów antykolonialnych. Po II wojnie światowej Ministerstwo Bezpieczeństwa Państwowego NRD, powszechnie znane jako Stasi, stało się synonimem rządowej ingerencji w życie osobiste obywateli. Ostatnio zaś, gdy powszechne protesty podczas

arabskiej wiosny zagroziły władzy dyktatorów, reżymy rządzące w Syrii, Egipcie i Libii starały się śledzić, jak krajowi dysydenci korzystają z internetu.

Dochodzenia przeprowadzone przez Bloomberg News i „Wall Street Journal" wykazały, że gdy tylko te dyktatury poczuły zagrożenie ze strony protestujących, natychmiast wyruszyły do zachodnich firm technologicznych na zakupy narzędzi służących inwigilacji. Reżym Asada w Syrii sprowadził pracowników Area SpA, włoskiej firmy zajmującej się inwigilacją; Syryjczycy powiedzieli im, że „pilnie potrzebują wytropić ludzi". W Egipcie tajna policja Mubaraka nabyła urządzenia umożliwiające przełamanie kodowania Skype'a i podsłuchiwanie połączeń działaczy opozycji. A w Libii, jak donosił „Wall Street Journal", dziennikarze i powstańcy, którzy w 2011 roku weszli do rządowego centrum monitoringu, znaleźli „całą ścianę czarnych urządzeń wielkości lodówki" pochodzących z francuskiej firmy Amesys. Urządzenia te „kontrolowały ruch w internecie" głównego libijskiego dostawcy usług internetowych, „czytając e-maile, odgadując hasła, śledząc czaty online i rysując powiązania między różnymi podejrzanymi".

Możliwość podsłuchiwania wymienianych przez ludzi wiadomości daje ogromną władzę tym, którzy to robią. Jeśli taka władza nie jest ograniczana przez rygorystyczny nadzór i odpowiedzialność, niemal na pewno będzie nadużywana. Wiara, że rząd USA może w głębokim sekrecie sterować potężną machiną inwigilacji i nie ulec jej pokusom, jest sprzeczna ze wszystkimi precedensami historycznymi i tym, co wiemy o naturze ludzkiej.

Oczywiście przekonanie, że Stany Zjednoczone są w kwestii inwigilacji wyjątkiem, byłoby naiwnością nawet przed rewelacjami Snowdena. W 2006 roku podczas wysłuchania w Kongresie na temat „Internet w Chinach: narzędzie wolności czy ujarzmiania?" kolejni mówcy potępiali amerykańskie firmy

technologiczne za okazywaną władzom w Pekinie pomoc w tłumieniu niezadowolenia w sieci. Przewodniczący wysłuchaniu kongresman Christopher Smith (republikanin z New Jersey) porównał współpracę Yahoo! z chińskimi tajnymi służbami do wydania Anny Frank hitlerowcom. Była to głośna tyrada, typowa dla amerykańskich urzędników, gdy mówią o reżymie niesprzymierzonym z USA.

Jednak nawet ci, którzy uczestniczyli w tym wysłuchaniu, nie mogli zignorować faktu, że odbywało się ono zaledwie dwa miesiące po publikacji „New York Timesa" ujawniającej ogromną skalę krajowych podsłuchów prowadzonych bez nakazu sądowego przez administrację Busha. W świetle tych rewelacji potępianie innych państw za prowadzenie inwigilacji we własnych krajach brzmiało raczej pusto. Kongresman Brad Sherman (demokrata z Kalifornii), który występował po kongresmanie Smisie, wskazał, że firmy technologiczne, którym nakazuje się opór wobec władz chińskich, powinny także ostrożnie podchodzić do żądań własnego rządu. „Inaczej – ostrzegał proroczo – podczas gdy prywatność mieszkańców Chin zostaje pogwałcona w niezwykle haniebny sposób, także i my w Stanach Zjednoczonych kiedyś być może odkryjemy, że jakiś przyszły prezydent, przyjmując bardzo szeroką interpretację konstytucji, czyta nasze e-maile. A wolałbym, by nie dochodziło do tego bez nakazu sądu".

W minionych dziesięcioleciach przywódcy USA wykorzystywali strach przed terroryzmem – nieustannie podsycany wyolbrzymianiem rzeczywistego zagrożenia – do uzasadnienia szerokiego zestawu skrajnych rozwiązań politycznych. Doprowadziło to do agresywnych wojen, stosowania tortur oraz zatrzymywania (a nawet zabijania) obywateli innych państw i obywateli amerykańskich bez stawiania im zarzutów. Jednak zrodzony przez ten strach wszechobecny tajny system inwigilacji, którego istnienia się nie podejrzewa, może okazać się

jego najtrwalszą spuścizną. Dzieje się tak, bo pomimo wszystkich historycznych porównań obecny skandal z inwigilacją przez NSA przybrał nowy wymiar na skutek roli, jaką w naszym codziennym życiu odgrywa internet.

Szczególnie dla młodszego pokolenia nie jest on jakąś wyodrębnioną, oddzielną domeną, w której realizuje się kilka życiowych funkcji. Jest nie tylko naszym urzędem pocztowym i naszym telefonem. Jest raczej epicentrum naszego świata, miejscem, gdzie robi się niemal wszystko. Tam zawiązuje się przyjaźnie, tam wybiera się lektury i filmy, tam organizuje się aktywność polityczną, tam tworzy się i przechowuje najbardziej osobiste informacje. Tam rozwijamy i wyrażamy swoją osobowość i tożsamość.

Zmiana *tej* sieci w system masowej inwigilacji pociąga za sobą takie konsekwencje, jakich nie miały żadne poprzednie państwowe programy szpiegowskie. Dotychczasowe były bardziej ograniczone i można było ich uniknąć. Jeśli pozwolimy, żeby inwigilacja w internecie zapuściła korzenie, będzie to oznaczało, że niemal wszystkie formy kontaktów międzyludzkich, naszego zachowania, a nawet samo myślenie podporządkujemy wszechstronnej kontroli państwa.

Od czasu, gdy go użyto po raz pierwszy, internet – zdaniem wielu – zdobył niezwykły potencjał: zdolność wyzwolenia setek milionów ludzi przez demokratyzację dyskursu politycznego i wyrównywania szans między tymi, którzy mają władzę, a bezsilnymi. Wolność internetu – umiejętność korzystania z sieci bez instytucjonalnych ograniczeń, kontroli społecznej czy państwowej i bez przejmującego strachu – jest niezbędnym warunkiem urzeczywistnienia tej możliwości. Zmiana internetu w system inwigilacji oznacza zatem przekreślenie jego zasadniczego potencjału. Co gorsza, internet staje się wówczas narzędziem ucisku, które grozi stworzeniem

najskrajniejszej i najbardziej opresyjnej ingerencji państwa, jaką zna historia ludzkości.

Dlatego właśnie to, co przedstawił Snowden, jest tak oszałamiające i tak niezwykle ważne. Odważając się ujawnić zdumiewające możliwości inwigilacji przez NSA i jeszcze bardziej zdumiewające ambicje Agencji, jasno pokazał, że stoimy na historycznym rozdrożu. Czy era cyfrowa pozwoli na wyzwolenie jednostki i swobody polityczne, którym tylko internet może dać początek, czy też raczej wprowadzi system wszechobecnego nadzoru i kontroli wykraczający poza marzenia największych nawet dawnych tyranów? W tej chwili obie drogi są możliwe. Nasze działania zadecydują, dokąd dojdziemy.

ROZDZIAŁ I

KONTAKT

Pierwszego grudnia 2012 roku otrzymałem wiadomość od Edwarda Snowdena, choć wówczas nie miałem pojęcia, że to on.

Nadawca e-maila podpisał się „Cincinnatus", nawiązując w ten sposób do rzymskiego rolnika Lucjusza Kwinkcjusza Cincinnatusa. W V wieku p.n.e., w obliczu zagrożenia najazdem, mianowano go dyktatorem Rzymu, by bronił miasta. Zapisał się w historii dzięki temu, co uczynił po pokonaniu wrogów: natychmiast i z własnej woli zrzekł się władzy i powrócił do pracy na roli. Uznany za „wzór cnót obywatelskich", Cincinnatus stał się symbolem sprawowania władzy politycznej w interesie publicznym oraz wartości ograniczenia czy nawet wyrzeczenia się rządów przez jednostkę dla wspólnego dobra.

E-mail zaczynał się od stwierdzenia: „Bezpieczeństwo komunikacji między ludźmi jest dla mnie bardzo ważne", i namawiał mnie do zainstalowania programu szyfrującego PGP. Autor wiadomości chciał bowiem przekazać mi informacje, które – jak pisał – na pewno mnie zainteresują. Opracowane w 1991 roku PGP oznacza „pretty good privacy" („całkiem niezła prywatność"); jest to wyrafinowane narzędzie do ochrony e-maili oraz innych form łączności internetowej przed inwigilacją i włamaniami do komputerów.

Zasada działania programu polega na tym, że osłania każdy e-mail ochronną tarczą w postaci hasła składającego się

z setek, a nawet tysięcy przypadkowych liczb oraz wielkich i małych liter.

Najbardziej rozwinięte agencje wywiadu na świecie – a do takich niewątpliwie należy NSA – dysponują oprogramowaniem do łamania haseł zdolnym generować miliard propozycji na sekundę. Jednak hasła kodowania PGP są tak długie i losowe, że nawet najbardziej wyrafinowane oprogramowanie potrzebuje lat, by je złamać. Ci, którzy szczególnie obawiają się monitorowania swoich połączeń – agenci wywiadu, szpiedzy, działacze na rzecz praw człowieka czy hakerzy – chronią swoje wiadomości tym właśnie programem kodującym. „Cincinnatus" napisał w e-mailu, że wszędzie szukał mego „publicznego klucza" PGP, narzędzia pozwalającego wymieniać zakodowane wiadomości, ale bezskutecznie; doszedł zatem do wniosku, że nie używam tego programu. Stwierdził więc: „To wystawia na ryzyko każdego, kto się z Panem komunikuje. Nie twierdzę, że wszystkie Pana wiadomości muszą być szyfrowane, ale przynajmniej powinien Pan zapewnić swoim korespondentom taką możliwość".

„Cincinnatus" przypomniał w tym miejscu skandal z generałem Davidem Petraeusem. Agenci odkryli jego pozamałżeński romans z dziennikarką Paulą Broadwell, analizując e-maile, jakie ta para wymieniała między sobą za pośrednictwem Google. To zaś położyło kres karierze generała, wcześniej mianowanego przez Baracka Obamę dyrektorem CIA.

Gdyby Petraeus zakodował swoje wiadomości przed powierzeniem ich Gmailowi, agenci nie zdołaliby ich odczytać – pisał „Cincinnatus". „Szyfrowanie ma znaczenie, i to nie tylko dla szpiegów i flirciarzy". Zainstalowanie programu szyfrującego e-maile „to absolutnie konieczny środek bezpieczeństwa dla każdego, kto chciałby się z Panem porozumieć". By zachęcić mnie do pójścia za jego radą, dodał: „Są tacy ludzie, którzy dysponują niewątpliwie interesującymi dla Pana informacjami, ale

nie będą mogli się z Panem porozumieć, póki nie będą pewni, że nikt po drodze nie przeczyta ich e-maili".

Potem zaproponował, że pomoże mi zainstalować program: „Jeśli potrzebna Panu pomoc, proszę dać mi znać albo poprosić o pomoc na Twitterze. Ma Pan wielu zaawansowanych technicznie zwolenników, którzy chętnie i natychmiast zaoferują pomoc". Podpisał się: „Dziękuję. C.".

Już dawno zamierzałem zainstalować w komputerze program szyfrujący. Od lat pisałem o WikiLeaks, sygnalistach (*whistleblowers*), kolektywie aktywistów internetowych znanym jako Anonymous i powiązanych z tym tematach. Od czasu do czasu porozumiewałem się także z ludźmi pracującymi na rzecz bezpieczeństwa narodowego. Większość z nich bardzo dba o bezpieczeństwo korespondencji i zapobiega wścibskiemu monitorowaniu. Jednak program jest skomplikowany, szczególnie dla kogoś takiego jak ja, kto niezbyt dobrze radzi sobie z programowaniem i komputerami. Była to więc jedna z tych rzeczy, do których się jakoś nigdy nie zabrałem.

Mail od C. nie skłonił mnie do działania. Ponieważ wiadomo było, że często zajmuję się sprawami ignorowanymi przez inne media, pisują do mnie ludzie oferujący „wielką sprawę", która zazwyczaj okazuje się niczym. Poza tym cały czas pracuję nad większą liczbą tematów, niż jestem w stanie ogarnąć. Dlatego też, żeby zostawić to, co robię, i zająć się nową sprawą, muszę mieć coś konkretnego. Mimo niejasnej aluzji, że „są tacy ludzie", którzy „dysponują niewątpliwie interesującymi informacjami", w e-mailu od C. nie znalazłem nic wystarczająco kuszącego. Przeczytałem go, ale nie odpowiedziałem.

Trzy dni później dostałem od C. kolejną wiadomość z prośbą o potwierdzenie, że poprzednia do mnie dotarła. Tym razem odpisałem szybko: „Otrzymałem i zamierzam się tym zająć.

Nie mam klucza PGP i nie wiem, jak to zrobić, postaram się jednak znaleźć kogoś, kto mi pomoże".

Odpisał jeszcze tego samego dnia, przysyłając jasną, łopatologiczną instrukcję do systemu PGP – typu „szyfrowanie dla bystrzaków". Pod koniec wskazówek, które – głównie z powodu własnej ignorancji – uznałem za skomplikowane i niejasne, napisał, że są to „same podstawy. Jeśli nie znajdzie Pan nikogo, kto by Pana przeprowadził przez instalację, generowanie i użytkowanie, proszę dać mi znać". I dodał: „Mogę ułatwić kontakt z ludźmi znającymi się na kryptografii niemal wszędzie na świecie".

Ten e-mail kończył się z większym polotem niż dwa poprzednie:

„Z kryptograficznym pozdrowieniem,
Cincinnatus".

Mimo szczerych zamiarów nigdy jakoś nie znalazłem czasu, by się tym zająć. Minęło siedem tygodni i świadomość tej zwłoki nieco mi ciążyła. A co, jeśli ten człowiek naprawdę ma ważny temat, który przegapię tylko dlatego, że nie zainstalowałem jednego programu komputerowego? Pomijając wszystko inne, wiedziałem, że kodowanie może mi się przydać w przyszłości, nawet jeśli „Cincinnatus" nie będzie miał mi nic ciekawego do zaoferowania.

Dwudziestego ósmego stycznia 2013 roku napisałem do niego, że znajdę kogoś, kto mi pomoże z instalacją, mam więc nadzieję, że za dzień czy dwa będę już gotów. Odpisał nazajutrz: „Wspaniała wiadomość! Jeśli potrzebuje Pan dalszej pomocy albo będzie miał w przyszłości pytania, bardzo proszę dać mi znać. Proszę przyjąć moje szczere podziękowania za popieranie prywatności korespondencji! Cincinnatus".

Znów jednak nic nie zrobiłem, zajęty wówczas innymi tematami i wciąż nieprzekonany, że C. ma coś wartego mojego czasu.

To nie była świadoma decyzja, żeby nic nie robić. Po prostu na mojej zawsze aż nazbyt długiej liście zadań instalowanie programu szyfrującego na prośbę nieznanej osoby nigdy nie stało się na tyle pilne, bym się na tym skupił kosztem innych spraw.

C. i ja wpadliśmy w Paragraf 22. On nie chciał powiedzieć mi niczego konkretnego o tym, co ma, a nawet kim jest i gdzie pracuje, dopóki nie zainstaluję szyfrowania. A ja bez zachęty w postaci konkretów nie spieszyłem się, by spełnić jego prośbę i poświęcić trochę czasu instalacji programu.

W obliczu mojej bezczynności C. nasilił działania. Wyprodukował dziesięciominutowy film wideo „PGP dla dziennikarzy". Wykorzystując software generujący głos, film instruował w łatwy sposób, krok po kroku, jak zainstalować program kodujący. Zawierał też diagramy i ilustracje.

A ja wciąż to ignorowałem. Jak mi później powiedział C., w tym momencie poczuł się zniechęcony. „To ja jestem gotów zaryzykować wolność, a nawet może życie – myślał – by przekazać temu facetowi tysiące ściśle tajnych dokumentów z najbardziej skrytej agencji w kraju – przeciek, który przyniesie dziesiątki, jeśli nie setki sensacyjnych dziennikarskich materiałów – a jemu się nawet nie chce zainstalować programu kodującego!".

Znalazłem się właśnie blisko utraty jednego z największych i obarczonych największymi konsekwencjami przecieków na temat bezpieczeństwa narodowego w historii Stanów Zjednoczonych.

Następny raz sprawa bezpieczeństwa kontaktów wróciła do mnie dziesięć tygodni później. 18 kwietnia poleciałem z domu w Rio de Janeiro do Nowego Jorku, gdzie miałem wygłosić kilka prelekcji na temat zagrożeń wynikających z sekretnych działań rządu i naruszania wolności obywatelskich.

Wylądowawszy na lotnisku Kennedy'ego, zobaczyłem, że czeka na mnie e-mail od dokumentalistki Laury Poitras:

„Czy przypadkiem nie wybierasz się do Stanów w najbliższym tygodniu? Chciałabym bardzo się z tobą skontaktować w jednej sprawie, najlepiej osobiście". Poważnie traktuję wszystkie wiadomości od Laury Poitras, jednej z najbardziej zdecydowanych, nieustraszonych i niezależnych osób, jakie znam. Kręciła film za filmem w bardzo ryzykownych warunkach, bez ekipy czy wsparcia ze strony firm medialnych, ze skromnym budżetem, jedną kamerą, napędzana wyłącznie własną determinacją. W kulminacyjnym momencie wojny w Iraku zapuściła się w sunnicki trójkąt, by nakręcić *Mój kraju!*, bezkompromisowe spojrzenie na życie pod amerykańską okupacją; ten film został nominowany do Oscara. Następny film, *Przysięgę*, kręciła w Jemenie, gdzie przez kilka miesięcy towarzyszyła dwóm Jemeńczykom – ochroniarzowi Osamy bin Ladena i jego kierowcy. Ostatnio Poitras pracowała nad filmem o inwigilacji przez NSA, co sprawiło, że władze nękały ją, ilekroć wjeżdżała do kraju lub go opuszczała.

Dzięki Laurze nauczyłem się czegoś cennego. Zanim poznaliśmy się w 2010 roku, Wydział Bezpieczeństwa Krajowego już kilkanaście razy zatrzymywał ją na lotnisku w chwili przyjazdu do Stanów Zjednoczonych. Przesłuchiwano ją, grożono jej, konfiskowano jej reporterskie notatki, filmy i laptopy. Laura jednak nie decydowała się publicznie mówić o tym nieustannym nękaniu, obawiając się, że reperkusje całkowicie uniemożliwią jej pracę. Zmieniło się to po wyjątkowo agresywnym przesłuchaniu na lotnisku Newark. Laura miała dość: „Moje milczenie sprawia, że jest coraz gorzej, a nie lepiej". Była gotowa, bym o tym napisał.

Artykuł, który zamieściłem w internetowym magazynie politycznym *Salon*, dokładnie opisywał nieustanne przesłuchania, jakim Poitras poddawano. Spotkał się ze znaczną uwagą, spowodował napływ wyrazów poparcia dla niej i potępienia dla prześladowców. Gdy po opublikowaniu artykułu wyjeżdżała

z kraju, tym razem nie przesłuchiwano jej i nie skonfiskowano materiałów. Nie nękano jej także w następnych miesiącach. Po raz pierwszy od lat Laura mogła swobodnie podróżować.

Zrozumiałem, że urzędnicy bezpieczeństwa narodowego nie lubią światła. Działają napastliwie i po bandycku tylko wtedy, gdy uważają, że są bezpieczni, w mroku. Dowiedzieliśmy się, że niejawność to podstawa nadużywania władzy, siła, która pozwala jej działać. Jedynym prawdziwym lekarstwem jest przejrzystość.

Na e-mail Laury odpowiedziałem od razu z lotniska: „Właśnie dziś rano przyleciałem do USA [...] Gdzie jesteś?". Umówiliśmy się na następny dzień w holu mego hotelu w Yonkers. Poszliśmy do restauracji, gdzie na nalegania Laury dwukrotnie zmienialiśmy stolik, by na pewno nikt nie mógł usłyszeć naszej rozmowy. Wtedy dopiero Laura powiedziała, o co chodzi. Oświadczyła, że chce ze mną przedyskutować „niezwykle ważną i poufną sprawę", więc bezpieczeństwo jest tu kluczowe.

Miałem przy sobie telefon komórkowy. Laura poprosiła, żebym albo wyjął z niego baterię, albo odniósł go do pokoju hotelowego. Przyznała, że to brzmi paranoicznie, ale rząd ma możliwość zdalnego aktywowania telefonów komórkowych i laptopów, by użyć ich do podsłuchu. Samo wyłączenie nie wystarczy – trzeba usunąć baterię. O tym, że to możliwe, słyszałem już wcześniej od działaczy na rzecz przejrzystości oraz hakerów, przypisywałem to jednak ich nadmiernej ostrożności. Tym razem potraktowałem informację poważnie, ponieważ jej źródłem była Laura. Sprawdziwszy, że z mojej komórki nie da się wyjąć baterii, odniosłem telefon do pokoju.

Gdy wróciłem do restauracji, Laura zaczęła mówić. Wyjaśniła, że otrzymała serię anonimowych e-maili od kogoś, kto wydaje się i uczciwy, i poważny. Ten człowiek twierdzi, że ma dostęp do niezwykle tajnych dokumentów obciążających rząd

USA, a dotyczących szpiegowania własnych obywateli i reszty świata. Postanowił ujawnić te dokumenty i wyraźnie zażyczył sobie, by przy ich omawianiu i publikacji współpracowała ze mną. W tamtym momencie nie powiązałem jej słów z e-mailami, które otrzymałem od „Cincinnatusa". Tamte spoczywały w głębi mej pamięci, ukryte.

Laura wyciągnęła z plecaka kilka kartek: dwa e-maile przysłane przez anonimowego korespondenta. Przeczytałem je tam, przy stoliku, od początku do końca.

Przykuwały uwagę.

Drugi z e-maili, wysłany kilka tygodni po pierwszym, zaczynał się: „Wciąż tu jestem". Jakby odpowiadając na pytanie, które pierwsze przyszło mi do głowy – kiedy będzie gotów udostępnić dokumenty – napisał: „mogę jedynie powiedzieć, że wkrótce".

Informator nalegał, by Laura zawsze usuwała baterie z telefonów komórkowych, zanim zacznie omawiać drażliwe tematy – albo przynajmniej wkładała telefony do zamrażalnika, gdzie ich potencjał podsłuchowy będzie znacznie mniejszy. Następnie powtórzył, że powinna pracować nad dokumentami ze mną, a w końcu dotarł do tego, co uważał za sedno swojej misji:

Szok tego pierwszego okresu [po ujawnieniu pierwszych dokumentów] zapewni wsparcie potrzebne do budowy sprawiedliwszego internetu, nie będzie to jednak działać na korzyść przeciętnego człowieka, chyba że nauka wyprzedzi prawo. Możemy wygrać ten etap dzięki zrozumieniu mechanizmów, które służą do naruszania naszej prywatności. Uda nam się zagwarantować wszystkim ludziom równą ochronę przed nieuzasadnionym przeszukaniem dzięki prawom uniwersalnym, ale tylko wtedy, jeśli techniczna społeczność będzie gotowa zmierzyć się z zagrożeniem i wypracować odpowiednie inżynierskie rozwiązania. Na koniec musimy wprowadzić zasadę, że potężni ludzie mogą cieszyć się prywatnością

jedynie wówczas, jeśli mogą się nią cieszyć także zwykli ludzie: zasadę ustanowioną przez prawa natury, a nie politykę człowieka.

– Jest prawdziwy – powiedziałem, doczytawszy do końca. – Nie wiem dlaczego, ale intuicyjnie czuję, że to poważna sprawa, że jest dokładnie tym, kim mówi.

– Ja też – odparła Laura. – Właściwie nie mam wątpliwości.

Na rozum i logikę Laura i ja wiedzieliśmy, że nasza wiara w prawdomówność informatora nie ma podstaw. Nie mieliśmy pojęcia, kto do niej pisze. To mógł być ktokolwiek. Mógł wymyślić sobie całą historię. Mogła to być także pułapka zastawiona przez rząd, by nas dopaść za współpracę przy przestępczym przecieku. A może był to ktoś, kto chciał zniszczyć naszą wiarygodność, przekazując nam do publikacji sfałszowane dokumenty.

Rozważaliśmy wszystkie te możliwości. Wiedzieliśmy, że tajny raport armii USA w 2008 roku uznał portal WikiLeaks za wroga państwa i proponował różne sposoby, na jakie można „wyrządzić szkodę [tej organizacji] i potencjalnie ją zniszczyć". W raporcie (który, o ironio, wyciekł do WikiLeaks) między innymi rozważano możliwość podsunięcia fałszywych dokumentów. Gdyby WikiLeaks opublikowało je jako autentyczne, zadałoby to poważny cios jego wiarygodności.

Laura i ja byliśmy świadomi wszystkich tych pułapek, ale podeszliśmy do nich sceptycznie, zawierzając intuicji. Coś nieuchwytnego, ale potężnego w tych e-mailach przekonywało nas, że autor jest autentyczny. Pisał kierowany głęboką wiarą w niebezpieczeństwo tkwiące w sekretnych działaniach rządu i wszechobecnym szpiegostwie; instynktownie rozpoznawałem jego polityczne zaangażowanie. Czułem więź z naszym korespondentem, z jego światopoglądem i najwyraźniej zżerającą go niecierpliwością.

Przez minione siedem lat w swojej pracy kierowałem się tymi samymi przekonaniami; niemal codziennie pisałem

o niebezpiecznych tendencjach w utajnianiu spraw przez państwo, nadużywaniu władzy, inwigilacji i naruszaniu wolności obywatelskich. Dziennikarzy, aktywistów i moich czytelników, ludzi podobnie zaniepokojonych tymi tendencjami, łączy pewien szczególny ton i postawa. Tłumaczyłem sobie, że komuś, kto nie ma głębokiej wiary i nie czuje tego niepokoju, trudno byłoby naśladować ten ton tak dokładnie, z taką autentycznością.

W jednym z końcowych fragmentów e-maila do Laury jej korespondent napisał, że wchodzi w ostatnią fazę działań koniecznych, by mógł udostępnić nam dokumenty. Potrzebował jeszcze czterech do sześciu tygodni, powinniśmy zatem czekać na wiadomość. Zapewnił nas, że się odezwie.

Trzy dni później ponownie spotkałem się z Laurą, tym razem na Manhattanie, by przeczytać kolejny e-mail od anonimowego informatora. Wyjaśniał w nim, dlaczego jest gotów zaryzykować wolność i prawdopodobnie narazić się na długoletnie więzienie, by tylko ujawnić dokumenty. Teraz czułem jeszcze głębsze przekonanie, że nasze źródło jest autentyczne, ale – jak powiedziałem swemu partnerowi Davidowi Mirandzie podczas powrotnego lotu do domu w Brazylii – postanowiłem przestać o tym myśleć.

– To się może skończyć na niczym. Może zmienić zdanie. Mogą go złapać.

David jest człowiekiem o ogromnej intuicji. Był dziwnie przekonany.

– Ta sprawa jest prawdziwa. On jest prawdziwy. To się wydarzy – stwierdził. – I to będzie coś wielkiego.

Po moim powrocie do Rio przez trzy tygodnie nic się nie działo, aż 11 maja otrzymałem e-mail od technika, dawnego współpracownika Laury. Pisał enigmatycznie, ale zrozumiale: „Hej, Glenn, zamierzam Cię nauczyć używania PGP. Czy masz jakiś

adres, na który mógłbym Ci coś wysłać, żeby Ci pomóc rozpocząć w przyszłym tygodniu?".

Najwyraźniej musiałem mieć to „coś", żeby móc pracować nad dokumentami z przecieku. To z kolei oznaczało, że nasz anonimowy korespondent odezwał się do Laury i wysłał jej to, na co czekaliśmy.

Technik nadał Federal Expressem paczkę z terminem dostawy za dwa dni. Nie wiedziałem, czego oczekiwać: programu czy samych dokumentów. Przez następne dwie doby nie potrafiłem się na niczym skupić. W dzień, kiedy przesyłka miała nadejść, czekałem do wpół do szóstej wieczorem i dłużej, ale bez skutku. Zadzwoniłem do FedExu i usłyszałem, że przesyłkę zatrzymano na cle „z nieznanych przyczyn". Minęły dwa dni. Potem pięć. Potem cały tydzień. Codziennie FedEx mówił to samo – że z nieznanych powodów przesyłka wciąż czeka na cle.

Oczywiście przyszła mi do głowy myśl, że brazylijska służba celna zatrzymała paczkę, ponieważ coś obudziło jej niepokój, ale wolałem jeszcze nie odrzucać bardziej prawdopodobnego wyjaśnienia: że to po prostu jedna z tych przypadkowych a drażniących biurokratycznych historii.

Laura nie bardzo chciała o tym rozmawiać ani przez telefon, ani przez internet, nie wiedziałem też dokładnie, co zawiera przesyłka.

Nareszcie, po mniej więcej dziesięciu dniach, FedEx dostarczył mi paczkę. W kopercie znalazłem dwa pendrive'y oraz napisaną na maszynie notatkę zawierającą dokładne instrukcje używania różnych programów komputerowych mających zapewnić maksimum bezpieczeństwa, a także liczne hasła w postaci ciągów znaków do kodowanych kont poczty elektronicznej i innych programów, o których nigdy nie słyszałem.

Nie miałem pojęcia, co to wszystko znaczy. Nigdy przedtem nie słyszałem o tych programach, choć wiedziałem, co to są

hasła w postaci ciągów znaków – składają się z całych przypadkowo zestawionych sekwencji zawierających litery małe i wielkie oraz znaki przestankowe, co ma utrudnić ich złamanie. Wobec tego, że Poitras wciąż okazywała głęboką niechęć do rozmowy telefonicznej lub internetowej, rosło moje zdenerwowanie: w końcu dostałem to, na co czekałem, ale nie miałem pojęcia, dokąd mnie to zaprowadzi.

Miałem się wkrótce dowiedzieć od możliwie najlepszego przewodnika.

Dzień po otrzymaniu przesyłki, 20 maja, Laura poinformowała mnie, że pilnie musimy porozmawiać, ale jedynie przez OTR (off-the-record), protokół kryptograficzny dla bezpiecznych rozmów w internecie. Używałem już wcześniej OTR, a teraz zdołałem zainstalować program czatu, założyłem konto i dodałem nazwisko Laury do listy znajomych. Pojawiła się natychmiast.

Spytałem, czy mam teraz dostęp do tajnych dokumentów. Wyjaśniła, że mogą pochodzić jedynie od naszego informatora, a nie od niej, i dodała zaskakującą informację: być może trzeba będzie natychmiast pojechać na spotkanie z nim do Hongkongu.

Zaskoczyło mnie to. Co ktoś mający dostęp do amerykańskich rządowych dokumentów o najwyższym stopniu tajności robi w Hongkongu? Co ma do tego wszystkiego Hongkong? Zakładałem, że nasz nieznany informator przebywa w stanie Maryland lub w Wirginii. Dlaczego ktoś taki jak on miałby być akurat w Hongkongu? Oczywiście zgodziłbym się udać dokądkolwiek, wolałbym jednak dostać więcej informacji o celu takiego wyjazdu, a fakt, że Laura nie mogła swobodnie rozmawiać, zmusił nas do odłożenia tej dyskusji na później.

Chciałem być pewien, że taki wyjazd ma sens, a konkretnie chciałem wiedzieć, czy udało się jej zweryfikować nasze źródło jako prawdziwe.

– Oczywiście, inaczej nie prosiłabym cię o wyjazd do Hongkongu – odparła zagadkowo. Założyłem, że to znaczy, iż dostała od informatora kilka poważnych dokumentów.

Powiedziała mi też o pewnym narastającym problemie. Informator denerwuje się dotychczasowym przebiegiem sprawy, szczególnie jednym nowym aspektem: możliwym zaangażowaniem „Washington Post". Nalegała, żebym porozmawiał z nim bezpośrednio, ułagodził go i uspokoił jego rosnącą niecierpliwość.

Nie minęła godzina, a informator przysłał mi e-mail.

Ten e-mail przyszedł z adresu verax@[redacted] „Verax" po łacinie oznacza „mówiący prawdę". Temat wiadomości brzmiał: „Musimy porozmawiać".

„Pracuję nad dużym projektem z naszą wspólną znajomą" – zaczynał się tekst wiadomości, co było dla mnie wskazówką, że to on, anonimowe źródło, dotychczas w kontakcie tylko z Laurą. „Niedawno musiał Pan odmówić nagłej podróży na spotkanie ze mną. Musi Pan się włączyć w tę sprawę – napisał. – Czy istnieje jakiś sposób, byśmy mogli szybko porozmawiać? Rozumiem, że nie dysponuje Pan zbyt zaawansowaną infrastrukturą bezpieczeństwa, ale poradzę sobie z tym, co Pan ma". Zasugerował, byśmy porozmawiali przez OTR, i podał mi swoją nazwę użytkownika.

Nie bardzo wiedziałem, co miał na myśli, mówiąc, że „odmówiłem nagłej podróży". Dałem wyraz zdziwieniu, że jest akurat w Hongkongu, ale bynajmniej nie odmówiłem wyjazdu. Przypisałem to jakiemuś nieporozumieniu i odpowiedziałem natychmiast: „Chcę zrobić wszystko, co się da, by się zaangażować w tę sprawę"; i dodałem, że możemy rozmawiać natychmiast. Wpisałem jego nazwę użytkownika na listę znajomych w OTR i czekałem.

Ledwo piętnaście minut później, mój komputer zadźwięczał, dając mi znać, że informator się połączył. Nieco zdenerwowany

kliknąłem na jego nazwę i napisałem: „Cześć". Odpowiedział – i tak zacząłem bezpośrednio rozmawiać z kimś, kto – jak zakładałem – był w posiadaniu nieznanej liczby tajnych dokumentów o amerykańskich programach inwigilacyjnych i kto chciał ujawnić przynajmniej część z nich.

Od razu powiedziałem mu, że jestem absolutnie zdecydowany, by zająć się tym tematem. „Jestem gotów zrobić wszystko, co konieczne, by o tym napisać" – powiedziałem. Informator – którego nazwiska, miejsca zatrudnienia, wieku i żadnych innych danych wciąż nie znałem – chciał wiedzieć, czy przyjadę do Hongkongu, by się z nim spotkać. Nie spytałem, co robi w Hongkongu; nie chciałem sprawiać wrażenia, że wyciągam z niego informacje.

Od samego początku postanowiłem, że pozwolę mu prowadzić. Gdyby chciał, żebym wiedział, dlaczego przebywa w Hongkongu, toby mi powiedział. A jeśli zechce, bym wiedział, jakie ma dokumenty i co zamierza pokazać, to też mi o tym powie. Taka bierna postawa przychodziła mi z trudnością. Jako były prawnik zaangażowany w spory sądowe, a obecnie dziennikarz jestem przyzwyczajony, że uzyskuję odpowiedzi, zadając bezpośrednie pytania, a tym razem chciałem dowiedzieć się setki różnych rzeczy.

Zakładałem jednak, że sytuacja wymaga delikatności. Cokolwiek z tego wszystkiego było prawdą, wiedziałem, że ten człowiek postanowił zrobić coś, co rząd USA uzna za bardzo poważne przestępstwo. A ponieważ nie dysponowałem niemal żadnymi informacjami, z kim właściwie rozmawiam, jaki jest jego sposób myślenia, jego motywy i obawy, oczywiście musiałem zachować ostrożność i powściągliwość. Nie chciałem go odstraszyć, zmusiłem się więc, by pozwalać informacjom napływać, zamiast je wyszarpywać.

– Oczywiście, że przyjadę do Hongkongu – powiedziałem, wciąż nie mając pojęcia, dlaczego akurat tam przebywa i dlaczego chce, bym przyjechał.

Tego dnia rozmawialiśmy online przez dwie godziny. Najbardziej niepokoił się o pewne dokumenty NSA, które przekazał Poitras, a ona – za jego zgodą – rozmawiała o nich z dziennikarzem z „Washington Post" Bartonem Gellmanem. Te dokumenty odnosiły się do jednej konkretnej sprawy: programu zwanego PRISM, umożliwiającego NSA przejmowanie prywatnych rozmów z największych światowych firm internetowych, w tym z Facebooka, Google'a, Yahoo! i Skype'a. Zamiast opublikować tę historię szybko i w mocnej formie, „Washington Post" wciągnął do sprawy duży zespół prawników, którzy teraz wysuwali rozliczne żądania i wygłaszali różnego rodzaju ostrzeżenia. Informator uznał, że „Post", otrzymawszy coś, co jego zdaniem było bezprecedensową dziennikarską sensacją, kieruje się raczej strachem niż przekonaniem i zdecydowaniem. Złościło go także to, że gazeta zaangażowała do sprawy tyle osób, obawiał się bowiem, że przeciągające się dyskusje mogą stanowić zagrożenie dla jego bezpieczeństwa.

– Nie podoba mi się, jak to się rozwija – powiedział. – Chciałem, żeby o tej jednej sprawie, PRISM, pisał ktoś inny, byś ty mógł skupić się na szerszych tematach, szczególnie masowym szpiegostwie w kraju, ale teraz naprawdę wolałbym, żebyś to ty się tym zajął. Od dawna czytam to, co piszesz, i wiem, że zrobisz to odważnie i dynamicznie.

– Jestem gotów i chętny – odparłem. – Zastanówmy się teraz, co mam zrobić.

– Przede wszystkim najważniejsze jest, żebyś przyjechał do Hongkongu – powiedział. Wciąż do tego powracał: *Natychmiast przyjedź do Hongkongu.*

Drugą istotną sprawą, którą omówiliśmy podczas pierwszej rozmowy, były cele naszego informatora. Z e-maili, które mi pokazała Laura, wiedziałem, że kieruje nim potrzeba powiedzenia światu o ogromnym aparacie szpiegowskim potajemnie budowanym przez rząd amerykański. Co jednak ma nadzieję osiągnąć?

– Chciałbym wywołać ogólnoświatową debatę na temat prywatności, wolności internetu i niebezpieczeństw inwigilacji przez państwo – powiedział. – Nie boję się tego, co się ze mną stanie. Zdaję sobie sprawę, że na skutek moich działań najprawdopodobniej nie będę już mógł żyć tak jak dotychczas. Pogodziłem się z tym.

A potem dodał coś zaskakującego: – Chcę się ujawnić jako osoba stojąca za tymi informacjami. Chcę wyjaśnić, dlaczego to robię i co mam nadzieję osiągnąć.

Napisał dokument z zamiarem zamieszczenia go w internecie, gdy jego tożsamość będzie już znana: manifest opowiadający się za prywatnością i przeciwko inwigilacji, który będą mogli podpisywać ludzie na całym świecie, okazując tym samym, że istnieje wszechświatowy ruch popierający ochronę prywatności.

Mimo niemal nieuniknionych konsekwencji ujawnienia się – długiego wyroku więzienia, jeśli nie gorzej – informator powtarzał, że „pogodził się" z takim kosztem.

– W tym wszystkim obawiam się tylko jednego – powiedział. – A mianowicie, że ludzie zobaczą te dokumenty, wzruszą ramionami i powiedzą: „Zakładaliśmy, że tak jest, ale nas to nie obchodzi". Nie chciałbym spaprać sobie życia na próżno.

– Bardzo wątpię, by tak się stało – zapewniłem go, ale nie byłem do końca przekonany, że mam rację. Po latach pisania o nadużyciach ze strony NSA wiedziałem, że czasami trudno jest przekonać ludzi, iż tajny nadzór ze strony państwa powinien być przedmiotem niepokoju; naruszenie prywatności często uważa się za abstrakcję. Co więcej, temat jest nieodmiennie bardzo skomplikowany, co dodatkowo utrudnia przyciągnięcie zainteresowania społeczeństwa.

Tu jednak, miałem wrażenie, chodziło o coś innego. Media zwracają uwagę na przecieki dokumentów o najwyższej tajności. A fakt, że ostrzeżenie pochodzi od kogoś pracującego

w aparacie bezpieczeństwa państwa – a nie od prawnika Amerykańskiego Związku Swobód Obywatelskich (American Civil Liberties Union, ACLU) czy działacza na rzecz wolności obywatelskich – niewątpliwie dodatkowo nada tej sprawie znaczenia.

Tego wieczoru rozmawiałem z Davidem o wyjeździe do Hongkongu. Wciąż raczej z niechęcią myślałem o rzuceniu wszystkiego, nad czym pracuję, by lecieć na drugi koniec świata na spotkanie z kimś, o kim nic nie wiem, nie znam nawet jego nazwiska. A co, jeśli to jakaś pułapka albo inne dziwactwo?

– Powiedz mu może, że najpierw chciałbyś zobaczyć kilka dokumentów, by się przekonać, że mówi serio i że jest to tego warte – zasugerował David.

Jak zwykle posłuchałem jego rady. Gdy następnego ranka nawiązaliśmy kontakt przez OTR, powiedziałem, że za kilka dni zamierzam polecieć do Hongkongu, ale najpierw chciałbym zobaczyć jakieś dokumenty, by się zorientować, w co się pakuję.

Znów usłyszałem, że wymaga to zainstalowania kilku programów. I tak przez następne dwa dni informator krok po kroku przeprowadzał mnie przez proces instalowania i użytkowania każdego programu, w tym, w końcu, kodowania PGP. Wiedząc, że jestem początkujący, okazywał ogromną cierpliwość, instruując mnie dosłownie na poziomie „kliknij na niebieski przycisk, teraz na OK, teraz przejdź do następnego ekranu".

Cały czas przepraszałem za mój brak umiejętności, za to, że musi mi poświęcać tyle godzin, by nauczyć mnie najbardziej podstawowych aspektów bezpiecznego komunikowania się.

– Nie ma sprawy – powiedział. – Większość z tego dość trudno zrozumieć. A akurat teraz mam dużo wolnego czasu.

Po zainstalowaniu wszystkich programów otrzymałem folder zawierający mniej więcej dwadzieścia pięć dokumentów: „Tylko dla pobudzenia apetytu. Czubek czubka góry lodowej" – kusił.

Zdekompresowałem folder, spojrzałem na listę dokumentów i na chybił trafił kliknąłem na jeden z nich. Na górze

strony pojawił się zapisany czerwonymi literami kod: „TOP SECRET/COMINT/NOFORN/". Oznaczało to, że dokument legalnie uznano za ściśle tajny, odnosił się do wywiadu komunikacji (COMINT) i nie wolno go było udostępniać obcokrajowcom, w tym organizacjom międzynarodowym i partnerom koalicyjnym (NOFORN). Oto, czarno na białym, tajny dokument z NSA, jednej z najbardziej skrytych agencji najpotężniejszego rządu na świecie. Nic o podobnym znaczeniu nigdy nie wyciekło z NSA w całej sześćdziesięcioletniej historii Agencji. Teraz zaś miałem w swoim posiadaniu dwadzieścia parę takich dokumentów. A osoba, z którą przez ostatnie dwa dni rozmawiałem przez kilka godzin, miała ich dużo, dużo więcej.

Pierwszy dokument był instrukcją przeznaczoną dla funkcjonariuszy NSA uczącą analityków nowych możliwości inwigilacji. W ogólny sposób omówiono w niej rodzaj informacji, o jakie analitycy mogą pytać (adresy e-mail, dane lokalizacyjne IP, numery telefonów) oraz rodzaje danych, jakie otrzymają w odpowiedzi (treść e-maili, telefoniczne metadane, zapisy czatów). Zasadniczo podsłuchiwałem w tej chwili urzędników NSA instruujących swych analityków, jak podsłuchiwać wybrane cele.

Puls mi przyspieszył, serce biło mocno. Przespacerowałem się kilka razy wokół domu, by się uspokoić, inaczej bowiem nie dałbym rady skupić się i w pełni pojąć tego, co czytam. Wróciłem do laptopa i znów na chybił trafił kliknąłem na któryś dokument, ściśle tajną prezentację w PowerPoincie zatytułowaną „PRISM/US-984XN Overview". Na każdej stronie widniały logo dziewięciu największych firm internetowych, w tym Google'a, Facebooka, Skype'a i Yahoo!.

Pierwsze slajdy przedstawiały program służący NSA do czegoś, co nazywała „zbiory wprost z serwerów następujących amerykańskich dostawców usług internetowych: Microsoft, Yahoo!, Google, Facebook, Paltalk, AOL, Skype, YouTube,

Apple". Wykres przedstawiał daty, kiedy poszczególne firmy włączono do programu.

Znów ogarnęło mnie takie podekscytowanie, że musiałem przestać czytać.

Informator powiedział mi także, że wysyła duży plik, do którego uzyskam dostęp dopiero we właściwym czasie. Postanowiłem na razie zapomnieć o tym niejasnym, choć znaczącym stwierdzeniu, zgodnie z postanowieniem, by pozwolić mu decydować, kiedy otrzymuję informacje – ale także dlatego, że czułem się niezwykle podekscytowany już tym, co miałem przed sobą.

Pierwszy rzut oka na zaledwie parę dokumentów przekonał mnie o dwóch rzeczach: po pierwsze, że muszę natychmiast lecieć do Hongkongu, i po drugie, że potrzebuję istotnego wsparcia instytucjonalnego. To zaś oznaczało włączenie do sprawy „Guardiana" – gazety i jej wydania internetowego, gdzie dziewięć miesięcy wcześniej zatrudniłem się jako codzienny felietonista. Teraz zamierzałem poinformować ich o sprawie, która, jak już wiedziałem, będzie prawdziwą bombą.

Połączyłem się przez Skype'a z Janine Gibson, brytyjską redaktor naczelną amerykańskiego wydania „Guardiana". Moja umowa z „Guardianem" gwarantowała mi pełną niezależność, co oznaczało, iż nikt nie może redagować ani nawet przeglądać moich tekstów przed ich publikacją. Piszę artykuł, a potem sam zamieszczam go bezpośrednio na stronie internetowej. Jedynym wyjątkiem od tego układu jest sytuacja, w której mój tekst może pociągać za sobą konsekwencje prawne dla gazety albo gdy staję przed niezwykłym dziennikarskim dylematem – wtedy muszę ich uprzedzić. W minionych dziewięciu miesiącach zdarzyło się to zaledwie raz czy dwa, to zaś oznaczało, że miałem bardzo niewiele do czynienia z wydawcami „Guardiana". Oczywiście ta historia niewątpliwie wymagała czujności. Zdawałem sobie też sprawę, że nie obejdzie się bez środków i wsparcia gazety.

– Janine, mam wielki temat – zacząłem od razu. – Zgłosił się do mnie informator z dostępem do najwyraźniej wielkiej ilości ściśle tajnych dokumentów z NSA. Pokazał mi już kilka i są one wstrząsające. Mówi, że ma dużo, dużo więcej. Z jakiegoś powodu przebywa w Hongkongu. Nie wiem jeszcze, dlaczego, ale chce, żebym do niego przyjechał po resztę. To, co mi dał, co widziałem, świadczy o szokującym...

– Jak się ze mną łączysz? – przerwała mi Gibson.

– Przez Skype'a.

– Sądzę, że nie powinniśmy o tym rozmawiać przez telefon – stwierdziła rozsądnie i zaproponowała, żebym wsiadł do samolotu do Nowego Jorku.

Podzieliłem się moim planem z Laurą: lecę do Nowego Jorku, pokazuję dokumenty „Guardianowi", wciągam ich w tę historię i skłaniam, żeby wysłali mnie do informatora. Laura zgodziła się spotkać ze mną w Nowym Jorku, żebyśmy razem wyruszyli do Hongkongu.

Poleciałem do Nowego Jorku nocnym samolotem i już przed dziewiątą rano następnego dnia, w piątek 31 maja, zarejestrowałem się w hotelu na Manhattanie, a potem spotkałem z Laurą. Pierwszą rzeczą, jaką zrobiliśmy, było kupno laptopa, który miał posłużyć mi jako „ściana powietrzna" – komputer nigdy niełączący się z internetem. Znacznie trudniej jest kontrolować komputer niepodłączany do sieci. Jedynym sposobem, w jaki służby wywiadowcze takie jak NSA mogą monitorować „ścianę powietrzną", jest uzyskanie fizycznego dostępu do komputera i umieszczenie urządzenia śledzącego na twardym dysku. Jeśli nigdy nie będę się z laptopem rozstawać, nie dopuszczę do tego typu wtargnięcia. Będę z niego korzystać do pracy nad materiałami, które chcę uchronić przed monitorowaniem – takimi jak dokumenty NSA – nie bojąc się, że zostanę wyśledzony.

Wepchnąłem nowy komputer do plecaka i pomaszerowaliśmy z Laurą pięć przecznic dalej do redakcji „Guardiana" w Soho.

Gibson już na nas czekała. Ruszyliśmy wprost do jej biura, gdzie dołączył do nas jej zastępca Stuart Millar. Laura usiadła na zewnątrz. Janine nie znała Laury, a ja chciałem móc rozmawiać całkiem swobodnie. Nie miałem pojęcia, jak wydawcy „Guardiana" zareagują na to, co mam. Wcześniej z nimi nie pracowałem, a w każdym razie nie nad czymś, co choć w przybliżeniu miałoby takie znaczenie.

Otworzyłem, folder przysłany przez informatora. Gibson i Millar usiedli razem przy stole i czytali dokumenty, od czasu do czasu mrucząc: „rany!", „o kurwa!" i tak dalej. Opadłem na kanapę i obserwowałem ich zaszokowane twarze, gdy w trakcie czytania dotarło do nich, co tak naprawdę im przyniosłem.

Poza dwudziestoma paroma dokumentami informator przysłał również manifest, który zamierzał umieścić w internecie, wzywając do podpisywania go w geście solidarności ze sprawą promowania prywatności i protestu przeciwko jej naruszaniu. Manifest był dramatyczny i poważny, ale należało tego oczekiwać, biorąc pod uwagę dokonany przez autora dramatyczny i poważny wybór, który na zawsze wywrócił mu życie do góry nogami. Jeśli o mnie chodzi, rozumiałem, że kogoś, kto był świadkiem konstruowania niejasnego, wszechobecnego i niewidzialnego systemu nadzoru ze strony państwa, bez kontroli czy weryfikacji, może poważnie niepokoić to, co widzi, i niebezpieczeństwa, jakie niesie. Oczywiście używał radykalnego tonu; rozumiałem dlaczego, choć nie byłem pewien, jak na manifest zareagują Gibson i Millar. Nie chciałem, by uznali, że mamy do czynienia z wariatem, szczególnie że po wielu godzinach rozmów z nim wiedziałem, iż myśli w sposób wyjątkowo racjonalny i wyważony.

Moje obawy szybko znalazły potwierdzenie.

– Niektórzy uznają to za kompletne wariactwo – orzekła Gibson.

– Tak, niektórzy ludzie i popierające NSA typy z mediów powiedzą, że to przypomina Unabombera Teda Kaczynskiego – zgodziłem się. – Ale ostatecznie najważniejsze są dokumenty, a nie on sam czy motywy, jakimi się kieruje, udostępniając nam te pliki. Poza tym każdy, kto robi coś tak skrajnego, musi mieć skrajne myśli. To nieuniknione.

Poza manifestem informator, który potem okazał się Snowdenem, napisał list do dziennikarzy, którym przekazywał archiwum dokumentów. Starał się w nim wyjaśnić swoje motywy i cele, a także przewidywał, jak głęboko zostanie potępiony:

Kieruję się jedynie chęcią poinformowania społeczeństwa o tym, co się robi w jego imieniu i co się robi przeciwko niemu. Rząd USA, w zmowie z państwami zależnymi, z których najważniejsze to Pięcioro Oczu – [oprócz Stanów Zjednoczonych] Wielka Brytania, Kanada, Australia i Nowa Zelandia – narzucił światu system tajnej, przenikającej wszystko inwigilacji, przed którą nie sposób się ukryć. Chroni krajowe systemy przed kontrolą obywateli dzięki utajnianiu i kłamstwom, siebie zaś broni przed oburzeniem (które mogłoby wybuchnąć w razie przecieków), wyolbrzymiając ograniczoną ochronę, jaką godzi się objąć tych, którymi rządzi. [...] Załączone dokumenty są prawdziwe i oryginalne, a przedstawiam je, by wszystkim pozwolić zrozumieć, jak działa system globalnej, biernej inwigilacji, i być może wypracować odpowiednią ochronę. Na dziś wszystkie nowe rejestry połączeń, które ten system może przyswoić i skatalogować, mają być przechowywane przez lata, a nowe „Magazyny Danych Masowych" (eufemistycznie zwane Magazynami Danych „Operacyjnych") są budowane na całym świecie, w tym największy w nowym centrum danych w Utah. Choć modlę się, by świadomość społeczeństwa i debata na ten temat doprowadziły do reform, należy pamiętać, że prowadzona przez ludzi polityka z czasem się zmienia i nawet konstytucję

można podważyć, gdy wymagają tego apetyty osób sprawujących władzę. By posłużyć się słowami znanymi z historii, nie mówmy już o zaufaniu do człowieka, ale powstrzymajmy go przed wyrządzaniem szkód okowom.

Od razu rozpoznałem to ostatnie zdanie jako parafrazę wypowiedzi Thomasa Jeffersona z 1798 roku, którą często cytowałem w swoich tekstach: „W kwestii władzy zatem nie mówmy już o zaufaniu do człowieka, ale powstrzymajmy go przed wyrządzaniem szkód okowom".

Przejrzawszy wszystkie dokumenty, w tym przesłanie Snowdena, Gibson i Millar dali się przekonać.

– Zasadniczo – podsumowała Gibson po dwóch godzinach od mego przyjścia – musisz lecieć do Hongkongu najszybciej jak się da. Na przykład jutro, OK?

Zatem „Guardian" postanowił w to wejść. Moja misja w Nowym Jorku zakończyła się sukcesem. Teraz wiedziałem, że Gibson zamierza energicznie zająć się tą sprawą, przynajmniej na razie.

Tego popołudnia Laura i ja udaliśmy się do osoby odpowiedzialnej w „Guardianie" za załatwianie spraw związanych z podróżami, by znaleźć najlepsze połączenie do Hongkongu. Wyglądało na to, że optymalnym rozwiązaniem jest szesnastogodzinny lot non stop liniami Cathay Pacific z lotniska JFK następnego dnia rano. Jednak akurat w chwili, gdy zaczynaliśmy celebrować zbliżające się spotkanie z naszym informatorem, zaczęły się komplikacje.

Pod koniec dnia Gibson oznajmiła, że chce włączyć w sprawę wieloletniego reportera „Guardiana" Ewena MacAskilla, który pracował w gazecie od dwudziestu lat.

– To świetny dziennikarz – powiedziała.

Zdając sobie sprawę z ogromu czekającego mnie przedsięwzięcia, wiedziałem, że będę potrzebował innych reporterów

„Guardiana" i – teoretycznie rzecz biorąc – nie miałem nic przeciwko temu.

– Chciałabym, żeby Ewan poleciał z wami do Hongkongu – powtórzyła Gibson.

Nie znałem MacAskilla, a co ważniejsze, nie znał go również informator, który wiedział jedynie o przyjeździe Laury i moim. Co więcej, podejrzewałem, że i Laura, która zawsze wszystko szczegółowo planuje, będzie wściekła z powodu tej nagłej zmiany. Miałem rację.

– Nic z tego. Absolutnie nie – zareagowała. – Nie możemy w ostatniej chwili dokooptowywać nowej osoby. A ja go w ogóle nie znam. Kto go sprawdził i zatwierdził?

Próbowałem wyjaśnić, co, jak sądziłem, stało za decyzją Gibson. W gruncie rzeczy nie znałem jeszcze „Guardiana" i wciąż mu nie w pełni ufałem; domyślałem się, że oni w ten sam sposób odnoszą się do mnie. Biorąc pod uwagę ryzyko, jakie „Guardian" podejmował przy tej sprawie, zapewne chcieli mieć na miejscu zaufanego człowieka, który im powie, co sądzi o naszym informatorze. Poza tym Gibson będzie potrzebowała pełnego wsparcia i zgody wydawców „Guardiana" w Londynie, którzy znali mnie jeszcze mniej niż ona. Zapewne chciała więc wprowadzić kogoś, dzięki komu Londyn poczuje się bezpieczniej.

– Nic mnie to nie obchodzi – powiedziała Laura. – Podróżowanie z trzecią osobą, jakimś nieznajomym, może przyciągnąć uwagę albo odstraszyć informatora.

W ramach kompromisu zaproponowała, żeby Ewen dołączył do nas kilka dni później, gdy już nawiążemy kontakt z informatorem w Hongkongu i pozyskamy jego zaufanie: – Dysponujesz środkami nacisku. Powiedz im, że nie mogą przysłać Ewena, póki nie będziemy gotowi.

Wróciłem do Gibson z – jak mi się wydawało – sensownym kompromisem, ale go odrzuciła.

– Wysyłam Ewena z wami, ale może spotkać się z informatorem, dopiero gdy Laura i ty będziecie gotowi.

Najwyraźniej podróż Ewena z nami do Hongkongu pozostawała poza dyskusją. Gibson musiała mieć pewność co do przebiegu wydarzeń i sposób na uspokojenie wszelkich obaw, jakie mogą żywić jej szefowie w Londynie. Ale Laura zdecydowanie upierała się, że musimy jechać sami.

– Jeśli informator będzie nas śledzić na lotnisku i niespodziewanie zobaczy tę trzecią osobę, której nie zna, spanikuje i zerwie kontakt. Nie ma mowy.

Jak dyplomata z Departamentu Stanu, który biega między adwersarzami na Bliskim Wschodzie w próżnej nadziei wypracowania porozumienia, wróciłem do Gibson, która udzieliła mi niejasnej odpowiedzi, sugerującej, że Ewen dojedzie za dwa dni. A może tak ją chciałem odczytać.

Tak czy inaczej, od osoby z działu podróży dowiedziałem się późno wieczorem, że kupiono bilet także dla Ewena – na następny dzień i ten sam lot. Nie zamierzali w tej sprawie ustąpić.

W samochodzie, którym następnego ranka jechaliśmy na lotnisko, między Laurą i mną doszło do pierwszej i jedynej kłótni. Zaraz po wyjeździe z hotelu powiedziałem jej, że Ewen jednak będzie nam towarzyszyć. Wybuchła gniewem; twierdziła, że wystawiam na szwank cały układ. To skandal, żeby na tak późnym etapie wprowadzać nieznajomą osobę. Nie miała zaufania do nikogo, kto nie został sprawdzony przy pracy nad tak delikatnym materiałem, i winiła mnie, że pozwoliłem „Guardianowi" na taką ingerencję.

Nie mogłem powiedzieć Laurze, że jej niepokój nie ma podstaw, próbowałem ją jednak przekonać, że „Guardian" nalegał i nie miałem wyjścia. A Ewen spotka się z informatorem, dopiero gdy będziemy gotowi.

Laury to nie obchodziło. By ją ułagodzić, zaproponowałem nawet, że nie polecę, ale natychmiast to odrzuciła. Samochód

utkwił w korku, a my przez dziesięć minut siedzieliśmy w nieszczęśliwym, gniewnym milczeniu.

Wiedziałem, że Laura ma rację; to nie powinno było się dziać w taki sposób. Przerwałem milczenie, mówiąc jej to. Zaproponowałem też, byśmy ignorowali Ewena i go wykluczyli, udając, że nie jest z nami.

– Jesteśmy po tej samej stronie – zaapelowałem do Laury. – Nie kłóćmy się. Biorąc pod uwagę, o co w tym chodzi, na pewno nie po raz ostatni dzieje się coś poza naszą kontrolą. – Prosiłem, byśmy skoncentrowali się na wspólnym pokonywaniu przeszkód. Z czasem emocje opadły.

Po przyjeździe na lotnisko Laura wyciągnęła z plecaka pendrive'a.

– Wiesz, co to jest? – spytała niezwykle poważnie.

– Co?

– Dokumenty – odparła. – Wszystkie.

Gdy przyjechaliśmy, Ewen czekał już przy bramce. Laura i ja byliśmy uprzejmi, ale chłodni; pilnowaliśmy, żeby czuł się wyłączony, żeby wiedział, iż nie odgrywa żadnej roli, póki nie będziemy gotowi mu jakiejś przydzielić. Ponieważ tylko na nim mogliśmy skupić niechęć, traktowaliśmy go jak dodatkowy bagaż, którym nas obarczono wbrew naszej woli. Nie było to miłe, ale zbyt rozpraszały mnie myśli o skarbach na pendrivie Laury, żeby się zastanawiać nad Ewenem.

W samochodzie Laura zrobiła mi pięciominutowy wykład na temat systemu bezpieczeństwa komputera i powiedziała, że w samolocie zamierza spać. Wręczyła mi swojego pendrive'a i zaproponowała, żebym podczas lotu zaczął przeglądać jej zestaw dokumentów. W Hongkongu, powiedziała, informator da mi mój własny.

Gdy samolot wystartował, wyciągnąłem mój nowy komputer, „ścianę powietrzną", wsunąłem pendrive Laury i zgodnie z jej instrukcjami ściągnąłem pliki.

Przez następnych szesnaście godzin mimo wyczerpania czytałem jeden dokument po drugim, gorączkowo robiąc notatki. Wiele z nich było tak samo istotnych i szokujących jak ta pierwsza prezentacja w PowerPoincie o PRISM, którą widziałem w Rio. A niektóre były jeszcze gorsze.

Jeden z pierwszych plików zawierał postanowienie tajnego sądu działającego w ramach Ustawy o nadzorowaniu zagranicznych wywiadów (Foreign Intelligence Surveillance Act, FISA), ustanowionego przez Kongres w 1978 roku po odkryciu przez komisję Churcha, że rząd od dziesięcioleci zajmuje się podsłuchiwaniem. Ustawa zakładała, że rząd może nadal prowadzić elektroniczną inwigilację, ale by nie dopuścić do nadużyć, za każdym razem powinien otrzymać zezwolenie sądu. Nigdy przedtem nie widziałem postanowienia sądu FISA. Niemal nikt nie widział. Ten sąd jest jedną z najbardziej tajnych instytucji rządowych. Wszystkie jego wyroki automatycznie stają się ściśle tajne i jedynie mała garstka osób jest upoważniona do dostępu do jego decyzji.

Postanowienie, które przeczytałem w samolocie do Hongkongu, było pod kilkoma względami wyjątkowe. Nakazywało firmie telekomunikacyjnej Verizon Business udostępnienie „wszystkich raportów o szczegółach połączeń" dotyczących „komunikacji (1) między Stanami Zjednoczonymi a zagranicą oraz (2) całkowicie wewnątrz Stanów Zjednoczonych, łącznie z miejscowymi połączeniami telefonicznymi". To znaczyło, że NSA potajemnie i bez wyjątku gromadzi rejestr połączeń telefonicznych co najmniej dziesiątków milionów Amerykanów. Nikt właściwie nie miał pojęcia, że administracja Obamy coś takiego robi. Teraz to tajne postanowienie sądu nie tylko mi to uświadomiło, ale dodatkowo stanowiło dowód.

Ponadto w postanowieniu sądu podano, że masowe gromadzenie rejestrów rozmów Amerykanów zostało autoryzowane przez Paragraf 215 USA Patriot Act. Tak radykalna interpretacja

Patriot Act była chyba jeszcze bardziej szokująca niż sama decyzja sądu.

Kontrowersyjny charakter Patriot Act, uchwalonego w następstwie ataku 11 września, wynikał głównie z faktu, że z „prawdopodobnej przyczyny" do „związku" obniżał standardy uzasadnienia wymaganego od rządu, gdy chciał on otrzymać „dokumentację firm". Wystarczyło zatem, by FBI wykazało, że dokumenty „mają związek" z planowanym dochodzeniem, a już mogło uzyskać dostęp do wysoce delikatnych i naruszających prywatność dokumentów takich jak historie chorób, transakcje bankowe czy zapisy połączeń telefonicznych.

Ale nikt – nawet jastrzębio nastawieni republikanie z Izby Reprezentantów, którzy w 2001 roku byli autorami Patriot Act, ani rzecznicy swobód obywatelskich, którzy przedstawiali ustawę w czarnych barwach – nie sądził, by prawo to upoważniało rząd USA do zbierania danych *o wszystkich*, masowo i bez skrupułów. A jednak taką właśnie interpretację prezentowało to tajne postanowienie sądu FISA, które przeczytałem na ekranie mojego laptopa podczas podróży do Hongkongu, nakazujące Verizonowi przekazać NSA wszystkie rejestry telefoniczne wszystkich jego amerykańskich klientów.

Przez dwa lata demokratyczni senatorowie Ron Wyden z Oregonu i Mark Udall z Kolorado krążyli po kraju, ostrzegając, że Amerykanie „osłupieją, gdy się dowiedzą" o „tajnej interpretacji prawa", jaką posługuje się administracja Obamy, by nadać sobie szerokie i nieznane wcześniej uprawnienia szpiegowskie. Ponieważ jednak te działania szpiegowskie i „tajne interpretacje" były utajnione, senatorowie – będący członkami senackiej Komisji Wywiadu – nie zdobyli się na to, by przedstawić społeczeństwu, co takiego obudziło ich niepokój, mimo że jako członków Kongresu chronił ich immunitet.

Zobaczywszy postanowienie sądu FISA, natychmiast zrozumiałem, że jest to przynajmniej część tych niewłaściwych

i radykalnych programów inwigilacji, o których mówili Wyden i Udall. Od razu pojąłem znaczenie postanowienia. Nie mogłem się już doczekać, kiedy będę mógł je opublikować, pewien, że ujawnienie go wywoła trzęsienie ziemi, a potem niewątpliwie głosy domagające się przejrzystości i odpowiedzialności. A był to zaledwie jeden z setek ściśle tajnych dokumentów, które przeczytałem w drodze do Hongkongu.

Raz jeszcze poczułem, że zmienia się mój ogląd tego, co zrobił nasz informator. Zdarzyło się to już trzykrotnie: gdy zobaczyłem e-maile adresowane do Laury, potem raz jeszcze, gdy zacząłem rozmawiać z informatorem, i po raz kolejny, gdy przeczytałem dwadzieścia parę dokumentów, które mi przysłał e-mailem. Dopiero teraz jednak czułem, że zaczynam w pełni uświadamiać sobie ogrom przecieku.

Podczas lotu Laura kilkakrotnie przychodziła do rzędu, w którym siedziałem, tuż przed ścianką działową. Na jej widok wyskakiwałem z fotela i staliśmy na wolnej przestrzeni przy ściance, oniemiali, oszołomieni, ledwo zdolni wydusić słowo.

Laura od lat zajmowała się inwigilacją prowadzoną przez NSA, sama też była nieustannie obiektem nadużyć Agencji. Ja już w wydanej w 2006 roku książce pisałem o zagrożeniach wynikających z nieograniczonej inwigilacji w kraju, ostrzegając przed bezprawiem i radykalizmem NSA. Oboje przebijaliśmy się żmudnie przez wielki mur tajemnicy osłaniający rządowe szpiegostwo. Jak można udokumentować działania Agencji okrytej tyloma warstwami oficjalnej tajemnicy? Ale teraz ten mur został pokonany. W naszym posiadaniu, w samolocie, znajdowały się tysiące dokumentów, które rząd desperacko starał się ukryć. Dysponowaliśmy dowodami, które niepodważalnie ukazywały, jak niszczono prywatność Amerykanów i ludzi na całym świecie.

W dostarczonym nam archiwum moją uwagę zwróciły dwie rzeczy. Pierwszą była znakomita organizacja materiału.

Informator stworzył liczne foldery, podzielone na subfoldery i sub-subfoldery. Wszystkie dokumenty, co do jednego, znajdowały się dokładnie tam, gdzie powinny. Nie znalazłem ani jednego źle umieszczonego czy źle oznaczonego pliku.

Całe lata broniłem heroicznych, moim zdaniem, działań Bradleya Manninga (obecnie Chelsea Manning), szeregowca w armii i sygnalisty, którego tak bardzo przeraziło postępowanie rządu Stanów Zjednoczonych – zbrodnie wojenne, a także systematyczne oszustwa – że zaryzykował wolność, by przez WikiLeaks ujawnić światu poufne dokumenty. Manninga krytykowano jednak (moim zdaniem niesprawiedliwie i niesłusznie) za przeciek dokumentów, których wcześniej nie czytał, czyli nie jak na przykład Daniel Ellsberg, który w latach 70. ubiegłego wieku przekazał prasie tak zwane Pentagon Papers, pokazujące kłamstwa administracji Richarda Nixona w sprawie wojny w Wietnamie. Ten zarzut, choć gołosłowny (Ellsberg należał do najbardziej oddanych obrońców Manninga, a sam Manning, jak się wydaje, co najmniej przejrzał dokumenty), często wysuwano, by zniweczyć wrażenie, że Manning działał w sposób heroiczny.

Jasne było, że źródłu z NSA nie da się postawić takich zarzutów. Nie było cienia wątpliwości, że uważnie przejrzał każdy przekazywany nam dokument, zrozumiał jego znaczenie, a potem umieścił w starannie zorganizowanej strukturze.

Drugą uderzającą cechą archiwum był odsłaniany przez nie zakres kłamstwa. Jeden z pierwszych folderów informator zatytułował *BOUNDLESS INFORMANT (NSA kłamie Kongresowi)*. Ten folder zawierał dziesiątki dokumentów pokazujących skomplikowane statystyki prowadzone przez NSA, a dotyczące liczby przechwytywanych przez Agencję e-maili i połączeń telefonicznych. Zawierał także dowód, że NSA codziennie gromadzi dane o telefonach i e-mailach milionów Amerykanów.

BOUNDLESS INFORMANT to nazwa programu NSA mającego z matematyczną dokładnością podliczać codzienną działalność

inwigilacyjną Agencji. Jedna ze znajdujących się w folderze map ukazywała, że przez trzydzieści dni, w tym cały luty 2013 roku, pewna jednostka NSA zgromadziła ponad *trzy miliardy* informacji o połączeniach z samego tylko amerykańskiego systemu komunikacji.

Informator dał nam jasny dowód, że urzędnicy NSA, zeznający na temat działalności Agencji przed Kongresem, kłamali wprost i wielokrotnie. Na przestrzeni lat wielu senatorów zadawało NSA pytania dotyczące szacunkowych danych o liczbie Amerykanów, których połączenia telefoniczne i e-mailowe są przechwytywane. Urzędnicy twierdzili, że nie są w stanie odpowiedzieć na to pytanie, ponieważ takich danych nie gromadzą i gromadzić nie mogą – a właśnie te dane w szerokim zakresie znajdowały się w dokumentach BOUNDLESS INFORMANT.

Jeszcze bardziej znaczący był fakt, że pliki – tak samo jak postanowienie sądu w sprawie Verizona – udowadniały, iż wysoki urzędnik bezpieczeństwa narodowego w administracji Obamy, dyrektor wywiadu krajowego James Clapper, kłamał przed Kongresem, gdy 12 marca 2013 roku senator Ron Wyden zadał mu pytanie: „Czy NSA zbiera w ogóle jakiekolwiek dane na temat milionów czy setek milionów Amerykanów?".

Odpowiedź Clappera był tyleż krótka, co kłamliwa: „Nie".

W ciągu szesnastu godzin niemal nieprzerwanego czytania udało mi się zapoznać z zaledwie niewielką częścią archiwum. Jednak gdy samolot lądował w Hongkongu, dwie rzeczy wiedziałem z całą pewnością. Po pierwsze, że nasz informator jest politycznie bardzo wyrobiony i wnikliwy, co wynikało z faktu, że rozumiał znaczenie większości dokumentów. Jest również wysoce racjonalny. Świadczył o tym sposób, w jaki wybrał, przeanalizował i opisał tysiące dokumentów, które teraz znalazły się w moim posiadaniu. Po drugie, że trudno byłoby odmówić mu statusu klasycznego sygnalisty. Jeśli ujawnienie dowodu, że najwyżsi rangą

urzędnicy bezpieczeństwa narodowego wprost kłamali przed Kongresem na temat krajowych programów szpiegowskich, nie czyni z człowieka niewątpliwego sygnalisty, to co czyni?

Wiedziałem, że im trudniej będzie rządowi i jego sojusznikom demonizować źródło przecieku, tym potężniejszy będzie efekt tego, co ujawnia. Dwa najczęściej używane do demonizacji sygnalistów hasła – „jest zaburzony psychicznie" i „jest naiwny" – w tym wypadku nie zadziałają.

Tuż przed lądowaniem przeczytałem ostatni plik. Choć nosił tytuł „README_FIRST", po raz pierwszy zauważyłem go dopiero pod koniec lotu. Ten dokument wyjaśniał, dlaczego informator postanowił zrobić to, co zrobił, a treścią i tonem przypominał manifest, który pokazałem wydawcom „Guardiana". Znajdowało się w nim jednak coś, czego nie było w innych: nazwisko informatora – wtedy dopiero je poznałem – i jasna przepowiednia, co go najprawdopodobniej spotka, gdy ujawni, kim jest. Ostatni fragment tekstu brzmiał:

Wiele osób będzie mnie szkalować za to, że nie włączam się w narodowy relatywizm, że nie odwracam wzroku od problemów [mojego] społeczeństwa ku odległemu, zewnętrznemu złu, nad którym nie mamy władzy i za które nie jesteśmy odpowiedzialni, ale obywatelstwo niesie ze sobą obowiązek kontrolowania najpierw własnego rządu, zanim zaczniemy poprawiać inne. Tu, w kraju, teraz, musimy znosić rząd, który bardzo niechętnie dopuszcza ograniczoną kontrolę i odmawia rozliczenia się z popełnianych przestępstw. Gdy młodzież z marginesu popełnia drobne występki, my jako społeczeństwo odwracamy wzrok, by nie widzieć, co ich czeka w największym na świecie systemie więziennictwa, ale gdy najbogatsi i najpotężniejsi dostawcy usług telekomunikacyjnych w kraju świadomie popełniają dziesiątki milionów wykroczeń, Kongres uchwala pierwsze prawo w naszym kraju, które zapewnia ich elitarnym przyjaciołom pełną, działającą wstecz

bezkarność – cywilną i karną – za przestępstwa, które zasługiwałyby na najdłuższe wyroki w historii [...]

Te firmy [...] zatrudniają najlepszych prawników w kraju i nie ponoszą żadnych konsekwencji. Gdy dochodzenie ujawnia, że urzędnicy na najwyższych szczeblach władzy, włącznie z wiceprezydentem, osobiście kierowali takim przestępczym przedsięwzięciem, co powinno się zdarzyć? Jeśli uważacie, że dochodzenie należy przerwać, a jego rezultaty superutajnić w dziale Szczególnie Chronionych Informacji zwanym STLW (STELLARWIND); że jakiekolwiek przyszłe dochodzenia powinny być zakazane na zasadzie, że ściganie osób nadużywających władzy jest sprzeczne z interesem narodowym; że musimy „patrzeć naprzód, a nie oglądać się za siebie", i że zamiast zamknąć nielegalny program, trzeba go rozszerzyć na innych przedstawicieli rządu – to będziecie mile widziani na salonach amerykańskiej władzy, bo tak właśnie się stało, a ja ujawniam świadczące o tym dokumenty.

Rozumiem, że zostanę ukarany za swoje działanie i że ujawnienie tych informacji społeczeństwu oznacza mój koniec. Będę zadowolony, jeśli choćby na chwilę uda się odsłonić rządzącą światem federację tajnych praw, nierównego wybaczenia i nieograniczonej władzy wykonawczej. Jeśli chcesz pomóc, przystąp do społeczności otwartego oprogramowania i walcz, by utrzymać przy życiu ducha wolnej prasy i wolnego internetu. Zajrzałem do najciemniejszych rządowych zakątków – to, czego się boją, to światło.

Edward Joseph Snowden, [redacted]
Alias w CIA: [redacted]
Numer identyfikacyjny w Agencji: xxxxxxxx
Były starszy doradca/Agencja Bezpieczeństwa Narodowego USA, pod przykrywką korporacji
Były oficer sztabowy/Centralna Agencja Wywiadowcza USA, pod przykrywką dyplomatyczną
Były wykładowca/Agencja Wywiadu Obronnego USA, pod przykrywką korporacji

ROZDZIAŁ 2

DZIESIĘĆ DNI W HONGKONGU

Przybyliśmy do Hongkongu wieczorem w niedzielę 2 czerwca. Zamierzaliśmy od razu spotkać się ze Snowdenem, więc zaraz po zainstalowaniu się w hotelu w eleganckiej części Kowloonu włączyłem komputer i poszukałem go na używanym przez nas kodowanym czacie. Jak niemal zawsze był tam i czekał.

Po wymianie kilku żartów na temat lotu zajęliśmy się logistyką spotkania.

– Możecie przyjechać do mnie do hotelu – powiedział.

To było pierwsze zaskoczenie – że mieszka w hotelu. Wciąż nie wiedziałem, dlaczego jest w Hongkongu, ale już wówczas zakładałem, że pojechał tam, by się ukryć. Wyobrażałem go sobie w jakiejś norze, tanim mieszkaniu, gdzie może sobie pozwolić na życie w cieniu bez regularnie wpływającego czeku, a nie w wygodnym hotelu, jawnie i za spore pieniądze.

Zmieniając plany, uznaliśmy jednak, że lepiej będzie poczekać ze spotkaniem do rana. To Snowden podjął tę decyzję, nadając kilku następnym dniom atmosferę superostrożności spod znaku płaszcza i szpady.

– Poruszanie się nocą może ściągnąć na was uwagę – powiedział. – Byłoby dziwne, gdyby dwójka Amerykanów przyjeżdżała wieczorem do hotelu i natychmiast wychodziła. Jeśli pojawicie się tu rano, będzie to wyglądać bardziej naturalnie.

Snowdena niepokoiła inwigilacja tak ze strony władz hongkońskich i chińskich, jak i amerykańskich. Bardzo obawiał

się, że mogą za nami chodzić miejscowi agenci wywiadu. Ponieważ miał ścisłe związki z amerykańskimi agencjami szpiegowskimi i wiedział, o czym mówi, zastosowałem się do jego życzenia. Czułem jednak rozczarowanie, że nie spotkamy się od razu.

Ponieważ Hongkong leży w strefie czasowej dokładnie dwanaście godzin wcześniejszej niż Nowy Jork, noc i dzień mi się przestawiły, więc mało spałem tej nocy, tak samo zresztą jak przez wszystkie podczas tej podróży. Jedynie częściowo wynikało to ze zmiany czasu – z takim trudem kontrolowałem podniecenie, że byłem w stanie zdrzemnąć się jedynie na półtorej, góra dwie godziny. Nie zmieniło się to przez cały czas pobytu w Hongkongu.

Następnego ranka Laura i ja spotkaliśmy się w foyer, a potem złapaliśmy taksówkę do hotelu Snowdena. To Laura ustalała szczegóły naszego spotkania. W drodze nie chciała rozmawiać, obawiając się, by kierowca nie okazał się tajnym agentem, a ja już nie byłem taki skłonny odrzucać podobnych obaw jako przejawu paranoi. Mimo ograniczeń udało mi się jednak wyciągnąć z Laury dość, by zrozumieć, jaki jest plan.

Mieliśmy udać się na drugie piętro hotelu Snowdena, tam bowiem znajdowały się sale konferencyjne. Wybrał konkretnie jedną z nich, uważając, że oferuje doskonałe wyważenie: dość oddalona, by nie zachęcać do zbyt wielkiego „ludzkiego ruchu", jak to określił, a równocześnie nie aż tak na uboczu, żebyśmy, czekając, ściągali na siebie uwagę.

Laura powiedziała, że po wejściu na drugie piętro mamy spytać pierwszego pracownika hotelu napotkanego w pobliżu wybranej sali, czy restauracja jest otwarta. Będzie to znak dla słuchającego w pobliżu Snowdena, że nikt nas nie śledził. W wyznaczonej sali mieliśmy usiąść na kanapie koło „ogromnego aligatora", który, jak potwierdziła Laura, był rodzajem dekoracji, a nie żywym zwierzęciem.

Snowden wyznaczył nam dwie pory spotkania: godzinę dziesiątą i dziesiątą dwadzieścia. Jeżeli nie pojawi się w ciągu dwóch minut od pierwszego terminu, mamy wyjść z sali i powrócić w drugim terminie, a on nas znajdzie.

– Skąd będziemy wiedzieć, że to on? – spytałem. Właściwie nic o nim nie wiedzieliśmy, nie znaliśmy jego wieku, rasy, wyglądu, niczego.

– Będzie trzymał kostkę Rubika – wyjaśniła.

Wybuchnąłem śmiechem; sytuacja wydawała się tak absurdalna, tak skrajna i nieprawdopodobna. To surrealistyczny międzynarodowy thriller, którego akcja toczy się w Hongkongu – pomyślałem.

Taksówka zatrzymała się przy wejściu do hotelu Mira, który, jak zauważyłem, także znajdował się w dzielnicy Kowloon, w bardzo handlowej okolicy wypełnionej smukłymi wieżowcami i eleganckimi sklepami. Trudno znaleźć miejsce, gdzie byłoby się bardziej na widoku. Po wejściu do foyer znów poczułem zaskoczenie – Snowden nie mieszkał w byle jakim hoteliku, ale wielkim i drogim, gdzie, jak wiedziałem, noc kosztowała kilkaset dolarów. Dlaczego – zastanawiałem się – ktoś, kto zamierza ujawnić sekrety NSA i potrzebuje wielkiej niejawności, pojechał do Hongkongu, by zamieszkać w pięciogwiazdkowym hotelu w jednej z najbardziej uczęszczanych części miasta? Nie było sensu rozważać tej tajemnicy – za kilka minut spotkam się z informatorem i zapewne uzyskam odpowiedzi na wszystkie pytania.

Podobnie jak wiele budynków w Hongkongu, hotel Mira wielkością dorównywał całej wsi. Laura i ja przez co najmniej piętnaście minut przemierzaliśmy przepastne hole, szukając wyznaczonego miejsca spotkania. Musieliśmy wjeżdżać windami, pokonywać wewnętrzne mostki i nieustannie pytać o wskazówki. Uznawszy, że znaleźliśmy się blisko właściwej sali, pierwszemu napotkanemu pracownikowi hotelu nieco

niezręcznie zadałem będące hasłem pytanie; potem musieliśmy wysłuchać prezentacji różnych opcji restauracyjnych.

Zaraz za rogiem ujrzeliśmy otwarte drzwi i leżącego na podłodze ogromnego aligatora z zielonego plastiku. Zgodnie z instrukcją siedliśmy na kanapie, zdenerwowani, czekając w milczeniu. Mała salka nie wydawała się mieć żadnej konkretnej funkcji, żadnego powodu, dla którego ktoś miałby do niej wchodzić, i nie znajdowało się w niej nic poza kanapą i aligatorem. Siedzieliśmy w milczeniu pięć minut; nikt się nie pojawił, więc wyszliśmy i w pobliskim pustym pokoju przeczekaliśmy cały kwadrans.

Dwadzieścia po dziesiątej wróciliśmy i znów zajęliśmy miejsca obok aligatora, na kanapie, która stała tyłem do wejścia, naprzeciwko dużego lustra. Po dwóch minutach usłyszałem za sobą ruch.

Nie odwróciłem się, by zobaczyć, kto wchodzi, tylko patrzyłem w lustro, w którym pojawiła się sylwetka idącego w naszą stronę mężczyzny. Dopiero gdy był blisko kanapy, odchyliłem głowę.

Pierwsze, co zobaczyłem, to nieułożona kostka Rubika, przekładana palcami lewej dłoni przybysza. Edward Snowden przywitał się, ale nie wyciągnął do nas ręki, ponieważ zgodnie z założeniem nasze spotkanie miało wyglądać na przypadkowe. Tak jak się umówili, Laura spytała o jedzenie w hotelu, on zaś odpowiedział, że jest niedobre. Ze wszystkich zaskakujących momentów w całym tym odcinku historii chwila naszego spotkania niosła chyba największą niespodziankę.

Snowden miał wówczas dwadzieścia dziewięć lat, wyglądał jednak przynajmniej kilka lat młodziej. Ubrany był w białą podkoszulkę z jakimś spłowiałym napisem, dżinsy i nijakie okulary. Nosił krótką, rzadką bródkę, ale wyglądał, jakby dopiero niedawno zaczął się golić. Miał miłą powierzchowność i wojskową postawę, ale był raczej szczupły i blady; tak samo

jak Laura i ja zachowywał się niezręcznie i nieco sztywno. Mógłby być dowolnym średnio głupawym chłopakiem zaraz po dwudziestce, pracującym w laboratorium komputerowym na uczelnianym kampusie.

Nie potrafiłem ułożyć tych fragmentów w spójny obraz. Właściwie nie myślałem o tym świadomie, ale z kilku powodów przypuszczałem, że Snowden jest starszy, po pięćdziesiątce, może nawet sześćdziesiątce. Po pierwsze, biorąc pod uwagę, że miał dostęp do tylu wrażliwych dokumentów, zakładałem, że zajmuje wysokie stanowisko w NSA. Poza tym jego spostrzeżenia i strategie nieodmiennie świadczyły o wyrafinowaniu i dobrej orientacji, co sprawiało, że uznałem go za weterana sceny politycznej. I na koniec wiedziałem, że jest gotów odrzucić swoje życie, zapewne do śmierci siedzieć w więzieniu za ujawnienie tego, co jego zdaniem świat musi wiedzieć, sądziłem więc, że zbliża się do końca kariery. By podjąć tak ekstremalną decyzję, uznałem, trzeba mieć za sobą wiele lat, nawet dziesięciolecia rozczarowań.

Nagłe odkrycie, że źródłem zdumiewającego skarbu w postaci materiałów NSA jest człowiek tak młody, okazało się jednym z najbardziej wytrącających z równowagi doświadczeń w moim życiu. W głowie mi wirowało od różnych możliwości. Czy to jakieś oszustwo? Czy zmarnowałem czas, lecąc przez pół świata? Jak ktoś tak młody mógł uzyskać dostęp to takiego rodzaju informacji, jakie widzieliśmy? Jak ten człowiek może być tak obeznany i doświadczony w sprawach wywiadu i szpiegostwa, jak nasze źródło najwyraźniej było? Może, myślałem, to tylko syn, asystent lub kochanek naszego informatora, który teraz zaprowadzi nas do właściwej osoby.

– No, to chodźcie ze mną – powiedział, najwyraźniej spięty. Laura i ja ruszyliśmy za nim, mamrocząc jakieś bezsensowne uwagi. Byłem zbyt zaskoczony i zagubiony, by wiele mówić, i widziałem, że Laura czuje to samo. Snowden

robił wrażenie czujnego, jakby wypatrywał potencjalnych szpiegów lub spodziewał się kłopotów. Szliśmy więc głównie w milczeniu.

Nie mając pojęcia, dokąd nas zabiera, weszliśmy do windy, wysiedliśmy na dziesiątym piętrze i dotarliśmy do jego pokoju. Snowden otworzył drzwi wyciągniętą z portfela kartą magnetyczną.

– Wchodźcie – powiedział. – Przepraszam za bałagan, ale od paru tygodni nie opuszczałem pokoju.

W pokoju rzeczywiście panował bałagan. Na stole piętrzyły się talerze z na wpół zjedzonymi, dostarczanymi do pokoju posiłkami, wszędzie leżały brudne ubrania. Snowden oczyścił jedno krzesło i poprosił, bym usiadł. Sam siadł na łóżku. Pokój był mały, dzieliło nas nie więcej niż półtora metra. Nasza rozmowa była napięta, niezręczna i sztywna. Natychmiast podniósł kwestię bezpieczeństwa, pytając, czy mam telefon komórkowy. Mój telefon działał jedynie w Brazylii, ale Snowden i tak nalegał, bym usunął baterię lub włożył telefon do lodówki w minibarze, co utrudni podsłuchiwanie rozmowy.

Tak samo, jak powiedziała mi Laura w kwietniu, Snowden stwierdził, że rząd Stanów Zjednoczonych jest w stanie zdalnie aktywować telefon komórkowy i zmienić go w urządzenie nasłuchowe. Wiedziałem więc, że taka technologia istnieje, ale wciąż przypisywałem ich niepokój czemuś na granicy paranoi. Jak się okazało, nie miałem racji. Rząd od lat wykorzystywał to rozwiązanie w dochodzeniach kryminalnych. W 2006 roku sędzia federalny, który przewodniczył procesowi rzekomych nowojorskich gangsterów, wydał wyrok, że używanie przez FBI tak zwanych wędrownych pluskiew – czyli przekształcenie czyjegoś telefonu komórkowego w urządzenie nasłuchowe drogą zdalnej aktywacji – jest legalne.

Gdy moja komórka znalazła się już w lodówce, Snowden zdjął z łóżka poduszki i ułożył pod drzwiami.

– To ze względu na niechcianych podsłuchiwaczy w holu – wyjaśnił. – Możliwe, że są tu mikrofony i kamery w suficie, ale to, o czym będziemy rozmawiać, i tak w końcu znajdzie się w wiadomościach – powiedział, nie całkiem żartując.

Wciąż nie miałem właściwie pojęcia, kim Snowden jest, gdzie pracuje ani co zrobił, nie mogłem więc być pewien, co nam zagraża w sensie inwigilacji czy czegoś w tym rodzaju. Cały czas wypełniało mnie jedynie poczucie niepewności.

Laura nie zadawała sobie trudu, żeby usiąść czy coś powiedzieć; być może po to, żeby rozładować własne napięcie, zaczęła rozpakowywać i ustawiać kamerę i statyw. Potem przypięła mnie i Snowdenowi mikrofony.

Rozmawialiśmy wcześniej o tym, że zamierza nas w Hongkongu filmować – ostatecznie była dokumentalistką pracującą nad filmem o NSA. To, co robiliśmy, siłą rzeczy stanie się wielką częścią jej materiału. Nie byłem jednak przygotowany, że zacznie tak od razu. Trudno było zaakceptować ten dysonans poznawczy – z jednej strony potajemne spotkanie z informatorem, który w oczach rządu USA popełnił poważne przestępstwo, z drugiej zaś rejestrowanie całego spotkania.

Po kilku minutach Laura była gotowa.

– No to zaczynam – oznajmiła, jakby była to rzecz najbardziej naturalna na świecie. Świadomość, że będziemy nagrywani, jeszcze bardziej pogłębiła panujące w pokoju napięcie.

Snowden i ja i tak czuliśmy się niezręcznie, a gdy tylko kamera ruszyła, natychmiast zaczęliśmy się zachowywać bardziej oficjalnie i mniej życzliwie; usztywniliśmy się, mówiliśmy wolniej. W ciągu wielu lat często mówiłem o tym, jak inwigilacja zmienia zachowanie się ludzi, omawiałem badania świadczące, że osoby świadome, iż są pod obserwacją, stają się bardziej ograniczone, mniej swobodne. Teraz sam widziałem i na własnej skórze czułem tę dynamikę.

Nie było na co czekać, więc rozpocząłem.

– Mam do ciebie wiele pytań, więc po prostu zacznę je zadawać, a potem to rozwiniemy – zacząłem.

– W porządku – powiedział Snowden, najwyraźniej tak samo jak ja z ulgą przyjmując przejście do konkretów.

W tym momencie miałem dwa główne cele. Ponieważ wszyscy wiedzieliśmy, że Snowden może zostać w każdej chwili aresztowany, przede wszystkim chciałem dowiedzieć się jak najwięcej o nim samym: jego życiu, jego pracy, co go doprowadziło do podjęcia takich a nie innych wyborów, co i jak konkretnie zrobił, żeby pozyskać te dokumenty, a także co robi w Hongkongu. Po drugie, chciałem zorientować się, czy jest uczciwy i całkiem szczery, czy nie ukrywa ważnych rzeczy dotyczących siebie samego i swoich poczynań.

Choć od blisko ośmiu lat pisałem o polityce, dla tego, co miałem teraz robić, ważniejsze było moje dawniejsze doświadczenie jako prawnika procesowego, co wiązało się z pozyskiwaniem zeznań świadków. Gdy świadkowie składają zeznania, prawnik siedzi z nimi godzinami, czasem całymi dniami. Prawo zmusza świadków, by się stawili i szczerze odpowiadali na pytania prawnika. Głównym celem jest odkrycie kłamstw, wyszukanie niekonsekwencji w tym, co mówią, i przebicie się przez wszelkie wymyślone opowieści, by dotrzeć do prawdy. Przyjmowanie zeznań to jedna z niewielu rzeczy, jakie naprawdę lubiłem w pracy prawnika; rozwinąłem też różne taktyki wyciągania ze świadków prawdy. Zawsze wiązało się to z bezlitosnym gradem pytań, często tych samych, ale zadawanych w różnych kontekstach, z różnych kierunków i pod różnymi kątami, by sprawdzić solidność opowiadanej przez nich historii.

Odchodząc od sposobu postępowania ze Snowdenem w internecie, gdzie zgadzałem się na bierność, tego dnia zastosowałem taktykę przesłuchań. Zadawałem mu pytania przez pięć godzin, bez przerwy na wizytę w łazience czy kanapkę. Rozpocząłem od wczesnego dzieciństwa, doświadczeń szkolnych,

historii pracy przed posadą w rządzie. Domagałem się wszystkich szczegółów, jakie tylko był w stanie sobie przypomnieć. Jak się dowiedziałem, Snowden urodził się w Karolinie Północnej, ale dorastał w Marylandzie. Był synem ludzi z niższej klasy średniej, pracujących dla rządu federalnego (jego ojciec przez trzydzieści lat był zatrudniony w Straży Przybrzeżnej). Szkoła średnia głęboko go nudziła i nigdy jej nie ukończył; znacznie bardziej niż lekcje interesował go internet.

Niemal od razu mogłem osobiście potwierdzić to, co widziałem już podczas rozmów online: Snowden był bardzo inteligentny i racjonalny, a jego procesy myślowe – metodyczne. Odpowiadał rzeczowo, wyraźnie i przekonująco. W niemal wszystkich przypadkach odpowiadał na pytania wprost, z rozmysłem i konsekwentnie. Nie kręcił i nie opowiadał niestworzonych historii, typowych dla ludzi niestabilnych emocjonalnie lub cierpiących na zaburzenia psychiczne. Jego opanowanie i konkretność budziły zaufanie.

Choć na podstawie kontaktów w internecie wyrabiamy sobie opinię o ludziach, musimy ich jednak spotkać osobiście, by naprawdę ich poznać. Wkrótce poczułem się lepiej i otrząsnąłem z początkowych wątpliwości i niepewności, z kim właściwie mam do czynienia. Wciąż jednak pozostawałem sceptyczny, ponieważ wiedziałem, że wiarygodność wszystkiego, co planowaliśmy zrobić, będzie zależała od wiarygodności tego, kim jest Snowden.

Kilka godzin poświęciliśmy historii jego zatrudnienia i ewolucji intelektualnej. Polityczne poglądy Snowdena zmieniły się znacząco po ataku 11 września; stał się znacznie większym „patriotą". W 2004 roku, w wieku dwudziestu lat, zaciągnął się do wojska, by wziąć udział w wojnie w Iraku, która – jak wówczas sądził – była szlachetną próbą wyzwolenia Irakijczyków z ucisku. Jednak po zaledwie kilku tygodniach podstawowego szkolenia zauważył, że więcej mówi się o zabijaniu Arabów niż

o wyzwalaniu kogokolwiek. Zanim w wypadku podczas ćwiczeń złamał obie nogi, co położyło kres jego wojskowej karierze, zdążył już poczuć głębokie rozczarowanie rzeczywistym celem wojny.

Wciąż jednak wierzył, że Stany Zjednoczone to kraj dobra, postanowił więc pójść za przykładem wielu członków swojej rodziny i pracować dla agencji federalnej. Choć nie ukończył szkoły średniej, udało mu się w młodym wieku znaleźć pracę. Nie miał jeszcze osiemnastu lat gdy zatrudniono go jako technika za trzydzieści dolarów za godzinę, a w 2002 roku otrzymał certyfikat operatora systemów w Microsofcie. Pracę dla rządu federalnego uważał jednak za szlachetną i obiecującą w sensie zawodowym, zgłosił się więc na strażnika w Centrum Zaawansowanych Badań nad Językiem na Uniwersytecie Maryland, w budynku potajemnie zarządzanym i używanym przez NSA. Jak mi powiedział, chodziło mu o to, żeby otrzymać certyfikat dostępu do tajnych informacji i w ten sposób wcisnąć się do zespołu technicznego.

Od urodzenia miał talent do spraw technicznych. Mimo młodego wieku i braku formalnego wykształcenia ta cecha, w połączeniu z wrodzoną inteligencją, umożliwiła mu szybką promocję w pracy – ze strażnika błyskawicznie awansował w 2005 roku na stanowisko eksperta technicznego CIA.

Wyjaśnił, że cała wspólnota wywiadów desperacko poszukiwała ludzi znających się na technologii. Rozrosła się w tak ogromny i rozległy system, że trudno było znaleźć dość pracowników do jego obsługi. Dlatego też agencje bezpieczeństwa narodowego musiały prowadzić rekrutację nietradycyjnymi kanałami. Posiadający odpowiednie umiejętności ludzie najczęściej byli młodzi, czasami wyalienowani i zazwyczaj nie błyszczeli w normalnych szkołach. Kulturę internetową często uznawali za bardziej stymulującą niż edukację w formalnych instytucjach i bezpośrednie kontakty międzyludzkie.

Snowden został cenionym członkiem zespołu komputerowego w NSA; wiedział i potrafił znacznie więcej niż większość jego starszych współpracowników z wyższym wykształceniem. Czuł, że znalazł dokładnie takie środowisko, w którym jego umiejętności zostaną docenione, a braki w jego życiorysie nie będą miały znaczenia.

W 2006 roku zmienił status z pracownika na umowę na etatowego członka zespołu, co dodatkowo zwiększyło otwierające się przed nim możliwości. Rok później dowiedział się, że CIA szuka kogoś do pracy przy systemach komputerowych za granicą. Jego szefowie wystawili mu znakomite referencje, został więc zatrudniony i wysłany do Szwajcarii. Stacjonował w Genewie przez trzy lata, aż do końca 2010 roku, pracując niejawnie pod przykrywką dyplomatyczną.

Według przedstawionego przez Snowdena opisu jego działań w Genewie był kimś znacznie więcej niż „administratorem systemu". Uważano go za najlepszego specjalistę do spraw cyberbezpieczeństwa w Szwajcarii; podróżował po całym regionie, rozwiązując problemy, z którymi nikt nie potrafił sobie poradzić. CIA wybrała go jako wsparcie dla prezydenta podczas szczytu NATO w Rumunii w 2008 roku. Mimo tego sukcesu to właśnie w okresie spędzonym w CIA zrodził się jego głęboki niepokój co do działań rządu na świecie.

– Ponieważ jako ekspert techniczny miałem dostęp do systemów komputerowych, widziałem wiele tajnych rzeczy – powiedział Snowden – i to często bardzo złych. Zacząłem rozumieć, że to, co mój kraj robi na świecie, bardzo odbiega od tego, czego mnie zawsze uczono. Taka świadomość z kolei skłania do przewartościowania różnych spraw i ich kwestionowania.

Podał jeden przykład: agenci CIA zamierzali zwerbować pewnego szwajcarskiego bankiera, by dostarczał im poufnych informacji. O transakcjach finansowych ludzi, którymi USA się interesowały. Jeden z tajnych agentów zaprzyjaźnił się

z bankierem, pewnego wieczoru go spił i zachęcił, by mimo tego wracał do domu samochodem. Gdy bankiera zatrzymała policja i aresztowała za prowadzenie w stanie nietrzeźwym, agent CIA zaproponował, że osobiście pomoże w sprawie czekających go zarzutów, pod warunkiem że bankier będzie współpracował z Agencją. Ostatecznie jednak rekrutacja się nie powiodła.

– Zniszczyli życie temu człowiekowi dla czegoś, co nawet nie wypaliło, a potem po prostu go z tym zostawili – powiedział Snowden. Dodał, że nie podobała mu się nie tylko sama sytuacja, ale też przechwałki agenta na temat metod, jakich używał, by złowić ofiarę.

Dodatkowo frustrujące dla Snowdena były podejmowane przez niego próby uświadomienia przełożonym problemów z bezpieczeństwem komputerów i z systemami, które jego zdaniem naruszały etykę.

– Te próby – wyjaśnił – niemal zawsze spotykały się z niepowodzeniem.

– Mówili: to nie twoje zadanie, albo: nie masz dość informacji, żeby wydawać takie sądy. Zasadniczo polecali, żebym się tym nie przejmował – powiedział. Wśród kolegów zyskał opinię człowieka, który wysuwa zbyt wiele zastrzeżeń, a to nie przysparzało mu sympatii przełożonych. – Wtedy właśnie naprawdę dostrzegłem, jak łatwo jest oddzielić władzę od odpowiedzialności i że im wyższy szczebel władzy, tym mniej nadzoru i konieczności rozliczania się z własnych działań.

Pod koniec 2009 roku Snowden, pozbawiony iluzji, uznał, że jest gotów odejść z CIA. To na tym etapie, pod koniec służby w Genewie, po raz pierwszy zaczął rozważać możliwość zostania sygnalistą i zorganizowania przecieku tajemnic.

– Czemu wówczas tego nie zrobiłeś? – spytałem.

W tamtym okresie myślał, a w każdym razie miał nadzieję, że wybór Baracka Obamy na prezydenta spowoduje częściowe ograniczenie największych nadużyć. Obejmując urząd, Obama

obiecywał, że nie dopuści do bezprawia w dziedzinie bezpieczeństwa narodowego, wcześniej usprawiedliwianego wojną z terrorem. Snowden spodziewał się, że przynajmniej najbardziej brutalne działania wywiadu i wojska ulegną złagodzeniu.

– Potem jednak okazało się, że Obama nie tylko kontynuuje, ale w wielu wypadkach wręcz rozszerza zakres tych nadużyć – wyjaśnił. – Zdałem sobie sprawę, że nie mogę czekać, aż jakiś kolejny przywódca to wszystko naprawi. Przywództwo oznacza, że najpierw się działa samemu i służy jako przykład dla innych, a nie czeka, aż ktoś inny mnie w tym wyręczy.

Niepokoiło go także, że publiczne nagłośnienie spraw, o jakich dowiedział się w CIA, może wyrządzić szkodę.

– Gdy się upublicznia sekrety CIA, szkodzi się ludziom – powiedział, nawiązując do tajnych agentów i informatorów. – Tego nie chciałem zrobić. Natomiast gdy upublicznia się sekrety NSA, szkodzi się tylko niewłaściwym systemom. To mi bardziej odpowiadało.

Snowden powrócił zatem do NSA, tym razem jako pracownik Dell Corporation, która podpisała kontrakt z Agencją. W 2010 roku wysłano go do Japonii, gdzie otrzymał znacznie wyższy poziom dostępu do sekretów inwigilacji niż przedtem.

– To, z czym się tam zetknąłem, naprawdę zaczęło mnie męczyć – powiedział Snowden. – W czasie rzeczywistym widziałem, jak drony obserwują ludzi, których mogą zabić. Widziałem całe wsie i co kto w nich robi. Widziałem, jak NSA śledzi, co poszczególni ludzie robią w internecie już w chwili, gdy uderzali w klawiaturę. Zdałem sobie sprawę, jak dalece inwazyjne stały się amerykańskie możliwości inwigilacji. Zdałem sobie sprawę z rzeczywistego zasięgu systemu. I niemal nikt nie wiedział, co się dzieje.

Coraz wyraźniej czuł potrzebę, *obowiązek*, upublicznienia tego, co wie.

– Im dłużej pracowałem w Japonii dla NSA, tym bardziej byłem przekonany, że nie mogę tego zatrzymać dla siebie.

Czułem, że przyczynianie się do ukrywania tego przed ludźmi jest niewłaściwe.

Później, gdy tożsamość Snowdena była już znana, reporterzy próbowali go przedstawić jako kogoś w rodzaju prymitywnego, pracującego na niskim szczeblu faceta, który przypadkiem natknął się na tajne informacje. Ale rzeczywistość jest całkiem inna.

Snowden wyjaśnił, że podczas pracy w NSA i CIA szkolono go na cyberagenta wysokiego szczebla, kogoś, kto włamuje się do wojskowych i cywilnych systemów innych państw, by kraść informacje lub przygotowywać ataki, nie pozostawiając śladów. W Japonii szkolenie przybrało na intensywności. Wyspecjalizował się w niezwykle wyrafinowanych metodach chronienia danych elektronicznych przed innymi agencjami wywiadu i otrzymał formalne świadectwo wysokiej klasy cyberagenta. W końcu Akademia Połączonych Kontrwywiadów należąca do Agencji Wywiadu Obronnego wybrała go, by na kursie uczył innych kontrwywiadu cybernetycznego.

Metod bezpieczeństwa operacyjnego, przy których upierał się w naszych kontaktach, nauczył się w CIA, a szczególnie w NSA. Nawet pomagał je projektować.

W lipcu 2013 roku „New York Times" potwierdził podane mi przez Snowdena informacje, donosząc, że „w 2010 roku, pracując dla firmy związanej kontraktem z Agencją Bezpieczeństwa Narodowego, Edward J. Snowden nauczył się, jak być hakerem" i „przekształcił się w takiego właśnie eksperta cyberbezpieczeństwa, jakich NSA desperacko werbuje". Artykuł dodawał, że pliki, do jakich Snowden miał dostęp, wskazują, iż „przeniesiono go na ofensywną stronę elektronicznego szpiegostwa czy cyberwojny, w której NSA przeszukuje systemy komputerowe innych państw, by kraść informacje lub przygotowywać ataki".

Choć w zadawanych Snowdenowi pytaniach starałem się zachować chronologię, często nie potrafiłem się powstrzymać,

by nie skakać naprzód, głównie powodowany niecierpliwością. Szczególnie pragnąłem dotrzeć do istoty tego, co mnie przede wszystkim interesowało: co tak naprawdę skłoniło Snowdena do odrzucenia kariery, przekształcenia się w potencjalnego przestępcę oraz złamania wymagań tajemnicy i lojalności, które od lat wkładano mu do głowy?

Zadawałem te same pytania na różne sposoby, a Snowden na różne sposoby odpowiadał, ale jego odpowiedzi robiły wrażenie zbyt powierzchownych, zbyt abstrakcyjnych, zbyt pozbawionych pasji i przekonania. Bez zahamowań mówił o systemach i technologii NSA, ale wyraźnie spinał się, gdy tematem stawał się on sam, szczególnie w reakcji na sugestię, że zrobił coś odważnego i niezwykłego, co wymagało psychologicznego wyjaśnienia. Jego odpowiedzi brzmiały bardziej abstrakcyjnie niż emocjonalnie, uznałem je więc za nie całkiem przekonujące. Świat ma prawo wiedzieć, co robi się z jego prywatnością – powiedział; czuł moralny obowiązek, by wystąpić przeciwko złemu postępowaniu; nie mógł z czystym sumieniem zachować milczenia na temat ukrytego zagrożenia dla wyznawanych przez niego wartości.

Wierzyłem, że naprawdę je wyznaje, pragnąłem jednak dotrzeć do tego, co go ostatecznie skłoniło do zaryzykowania życia i wolności w obronie tych wartości, a miałem wrażenie, że nie słyszę prawdziwej odpowiedzi. Może sam jej w gruncie rzeczy nie znał; może podobnie jak wielu Amerykanów, szczególnie zagłębionych w kulturze bezpieczeństwa narodowego, nie chciał zbyt głęboko kopać. Ja jednak potrzebowałem wyjaśnienia.

Pomijając inne aspekty, musiałem mieć pewność, że dokonał wyboru, rzeczywiście i racjonalnie rozumiejąc konsekwencje. Nie chciałem wspierać go w podejmowaniu tak wielkiego ryzyka bez przekonania, że czyni to z pełną świadomością i z własnej woli.

W końcu Snowden udzielił mi odpowiedzi, w której brzmiały życie i prawda.

– Prawdziwą miarą wartości człowieka nie jest to, w co mówi, że wierzy, ale co robi w obronie swoich przekonań – powiedział. – Jeśli nasze przekonania nie skłaniają nas do działania, to zapewne nie są prawdziwe.

Skąd wziął taką miarę oceny własnej wartości?

– Z wielu miejsc, wielu różnych doświadczeń – odparł. W dzieciństwie czytał dużo greckiej mitologii, poza tym wielkie wrażenie wywarła na nim książka Josepha Campbella *Bohater o tysiącu twarzy*, jego zdaniem znajdująca „wspólny wątek opowieści, które wszyscy znamy". Główną nauką, jaką wysnuł z tej książki, było to, że „to my nadajemy życiu znaczenie przez nasze działania i historie, które w ich ramach tworzymy". Człowieka definiują jego działania i tylko tym jest.

– Nie chcę być kimś, kto boi się działać w obronie swoich zasad.

Ten temat, ten moralny twór służący ocenie tożsamości i wartości, Snowden spotykał wielokrotnie na swojej drodze rozwoju intelektualnego, w tym także – wyjaśnił z pewnym zażenowaniem – w grach wideo. Lekcja moralności, jaką z nich wyciągnął, mówiła, że jedna osoba, nawet najbardziej bezsilna, może naprawić wielką niesprawiedliwość.

– Bohater jest często zwykłym człowiekiem, który staje w obliczu ogromnej niesprawiedliwości wyrządzanej przez potężne siły i ma wybór: uciec w strachu lub walczyć o swoje przekonania. A historia pokazuje, że pozornie zwykli ludzie potrafią zatriumfować nawet nad najpotężniejszymi przeciwnikami, jeśli wystarczająco mocno wierzą w sprawiedliwość.

To nie on pierwszy powiedział mi, że gry wideo istotnie przyczyniły się do kształtowania światopoglądu. Przed laty zapewne bym parsknął lekceważąco, ale nauczyłem się już akceptować fakt, że dla pokolenia Snowdena rola gier w kształtowaniu świadomości politycznej, racji moralnych i zrozumienia swego miejsca w świecie była równie znacząca jak literatura, telewizja i film. Także w grach występują skomplikowane, skłaniające

do rozważań dylematy moralne, a szczególnie dotyczy to ludzi, którzy zaczynają kwestionować wpajane im zasady.

Wczesne rozważania moralne Snowdena – wynikające z pracy, która kształtowała, jak powiedział, „model tego, kim chcemy zostać i dlaczego" – rozwinęły się w poważną, dorosłą introspekcję na temat obowiązków etycznych i psychologicznych granic.

– To, co ludzi utrzymuje w stanie pasywności i posłuszeństwa – powiedział – to strach przed reperkusjami, ale gdy już raz się człowiek wyzwoli z przywiązania do rzeczy, które nie mają znaczenia – pieniędzy, kariery zawodowej, bezpieczeństwa – to ten strach daje się pokonać.

Równie centralną rolę w światopoglądzie Snowdena zajmowała bezprecedensowa wartość internetu. Tak samo jak dla wielu osób z jego pokolenia, w jego oczach, internet nie był jakimś odrębnym narzędziem, wykorzystywanym do wybranych zadań. Był to świat, w którym rozwijał się jego umysł i osobowość, miejsce samo w sobie, oferujące wolność, możliwości eksploracji oraz potencjał intelektualnego rozwoju i zrozumienia.

W oczach Snowdena wyjątkowe cechy internetu były wielką wartością, zasługującą na zachowanie za wszelką cenę. Jako nastolatek wykorzystywał internet do zgłębiania idei i do rozmów z ludźmi z odległych miejsc oraz całkowicie innych środowisk, z którymi nigdy by inaczej się nie zetknął.

– Zasadniczo internet pozwolił mi poczuć wolność i zbadać moje możliwości jako istoty ludzkiej – powiedział Snowden, wyraźnie ożywiony, nawet pełen pasji, gdy mówił o wartości internetu. – Dla wielu dzieciaków internet to sposób na samospełnienie. Pozwala im badać, kim są i kim chcą być, ale jest to możliwe jedynie przy zachowaniu prywatności i anonimowości, bo wtedy można popełniać błędy, ale one nas nie obciążają. Obawiam się, że moje pokolenie jako ostatnie mogło cieszyć się taką wolnością.

Zacząłem rozumieć, jaką rolę odegrało to w jego decyzji.

– Nie chcę żyć w świecie, w którym nie ma prywatności ani wolności, w którym gasi się tę wyjątkową wartość internetu – stwierdził. Czuł się w obowiązku zrobić, co w jego mocy, by do tego nie dopuścić, a raczej, by umożliwić innym dokonanie wyboru: działać czy nie w obronie tych wartości.

Snowden cały czas podkreślał, że jego celem nie jest zniszczenie zdolności NSA do wyeliminowania prywatności.

– Dokonanie takiego wyboru to nie moja rola – powiedział. Chciał natomiast, by obywatele USA i ludzie na całym świecie wiedzieli, co dzieje się z ich prywatnością, by ich o tym poinformować. – Nie zamierzam niszczyć tych systemów – twierdził – tylko pozwolić wszystkim zadecydować, czy mają one trwać dalej.

Sygnaliści tacy jak Snowden to często osoby, które w życiu spotykają się z odrzuceniem jako samotnicy czy osoby przegrane. Snowden był tego przeciwieństwem: jego życie wypełniały sprawy, które większość ludzi uznaje za najcenniejsze. Decyzja o ujawnieniu dokumentów oznaczała porzucenie dziewczyny, którą kochał od wielu lat, życia na rajskich Hawajach, wspierającej go rodziny, stabilnej kariery zawodowej, sporych zarobków.

Gdy w 2011 roku pobyt w Japonii dobiegł końca, Snowdena, wciąż jako pracownika Dell Corporation, przeniesiono na nowe stanowisko, tym razem w ośrodku NSA w Marylandzie. Wraz z premiami miał w tym roku zarobić ponad dwieście tysięcy dolarów, pracując z Microsoftem i innymi firmami technologicznymi nad budową bezpiecznych systemów przechowywania danych i dokumentów dla CIA i innych agencji.

– Świat robił się coraz gorszy – powiedział Snowden o tym okresie. – Na swoim stanowisku widziałem, że państwo, a szczególnie NSA, pracuje ręka w rękę z prywatnymi firmami technologicznymi, by uzyskać pełen dostęp do komunikacji między ludźmi.

Przez całe pięć godzin trwającego tamtego dnia przesłuchania – co więcej, przez cały czas wszystkich naszych rozmów w Hongkongu – Snowden zachowywał niemal stoicki spokój i rzeczowy ton. Wyjaśniając jednak, co ostatecznie skłoniło go do działania, okazał ożywienie, nawet poruszenie.

– Zdałem sobie sprawę – powiedział – że budują system, którego celem jest eliminacja wszelkiej prywatności, globalnie. Tworzony, by NSA mogła gromadzić, przechowywać i analizować wszystkie przekazywane drogą elektroniczną wiadomości.

To właśnie ostatecznie umocniło Snowdena w postanowieniu, że zostanie sygnalistą. Przez część 2012 roku ściągał dokumenty, które świat, jego zdaniem, powinien zobaczyć. Niektóre kopiował nie do publikacji, ale jedynie po to, by dziennikarze mogli zrozumieć kontekst systemów, o których będą pisać.

W początkach 2013 roku uznał, że jest jeszcze jeden zestaw dokumentów, które chciałby upublicznić, ale z Della nie miał do nich dostępu. Mógłby do nich dotrzeć, jedynie gdyby objął stanowisko analityka infrastruktury, na którym oficjalnie wolno by mu było wchodzić w zasoby nieopracowanych danych NSA.

Dlatego też złożył podanie o oferowane wówczas na Hawajach stanowisko w związanej kontraktem z NSA prywatnej firmie Booz Allen Hamilton, należącej do największych i najpotężniejszych firm przemysłu obronnego, zatrudniającej wielką liczbę byłych funkcjonariuszy rządowych. Zarabiał tam mniej, ale ta praca umożliwiła mu ściągnięcie ostatniego zestawu dokumentów, które jego zdaniem były niezbędne do pełnego obrazu szpiegostwa NSA. Co ważniejsze, ten dostęp pozwolił mu zgromadzić informacje na temat prowadzonego przez Agencję tajnego monitoringu całej infrastruktury telekomunikacyjnej wewnątrz Stanów Zjednoczonych.

W połowie maja 2013 roku Snowden poprosił o dwutygodniowy urlop w celu leczenia zdiagnozowanej u niego rok wcześniej padaczki. Spakował bagaże, w tym kilka pendrive'ów pełnych

dokumentów NSA oraz cztery puste laptopy do użytku w różnych celach. Nie powiedział swojej dziewczynie, dokąd jedzie; już poprzednio często zdarzało się, że nie wolno mu było zdradzić, dokąd podróżuje służbowo. Wolał utrzymać ją w niewiedzy, by rząd jej nie nękał po ujawnieniu jego tożsamości.

Dwudziestego maja przyleciał z Hawajów do Hongkongu, zameldował się w hotelu Mira pod własnym nazwiskiem i od tamtego czasu się stamtąd nie ruszał.

Snowden przebywał w hotelu całkiem jawnie, płacił własną kartą kredytową, ponieważ – jak wyjaśnił – wiedział, że jego ruchy zostaną bardzo dokładnie zbadane przez rząd, media i wszystkich innych. Nie chciał dopuścić do twierdzenia, że jest jakimś obcym agentem; taki zarzut łatwiej byłoby mu postawić, gdyby ten czas spędzał w ukryciu. Pragnął zademonstrować, że wszystkie jego ruchy można prześledzić, że nie ma żadnego spisku i że działa na własną rękę. W oczach władz hongkońskich i chińskich wyglądał na normalnego biznesmena, a nie kogoś, kto się czai.

– Nie zamierzam ukrywać, kim jestem – powiedział – więc nie mam powodu się chować i dawać pożywkę teoriom konspiracyjnym czy kampaniom demonizowania mnie.

W końcu zadałem pytanie, które mnie dręczyło od naszej pierwszej rozmowy w internecie: dlaczego, zdecydowawszy się już ujawnić dokumenty, na miejsce swego pobytu wybrał Hongkong? Odpowiedź Snowdena pokazała, że decyzję poprzedził charakterystyczną dla siebie, staranną analizą.

Przede wszystkim, powiedział, chodziło mu o zapewnienie sobie fizycznego bezpieczeństwa przed służbami USA w trakcie pracy nad dokumentami z Laurą i ze mną. Gdyby władze amerykańskie odkryły jego plan ujawnienia dokumentów, starałyby się mu w tym przeszkodzić, aresztując go lub gorzej. Hongkong, choć na wpół niezależny, stanowił jednak część terytorium Chin, Snowden uznał więc, że amerykańskim agentom trudniej będzie

tu działać niż w innych miejscach, które rozważał jako schronienie – takich jak niewielkie państwa latynoamerykańskie, Ekwador czy Boliwia. Hongkong będzie również mniej chętny i podatny na amerykańskie naciski, by go przekazać władzom amerykańskim, niż niewielkie państwa europejskie, na przykład Islandia.

Choć w wyborze miejsca pobytu Snowden kierował się głównie możliwością publicznego udostępnienia dokumentów, nie była to jedyna przesłanka. Chodziło mu także o to, by znaleźć się gdzieś, gdzie ludzie podzielają jego wartości polityczne. Jak wyjaśnił, mieszkańcy Hongkongu, choć formalnie poddani represyjnym rządom władz chińskich, walczyli, by zachować podstawowe wartości polityczne, i stworzyli żywy klimat niezgody. Snowden wskazał, że Hongkong miał demokratycznie wybranych przywódców i był miejscem wielkich protestów ulicznych, w tym dorocznego marszu przeciwko masakrze studentów na pekińskim placu Tiananmen w 1989 roku.

Istniały inne miejsca, do których mógł się udać, a które jeszcze lepiej chroniłyby go przed potencjalną reakcją USA, w tym same Chiny. Istniały też inne miejsca, gdzie panowała większa swoboda polityczna. Uznał jednak, że w Hongkongu znajdzie najlepsze połączenie fizycznego bezpieczeństwa i politycznej siły.

Niewątpliwie ten wybór miał również wady i Snowden był ich wszystkich świadomy – przede wszystkim chodziło o związek miasta z Chinami, co ułatwi pracę krytykom. Wybór idealny jednak nie istniał.

– Wszystkie moje opcje były złe – mówił często. Hongkong rzeczywiście zapewniał mu pewne bezpieczeństwo i swobodę ruchów, które trudno byłoby znaleźć gdzie indziej.

Zgromadziwszy fakty dotyczące tej historii, miałem jeszcze jeden cel: upewnić się, że Snowden rozumie, co go prawdopodobnie spotka, gdy jego tożsamość jako źródła ujawnionych dokumentów stanie się znana.

Zdaniem wielu osób z całego spektrum politycznego, administracja Obamy wydała bezprecedensową wojnę sygnalistom. Prezydent, który w kampanii obiecywał „najbardziej przejrzystą administrację w historii" i deklarował szczególną ochronę sygnalistów, których nazywał „szlachetnymi" i „odważnymi" ludźmi, postępuje wręcz przeciwnie.

Z tytułu Ustawy o szpiegostwie z 1917 roku administracja Obamy wytoczyła sprawy w sumie siedmiu osobom winnym przecieków – więcej niż wszystkie poprzednie rządy w historii Stanów Zjednoczonych *razem wzięte,* a nawet dwukrotnie więcej. Ustawa o szpiegostwie została przyjęta podczas I wojny światowej, by umożliwić Woodrowowi Wilsonowi kryminalizację wystąpień antywojennych, a jej sankcje są poważne – obejmują wyroki dożywocia, a nawet śmierci.

Nie było wątpliwości, że ręka prawa będzie ciężka. Departament Sprawiedliwości w rządzie Obamy postara się, by Snowden do końca życia siedział w ciężkim więzieniu, poza tym może oczekiwać, że zostanie powszechnie uznany za zdrajcę.

– Jak sądzisz, co się z tobą stanie, gdy ujawnisz się jako źródło przecieku? – spytałem.

Snowden odpowiedział natychmiast, szybko, co jasno wskazywało, że wielokrotnie rozważał już to pytanie.

– Oskarżą mnie o naruszenie Ustawy o szpiegostwie. O popełnienie poważnego przestępstwa. O pomoc wrogom Ameryki. O wystawienie na szwank bezpieczeństwa narodowego. Jestem pewien, że wyciągną każdy szczegół z mojej przeszłości, prawdopodobnie niektóre wyolbrzymią, a może nawet sfabrykują, by mnie maksymalnie oczernić.

Powiedział, że nie chce trafić do więzienia.

– Postaram się tego uniknąć. Jednak jeśli taki będzie skutek tego wszystkiego, a wiem, że jest to bardzo prawdopodobne, to już jakiś czas temu pogodziłem się z tym, co mi zrobią. Jedyną rzeczą, z którą nie potrafię się pogodzić, jest bezczynność.

Tego pierwszego dnia i we wszystkie następne zdecydowanie Snowdena i spokojne rozważania o tym, co mu niesie przyszłość, zaskakiwały i robiły wrażenie. Ani razu nie widziałem, żeby okazał choć cień żalu, strachu czy niepokoju. Wyjaśnił otwarcie, że dokonał wyboru, rozumie możliwe konsekwencje i jest na nie gotowy.

Wydawało się, że ta decyzja jest dla niego źródłem siły. Rozważając, jak rząd USA może go potraktować, pozostawał całkowicie opanowany. Widok tego dwudziestodziewięcioletniego mężczyzny, który w ten sposób reaguje na rysującą się groźbę spędzenia kilkudziesięciu lat, a może i całego życia w więzieniu o zaostrzonym rygorze – czyli perspektywa, która mogłaby niemal każdego śmiertelnie przerazić – działał zdecydowanie inspirująco. A jego odwaga okazała się zaraźliwa: Laura i ja wielokrotnie przyrzekliśmy sobie nawzajem i Snowdenowi, że wszelkie działania i decyzje, jakie od tej pory podejmiemy, będą honorować jego wybór. Czułem się w obowiązku, by przedstawić całą sprawę w takim duchu, jaki ożywiał działanie samego Snowdena: odwagi wyrastającej z przekonania, że robimy to, co uważamy za słuszne, że nie damy się zastraszyć ani powstrzymać bezpodstawnym groźbom wrogo nastawionych urzędników, którzy chcą ukryć własne nadużycia.

Po pięciogodzinnym przesłuchaniu nie miałem już żadnych wątpliwości, że wszystkie twierdzenia Snowdena są prawdziwe, a jego motywy przemyślane i szczere. Zanim się rozstaliśmy, powrócił do tematu, który podnosił już wielokrotnie: upierał się, by przedstawić się jako źródło dokumentów i by uczynić to publicznie w pierwszym artykule, jaki opublikujemy.

– Każdy, kto robi coś tak znaczącego, ma obowiązek wyjaśnić, dlaczego to zrobił i co ma nadzieję osiągnąć – powiedział. Nie chciał też, by jego ukrywanie się pogłębiło atmosferę strachu podsycaną przez rząd USA.

Ponadto Snowden był pewien, że gdy tylko nasze artykuły zaczną się pojawiać, NSA i FBI szybko zidentyfikują źródło przecieku. Nie podjął wszystkich kroków, jakie mógł, by zatrzeć za sobą ślady, ponieważ nie chciał, by jego współpracownicy stali się przedmiotem śledztwa czy fałszywych oskarżeń. Twierdził, że gdyby do końca wykorzystał nabyte umiejętności, to w połączeniu z niezwykle luźnym systemem zabezpieczeń w NSA potrafiłby zatrzeć ślady, mimo że ściągnął tak wiele ściśle tajnych dokumentów. Zamiast tego wolał zostawić przynajmniej kilka elektronicznych tropów, co oznaczało, że trzymanie się w cieniu nie wchodziło już w grę.

Choć nie chciałem pomagać rządowi w zidentyfikowaniu źródła przecieku, podając wprost nazwisko sygnalisty, Snowden przekonał mnie, że odkrycie jego tożsamości jest nieuniknione. Co więcej, postanowił sam się przedstawić publicznie, zanim rząd zrobi to za niego.

Obawiał się jedynie, by ujawnienie się nie odciągnęło uwagi od treści jego informacji.

– Wiem, że media wszystko personalizują, a rząd będzie chciał zrobić ze mnie główny temat, zaatakować posłańca – powiedział. Zamierzał od razu po przedstawieniu się zniknąć z pola widzenia, by w pełnym świetle została tylko NSA i jej szpiegowska działalność. – Jak to się już stanie – powiedział – nie będę się więcej spotykać z mediami. Nie chcę stać się głównym tematem tej sprawy.

Ja z kolei uważałem, że lepiej nie odsłaniać tożsamości Snowdena w pierwszym artykule, tylko odczekać tydzień, byśmy mogli opublikować pierwszy zbiór spraw bez zakłóceń tego rodzaju. Nasz pomysł był prosty: publikować jeden wielki temat po drugim, codziennie, w dziennikarskiej odmianie wojskowej taktyki „*shock and awe*" (szoku i przerażenia), zaczynając jak najprędzej i w kulminacyjnym momencie odsłaniając źródło. Pod koniec spotkania wszyscy się na to zgodziliśmy. Mieliśmy plan.

Przez pozostałe dni spędzone w Hongkongu codziennie spotykałem się ze Snowdenem na długie rozmowy. Nigdy nie udało mi się zasnąć w nocy na dłużej niż dwie godziny, a nawet i to było możliwe jedynie dzięki środkom nasennym. Resztę czasu poświęcałem na pisanie artykułów na podstawie dokumentów Snowdena.

Snowden pozostawił Laurze i mnie decyzję, które wątki należy omówić, w jakiej kolejności i w jaki sposób. Jednak pierwszego dnia – tak samo jak wiele razy przedtem i potem – podkreślał, jakie to istotne, byśmy bardzo rozważnie akceptowali wszelkie materiały.

– Wybrałem te dokumenty, ze względu na interes publiczny – stwierdził. – Polegam jednak na was, że kierując się dziennikarskim osądem, opublikujecie jedynie te, które społeczeństwo powinno zobaczyć i które można ujawnić, nie wyrządzając szkody niewinnym ludziom.

Było to istotne choćby dlatego, że nie można by liczyć na rzeczywistą debatę publiczną, gdyby rząd USA potrafił uzasadnić, iż publikacja dokumentów wystawiła na szwank czyjeś życie. Snowden doskonale to wiedział.

Podkreślał także, jak ważna jest publikacja dokumentów w sposób dziennikarski – to znaczy przy wykorzystaniu mediów, w artykułach, które omówią materiały w odpowiednim kontekście, a nie po prostu hurtowo zamieszczą. Jego zdaniem taki sposób zapewniał lepszą ochronę prawną, a co ważniejsze, pozwalał czytelnikom przyswoić sobie informacje w sposób bardziej uporządkowany i racjonalny.

– Gdybym chciał po prostu zamieścić je wszystkie *en masse* w internecie, to sam bym to zrobił – powiedział. – Ale chcę, żebyście opisali tę sprawę, jeden artykuł za drugim, ułatwiając ludziom zrozumienie tego, co powinni wiedzieć.

Zgodziliśmy się, że tym właśnie będziemy się kierować przy publikacji. Snowden kilkakrotnie wyjaśniał, że od początku

zamierzał powierzyć tę sprawę Laurze i mnie, bo wiedział, że przedstawimy ją w ostry sposób i nie przestraszymy się gróźb ze strony rządu. Często nawiązywał do „New York Timesa" i innych dużych koncernów mediowych, którym zdarzało się wstrzymać publikację na życzenie rządu. Choć chodziło mu o bezkompromisowe dziennikarstwo, zależało mu także, by dziennikarze byli bardzo dokładni i mieli tyle czasu, ile potrzeba, na sprawdzenie, czy wszystkie fakty są niepodważalne, a dokumenty dokładnie zweryfikowane.

– Niektóre dokumenty, które wam daję, nie są do publikacji, ale mają wam samym pomóc zrozumieć, jak ten system działa, byście potrafili go we właściwy sposób naświetlić – powiedział.

Zaraz po powrocie do hotelu po pierwszym spotkaniu ze Snowdenem napisałem cztery artykuły, mając nadzieję, że „Guardian" zacznie je od razu publikować. Sprawa była dość pilna – potrzebowaliśmy Snowdena, żeby omówił z nami tyle dokumentów, ile się da, zanim w taki czy inny sposób stanie się nieosiągalny dla dalszych rozmów.

Był jeszcze jeden powód pośpiechu. W taksówce, którą jechaliśmy na lotnisko Kennedy'ego, Laura po raz pierwszy poinformowała mnie, że na temat dokumentów Snowdena rozmawiała z kilkoma dużymi koncernami mediowymi i reporterami. Należał do nich Barton Gellman, dwukrotny zdobywca Nagrody Pulitzera, który dawniej był zatrudniony w „Washington Post", a teraz współpracował z nimi jako wojny strzelec. Próbując przekonać parę osób do wspólnej pracy nad archiwum Snowdena, Laura napotkała trudności, ale Gellman, który od dawna zajmował się kwestiami inwigilacji, bardzo zainteresował się całą historią.

Na podstawie rekomendacji Laury Snowden zgodził się dać Gellmanowi „kilka dokumentów" z intencją, by razem z Laurą napisali o paru konkretnych tematach i opublikowali to w „Washington Post".

Szanowałem Gellmana, ale nie mogłem tego samego powiedzieć o „Washington Post", który w mojej ocenie jest sercem waszyngtońskiej mediowej bestii i uosabia wszystkie najgorsze cechy amerykańskich mediów politycznych: nadmierną bliskość ze sferami rządowymi, uwielbienie dla instytucji bezpieczeństwa narodowego, rutynowe wyciszanie przeciwnych opinii. Krytyk mediów Howard Kurtz, pracujący zresztą dla tejże gazety, wykazał w 2004 roku, jak przed inwazją na Irak systematycznie nagłaśniano prowojenne głosy, równocześnie bagatelizując lub pomijając wypowiedzi wojnie przeciwne. Polityka informacyjna „Post", podsumował Kurtz, była „uderzająco jednostronna" w poparciu dla inwazji. Strona redakcyjna „Post" wciąż głośno i bezmyślnie opowiadała się za amerykańskim militaryzmem, tajnością i inwigilacją.

„Post" otrzymał sensacyjny materiał, którego nie szukał i którego źródło przecieku – Snowden – początkowo nie wybrał (ale na które zgodził się po rekomendacji Laury). Co więcej, mój pierwszy szyfrowany czat ze Snowdenem wziął się z jego gniewu na lękliwe podejście „Post".

Wśród moich nielicznych – na przestrzeni lat – krytycznych uwag wobec WikiLeaks znalazła się ta, że także i oni czasami przekazywali znaczące sensacje tym właśnie należącym do establishmentu organizacjom mediowym, które najbardziej starają się chronić rząd, zarazem zwiększając swój status i znaczenie. Publikowane na wyłączność materiały dotyczące tajnych dokumentów budują status publikacji i renomę dziennikarza, który podał je do wiadomości. Znacznie sensowniej jest przekazywać takie sensacje niezależnym dziennikarzom i organizacjom mediowym, tym samym wzmacniając ich głos, podnosząc ich status i maksymalizując wpływ.

Co więcej, wiedziałem, że „Post" posłusznie dostosuje się do niepisanych reguł, określających jak establishmentowe media relacjonują rządowe sekrety. Zgodnie z tymi regułami, które

pozwalają rządowi kontrolować ujawniane sprawy i minimalizować, a nawet neutralizować ich wpływ, wydawcy najpierw zwracają się do urzędników i informują ich, co zamierzają opublikować. Urzędnicy bezpieczeństwa narodowego tłumaczą wówczas wydawcom, w jaki sposób ta publikacja rzekomo narazi na szwank bezpieczeństwo narodowe. Toczą się negocjacje, co zostanie opublikowane, a co nie. Często utajnia się informację, która w oczywisty sposób powinna zostać ujawniona. To właśnie kierowało w 2005 roku wydawcami „Post", gdy donosząc o istnieniu więzień CIA, zataili nazwy krajów, w których przetrzymywano więźniów, tym samym pozwalając Agencji dalej stosować bezprawie.

Na skutek tego samego procesu „New York Times" ukrywał fakt, że NSA bez odpowiednich uprawnień prowadzi podsłuchy, *przez ponad rok* od chwili, gdy reporterzy Jim Risen i Eric Lichtblau byli gotowi o tym napisać w połowie 2004 roku. Prezydent Bush wezwał wówczas wydawcę Arthura Sulzbergera i redaktora naczelnego Billa Kellera do Gabinetu Owalnego, gdzie niedorzecznie ich przekonywał, że ujawnienie faktu szpiegowania Amerykanów przez NSA bez wymaganych prawem nakazów oznacza pomaganie terrorystom. „New York Times" blokował publikację artykułu przez piętnaście miesięcy – aż do końca 2005 roku, czyli wydrukował go już po ponownym wyborze Busha (co oznaczało, że społeczeństwo dokonywało wyboru, nie wiedząc, że ubiegający się o reelekcję prezydent bez nakazu sądowego podsłuchuje Amerykanów). „New York Times" ostatecznie opublikował artykuł o NSA, ale jedynie dlatego, że zdenerwowany Risen zamierzał napisać o tym w książce, a gazeta nie chciała odpuścić takiej sensacji.

Trzeba też wspomnieć, jakim tonem należące do establishmentu koncerny mediowe dyskutują o karygodnych posunięciach rządu. Amerykańska kultura dziennikarska wymaga, by reporterzy unikali wszelkich wyraźnych bądź deklaratywnych

oświadczeń, a w artykułach zamieszczali także stanowisko rządu, odnosząc się do niego z szacunkiem, choćby było pozbawione sensu. Posługują się tu czymś, co Eric Wemple, felietonista tegoż „Washington Post", wyśmiewa jako „język środka drogi": nigdy nie mówić nic konkretnego, prawdziwym zdarzeniom i wykrętom rządu nadawać tę samą wiarygodność. Wszystko to razem rozmywa rewelacje, tworząc z nich niejasną, niespójną, często pozbawioną znaczenia masę. Przede wszystkim zaś gazety nieodmiennie przypisują wielkie znaczenie oficjalnym twierdzeniom, nawet wówczas, gdy twierdzenia te są w oczywisty sposób kłamliwe lub zwodnicze.

To właśnie takie strachliwe, służalcze dziennikarstwo skłaniało „New York Timesa", „Post" i inne media do pomijania słowa „tortury" w artykułach na temat technik przesłuchiwania za czasów Busha, choć bez skrupułów posługiwali się tym słowem do opisania dokładnie tych samych sposobów, jeśli stosowały je inne rządy na całym świecie. Było to fiasko mediów, publikujących pozbawione podstaw rządowe twierdzenia na temat Saddama i Iraku, by zbudować poparcie Amerykanów dla wojny opartej na fałszywych przesłankach, które amerykańskie media raczej przerysowywały, niż analizowały.

Kolejną niepisaną zasadą mającą chronić rząd jest ta, że media publikują jedynie kilka takich tajnych dokumentów, a potem przestają. O takim archiwum jak Snowdena napiszą tak, by ograniczyć jego wpływ – opublikują kilka artykułów, ucieszą się pochwałami za „wielką sensację", odbiorą nagrody, a potem dadzą sobie spokój, co sprawi, że nic się tak naprawdę nie zmieni. Snowden, Laura i ja uzgodniliśmy, że prawdziwe doniesienia na temat dokumentów NSA muszą mieć formę nieustępliwego zamieszczania jednego tekstu po drugim, bez przerwy, aż zostaną ujawnione wszystkie sprawy mogące interesować opinię publiczną – niezależnie od tego, jaki gniew wywołają ani jakie groźby sprowokują.

Od naszej pierwszej rozmowy Snowden jednoznacznie uzasadniał, dlaczego nie ma dość zaufania do głównych koncernów mediowych, by powierzyć im swoją historię; cały czas nawiązywał do faktu, że „New York Times" zataił sprawę prowadzonych przez NSA podsłuchów. Doszedł do przekonania, że ukrycie tej informacji przez gazetę mogło zmienić wynik wyborów prezydenckich w 2004 roku.

– Ukrycie tej historii zmieniło historię – powiedział.

Chodziło mu o takie opisanie wynikającego z dokumentów ogromnego zakresu szpiegowania NSA, by wymusić długą debatę publiczną niosącą rzeczywiste konsekwencje, a nie wywołać jednorazową sensację, która nie załatwi niczego poza pochwałami dla reportera. Debata wymaga bezpardonowego ujawniania, pogardy dla wątpliwych rządowych wykrętów, zdecydowanej obrony szlachetnych pobudek działania Snowdena i jednoznacznego potępienia NSA – czyli właśnie tego, co „Post" zwykle blokuje. Wiedziałem, że „Post" jedynie rozwadniał znaczenie takich odkryć. Fakt, że otrzymali zbiór dokumentów Snowdena, wydawał się całkowicie sprzeczny ze wszystkim, co moim zdaniem staraliśmy się osiągnąć.

Jak zwykle Laura miała przekonujące uzasadnienie swojej decyzji. Przede wszystkim uważała, że lepiej będzie włączyć w te rewelacje oficjalny Waszyngton, by tym trudniej było je zdezawuować czy nawet nadać im kryminalny charakter. Jeśli ulubiona gazeta Waszyngtonu zacznie donosić na temat przecieku, rządowi trudniej przyjdzie demonizowanie zaangażowanych w niego osób.

Ponadto, jak wytknęła mi Laura, ani ona, ani Snowden przez dość długi czas nie mogli się ze mną porozumieć, ponieważ nie miałem zainstalowanego programu szyfrującego, zatem to ona początkowo niosła ciężar posiadania tysięcy ściśle tajnych dokumentów NSA. Czuła potrzebę znalezienia kogoś, komu może powierzyć ten sekret, i współpracy z instytucją, która zapewni

jej jakąś ochronę. Nie chciała też sama jechać do Hongkongu. Skoro początkowo nie mogła rozmawiać ze mną, a informator uważał, że ktoś inny powinien napisać o sprawie PRISM, udała się do Gellmana.

Rozumiałem przyczyny, dla których Laura rozmawiała z „Post", ale nigdy się z nimi nie zgodziłem. Pomysł, że potrzebujemy włączyć w sprawę oficjalny Waszyngton, był w moich oczach dokładnie takim rodzajem podejścia – niechęci do podjęcia ryzyka, przestrzegania niepisanych reguł – jakiego chciałem uniknąć. Jako dziennikarze nie różniliśmy się niczym od pracowników „Post", a przekazanie im dokumentów po to, by zyskać ochronę, moim zdaniem wzmacniało te właśnie przesłanki, które zamierzaliśmy podważyć. Choć ostatecznie Gellman wykorzystał otrzymane materiały do napisania kilku znakomitych i ważnych tekstów, sam Snowden miał później żałować wciągnięcia w sprawę „Post", choć początkowo zdecydował się przyjąć rekomendację Laury.

Snowdena denerwowała nadmierna, jego zdaniem, zwłoka oraz nieostrożność związana z angażowaniem tak wielu ludzi w dyskusje nad dokumentami, a szczególnie strach, o którym świadczyły nieustanne konferencje „Post" z prawnikami. Rozzłościło go, że Gellman na prośbę prawników i wydawców „Post" odmówił przyjazdu na spotkanie do Hongkongu, gdzie mogliby razem przejrzeć dokumenty.

Jak mi to relacjonowali Snowden i Laura, prawnicy „Post" odradzili Gellmanowi wyjazd; zalecali także Laurze, by nie jechała, i wycofali ofertę pokrycia jej kosztów podróży. Opierali się na absurdalnej, napędzanej strachem teorii, że wszelkie rozmowy o ściśle tajnych informacjach prowadzone w Chinach, czyli państwie przesiąkniętym inwigilacją, mogą zostać podsłuchane przez chiński rząd. To z kolei grozi uznaniem, że „Post" nierozważnie udostępnił tajemnice Chińczykom, a dalej postawieniem zarzutów z tytułu Ustawy o szpiegostwie samej gazecie i Gellmanowi.

Na swój stoicki i wyciszony sposób Snowden był wściekły. Zburzył sobie życie i wystawił je na ogromne ryzyko, by ujawnić tę historię. Niemal nic go nie chroniło, a jednak ten ogromny koncern mediowy, dysponujący wszechstronnym wsparciem prawnym i instytucjonalnym, nie chciał podjąć nawet drobnego ryzyka i wysłać reportera na spotkanie z nim do Hongkongu.

– Jestem gotów, żeby wystawiając się na ogromne osobiste ryzyko, wręczyć im ten wielki temat, a oni nawet nie chcą wsiąść do samolotu – powiedział. Był to właśnie taki rodzaj strachliwej, niechętnej do podejmowania ryzyka uniżoności wobec rządu ze strony naszego „bezkompromisowego korpusu prasowego", który od lat potępiałem.

Co się stało, to się nie odstanie, i ani on, ani ja nie mogliśmy tego zmienić. Jednak tej drugiej nocy spędzonej w Hongkongu, po spotkaniu ze Snowdenem, postanowiłem, że to nie „Washington Post", mętny i prorządowy, strachliwy i niezdecydowany, nada kształt temu, jak NSA i Snowden będą dalej postrzegani. Kto pierwszy opublikuje tę historię, zadecyduje o sposobie, jak będzie się o niej mówić, a ja zdecydowanie chciałem, by rolę tę objął „Guardian" i ja. Chcąc, żeby ta sprawa wywołała odpowiedni efekt, należało łamać niepisane reguły establishmentowego dziennikarstwa mające osłabić wpływ ujawnień i chronić rząd. „Post" by tego nie zrobił – ja tak.

Dlatego też po powrocie do pokoju ukończyłem pracę nad czterema artykułami. Pierwszy dotyczył tajnego wyroku sądu FISA, który zmuszał Verizon, jedno z największych amerykańskich towarzystw telekomunikacyjnych, do przekazania NSA wszystkich rejestrów rozmów telefonicznych wszystkich Amerykanów. Drugi artykuł relacjonował historię programu podsłuchów prowadzonego bez odpowiednich zezwoleń za prezydentury Busha; oparłem go na ściśle tajnym wewnętrznym raporcie inspektora generalnego NSA z 2009 roku. Trzeci omawiał program BOUNDLESS INFORMANT, ostatni zaś

dotyczył programu PRISM, o którym dowiedziałem się po raz pierwszy jeszcze w domu w Brazylii. To tę sprawę uznałem za szczególnie pilną, ponieważ nad nią właśnie pracował „Post".

Trzeba było działać szybko i musieliśmy skłonić „Guardiana" do natychmiastowej publikacji. Czekałem niecierpliwie do chwili, aż redaktorzy „Guardiana" obudzą się w Nowym Jorku. Co pięć minut sprawdzałem, czy Janine Gibson już się zalogowała na czat Google'a, przez który zazwyczaj się porozumiewaliśmy. Gdy zobaczyłem, że już jest, natychmiast wysłałem jej wiadomość: „Musimy porozmawiać".

Wiedzieliśmy już, że rozmowa przez telefon lub Google'a nie wchodzi w grę. Oba kanały były zbyt niebezpieczne. Nie udało nam się połączyć przez OTR, Janine zasugerowała więc, byśmy spróbowali Cryptocata, niedawno stworzonego szyfrowanego programu mającego utrudnić rządową inwigilację. Stał się on naszym głównym środkiem łączności przez cały czas mego pobytu w Hongkongu.

Opowiedziałem jej o spotkaniu ze Snowdenem, o tym, że jestem przekonany o autentyczności i jego samego, i dostarczonych przez niego dokumentów. Dodałem też, że napisałem już kilka artykułów. Janine szczególnie poruszyła sprawa Verizona.

– Świetnie. Artykuł jest gotowy. Jeśli potrzebne są drobne poprawki redakcyjne, to w porządku, wprowadźmy je – powiedziałem. Podkreśliłem, jak ważny jest pośpiech: – Puśćmy to już teraz.

Pojawił się jednak pewien problem. Wydawcy „Guardiana" spotkali się z prawnikami gazety, ci zaś wygłaszali alarmujące ostrzeżenia. Janine powtórzyła mi, co od nich usłyszała: rząd USA może (aczkolwiek budziłoby to wątpliwości) przedstawić publikowanie poufnych informacji jako pogwałcenie Ustawy o szpiegostwie, nawet jeśli chodzi o gazety. Dotychczas rząd nie posuwał się do stawiania oskarżeń koncernom mediowym, ale tylko jeśli media przestrzegały niepisanych zasad umożliwiających

urzędnikom wcześniejszy wgląd w publikację i szansę przedstawienia argumentów, dlaczego taka publikacja mogłaby zaszkodzić bezpieczeństwu narodowemu. W ten sposób, twierdzili prawnicy „Guardiana", gazeta pokazuje, że nie zamierza zaszkodzić bezpieczeństwu narodowemu przez ujawnienie ściśle tajnych dokumentów, a zatem nie przejawia „zbrodniczych zamiarów", warunku koniecznego do postawienia zarzutów.

Nie było dotychczas przecieku dokumentów z NSA, nie mówiąc już o przecieku o takich rozmiarach i takiej wrażliwości. Prawnicy uważali, że istnieje potencjalne ryzyko działań prawnych, i to nie tylko przeciwko Snowdenowi, ale – biorąc pod uwagę historię administracji Obamy – także samej gazecie. Parę tygodni przed moim wyjazdem do Hongkongu ujawniono, że Departament Sprawiedliwości uzyskał nakaz sądowy pozwalający mu przeczytać e-maile reporterów i redaktorów agencji Associated Press w celu znalezienia źródła pewnej historii.

Później pojawiło się jeszcze bardziej alarmujące doniesienie: że Departament Sprawiedliwości złożył w sądzie zaprzysiężone oświadczenie, w którym oskarżył szefa waszyngtońskiego biura telewizji Fox News Jamesa Rosena o „współudział" w rzekomym przestępstwie popełnionym przez informatora, argumentując, że dziennikarz „udzielił pomocy w przestępstwie" polegającym na ujawnieniu tajnych informacji, a pomoc ta polegała na bliskiej współpracy z informatorem.

Dziennikarze od już paru lat obserwowali, że administracja Obamy przypuszcza bezprecedensowy atak na media. Sprawa Rosena oznaczała jednak znaczącą eskalację. Kryminalizacja współpracy ze źródłem informacji jako „współudział w przestępstwie" oznaczała kryminalizację całego dziennikarstwa śledczego – żaden reporter nigdy nie pozyskuje tajnych informacji bez współpracy ze swoim źródłem. Taka atmosfera sprawiła, że wszyscy prawnicy mediów, w tym „Guardiana", stali się superostrożni, a nawet lękliwi.

– Mówią, że FBI może przyjść, zamknąć biuro i zabrać nasze kartoteki – powiedziała Gibson.

Uznałem to za absurd. Sam pomysł, że rząd USA miałby zamknąć tak znaczącą gazetę jak „Guardian US" i przeszukać jej biuro, należał do gatunku nadmiernie ostrożnych rad, które jeszcze w czasach mojej kariery sądowej budziły we mnie nienawiść do mało pomocnych, przesadnych ostrzeżeń prawników. Wiedziałem jednak, że Gibson nie może – i nie zechce – tych rad po prostu odrzucić.

– Co to oznacza dla naszej sprawy? – spytałem. – Kiedy możemy publikować?

– Nie jestem pewna, Glenn – odparła Gibson. – Wpierw musimy wszystko wyjaśnić. Jutro znów spotykamy się z prawnikami i wtedy będziemy wiedzieć więcej.

Ogarnął mnie niepokój. Nie miałem pojęcia, jak zareagują wydawcy „Guardiana". Moja niezależność w „Guardianie" i fakt, że pisałem artykuły bez konsultacji z redaktorem, ale na pewno nie na tematy tak wrażliwe jak ten, oznaczały, że poruszam się po nieznanym terenie. W gruncie rzeczy cała historia była zupełnym NOVUM: nie sposób było przewidzieć, jak kto zareaguje, bo nic takiego wcześniej się nie wydarzyło. Czy wydawcy się ugną, dadzą się przestraszyć amerykańskim groźbom? Czy postanowią całymi tygodniami negocjować z rządem? Czy zdecydują, że lepiej, by to „Post" pierwszy opublikował tę historię, bo wtedy poczują się bezpieczni?

Byłem gotów natychmiast przesłać redakcji artykuł o Verizonie; mieliśmy dokument FISA, a jego autentyczność nie budziła wątpliwości. Nie widziałem powodu, by choć minutę dłużej odmawiać Amerykanom prawa do wiedzy, jak rząd traktuje ich prywatność. Równie paląca była sprawa moich zobowiązań wobec Snowdena. Dokonał wyboru, który świadczył o odwadze, pasji i sile. Chciałem, by moje teksty przenikał ten sam duch, oddający sprawiedliwość poświęceniu Snowdena. Jedynie śmiałe dziennikarstwo mogło nadać tematowi siłę niezbędną

do pokonania atmosfery strachu, jaką rząd narzucił dziennikarzom i ich źródłom. Paranoidalne ostrzeżenia prawników i wahanie „Guardiana" stanowiły antytezę takiej śmiałości.

Tego wieczoru zadzwoniłem do Davida i opowiedziałem mu, że coraz bardziej martwię się postępowaniem „Guardiana". Przedyskutowałem swoje niepokoje także z Laurą. Ustaliliśmy, że damy „Guardianowi" jeszcze jeden dzień na publikację pierwszego artykułu, a potem zaczniemy badać inne opcje.

Kilka godzin później do mojego pokoju przyszedł Ewen MacAskill, by dowiedzieć się, co ze Snowdenem, którego wciąż jeszcze nie poznał. Podzieliłem się z nim moimi obawami.

– Nie musisz się martwić – uspokajał mnie. – Nie dadzą się zastraszyć.

Alan Rusbridger, wieloletni redaktor naczelny „Guardiana", jest „bardzo zaangażowany" – zapewnił mnie Ewen – i „zdecydowany publikować".

Wciąż uważałem Ewena za człowieka firmy, ale żywiłem już do niego nieco cieplejsze uczucia, szczególnie że on też chciał szybko nagłośnić sprawę. Po jego wyjściu powiedziałem o nim Snowdenowi, dodając, że Ewen to nasz „opiekun" z „Guardiana" i że chciałbym, by następnego dnia się z nim spotkał. Wyjaśniłem, że włączenie Ewena jest ważnym krokiem, by wydawcy gazety czuli się na tyle spokojni, by publikować.

– Nie ma sprawy – odparł Snowden. – Wiecie jednak, że będzie wam patrzył na ręce, po to go przysłali.

Ich spotkanie było ważne. Następnego ranka Ewen nam towarzyszył i przez jakieś dwie godziny przepytywał Snowdena, głównie na te same tematy, co ja dzień wcześniej.

– Skąd mogę wiedzieć, że jesteś tym, kim mówisz? – spytał Ewen na koniec. – Czy masz jakiś dowód?

Snowden wyciągnął z walizki plik dokumentów: nieważny już paszport dyplomatyczny, kartę identyfikacyjną CIA, prawo jazdy i inne rządowe legitymacje.

Z pokoju hotelowego wyszliśmy razem z Ewenem.

– Jestem przekonany, że jest autentyczny – powiedział Ewen. – Nie mam żadnych wątpliwości.

Jego zdaniem nie było powodu, by dłużej czekać: – Jak tylko wrócimy do hotelu, zadzwonię do Alana i powiem mu, że powinniśmy ruszać z tekstami.

Od tego momentu Ewen został pełnoprawnym członkiem naszego zespołu. Laura i Snowden od razu poczuli się z nim swobodnie, a musiałem przyznać, że ja też. Zdaliśmy sobie sprawę, że nasze podejrzenia nie miały podstaw: za uprzejmym, ojcowskim wyglądem Ewena krył się odważny reporter pragnący rozwinąć tę historię dokładnie tak, jak i ja uważałem za konieczne. Nie przyjechał, by narzucać instytucjonalne ograniczenia, ale by o nich donosić, a czasami pomagać je pokonać. Co więcej, podczas naszego pobytu w Hongkongu to Ewen czasami prezentował najbardziej radykalne stanowisko, opowiadając się za ujawnieniem spraw, co do których nawet Laura i ja – a zresztą także Snowden – nie mieliśmy pewności, czy już należy to robić. Szybko zdałem sobie sprawę, że jego poparcie dla dynamicznego, ostrego relacjonowania sprawy w „Guardianie" miało zasadnicze znaczenie dla pełnej akceptacji Londynu dla naszych działań.

Gdy tylko w Londynie zaczął się dzień, Ewen i ja zadzwoniliśmy razem do Alana. Chciałem wyraźnie dać do zrozumienia, że oczekuję – a nawet żądam – by „Guardian" zaczął publikować tego dnia. Chciałem też wyraźnie usłyszeć, jakie jest stanowisko gazety. Już wówczas – drugiego dnia w Hongkongu – właściwie podjąłem decyzję, że jeśli wyczuję poważne wahanie, pójdę z całą sprawą gdzie indziej.

– Jestem gotów opublikować artykuł na temat Verizonu i nie mogę zrozumieć, dlaczego tego jeszcze nie robimy – powiedziałem Alanowi wprost. – Skąd ta zwłoka?

Zapewnił mnie, że nie ma zwłoki.

– Zgadzam się. Jesteśmy gotowi do publikacji. Janine ma mieć dziś po południu ostatnie spotkanie z prawnikami. Jestem pewien, że potem opublikujemy.

Wskazałem na związek „Post" z historią o PRISM, co tylko podsycało moje przekonanie o pilności sprawy. Alan mnie wówczas zaskoczył: nie tylko chciał jako pierwszy opublikować artykuły o NSA, chciał też jako pierwszy opublikować konkretnie artykuł o PRISM, odbierając sensację „Post".

– Nie ma powodu, dla którego mielibyśmy im ustępować – powiedział.

– Bardzo się cieszę.

Różnica czasu między Londynem a Nowym Jorkiem wynosiła cztery godziny, musieliśmy więc trochę poczekać, zanim Janine przyjdzie do biura, i jeszcze dłużej, zanim spotka się z prawnikami. Spędziłem ten czas z Ewenem, pracując nad artykułem o PRISM, uspokojony, że Rusbridger działa tak dynamicznie, jak trzeba.

Tego dnia ukończyliśmy artykuł o PRISM i używając programu szyfrującego, wysłaliśmy nasz tekst do Janine i Stuarta Millara w Nowym Jorku. Mieliśmy już dwie potężne sensacje gotowe do publikacji: Verizon i PRISM. Moja cierpliwość, moja chęć czekania już się wyczerpywały.

Janine rozpoczęła spotkanie z prawnikami o trzeciej po południu czasu nowojorskiego – czyli o trzeciej nad ranem w Hongkongu – i siedziała z nimi przez dwie godziny. Nie kładłem się, czekając na rezultaty. Gdy w końcu połączyłem się z Nowym Jorkiem, chciałam usłyszeć tylko jedno: natychmiast publikujemy artykuł o Verizonie.

Do tego jednak nie doszło. Janine wyjaśniła, że wciąż istnieją „poważne" kwestie prawne. Po ich rozwiązaniu „Guardian" musi poinformować przedstawicieli rządu o naszych planach, by dać im szansę na przekonanie nas do zaniechania tematu. Ten proces budził moją głęboką niechęć i potępienie. Akceptowałem

fakt, że „Guardian" będzie musiał pozwolić rządowi przedstawić argumenty przeciwko publikacji, pod warunkiem że proces ten nie stanie się sposobem na odwlekanie sprawy całymi tygodniami i osłabianie jej wpływu.

– To brzmi, jakby od publikacji dzieliły nas jeszcze dni, nawet tygodnie, a nie godziny – napisałem do Janine, starając się w czacie przekazać całą moją irytację i niecierpliwość. – Pozwól, że powtórzę, iż podejmę wszystkie konieczne kroki, by ta historia natychmiast została opublikowana.

Groźba była zawoalowana, ale niewątpliwa: jeśli nie mogę natychmiast wydrukować tych materiałów w „Guardianie", pójdę z nimi gdzie indziej.

– Tak, dałeś to już jasno do zrozumienia – odparła zwięźle.

W Nowym Jorku dzień się już kończył i wiedziałem, że przynajmniej do następnego ranka nic się nie wydarzy. Czułem się sfrustrowany, a wówczas już bardzo niespokojny. „Post" pracował nad artykułem o PRISM, a Laurę, która miała być pod nim podpisana, Gellman zawiadomił, że zamierzają opublikować go w niedzielę, czyli za pięć dni.

Omawiając tę kwestię z Davidem i Laurą, zdałem sobie sprawę, że nie mam ochoty już dłużej czekać na „Guardiana". Zgodziliśmy się, że trzeba zacząć rozglądać się za alternatywami. Telefony do magazynu „Nation" i portalu „Salon", gdzie publikowałem od lat, szybko przyniosły owoce. Oba w ciągu kilku godzin odpowiedziały, że z radością od razu puszczą artykuły o NSA, i zaoferowały wszelką możliwą pomoc, w tym prawników gotowych natychmiast zweryfikować artykuły.

Świadomość, że istnieją dwa uznane polityczne serwisy gotowe i chętne, by wydrukować artykuły o NSA, dodała mi odwagi. Jednak w rozmowach z Davidem doszliśmy do wniosku, że istnieje jeszcze potężniejsza możliwość: stworzenie własnej witryny internetowej, nazwanej NSAdisclosures.com, i umieszczanie w niej artykułów bez zależności od jakiegokolwiek

koncernu mediowego. Gdy raz publicznie ogłosimy, że posiadamy ogromny skarbiec tajnych dokumentów o szpiegowskich praktykach NSA, z łatwością zwerbujemy wolontariuszy: redaktorów, prawników, dokumentalistów i osoby chętne, by udzielić nam wsparcia finansowego, cały zespół motywowany jedynie umiłowaniem przejrzystości i prawdziwego, zaczepnego dziennikarstwa.

Od samego początku uważałem, że dokumenty Snowdena umożliwiają naświetlenie nie tylko sekretnego szpiegostwa NSA, ale i korumpującej dynamiki prasy związanej z establishmentem. Ujawnienie najważniejszej od lat sprawy przez nowy, niezależny model dziennikarstwa, działający bez wsparcia jakiejkolwiek wielkiej organizacji mediowej, niezwykle by mi odpowiadało. Mocno podkreślałoby, że gwarantowana w pierwszej poprawce do konstytucji USA wolność prasy i możliwość uprawiania znaczącego dziennikarstwa nie wymagają przynależności do wielkiego koncernu. Gwarancja wolnej prasy chroni nie tylko dziennikarzy pracujących dla korporacji, ale każdego, kto zajmuje się dziennikarstwem – zatrudnionego na stałe czy nie. Co więcej, odwaga, jaką znamionuje taki krok – *opublikujemy tysiące supertajnych dokumentów NSA bez ochrony wielkiej korporacji mediowej* – doda śmiałości innym i pomoże rozbić panujący obecnie nastrój strachu.

Tej nocy znów niemal nie mogłem spać. Wczesne godziny ranne w Hongkongu spędziłem, dzwoniąc do ludzi, których opinie sobie cenię: przyjaciół, prawników, dziennikarzy, dawnych bliskich współpracowników. Wszyscy udzielili mi tej samej rady, która w gruncie rzeczy mnie nie zdziwiła: robienie tego na własną rękę, nie w ramach istniejącej struktury mediów, jest zbyt ryzykowne. Chciałem usłyszeć argumenty przeciwko niezależnemu działaniu, a oni dostarczyli mi wiele sensownych.

Późnym rankiem, wysłuchawszy wszystkich ostrzeżeń, zatelefonowałem do Davida, równocześnie rozmawiając z Laurą

przez internet. Szczególnie David przekonywał mnie, że zwrócenie się do „Salonu" lub „Nation" oznaczałoby nadmierną ostrożność i lękliwość – „krok wstecz", jego zdaniem – i że jeśli „Guardian" zamierza dalej zwlekać, jedynie publikacja na niezależnej stronie internetowej może oddać nieustraszonego ducha przenikającego takie dziennikarstwo, jakie mi odpowiada. Był również przekonany, że ten krok stanowiłby inspirację dla innych na całym świecie. Laura, początkowo nastawiona sceptycznie, dała się przekonać, że tak śmiały ruch i stworzenie globalnej sieci osób oddanych sprawie przejrzystości NSA uwolniłoby olbrzymi przypływ mocy.

W miarę jak w Hongkongu zbliżało się popołudnie, postanowiliśmy wspólnie, że jeśli „Guardian" nie zdecyduje się na publikację do końca dnia – który na Wschodnim Wybrzeżu jeszcze się nie zaczął – odejdę i natychmiast umieszczę artykuł o Verizonie na naszej nowej stronie. Rozumiałem związane z tym ryzyko, ale też przenikało mnie podniecenie podjętą decyzją. Wiedziałem, że taki alternatywny plan doda mi sił w rozmowach z „Guardianem". Czułem, że nie muszę się ich trzymać, by publikować, a wyzwolenie się z więzów zawsze dodaje energii.

Tego samego popołudnia, rozmawiając ze Snowdenem przez internet, przedstawiłem mu nasz plan.

– To dość ryzykowne – odpisał. – Ale odważne. Podoba mi się.

Udało mi się trochę przespać; zbudziłem się późnym popołudniem, a potem musiałem pogodzić się z faktem, że wciąż kilka godzin dzieli mnie od środowego ranka w Nowym Jorku. Wiedziałem, że w jakiś sposób muszę przekazać „Guardianowi" ultimatum. Chciałem mieć to z głowy.

Gdy tylko zobaczyłem, że Janine jest online, spytałem, jakie są plany.

– Czy dziś publikujemy?

– Mam nadzieję – odpowiedziała.

Nie podobała mi się jej niepewność. „Guardian" zamierzał tego ranka porozumieć się z NSA, by poinformować ich o naszych zamiarach. Gdy odpowiedzą, będziemy znać terminarz publikacji.

– Nie rozumiem, dlaczego zamierzamy czekać – powiedziałem, straciwszy cierpliwość do obaw redakcji. – Sprawa jest jasna i bezdyskusyjna, to dlaczego ma nas obchodzić, co ich zdaniem powinniśmy, a czego nie powinniśmy publikować?

Niezależnie od pogardy, jaką budził we mnie cały ten proces – rząd nie powinien być partnerem wydawniczym decydującym, co można publikować – wiedziałem, że ten konkretny artykuł o postanowieniu sądu FISA, ujawniający systematyczne gromadzenie rejestrów połączeń telefonicznych Amerykanów, nie może budzić żadnych sensownych obaw o nasze bezpieczeństwo narodowe. Sam pomysł, że „terroryści" mieliby skorzystać na publikacji nakazu sądu był śmiechu wart: każdy, nawet zupełnie początkujący terrorysta – już wie, że rząd usiłuje monitorować ich połączenia telefoniczne. Ci, którzy mogą się czegoś dowiedzieć z naszego artykułu, to nie „terroryści", ale naród amerykański.

Janine powtórzyła to, co powiedzieli jej prawnicy „Guardiana". Twierdziła, że błędnie zakładam, iż gazeta się przestraszy i nie opublikuje artykułu. Natomiast jest to wymóg prawny – wyjaśniła – by usłyszeć, co ma do powiedzenia rząd USA. Zapewniła mnie jednak, że nie da się zastraszyć ani zbić z tropu niejasnymi i lekceważącymi uwagami o bezpieczeństwie narodowym.

Nie zakładałem, że „Guardian" da się zastraszyć; po prostu nie wiedziałem. Obawiałem się także, że rozmowy z rządem w najlepszym razie wszystko znacznie opóźnią. „Guardian" rzeczywiście znany był z energicznego, bezkompromisowego dziennikarstwa; dlatego zresztą w ogóle do nich przeszedłem. Uważałem także, że mają prawo pokazać, jak zamierzają postąpić w tej sytuacji, a ja nie mam prawa zakładać najgorszego

scenariusza. Deklaracja niezależności złożona przez Janine nieco mnie uspokoiła.

– OK – powiedziałem, zgadzając się na zwłokę. – Powtarzam jednak, że z mojego punktu widzenia musimy to opublikować *dzisiaj* – napisałem.

Mniej więcej w południe czasu nowojorskiego Janine zawiadomiła mnie, że dzwonili do NSA i Białego Domu z informacją o zamierzonej publikacji ściśle tajnego materiału. Nikt jednak nie oddzwonił. Biały Dom tego ranka nominował Susan Rice na doradcę do spraw bezpieczeństwa narodowego. Spencer Ackerman, nowy reporter „Guardiana" do spraw bezpieczeństwa narodowego, który miał dobre kontakty w Waszyngtonie, poinformował Janine, że wszyscy oficjele „zajmują się" Susan Rice.

– W tej chwili uważają, że nie potrzebują do nas oddzwaniać – napisała Janine. – Szybko się nauczą, że muszą odpowiadać na moje telefony.

O trzeciej nad ranem – trzeciej po południu w Nowym Jorku – wciąż panowało milczenie. Nikt także nie porozumiał się z Janine.

– Czy daliście im jakiś termin końcowy, czy też mają się z nami porozumieć, jak im przyjdzie ochota? – napisałem sarkastycznie.

„Guardian" powiedział NSA, że chce z nimi porozmawiać „przed końcem dnia".

– A jeśli się do tej pory nie odezwą? – spytałem.

– Wtedy podejmiemy decyzję – odpowiedziała Janine. I dodała informację o kolejnym komplikującym sprawę elemencie: jej szef Alan Rusbridger właśnie wyleciał z Londynu do Nowego Jorku, by nadzorować publikację artykułów dotyczących NSA. To oznaczało, że przez mniej więcej siedem najbliższych godzin będzie niedostępny.

– Czy możesz to opublikować bez Alana? – zapytałem. Jeśli odpowiedź będzie brzmiała „nie", to nie ma szans, by artykuł

ukazał się tego dnia. Samolot Alana miał lądować na lotnisku JFK dopiero późnym wieczorem.

– Zobaczymy – odparła.

Miałem wrażenie, że natykam się na dokładnie taką instytucjonalną przeszkodę w bezkompromisowym dziennikarstwie, jakiej, wiążąc się z „Guardianem", miałem nadzieję uniknąć – niepewność prawną, konsultacje z urzędnikami rządowymi, instytucjonalną hierarchię, niechęć do podejmowania ryzyka, zwlekanie.

Po krótkiej chwili, mniej więcej kwadrans po trzeciej, zastępca Janine Stuart Millar przysłał mi wiadomość: „Rząd oddzwonił. Janine właśnie z nimi rozmawia".

Czekałem, jak mi się wydawało, całą wieczność. Mniej więcej godzinę później odezwała się Janine i opowiedziała, co się działo. W konferencji telefonicznej brało udział ponad dziesięciu wysokich rangą urzędników z różnych agencji, w tym NSA, Departamentu Sprawiedliwości i Białego Domu. Początkowo traktowali ją protekcjonalnie, ale przyjaźnie, mówiąc, że nie rozumie „kontekstu" nakazu sądu w sprawie Verizona. Chcieli się z nią spotkać „jakoś w przyszłym tygodniu", by wyjaśnić jej całą sprawę.

Gdy Janine odpowiedziała, że zamierza opublikować artykuł tego dnia i uczyni to, o ile nie usłyszy bardzo konkretnych powodów, by tego nie robić, stali się bardziej bojowi, a nawet zaczęli posługiwać się pogróżkami. Powiedzieli jej, że nie jest „poważną dziennikarką", a „Guardian" nie jest „poważną gazetą", skoro nie chce dać rządowi więcej czasu na przekonanie jej do swego stanowiska.

– Żaden normalny koncern mediowy nie publikowałby tak szybko, nie spotykając się najpierw z nami – powiedzieli, najwyraźniej grając na czas.

Pamiętam, że pomyślałem: zapewne mają rację. W tym właśnie rzecz. Obowiązujące reguły pozwalają władzom

kontrolować i neutralizować proces zbierania informacji, eliminują rozbieżne interesy prasy i rządu. Uważałem, że powinni od początku wiedzieć, iż te niezdrowe zasady w tym wypadku nie znajdą zastosowania. Te artykuły ujrzą światło dzienne zgodnie z innymi regułami, definiującymi niezależnych, a nie posłusznych dziennikarzy.

Podobał mi się ton Janine, zdecydowany i bezkompromisowy. Podkreśliła, że choć nieustannie wracała do tego pytania, nie usłyszała ani jednego konkretu, w jaki sposób publikacja miałaby zagrozić bezpieczeństwu narodowemu. Niemniej jednak nie chciała obiecać, że artykuł ukaże się już tego dnia. Na koniec rozmowy powiedziała: „Zobaczę, czy uda mi się porozumieć z Alanem, i wtedy podejmiemy decyzję".

Odczekałem pół godziny.

– Czy publikujemy dzisiaj, czy nie? Tylko tyle chcę wiedzieć – spytałem wprost.

Wykręciła się od odpowiedzi; Alan był nieosiągalny. Oczywiście rozumiałem, że Gibson znajduje się w bardzo trudnym położeniu: z jednej strony przedstawiciele rządu USA oskarżają ją o nieostrożność, z drugiej strony ja stawiam jej coraz bardziej bezkompromisowe żądania. Do tego jeszcze redaktor naczelny gazety siedzi w samolocie. Wszystko to oznaczało, że na nią spadło podjęcie jednej z najtrudniejszych i pociągających największe konsekwencje decyzji w liczącej ponad 190 lat historii gazety.

Porozumiewając się online z Janine, cały czas rozmawiałem przez telefon z Davidem.

– Zbliża się piąta po południu – mówił David. – To termin, jaki im wyznaczyłeś. Pora na decyzję. Muszą opublikować teraz albo ty musisz im powiedzieć, że odchodzisz.

Miał rację, jednak wciąż się wahałem. Odejście z „Guardiana" tuż przed publikacją jednego z największych przecieków dotyczących bezpieczeństwa narodowego wywołałoby wielki

skandal w mediach. Zaszkodziłoby „Guardianowi", ponieważ musiałbym się jakoś publicznie wytłumaczyć; to z kolei zmusiłoby ich do obrony, najprawdopodobniej przez atak na mnie. Zrobiłby się cyrk, wielkie przedstawienie, które przyniosłoby szkodę wszystkim stronom. A co więcej, odciągnęłoby uwagę od tego, co najważniejsze – od tego, co robi NSA.

Musiałem także przyznać się przed samym sobą do strachu. Publikacja setek, jeśli nie tysięcy ściśle tajnych dokumentów NSA będzie ryzykowna nawet w ramach tak dużej organizacji jak „Guardian". Robienie tego na własną rękę, bez ochrony instytucjonalnej, to ryzyko dodatkowo pogłębia. W głowie odbijały mi się echem wszystkie mądre przestrogi przyjaciół i prawników, do których wcześniej dzwoniłem.

– Nie masz wyboru – powiedział David, gdy wciąż się wahałem. – Skoro boją się publikacji, to nie jest to miejsce dla ciebie. Nie możesz kierować się strachem, bo niczego nie osiągniesz. Tej lekcji udzielił ci właśnie Snowden.

Razem ułożyliśmy, co mam przesłać Janine przez czat: „Jest piąta po południu, upływa termin, jaki wam podałem. Jeśli nie opublikujecie materiału natychmiast – w ciągu najbliższych trzydziestu minut – to niniejszym rozwiązuję swoją umowę z «Guardianem»". Już prawie nacisnąłem „wyślij", ale jeszcze się zawahałem. Ten tekst zanadto brzmiał jak ultimatum. Odejście z „Guardiana" w takich warunkach oznaczałoby, że wszystko zostanie upublicznione, łącznie z tą wiadomością. Złagodziłem więc ton: „Rozumiem, że macie swoje obawy i musicie postępować tak, jak waszym zdaniem należy. Ja jednak też muszę postępować tak, jak moim zdaniem należy. Przykro mi, że się nam nie udało". I nacisnąłem „wyślij".

Po piętnastu sekundach w moim hotelowym pokoju zadzwonił telefon.

– Uważam, że jesteś okropnie niesprawiedliwy – powiedziała Janine, wyraźnie roztrzęsiona. Gdybym odszedł, „Guardian" – który nie posiadał żadnych dokumentów – straciłby cały temat.

– Moim zdaniem to wy jesteście niesprawiedliwi – odparłem. – Cały czas pytam, kiedy zamierzacie opublikować, a ty odmawiasz mi odpowiedzi, stosujesz uniki.

– *Zamierzamy* dziś opublikować – zaprotestowała Janine.

– Najdalej za pół godziny. Wprowadzamy ostatnie redakcyjne poprawki, opracowujemy tytuły i formatujemy. Pojawi się nie później niż o wpół do szóstej.

– OK, jeśli taki jest plan, to w porządku – powiedziałem.

– Oczywiście zaczekam pół godziny.

Za dwadzieścia szósta Janine przesłała mi czatem link, na który czekałem od paru dni.

– Jest na stronie – powiedziała.

NSA codziennie gromadzi rejestry rozmów milionów klientów Verizona – brzmiał tytuł, a dalej biegł podtytuł: *Raport specjalny: Ściśle tajne postanowienie sądu, nakazujące Verizonowi przekazanie wszystkich danych o połączeniach, odsłania skalę inwigilacji w kraju pod rządami Obamy.*

Potem następował link do pełnej treści nakazu sądu FISA. Pierwsze trzy akapity relacjonowały całą sprawę:

Zgodnie z wydanym w kwietniu ściśle tajnym nakazem sądowym Agencja Bezpieczeństwa Narodowego gromadzi obecnie rejestry połączeń milionów amerykańskich klientów Verizona, jednej z największych firm telekomunikacyjnych w USA.

Nakaz, którego kopią „Guardian" dysponuje, poleca Verizonowi, by w „ciągły sposób, codziennie" przekazywał NSA informacje o wszystkich połączeniach telefonicznych dokonywanych w ramach jego systemu, tak wewnątrzkrajowych, jak i między USA a innymi państwami.

Ten dokument po raz pierwszy pokazuje, że za administracji Obamy rejestry połączeń milionów obywateli USA są gromadzone na oślep i masowo – niezależnie od tego, czy obywatele ci są podejrzewani o jakieś wykroczenia.

Odzew na artykuł był natychmiastowy i potężny, przekraczający wszystko, czego się mogłem spodziewać. Tego wieczoru sprawa NSA okazała się głównym tematem w krajowych wiadomościach, zdominowała dyskusje polityczne i medialne. Zalały mnie prośby o wywiad od niemal wszystkich ogólnokrajowych stacji telewizyjnych: CNN, MSNBC, NBC, programów *Today Show, Good Morning America* i innych. Przez wiele godzin rozmawiałem z Hongkongu z życzliwie nastawionymi dziennikarzami telewizyjnymi, którzy prowadzili ze mną wywiady – dość niezwykłe doświadczenie w karierze osoby piszącej na tematy polityczne – a wszyscy traktowali ten temat jako znaczące wydarzenie i prawdziwy skandal.

Rzecznik Białego Domu natychmiast zaczął bronić programu masowego gromadzenia danych jako „niezwykle istotnego narzędzia chroniącego naród przed groźbą terroryzmu". Dianne Feinstein, demokratyczna przewodnicząca senackiej Komisji Wywiadu, należąca w Kongresie do najbardziej niewzruszonych zwolenników państwa opartego na instytucjach bezpieczeństwa narodowego w ogóle, a amerykańskiej inwigilacji w szczególności, powróciła do pełnego strachu stylu powszechnego po 11 września, mówiąc dziennikarzom, że program jest konieczny, ponieważ „ludzie chcą bezpiecznej ojczyzny".

Jednak niemal nikt nie potraktował tych twierdzeń poważnie. Popierający Obamę „New York Times" zamieścił ostre potępienie administracji. W artykule redakcyjnym zatytułowanym *Obława prezydenta Obamy* dziennik napisał: „Pan Obama potwierdza truizm, że władza wykonawcza wykorzysta wszystkie uprawnienia, jakie otrzyma, a prawdopodobnie ich nadużyje". Kpiąc z rutynowego odwoływania się administracji do „terroryzmu", aby usprawiedliwiać program, artykuł stwierdzał: „administracja utraciła teraz wszelką wiarygodność" (kilka godzin po opublikowaniu powyższego oświadczenia „New

York Times" złagodził je nieco przez dodanie „w tej kwestii", co wywołało pewne kontrowersje).

Demokratyczny senator Mark Udall wydał oświadczenie, w którym stwierdził: „Ten rodzaj inwigilacji na wielką skalę powinien niepokoić nas wszystkich. Jest to ten rodzaj nadużycia ze strony rządu, który, jak powtarzałem, Amerykanie uznają za szokujący". Amerykańska Unia Swobód Obywatelskich (ACLU) ogłosiła: „Z punktu widzenia swobód obywatelskich trudno o bardziej niepokojący program [...] Idzie dalej niż Orwell i dostarcza kolejnego dowodu, w jak wielkim zakresie podstawowe prawa demokratyczne są podporządkowywane żądaniom agencji wywiadu, których nikt nie rozlicza". Były wiceprezydent Al Gore na Twitterze podał link do naszego artykułu i napisał: „Czy tylko ja tak uważam, czy powszechna inwigilacja naprawdę jest nieprzyzwoita i oburzająca?".

Wkrótce po opublikowaniu artykułu Associated Press otrzymała od niewymienionego z nazwiska senatora potwierdzenie tego, co już podejrzewaliśmy – że program masowego gromadzenia rejestrów połączeń telefonicznych trwa od lat i obejmuje wszystkie większe amerykańskie firmy telekomunikacyjne, nie tylko Verizon.

Pisałem i mówiłem o NSA od siedmiu lat, ale żadna wiadomość nigdy nawet w przybliżeniu nie wywołała takiego zainteresowania i namiętności. Nie było czasu na analizowanie, dlaczego odbiła się aż takim echem i wywołała tak ogromną falę zainteresowania i oburzenia; jak na razie zamierzałem płynąć na tej fali, nie próbując jej zrozumieć.

W Hongkongu było południe, gdy skończyłem udzielać wywiadów i udałem się wprost do hotelu Snowdena. Kiedy wszedłem do jego pokoju, oglądał właśnie CNN. Zaproszeni goście dyskutowali o NSA, zaszokowani zasięgiem szpiegowania. Prowadzący byli pełni gniewu, że to wszystko czyniono w tajemnicy.

– Wszędzie o tym mówią – powiedział podekscytowany Snowden. – Oglądałem wszystkie twoje wywiady. Najwyraźniej do wszystkich to dotarło.

W tamtej chwili wypełniało mnie poczucie, że coś osiągnąłem. Największa obawa Snowdena – że zmarnuje sobie życie na rewelacje, które nikogo nie będą obchodzić – okazała się nieuzasadniona od razu pierwszego dnia: nie dostrzegliśmy ani cienia obojętności czy apatii. Laura i ja pomogliśmy mu rozpętać dokładnie taką dyskusję, jaka zdaniem nas obojga była pilnie potrzebna – a teraz widziałem, jak Snowden obserwuje jej rozwój.

Biorąc pod uwagę, że zamierzał ujawnić się po pierwszym tygodniu artykułów, obaj wiedzieliśmy, że jego wolność może się niedługo skończyć. Moja przygnębiająca pewność, że wkrótce stanie się celem ataku – że będzie obiektem nagonki, jeśli w ogóle nie znajdzie się pod kluczem jako przestępca – kładła się cieniem na wszystko, co robiliśmy. Wydawał się tym całkiem nie przejmować, ja jednak zamierzałem na wszelkie sposoby uzasadniać jego wybór, maksymalnie odsłaniać wartość odkryć, które mimo wielkiego osobistego ryzyka postanowił pokazać światu. Dobrze zaczęliśmy, ale był to dopiero początek.

– Wszyscy myślą, że to jednorazowa historia, pojedyncza sensacja – zauważył Snowden. – Nikt nie wie, że to sam czubek góry lodowej, że będzie dużo, dużo więcej.

Odwrócił się do mnie:

– Co dalej i kiedy?

– PRISM – odparłem. – Jutro.

Wróciłem do hotelu i choć zbliżała się szósta bezsenna noc, po prostu nie potrafiłem się wyłączyć. Adrenalina zbytnio mnie nakręcała. O wpół do piątej, mając nadzieję na chwilę odpoczynku, wziąłem coś na sen i nastawiłem budzik na wpół do ósmej. Wiedziałem, że wtedy wydawcy „Guardiana" w Nowym Jorku będą się logować do internetu.

Tego dnia Janine pojawiła się w pracy wcześnie. Pogratulowaliśmy sobie nawzajem i cieszyliśmy się reakcją na artykuł. Natychmiast wyczułem, że ton naszej rozmowy radykalnie się zmienił. Właśnie pokonaliśmy razem znaczące dziennikarskie wyzwanie. Janine była dumna z artykułu, ja byłem dumny z jej oporu wobec rządowego zastraszania i z decyzji o publikacji. „Guardian" odważnie i w godny podziwu sposób wywiązał się z zadania.

Choć wówczas wydawało nam się, że doszło do znacznego opóźnienia, patrząc na sprawę z perspektywy czasu trzeba przyznać, że „Guardian" posuwał się w godnym uwagi tempie i z odwagą, większą niż – jestem pewien – jakakolwiek inna firma mediowa porównywalnej wielkości i znaczenia. A Janine wyraźnie mówiła, że gazeta nie zamierza spocząć na laurach.

– Alan nalega, byśmy dziś opublikowali PRISM – powiedziała. To mnie oczywiście uszczęśliwiło.

Ujawnienie sprawy PRISM było tak istotne przede wszystkim dlatego, że program ten pozwalał NSA otrzymywać właściwie wszystko, co chciała, od firm internetowych, których produktów używają obecnie setki milionów ludzi na całym świecie jako głównego środka do komunikowania się. Działania Agencji zostały umożliwione przez ustawy wprowadzone przez rząd USA po 11 września, nadające NSA ogromną władzę kontrolną nad Amerykanami i możliwość prowadzenia powszechnej, masowej inwigilacji całych zagranicznych populacji.

Podstawę prawną inwigilacji przez NSA stanowi obecnie uchwalona w 2008 roku Ustawa o poprawkach do ustawy o FISA. Zatwierdził ją Kongres przy poparciu obu partii – Demokratycznej i Republikańskiej – w następstwie skandalu z prowadzonym przez NSA nieuprawnionym podsłuchiwaniem z epoki Busha, a jej głównym rezultatem było to, że praktycznie zalegalizowała istotę nielegalnego programu. Jak ujawnił skandal, Bush potajemnie upoważnił NSA do podsłuchiwania

Amerykanów i innych osób na terenie Stanów Zjednoczonych, uzasadniając ten rozkaz potrzebą przeciwdziałania działaniom terrorystycznym. Decyzja prezydenta odrzucała wymóg uzyskiwania zatwierdzonych przez sąd nakazów, zazwyczaj koniecznych w przypadku szpiegowania wewnątrz kraju, i doprowadziła do tajnej inwigilacji co najmniej tysięcy osób na terenie Stanów Zjednoczonych.

Mimo protestów, że program jest nielegalny, ustawa o poprawkach do FISA z 2008 roku częściowo go uprawomocniła, zamiast położyć mu kres. Ustawa opiera się na rozróżnieniu między „podmiotami USA" (obywatele amerykańscy i osoby legalnie przebywające na terytorium Stanów Zjednoczonych) a wszystkimi innymi osobami. NSA wciąż musi uzyskać indywidualny nakaz od sądu FISA, jeśli zamierza kontrolować rozmowy telefoniczne i e-maile konkretnego podmiotu amerykańskiego.

Żaden indywidualny nakaz nie jest jednak potrzebny do inwigilacji innych osób, *nawet wówczas, jeśli komunikują się one z podmiotami amerykańskimi.* Zgodnie z paragrafem 702 ustawy z 2008 roku wystarczy, jeśli NSA raz w roku przedstawi sądowi FISA ogólne wytyczne określające cele w danym roku – wystarczy kryterium, że inwigilacja „wspomoże uprawnione działania wywiadu za granicą" – i już otrzymuje ogólną zgodę na działanie. Gdy sąd FISA na tych zezwoleniach postawi stempel „zatwierdzono", NSA ma prawo podjąć inwigilację dowolnego obcokrajowca; może też zmusić firmy telekomunikacyjne i internetowe do zapewnienia jej dostępu do wszelkich form łączności nie-Amerykanów, w tym także nawiązywanej z podmiotami amerykańskimi w takich formach jak czaty na Facebooku, e-maile z Yahoo! czy wyszukiwania w Google'u. Nie ma potrzeby przekonywania sądu, że dana osoba jest winna przestępstwa ani nawet, że są powody, by traktować ją podejrzliwie. Nie ma też obowiązku filtrowania podmiotów amerykańskich, które w tym procesie będą inwigilowane.

Redaktorzy „Guardiana" musieli teraz zacząć od powiadomienia rządu o zamiarze opublikowania materiałów o PRISM. Znów zamierzaliśmy dać im czas do końca dnia pracy czasu nowojorskiego. Mieli więc cały dzień na zgłaszanie wszelkich zastrzeżeń, co odbierało siłę nieuniknionym utyskiwaniom, że brakuje im czasu na reakcję. Równie istotne było jednak zebranie komentarzy tych serwisów internetowych, które, według dokumentów NSA, zapewniły Agencji bezpośredni dostęp do swoich serwerów: Facebooka, Google'a, Apple'a, YouTube'a, Skype'a i pozostałych.

Przed nami znów ciągnęły się godziny czekania, wróciłem więc do hotelu Snowdena, gdzie Laura pracowała z nim nad różnymi sprawami. W tym okresie, przekroczywszy ważny próg – publikację pierwszego sensacyjnego materiału – Snowden z wyraźnie większą czujnością zaczął podchodzić do swojego bezpieczeństwa. Po moim wejściu położył przy drzwiach dodatkowe poduszki. Kilkakrotnie, gdy chciał otworzyć kodowane pliki, nakładał na głowę koc, by kamery w suficie nie wyłapały używanych przez niego haseł. Zadzwonił telefon – a my wszyscy zamarliśmy, któż to może być? Po kilku dzwonkach Snowden ostrożnie podniósł słuchawkę. Obsługa hotelowa pytała, czy nie chciałby, żeby sprzątnęli mu pokój.

– Nie, dziękuję – odparł krótko.

Podczas naszych spotkań w pokoju Snowdena zawsze panowało napięcie, a zwiększyło się jeszcze, gdy zaczęliśmy publikować. Nie mieliśmy pojęcia, czy NSA zidentyfikowała źródło przecieku. Jeśli tak, czy wiedzieli, gdzie Snowden przebywa? Czy wiedzieli to agenci hongkońscy albo chińscy? W każdej chwili ktoś mógł zapukać do drzwi i położyć natychmiastowy i nieprzyjemny kres naszej wspólnej pracy.

W tle cały czas był włączony telewizor i wydawało się, że nieustannie ktoś coś mówi o NSA. Po ujawnieniu sprawy Verizonu programy publicystyczne zajmowały się niemal

wyłącznie „masowym gromadzeniem", „rejestrami połączeń lokalnych" i „nadużywaniem kontroli". Wybierając kolejne tematy, Laura i ja przyglądaliśmy się Snowdenowi śledzącemu wywołane przez siebie zamieszanie.

Potem, o drugiej nad ranem czasu hongkońskiego, odezwała się Janine.

– Zdarzyło się coś niezwykle dziwnego – powiedziała. – Wszystkie firmy internetowe absolutnie zaprzeczają temu, co jest w dokumentach NSA. Twierdzą, że nigdy nie słyszały o PRISM.

Zaczęliśmy rozważać możliwe przyczyny ich zaprzeczeń. Być może dokumenty NSA przesadnie oceniały możliwości Agencji. Być może firmy po prostu kłamały albo osoby, z którymi „Guardian" rozmawiał, nic nie wiedziały o układzie swego pracodawcy z NSA. A może PRISM było po prostu wewnętrznym kryptonimem używanym przez NSA, ale nigdy nieudostępnionym tym firmom.

Niezależnie od przyczyny musieliśmy na nowo napisać artykuł – nie tylko po to, by zamieścić zaprzeczenia, ale także, by uwypuklić dziwną rozbieżność między dokumentami NSA a stanowiskiem firm internetowych.

– Nie zajmujmy w tej sprawie stanowiska. Opiszmy tę rozbieżność i niech rozmawiają o tym publicznie – zaproponowałem. Taka sprawa zmusi do otwartej dyskusji o tym, co przemysł internetowy zgodził się zrobić z komunikacją swoich użytkowników. Jeśli ich wersja odbiega od dokumentów NSA, będą musieli to omówić na oczach świata – i tak powinno być.

Janine zgodziła się i dwie godziny później przysłała mi nowy projekt artykułu o PRISM. Tytuł brzmiał:

Program NSA pod nazwą PRISM ściąga dane użytkowników Apple'a, Google'a i innych

Ściśle tajny program NSA pod nazwą PRISM umożliwia bezpośredni dostęp do serwerów firm, w tym Google'a, Apple'a i Facebooka

Firmy zaprzeczają, jakoby wiedziały o programie działającym od 2007 roku

Zacytowawszy dokumenty NSA opisujące działanie PRISM, artykuł podawał: „Choć dokument Agencji twierdzi, że program działa przy współpracy firm, wszyscy, którzy w czwartek odpowiedzieli na prośbę «Guardiana» o komentarz, zaprzeczyli, jakoby wiedzieli o takim programie". Moim zdaniem artykuł wyglądał świetnie, a Janine obiecała, że ukaże się w ciągu pół godziny.

Czekałem niecierpliwie, licząc minuty, gdy odezwał się brzęczyk zapowiadający wiadomość na czacie. Miałem nadzieję, że to Janine zawiadamia mnie o publikacji artykułu. Rzeczywiście wiadomość pochodziła od Janine, ale jej treść była zaskakująca.

– „Post" właśnie opublikował swój artykuł o PRISM – powiedziała.

Jak to się stało, że „Post" nagle przesunął planowany termin publikacji o trzy dni?

Laura wyciągnęła od Bartona Gellmana, że „Post" dowiedział się o naszych zamiarach po porannym spotkaniu „Guardiana" z urzędnikami amerykańskiego rządu na temat programu PRISM. Jeden z tych urzędników, wiedząc, że „Post" pracuje nad podobnym tematem, przekazał im tę informację, a gazeta przyspieszyła termin publikacji, byśmy nie odebrali im sensacyjnego tematu.

Znienawidziłem cały proces uzgodnień jeszcze bardziej: amerykański urzędnik wykorzystał procedurę wymaganą przed publikacją, rzekomo mającą chronić bezpieczeństwo narodowe, by zapewnić pierwszeństwo swojej ulubionej gazecie!

Gdy już przetrawiłem tę informację, zauważyłem, że Twitter aż pęka od komentarzy na temat artykułu „Post". Przeczytawszy

go jednak, zauważyłem, że czegoś w nim brakuje – nie wspomniano o rozbieżnościach między wersją NSA a oświadczeniami firm internetowych.

Artykuł zatytułowany *Wywiad USA i brytyjski używają obszernego, tajnego programu do czerpania danych z dziewięciu amerykańskich firm internetowych*, podpisany przez Gellmana i Laurę, podawał: „Agencja Bezpieczeństwa Narodowego i FBI podłączają się bezpośrednio do centralnych serwerów dziewięciu czołowych amerykańskich firm internetowych, czerpiąc z nich czaty audio i wideo, zdjęcia, e-maile, dokumenty i rejestry połączeń, co umożliwia analitykom śledzenie zagranicznych podmiotów". Co istotne, twierdził także, że tych dziewięć firm „świadomie uczestniczy w działaniu PRISM".

Nasz własny artykuł o PRISM, o nieco innym wydźwięku i ostrożniej sformułowany, ukazał się dziesięć minut później; podkreślono w nim zdecydowane zaprzeczenia wszystkich dziewięciu firm.

Raz jeszcze reakcja okazała się wybuchowa. Co więcej, międzynarodowa. O ile firmy telekomunikacyjne zazwyczaj działają na terenie jednego kraju, o tyle internetowi giganci są globalni. Dla miliardów ludzi na całym świecie, w krajach na wszystkich kontynentach Facebook, Gmail, Skype i Yahoo! to podstawowe środki komunikowania się. Fakt, że te firmy weszły w tajne układy z NSA, by zapewnić Agencji dostęp do połączeń klientów, wywołał szok na całym świecie.

Zaczęto też domyślać się, że wcześniejsza historia o Verizonie nie była odosobniona: dwa artykuły oznaczały już poważny przeciek z NSA.

W dniu, w którym ukazał się artykuł o PRISM, po raz ostatni na wiele miesięcy byłem w stanie przeczytać i odpowiedzieć na otrzymane e-maile. Niemal wszystkie większe koncerny mediowe na świecie prosiły o wywiad. Ogólnoświatowa debata, którą Snowden chciał wywołać, już się toczyła – po zaledwie

dwóch dniach publikacji. Myślałem o potężnej skarbnicy jeszcze niewykorzystanych dokumentów, o tym, co to może oznaczać dla mego życia, o wpływie, jaki to wywrze na cały świat, i o tym, jak zareaguje rząd USA, gdy zda sobie sprawę, co go spotkało.

Ten dzień był powtórką poprzedniego: wczesne poranne godziny w Hongkongu spędziłem, udzielając wywiadów programom publicystycznym nadawanym w Stanach Zjednoczonych w porze największej oglądalności. W ten sposób ustalił się wzorzec, który utrzymał się przez cały czas spędzony w Hongkongu – nocą praca z „Guardianem" nad artykułami, rano wywiady dla mediów, a potem dołączałem do Laury i Snowdena w jego pokoju hotelowym.

Często jeździłem po Hongkongu taksówkami o trzeciej czy czwartej nad ranem do studiów telewizyjnych, nieodmiennie pamiętając o udzielonych mi przez Snowdena instrukcjach o „bezpieczeństwie operacyjnym" – nigdy nie rozstawać się z komputerem i pendrive'ami pełnymi dokumentów, by nie dopuścić do majstrowania przy nich albo kradzieży. Jeździłem po wyludnionych ulicach Hongkongu zawsze z ciężkim plecakiem na ramionach, niezależnie dokąd i o jakiej porze. Cały czas walczyłem z paranoją, często jednak łapałem się na tym, że spoglądam przez ramię, a ilekroć ktoś się zbliża, mocniej chwytam plecak.

Gdy już skończyłem brać udział w całej serii wywiadów telewizyjnych, ruszałem z powrotem do pokoju Snowdena, gdzie Laura, Snowden i ja – czasami także Ewen McAskill – kontynuowaliśmy pracę, przerywając jedynie, by zerkać na telewizję. Zdumiewała nas tak pozytywna reakcja, solidne zainteresowanie mediów ujawnianymi tematami, a także gniew większości komentatorów skierowany nie przeciwko tym, którzy wprowadzili jawność, tylko przeciwko ogromnej państwowej inwigilacji.

Mogłem teraz zrealizować jedną z naszych zamierzonych strategii, czyli wyzywająco i z pogardą odpowiedzieć na rządową taktykę przywoływania 11 września jako uzasadnienia dla szpiegowania. Zacząłem podważać wyświechtane i przewidywalne zarzuty wysuwane przez Waszyngton, że naraziliśmy bezpieczeństwo narodowe na ryzyko, że pomagamy terrorystom, że popełniliśmy przestępstwo, ujawniając tajemnice narodowe.

Czułem dość odwagi, by twierdzić, że są to łatwe do przejrzenia, manipulatorskie strategie urzędników rządowych, których przyłapano na czymś, czego się wstydzą i co zaszkodziło ich reputacji. Takie ataki nie powstrzymają nas przed pisaniem – opublikujemy znacznie więcej artykułów na tematy z dokumentów, niezależnie od sianej przez rząd paniki i gróźb, wypełniając swój dziennikarski obowiązek. Chciałem jasno postawić sprawę: zwykłe taktyki zastraszania i demonizacji nie zdadzą się na nic. Mimo takiej naszej postawy w tych pierwszych dniach większość mediów okazywała nam poparcie.

To mnie zdumiało, ponieważ szczególnie od czasów 11 września (choć także i wcześniej) amerykańskie media na ogół zachowywały się niezwykle lojalnie wobec rządu, a zatem nieprzychylnie, czasem nawet napastliwie wobec tych, którzy ujawniali jego sekrety.

Gdy WikiLeaks zaczęło publikować tajne dokumenty dotyczące wojen w Iraku i Afganistanie, w tym depesze dyplomatyczne, dziennikarze przodowali w wezwaniach do wniesienia oskarżenia przeciwko portalowi, co samo w sobie było zdumiewające. Instytucja, której zadaniem było patrzenie władzy na ręce, nie tylko potępiła, ale wręcz usiłowała kryminalizować jedno z najbardziej znaczących od lat działań na rzecz przejrzystości. To, co uczyniło WikiLeaks – otrzymanie poufnych informacji od źródła wewnątrz rządu, a następnie ujawnienie tego światu – to właściwie to, co organizacje mediowe robią cały czas.

Oczekiwałem, że amerykańskie media odniosą się do mnie wrogo, szczególnie że nadal publikowaliśmy artykuły i zaczął się już rysować bezprecedensowy zakres przecieku. Co więcej, jako surowy krytyk dziennikarskiego establishmentu i wielu jego czołowych postaci byłem – jak mi się wydawało – magnesem przyciągającym taką wrogość. Miałem niewielu sprzymierzeńców w tradycyjnych mediach. Działalność większości z nich atakowałem publicznie, często i bezlitośnie. Spodziewałem się zatem, że zwrócą się przeciwko mnie, gdy tylko nadarzy im się okazja; jednak w tym pierwszym tygodniu występowanie w mediach było prawdziwym świętem miłości, i to nie tylko wtedy, gdy byłem na wizji.

W czwartek, piątego dnia w Hongkongu, Snowden powiedział mi zaraz na wstępie, że ma „nieco niepokojące" wieści. Podłączone do internetu urządzenie bezpieczeństwa zainstalowane w domu, który dzielił ze swoją dziewczyną na Hawajach, wykryło, że przyszły go szukać dwie osoby z NSA – jedna z kadr, druga z Agencji – oraz z policji.

Snowden wyciągnął z tego wniosek, że NSA go prawdopodobnie zidentyfikowała jako źródło przecieku, ja jednak potraktowałem to sceptycznie.

– Gdyby sądzili, że to ty, przysłaliby całą gromadę agentów FBI z nakazem rewizji i zapewne drużynę SWAT, a nie jednego funkcjonariusza NSA i kogoś z kadr.

Uznałem, że to automatyczna, rutynowa kontrola wywołana parotygodniową i niewyjaśnioną nieobecnością pracownika. Snowden zastanawiał się jednak, czy przypadkiem tak nielicznej delegacji nie chodziło o uniknięcie uwagi mediów albo niedopuszczenie do próby usunięcia dowodów.

Cokolwiek oznaczała ta wiadomość, podkreślała potrzebę szybkiego przygotowania artykułów i wideo, na którym Snowden przedstawi się jako źródło przecieków. Zdecydowanie chcieliśmy, żeby świat usłyszał o Snowdenie, jego działaniach

i motywach od niego samego, a nie z demonizującej go kampanii, którą na pewno rozpęta rząd USA w czasie, gdy on się ukrywa lub jest aresztowany i nie może sam mówić za siebie.

Zamierzaliśmy opublikować jeszcze dwa artykuły – jeden tego dnia, kolejny w sobotę – a w niedzielę zamieścić duży artykuł o Snowdenie razem z nagranym z nim wywiadem i wydrukowaną sesją pytań i odpowiedzi prowadzoną przez Ewena.

Przez poprzednie czterdzieści osiem godzin Laura montowała nagranie z mojej pierwszej rozmowy ze Snowdenem, powiedziała jednak, że jest zbyt szczegółowe, za długie i zbyt rwane, żeby się je dało wykorzystać. Chciała nakręcić nowy wywiad, bardziej spójny i konkretny, napisała mi więc około dwudziestu pytań, które miałem mu zadać. Gdy Laura ustawiała kamerę i pokazywała nam, gdzie mamy usiąść, dodałem kilka własnych.

– Hmmm... Nazywam się Ed Snowden – zaczynał się legendarny już film. – Mam 29 lat. Pracuję w Booz Allen Hamilton jako analityk infrastruktury dla NSA na Hawajach.

Snowden udzielał rzeczowych, konkretnych, racjonalnych odpowiedzi na wszystkie pytania. Dlaczego postanowił ujawnić te dokumenty? Dlaczego było to dla niego tak ważne, że poświęcił własną wolność? Jakie odkrycia są najbardziej znaczące? Czy w tych dokumentach jest coś nielegalnego lub przestępczego? Co go, jego zdaniem, spotka?

Podając przykłady nielegalnej, inwazyjnej inwigilacji, stał się ożywiony i podekscytowany. Jednak dopiero gdy go spytałem, jakich reperkusji oczekuje, okazał zdenerwowanie, bo obawiał się, że rząd może wziąć odwet na jego rodzinie i dziewczynie. Powiedział, że będzie unikać z nimi kontaktu, by ograniczyć to ryzyko; wie jednak, że nie może ich w pełni chronić.

– To jedyna rzecz, która nie daje mi spać: co się z nimi stanie – powiedział, a do oczu napłynęły mu łzy.

Gdy Laura zajmowała się montażem, Ewen i ja dopracowywaliśmy kolejne artykuły. Trzeci, opublikowany tego samego

dnia, ujawniał ściśle tajną prezydencką dyrektywę, podpisaną przez Baracka Obamę w listopadzie 2012 roku, nakazującą Pentagonowi i związanym z nim agencjom przygotować się do serii ofensywnych cyberoperacji na całym świecie. W pierwszym paragrafie pisaliśmy: „«Guardian» dotarł do ściśle tajnej prezydenckiej dyrektywy [polecającej] wysokim rangą urzędnikom agencji bezpieczeństwa narodowego i wywiadu sporządzenie listy potencjalnych zagranicznych celów amerykańskich cyberataków".

Czwarty artykuł, który zgodnie z planem ukazał się w sobotę, dotyczył BOUNDLESS INFORMANT, programu NSA do śledzenia danych, i przedstawiał raporty świadczące, że Agencja gromadzi, analizuje i przechowuje miliardy rozmów telefonicznych i e-maili do i od Amerykanów. Stawiał również pytanie, czy urzędnicy NSA nie kłamali przed Kongresem, gdy odmówili senatorom podania liczby przechwyconych w kraju wiadomości, twierdząc, że nie przechowują takich zapisów i nie są w stanie gromadzić takich danych.

Po publikacji artykułu o BOUNDLESS INFORMANT Laura i ja planowaliśmy spotkanie w hotelu Snowdena. Jednak przed wyjściem z pokoju, siedząc na łóżku, ni stąd, ni zowąd przypomniałem sobie „Cincinnatusa", mojego anonimowego korespondenta sprzed sześciu miesięcy, który bombardował mnie e-mailami, domagając się instalacji PGP. Może on też miał dla mnie ważny temat? Z pewnym trudem odszukałem jeden z jego dawnych listów.

„Hej, dobre wieści – napisałem do niego. – Wiem, że to trochę trwało, ale w końcu zacząłem używać poczty PGP. Jeśli więc wciąż jest Pan zainteresowany, jestem gotów do rozmowy o każdej porze". I nacisnąłem „wyślij".

Gdy przyszedłem do Snowdena, spojrzał na mnie kpiąco: – Nawiasem mówiąc, ten „Cincinnatus", do którego właśnie napisałeś, to ja.

Chwilę trwało, zanim doszedłem do siebie. Ta osoba, która wiele miesięcy temu nalegała, bym zaczął używać szyfrowanej poczty, to... Snowden? Zatem nasz pierwszy kontakt nastąpił nie miesiąc temu, w maju, ale pół roku wcześniej. Starał się ze mną skontaktować w sprawie przecieku, zanim porozumiał się z Laurą czy kimkolwiek innym.

Z każdym mijającym dniem, z każdą wspólnie spędzoną godziną zacieśniały się łączące nas więzi. Skrępowanie i napięcie z naszego pierwszego spotkania szybko przerodziło się w relację opartą na współpracy, zaufaniu i wspólnym celu. Wiedzieliśmy, że razem rozpoczęliśmy jedno z najbardziej znaczących wydarzeń w naszym życiu.

Jednak po opublikowaniu artykułu o BOUNDLESS INFORMANT dość swobodny nastrój, jaki udało nam się zachować dzięki wzajemnemu zaufaniu, ustąpił wyczuwalnemu niepokojowi. Niecała doba dzieliła nas od ujawnienia tożsamości Snowdena, a to, jak wiedzieliśmy, wszystko zmieni – przede wszystkim dla niego. Nasza trójka przeżyła razem krótkie, ale wyjątkowo intensywne i satysfakcjonujące doświadczenie. Jeden z nas, Snowden, miał wkrótce odłączyć się od naszej grupy, być może znaleźć się na długi czas w więzieniu – ten fakt od samego początku wisiał w powietrzu i, przynajmniej na mnie, działał przygnębiająco. Jedynie on sam wydawał się tym nie przejmować. Teraz do naszych rozmów wkradł się wisielczy humor.

– Optuję za dolną pryczą w Guantanamo – żartował Snowden, gdy rozważaliśmy nasze perspektywy. Dyskutując o przyszłych artykułach, mówił na przykład: – To się znajdzie w akcie oskarżenia. Pytanie tylko, czy w moim, czy w twoim.

Przeważnie jednak zachowywał niezwykły spokój. Nawet teraz, gdy mijały minuty jego wolności, chodził spać o wpół do jedenastej wieczorem, tak samo jak przez wszystkie dni mego pobytu w Hongkongu. Mnie z trudem udawało się zasnąć na dwie godziny, on jednak utrzymywał regularny rytm.

– No dobra, idę na siano – oświadczał spokojnie co wieczór i szedł spać na siedem i pół godziny, by następnego ranka pojawić się znów w doskonałej formie.

Na pytanie, jak udaje mu się tak dobrze sypiać w tych okolicznościach, oświadczył, że nie ma żadnych wątpliwości co do tego, co zrobił, więc ma spokojne noce.

– Sądzę, że nie zostało mi wiele nocy z wygodną poduszką, więc powinienem je możliwie dobrze wykorzystać – żartował.

W niedzielne popołudnie czasu hongkońskiego Ewen i ja wprowadzaliśmy ostatnie drobne zmiany w artykule przedstawiającym światu Snowdena, a Laura kończyła montaż wideo. Rozmawiałem z Janine – która zalogowała się na czat, gdy tylko w Nowym Jorku zaczął się poranek – o szczególnym znaczeniu starannego przygotowania tego materiału, a także o tym, że czuję się osobiście zobowiązany, by oddać sprawiedliwość decyzjom Snowdena. Darzyłem coraz większym zaufaniem moich kolegów z „Guardiana", ich umiejętności redakcyjne i ich odwagę. W tym wypadku jednak w materiale, który miał przedstawić Snowdena światu, chciałem sam zatwierdzać wszystkie poprawki, duże i małe.

Nieco później do mego pokoju przyszła Laura, by Ewenowi i mnie pokazać swój film. Oglądaliśmy w milczeniu. Film był znakomity – zdjęcia oszczędne, a montaż świetny – ale o jego sile stanowiły przede wszystkim słowa wypowiadane przez Snowdena. Emanował przekonaniem, pasją i zaangażowaniem, czyli demonstrował te cechy, które skłoniły go do działania. Wiedziałem, że jego odważne przyznanie się do tego, co zrobił, i wzięcie odpowiedzialności za swoje działania, odmowa życia w ukryciu jako ścigana zwierzyna, staną się inspiracją dla milionów ludzi.

Najbardziej pragnąłem, żeby świat zobaczył nieustraszony charakter Snowdena. Przez minioną dekadę rząd USA bardzo

starał się demonstrować swoją nieograniczoną potęgę. Rozpoczynał wojny, torturował i więził ludzi bez wyroków, używał dronów do zabijania poza wymiarem sprawiedliwości. A posłańcy nie byli chronieni: sygnalistów obrażano i prześladowano, dziennikarzy więziono i obsypywano groźbami. Starannie inscenizując zastraszanie każdego, kto stanowiłby poważniejsze wyzwanie, rząd starał się udowodnić narodowi, że jego władza nie jest ograniczona prawem, etyką, moralnością ani konstytucją: *patrzcie, co możemy zrobić i co zrobimy tym, którzy przeszkadzają nam w realizacji celów.*

Snowden nie dał się zastraszyć i okazał to tak bezpośrednio, jak to tylko możliwe. Odwaga jest zaraźliwa. Wiedziałem, że skłoni wiele osób do działania.

W niedzielę o drugiej po południu czasu nowojorskiego „Guardian" opublikował materiał przedstawiający Snowdena światu: *Edward Snowden. Sygnalista, który ujawnił inwigilację przez NSA*. Nad artykułem znajdowało się dwunastominutowe wideo Laury. Pierwsze zdanie brzmiało: „Osobą odpowiedzialną za jeden z najważniejszych przecieków w politycznej historii USA jest Edward Snowden, dwudziestodziewięcioletni były technik CIA, obecnie zatrudniony w Booz Allen Hamilton, firmie pracującej na rzecz przemysłu obronnego". Artykuł omawiał życiorys Snowdena, przedstawiał jego motywy i dodawał, że „Snowden zapisze się w historii jako jeden z najważniejszych amerykańskich sygnalistów obok Daniela Ellsberga i Bradleya Manninga". Zacytowałem dawny list, który Snowden wysłał do Laury i do mnie: „Rozumiem, że zostanę ukarany za swoje działanie [...]. Będę zadowolony, jeśli choć na chwilę uda się odsłonić rządzącą światem federację tajnych praw, nierównego wybaczania i nieograniczonej władzy wykonawczej".

Reakcja na artykuł i wideo przerosła wszystko, czego kiedykolwiek doświadczyłem. Sam Ellsberg napisał następnego dnia w „Guardianie", że „w historii Ameryki nie było ważniejszego

przecieku niż ujawnienie materiałów NSA przez Edwarda Snowdena – a to zdecydowanie obejmuje także Pentagon Papers sprzed czterdziestu lat".

Tylko w ciągu pierwszych kilku dni kilkaset tysięcy osób wkleiło ten link w swoje konto na Facebooku. Niemal trzy miliony osób obejrzało wywiad na YouTube. Wiele innych obejrzało go w internetowym wydaniu „Guardiana". Powszechną reakcją był szok i podziw dla odwagi Snowdena.

Laura, Snowden i ja razem śledziliśmy odpowiedź na jego ujawnienie się; równocześnie rozważałem z dwoma strategami mediowymi z „Guardiana", w których programach telewizyjnych powinienem zgodzić się wystąpić. Ustaliliśmy, że pojawię się w *Morning Joe* w MSNBC, a następnie w *The Today Show* w NBC – dwóch najwcześniejszych. To powinno ukierunkować informacje o Snowdenie na cały dzień.

Zanim jednak zdołałem dotrzeć na te wywiady, o piątej rano – zaledwie parę godzin po publikacji artykułu – zadzwonił do mnie mój długoletni czytelnik mieszkający w Hongkongu, z którym w tym tygodniu od czasu do czasu się kontaktowałem. Podczas rozmowy wskazał, że wkrótce cały świat będzie szukać Snowdena w Hongkongu, i twierdził, że to niezwykle istotne, by Snowden miał w mieście prawników o dobrych kontaktach. Skontaktował się z dwoma najlepszymi w mieście prawnikami zajmującymi się prawami człowieka, którzy są gotowi go reprezentować. Czy mogą przyjść już teraz do mnie do hotelu?

Uzgodniliśmy, że spotkamy się nieco później, około ósmej rano. Położyłem się i zasnąłem, ale telefon obudził mnie o siódmej, godzinę przed ustaloną porą.

– Jesteśmy już tutaj, na dole, w pana hotelu – powiedział mój znajomy. – Są ze mną obaj prawnicy. Hol jest pełen fotografów i reporterów. Media szukają hotelu Snowdena i na pewno go zaraz znajdą, prawnicy zaś mówią, że koniecznie muszą się do niego dostać przed mediami.

Ledwo obudzony naciągnąłem na siebie pierwsze ubranie, jakie wpadło mi w ręce, i po omacku podszedłem do drzwi. Ledwo je otworzyłem, oślepiły mnie lampy błyskowe kilku aparatów fotograficznych. Media najwyraźniej zapłaciły komuś z personelu, by dostać numer mojego pokoju. Dwie kobiety przedstawiły się jako reporterki z hongkońskiego biura „Wall Street Journal"; pozostali, w tym człowiek z dużym aparatem fotograficznym, byli z Associated Press.

Zarzucili mnie pytaniami i otoczyli, tworząc wokół mnie przesuwający się krąg. Wepchnęli się za mną do windy, zadając jedno pytanie za drugim. Odpowiadałem krótkimi, niewiele wyjaśniającymi zdaniami.

Na dole w holu do grupy dołączyli kolejni reporterzy i fotograficy. Rozglądałem się za moim czytelnikiem i prawnikami, nie mogłem jednak zrobić nawet dwóch kroków, bo otoczono mnie ze wszystkich stron.

Obawiałem się, że cała gromada będzie za mną chodzić, co uniemożliwi prawnikom dotarcie do Snowdena. Uznałem w końcu, że najlepiej będzie zaimprowizować w holu konferencję prasową i odpowiedzieć na pytania reporterów w nadziei, że potem sobie pójdą. Po mniej więcej kwadransie większość z nich się rozproszyła.

Nagle z wielką ulgą dostrzegłem Gill Phillips, głównego radcę prawnego „Guardiana", która zatrzymała się w Hongkongu w drodze z Australii do Londynu, by zapewnić Ewenowi i mnie wsparcie prawne. Powiedziała mi, że spróbuje zbadać, jakie „Guardian" ma prawne możliwości, żeby chronić Snowdena.

– Alan zdecydowanie chce, byśmy okazali mu każdą pomoc, jaką tylko legalnie możemy – powiedziała.

Próbowaliśmy dalej rozmawiać, ale wokół kręciło się jeszcze kilku reporterów, więc brakowało nam prywatności.

W końcu znalazłem mego czytelnika z dwoma prawnikami. Zastanawialiśmy się, jak to zrobić, by móc swobodnie omówić

sprawy, i w końcu wszyscy poszliśmy do pokoju Gill. Zamknęliśmy drzwi przed nosem garstce reporterów, która wciąż próbowała nas śledzić.

Natychmiast przeszliśmy do konkretów. Prawnicy chcieli jak najszybciej porozumieć się ze Snowdenem, żeby otrzymać formalną zgodę na reprezentowanie go, bo dopiero wtedy będą mogli działać na jego rzecz.

Gill gorączkowo wydzwaniała do różnych osób, by sprawdzić ich obu – bo przecież ich nie znaliśmy – zanim powierzymy im Snowdena. Udało jej się potwierdzić, że rzeczywiście są znani i cieszą się dobrą opinią w środowisku obrońców praw człowieka i azylantów, a w Hongkongu mają przydatne polityczne koneksje. Podczas gdy Gill „z należytą starannością" improwizowała, ja zalogowałem się na czat. I Snowden, i Laura byli podłączeni.

Laura, która mieszkała teraz w hotelu Snowdena, nie wątpiła, że to tylko kwestia czasu, zanim reporterzy znajdą także i ich. Snowden chciał jak najszybciej opuścić swój pokój. Powiedziałem mu o prawnikach, którzy byli gotowi po niego pójść. Wyraził chęć, by zabrali go w jakieś bezpieczne miejsce. Nadszedł czas, powiedział, „rozpocząć tę część planu, w której proszę świat o ochronę i sprawiedliwość".

– Muszę jednak wydostać się z hotelu nierozpoznany przez reporterów – powiedział. – Inaczej pójdą za mną, gdziekolwiek się udam.

Przekazałem jego słowa prawnikom.

– Czy ma jakiś pomysł, jak temu zapobiec? – spytał jeden z nich.

Powtórzyłem Snowdenowi pytanie.

– Jestem w trakcie zmieniania swego wyglądu – wyjaśnił. Najwyraźniej myślał o tym już wcześniej. – Mogę zmienić się nie do poznania.

Uznałem, że nadszedł czas, by prawnicy rozmawiali z nim bezpośrednio. Przedtem jednak Snowden musiał wyrecytować

oficjalną formułkę, że ich zatrudnia, bo bez tego nie mogli go reprezentować. Wysłałem formułkę do Snowdena, on ją przepisał i odesłał. Wtedy prawnicy przejęli komputer i zaczęli rozmawiać z nim bezpośrednio.

Dziesięć minut później oznajmili, że udają się natychmiast do hotelu Snowdena, tam się z nim spotkają i postarają się go niezauważenie wyprowadzić.

– I co z nim później zrobicie? – spytałem.

Odparli, że prawdopodobnie zabiorą go do misji ONZ w Hongkongu i złożą formalny wniosek o ochronę przed rządem USA, uzasadniając, że Snowden jest uchodźcą i stara się o azyl. Albo – powiedzieli – spróbują zorganizować „bezpieczną kryjówkę".

Jak jednak pomóc prawnikom wydostać się z hotelu tak, by ich nie zauważono? Ustaliliśmy plan: wyjdę z pokoju razem z Gill i zejdę do holu, by odciągnąć reporterów, którzy wciąż czekali pod drzwiami, a zapewne pójdą za mną. Prawnicy odczekają wówczas parę minut i opuszczą hotel; miejmy nadzieję, że nikt ich nie będzie śledzić.

Podstęp się udał. Po półgodzinnej rozmowie z Gill w galerii handlowej przylegającej do naszego hotelu wróciłem do pokoju i, niespokojny, zadzwoniłem na telefon komórkowy jednego z prawników.

– Zdążył wyjść z pokoju, tuż zanim na całym piętrze zaroiło się od dziennikarzy – usłyszałem. – Umówiliśmy się u niego w hotelu – przed tym samym pokojem z aligatorem, w którym się pierwszy raz spotkaliśmy, jak się później dowiedziałem – a potem przeszliśmy kładką do sąsiedniej galerii handlowej i w końcu do samochodu. Jest teraz z nami.

Dokąd go zabierają?

– Lepiej nie rozmawiać przez telefon – odparł prawnik. – Na razie będzie bezpieczny.

Poczułem ulgę, że Snowden jest w dobrych rękach, wiedziałem jednak, że być może już nigdy się z nim nie spotkamy ani

nie porozmawiamy – w każdym razie nie jako z wolnym człowiekiem. Całkiem możliwe, że następnym razem zobaczymy go w telewizji, w pomarańczowym więziennym kombinezonie i w kajdankach, w amerykańskim sądzie, oskarżonego o szpiegostwo.

Gdy rozważałem, co zaszło, ktoś zapukał do moich drzwi. Był to dyrektor hotelu, który przyszedł powiedzieć, że nieustannie dzwoni telefon, a rozmówcy chcą połączyć się z moim pokojem (poinstruowałem recepcję, by blokowano wszystkie telefony do mnie). Ponadto hol jest pełen dziennikarzy, fotografów i operatorów, czekających, kiedy się pojawię.

– Jeśli pan sobie życzy – powiedział – możemy pomóc panu opuścić hotel tylną windą i wyjściem, gdzie nikt pana nie zobaczy. Gdyby pan się zgodził, to prawnik „Guardiana" zarezerwował panu pokój w innym hotelu pod innym nazwiskiem.

W języku dyrekcji hotelu oznaczało to najwyraźniej: „Chcemy, by pan się wyniósł, bo powoduje pan zamieszanie". Wiedziałem jednak, że to dobry pomysł, jeśli miałem pracować w pewnej prywatności; wciąż też miałem nadzieję na utrzymanie kontaktu ze Snowdenem. Spakowałem więc torby, wyszedłem za dyrektorem tylnym wyjściem, spotkałem się z Ewenem w czekającej już taksówce, a potem zameldowałem się w innym hotelu pod nazwiskiem prawnika „Guardiana".

Natychmiast zalogowałem się do internetu, mając nadzieję na kontakt ze Snowdenem. Pojawił się po kilku minutach.

– Nic mi nie jest – powiedział. – Jestem teraz w kryjówce, nie wiem jednak, ani jak jest bezpieczna, ani jak długo tu będę. Będę musiał przenosić się z miejsca na miejsce, a nie bardzo mogę tu polegać na dostępie do internetu, trudno więc przewidzieć, kiedy i jak często będę się łączył.

Ewidentnie nie chciał podawać żadnych szczegółów o miejscu swego pobytu, a ja nie chciałem ich znać. Miałem bardzo ograniczone możliwości, jeśli chodzi o pomoc w ukrywaniu go.

Był teraz człowiekiem najbardziej na świecie poszukiwanym przez najpotężniejszy na świecie rząd. Stany Zjednoczone zażądały już od władz Hongkongu, by go aresztowały i przekazały władzom amerykańskim.

Rozmawialiśmy krótko i mało konkretnie, obaj wyrażając nadzieję, że uda nam się zachować kontakt. Życzyłem mu bezpieczeństwa.

Gdy w końcu dotarłem do studia, by udzielić wywiadu w programach *Morning Joe* i *The Today Show,* natychmiast zauważyłem, że zmienił się ton zadawanych mi pytań. Zamiast rozmawiać ze mną jako z reporterem, prowadzący woleli atakować nowy cel: samego Snowdena, zagadkową postać kryjącą się w Hongkongu. Wielu amerykańskich dziennikarzy powróciło do zwykłej dla nich roli: służby rządowi. Ważne było już nie to, że dziennikarze ujawnili poważne nadużycia ze strony NSA, tylko że pracujący dla rządu Amerykanin „sprzeniewierzył się" swoim obowiązkom, popełnił przestępstwo, a następnie „uciekł do Chin".

Moje rozmowy z obiema prowadzącymi, Miką Brzezinski i Savannah Guthrie, były cierpkie i ostre. Po tygodniu spędzonym niemal bez snu brakowało mi cierpliwości do zawartej w ich pytaniach krytyki Snowdena: uważałem, że dziennikarze powinni chwalić, a nie demonizować kogoś, kto umożliwił największą od lat przejrzystość działań rządu.

Po jeszcze kilku dniach spędzonych na udzielaniu wywiadów uznałem, że pora opuścić Hongkong. Nie miałem już szans na spotkanie ze Snowdenem, nie byłem w stanie mu tam pomóc, czułem się natomiast wyczerpany fizycznie, emocjonalnie i psychicznie. Marzyłem o powrocie do Rio.

Zamierzałem lecieć do domu przez Nowy Jork i zatrzymać się tam na jeden dzień wywiadów – po prostu żeby pokazać, że mogę i chcę. Znajomy prawnik odwiódł mnie jednak od tego

pomysłu, tłumacząc, że nie ma sensu podejmować tego rodzaju ryzyka, póki nie wiemy, jak rząd zamierza reagować.

– Właśnie umożliwiłeś największy w historii USA przeciek dotyczący bezpieczeństwa narodowego i występowałeś we wszystkich telewizjach z wysoce wyzywającym przekazem – powiedział. – Planowanie wyjazdu do USA będzie miało sens dopiero wtedy, gdy będziemy mieć pojęcie o reakcji Departamentu Sprawiedliwości.

Byłem innego zdania. Uważałem, że to niemożliwe, by administracja Obamy aresztowała dziennikarza w trakcie tak znaczącej pracy reporterskiej. Czułem się jednak zbyt zmęczony, by spierać się lub podejmować ryzyko. Poprosiłem więc „Guardiana" o zarezerwowanie mi lotu do Rio przez Dubaj, bez zbliżania się do USA. Na razie, tłumaczyłem sobie, zrobiłem już dość.

ROZDZIAŁ 3

GROMADZIĆ WSZYSTKO

Archiwum dokumentów zgromadzone przez Edwarda Snowdena zdumiało mnie zarówno wielkością, jak i swoim zakresem. Choć od lat pisałem o niebezpieczeństwach wynikających z inwigilacji prowadzonej przez USA, ogrom szpiegowskiego systemu naprawdę mnie zaskoczył. Szczególnie w połączeniu z faktem, że był tworzony właściwie bez kontroli i ograniczeń.

Ci, którzy wdrażali tysiące opisanych w archiwum Snowdena dyskretnych programów inwigilacji, niewątpliwie nie chcieli, by dowiedziało się o nich amerykańskie społeczeństwo. Wiele z nich było wymierzonych wprost w Amerykanów. Ale celem masowej inwigilacji było również kilkadziesiąt państw, w tym kraje demokratyczne uważane za sojuszników USA, wśród nich Francja, Brazylia, Indie czy Niemcy.

Archiwum Snowdena było starannie uporządkowane. Jednak jego rozmiary i złożoność utrudniały pracę. Właściwie każda jednostka i wydział ogromnie rozległej struktury NSA, a w niektórych wypadkach także sprzymierzone z nią zagraniczne agencje wywiadowcze, produkowały dziesiątki tysięcy dokumentów. Zaskoczyło mnie również to, że niektóre dokumenty były bardzo świeże – większość pochodziła z 2011 i 2012 roku, wiele z 2013, a kilka wręcz z marca i kwietnia. Powstały więc zaledwie dwa miesiące przed naszym spotkaniem w Hongkongu.

Zdecydowaną większość dokumentów oznaczono jako „ściśle tajne". Przeważająca ich część nosiła adnotację „FVEY", mogły być więc udostępniane wyłącznie czterem najbliższym sojusznikom NSA z tak zwanego Sojuszu Pięciorga Oczu („Five Eyes": Stany Zjednoczone, Wielka Brytania, Kanada, Australia i Nowa Zelandia). Niektóre były jawne wyłącznie dla Amerykanów („NOFORN", co oznaczało „nie dla cudzoziemców"). Niektóre dokumenty z archiwum Snowdena, takie jak nakaz sądu nadzorującego działalność wywiadowczą (sąd FISA) zezwalający na pozyskiwanie zapisów rozmów telefonicznych oraz prezydencka dyrektywa Obamy o przygotowaniu ofensywnych cyberoperacji, należały do najściślej strzeżonych tajemnic rządu USA.

Rozszyfrowanie archiwum i stosowanych w nim pojęć ze specyficznego słownika NSA wymagało ode mnie intensywnej nauki. Język Agencji, stosowany w wewnętrznej komunikacji i w kontaktach z partnerami, okazał się z jednej strony biurokratyczny i sztywny, z drugiej bywał ironiczny i chełpliwy. Ale większość dokumentów została napisana językiem technicznym, napakowanym odstręczającymi akronimami i kryptonimami. Żeby je zrozumieć, trzeba było znać inne dokumenty Agencji.

Snowden przewidział ten problem. Dołączył glosariusze akronimów i nazw programów oraz słowniki terminologii stosowanej w Agencji. Ale i tak części dokumentów nie sposób było zrozumieć po pierwszym, drugim czy nawet trzecim czytaniu. Ich znaczenie wyłaniało się dopiero wtedy, gdy złożyłem je z fragmentami innych plików i skonsultowałem się z wybitnymi światowymi specjalistami od inwigilacji, kryptografii, hakerstwa, historii NSA i ram prawnych działań amerykańskiego wywiadu.

Dodatkową trudność stanowił fakt, że dokumenty ułożone były często nie według tematów, ale oddziałów Agencji, w których powstały. Do tego wymieszane były z mnóstwem

materiałów nieistotnych albo ściśle technicznych. Choć obmyślony przez „Guardiana" program pozwalający przeszukiwać pliki według kluczowych słów okazał się niezwykle przydatny, nie był on wystarczająco wszechstronny. Proces przyswajania archiwum okazał się mozolny i powolny. Ale w końcu to, co Snowden ujawnił, ułożyło się w obraz złożonej sieci inwigilacji, jej strategii i celów. Wśród nich byli Amerykanie (choć misja założycielska NSA zdecydowanie ich nie obejmowała) i nie-Amerykanie. Archiwum Snowdena ujawniało środki techniczne stosowane do inwigilacji: serwery internetowe, satelity, podwodne kable światłowodowe, krajowe i zagraniczne systemy telefoniczne, komputery osobiste. Wskazywało jednostki mające być celem szczególnie inwazyjnych form szpiegowania – od domniemanych terrorystów i przestępców po demokratycznie wybranych przywódców państw będących sojusznikami Ameryki, a nawet zwykłych amerykańskich obywateli. Rzucało światło na ogólne strategie i cele NSA.

Na czele listy Snowden umieścił dokumenty najbardziej istotne, mające najszerszy zakres. Ukazywały one, jak wielkiego terytorium dotyczy działalność Agencji. Ale także jej kłamstwa, a nawet działania niezgodne z prawem. Jednym z nich był program BOUNDLESS INFORMANT. Jego istnienie świadczyło o tym, że NSA z matematyczną dokładnością liczy wszystkie połączenia telefoniczne i e-maile wysyłane codziennie na całym świecie. Snowden umieścił dokumenty dotyczące tego programu na samym początku swojej listy nie tylko dlatego, że pokazywał on, ile rozmów i e-maili – dosłownie miliardy każdego dnia – gromadzi i przechowuje NSA. Także dlatego, że program stanowił dowód, iż szef NSA Keith Alexander i inni funkcjonariusze Agencji kłamali przed Kongresem, powtarzając, że nie są w stanie podać żadnych dokładnych liczb dotyczących ich działalności. A przecież BOUNDLESS INFORMANT służył gromadzeniu tych danych.

Jak pokazuje powyższy slajd na temat BOUNDLESS INFORMANT, w ciągu jednego miesiąca, poczynając od 8 marca 2013 roku, jedna jednostka NSA (Global Access Operations) zebrała dane na temat ponad trzech miliardów połączeń telefonicznych i e-maili, które przeszły przez amerykański system telekomunikacyjny. To więcej niż wszystkie dane zebrane z Rosji, Meksyku i niemal wszystkich państw europejskich i tyle mniej więcej, co zebrano z Chin.

W sumie w ciągu zaledwie trzydziestu dni jednostka ta zgromadziła dane dotyczące ponad 97 miliardów e-maili i 124 miliardów połączeń telefonicznych z całego świata.

Kolejny dokument na temat programu BOUNDLESS INFORMANT wyszczególniał dane zgromadzone w ciągu trzydziestu dni z Niemiec (500 milionów), Brazylii (2,3 miliarda) i Indii (13,5 miliarda). Inne pliki ukazywały gromadzenie metadanych we współpracy z rządami Francji (70 milionów), Hiszpanii (60 milionów), Włoch (47 milionów), Holandii (1,8 miliona), Norwegii (33 miliony) i Danii (23 miliony).

Mimo że zgodnie ze swoim statutem NSA skupia się na „wywiadzie zagranicznym", dokumenty potwierdzają, że równie ważnym obiektem tajnej inwigilacji jest dla Agencji społeczeństwo amerykańskie. Szczególnie jasno mówił o tym ściśle tajny nakaz wydany przez sąd FISA, zmuszający firmę telekomunikacyjną Verizon do przekazywania Agencji wszystkich informacji na temat połączeń telefonicznych jej klientów, a więc „telefonicznych metadanych". Nakaz, oznaczony jako „NOFORN", posługiwał się językiem jasnym i niepozostawiającym wątpliwości:

NINIEJSZYM NAKAZUJE SIĘ, by po doręczeniu niniejszego Nakazu Kurator Rejestrów wydał Agencji Bezpieczeństwa Narodowego (NSA), i o ile Sąd nie postanowi inaczej codziennie wydawał w sposób ciągły, przez okres obowiązywania niniejszego Nakazu, elektroniczne kopie następujących przedmiotów materialnych: szczegółowe rejestry połączeń, czyli „metadane telefoniczne" tworzone przez Verizon, a dotyczące połączeń między Stanami Zjednoczonymi a zagranicą, wewnątrz Stanów Zjednoczonych, w tym połączeń lokalnych.

Metadane telefoniczne obejmują kompleksowe informacje o routingu połączeń, w tym, choć nie wyłącznie, informacje identyfikujące połączenie (np. numer telefonu wywołującego i wywoływanego, numer IMSI [przypisany każdej karcie SIM – przyp. red.], numer IMEI [przypisany każdemu telefonowi komórkowemu – przyp. red.], miejsce, z którego dokonywane jest połączenie, numery kart telefonicznych oraz czas i długość trwania rozmowy).

Masowe gromadzenie danych telefonicznych przez USA to jedno z najbardziej znaczących odkryć w archiwum Snowdena. Ale pełne było ono informacji na temat wszelkiego typu tajnych programów inwigilacji. Od zakrojonego na wielką skalę PRISM (system ściągania danych z serwerów największych światowych firm internetowych) czy PROJECT BULLRUN (wspólnego przedsięwzięcia NSA i jej brytyjskiego odpowiednika GCHQ – Government Communications Headquarters, czyli Centrali Łączności Rządowej), mającego na celu łamanie najpopularniejszych form kodowania używanych dla zabezpieczenia transakcji online, aż po mniejsze przedsięwzięcia, których wiele mówiące nazwy odzwierciedlały ducha wyższości i pogardy: EGOTISTICAL GIRAFFE („egotystyczna żyrafa"), skupiony na sieci Tor zapewniającej użytkownikom anonimowość wyszukiwania online; MUSCULAR („umięśniony"), umożliwiający

wchodzenie w prywatne sieci Google'a i Yahoo!; czy OLYMPIA, kanadyjski program inwigilacji brazylijskiego Ministerstwa Górnictwa i Energetyki.

Większość programów inwigilacji rzekomo dotyczyła osób podejrzanych o terroryzm, jednak wielka ich część ewidentnie nie miała nic wspólnego z bezpieczeństwem narodowym. Dokumenty z archiwum Snowdena nie pozostawiają wątpliwości, że NSA angażowała się również w nie mniejszym stopniu w wywiad gospodarczy, szpiegowanie dyplomatów i przebiegającą niejawnie inwigilację całych grup ludności.

Patrząc na całość archiwum Snowdena, można było wysnuć jeden prosty wniosek: rząd USA zbudował system, którego celem jest całkowita, globalna eliminacja elektronicznej prywatności. Nie jest to bynajmniej przesada, ale dosłowny, jasno sformułowany cel inwigilującego państwa: gromadzenie, przechowywanie, monitorowanie i analizowanie wszystkich połączeń elektronicznych między ludźmi na całym świecie. NSA kieruje się przy tym jednym, nadrzędnym celem: nie dopuścić, by jakiekolwiek połączenia elektroniczne wymknęły się z jej systemu inwigilacji.

Ten cel osiąga się poprzez nieustanne rozszerzanie zasięgu NSA. Wykorzystując swoje pełnomocnictwa, Agencja bez przerwy stara się identyfikować połączenia elektroniczne, które nie były przez nią dotąd rejestrowane i magazynowane, a potem rozwija nowe technologie, by wypełnić lukę. Nie potrzebuje szczególnego uzasadnienia, by gromadzić pojedyncze połączenia elektroniczne, ani dowodów, że jej cele są o cokolwiek podejrzane. Misją NSA jest to, co sama Agencja nazywa „SIGINT" – zdobywanie danych wywiadowczych z wszelkich rodzajów sygnałów elektronicznych. A już sam fakt, że ma ona możliwość gromadzenia danych teleinformatycznych, sam w sobie staje się uzasadnieniem, by je gromadzić.

Podporządkowana Pentagonowi NSA jest największą agencją wywiadowczą na świecie. Do tego gros jej działalności podsłuchowej prowadzone jest w ramach międzynarodowego Sojuszu Pięciorga Oczu. Aż do wiosny 2014 roku, gdy zaogniła się debata na temat rewelacji Snowdena, na czele Agencji stał czterogwiazdkowy generał Keith B. Alexander, który kierował nią od 2005 roku. W tym czasie energicznie rozbudowywał on i rozszerzał wpływy NSA, stając się, jak napisał reporter James Bamford, „najpotężniejszym szefem wywiadu w historii Ameryki".

NSA „dysponowała już monstrualną ilością danych, gdy Alexander objął kierownictwo Agencji – zauważył dziennikarz «Foreign Policy» Shane Harris – ale pod jego nadzorem zasięg, skala jej działalności, a także ambicje poszły znacznie dalej niż najśmielsze wyobrażenia jego poprzedników". Nigdy przedtem „żadna agencja rządowa USA nie miała możliwości ani uprawnień, by gromadzić i przechowywać tak wielką liczbę informacji elektronicznych". Były urzędnik administracji, który pracował z szefem NSA, powiedział Harrisowi, że „strategia Alexandra" była jasna: „Potrzebuję wszystkich danych". Harris dodał: „I chce się tego trzymać, jak długo będzie mógł".

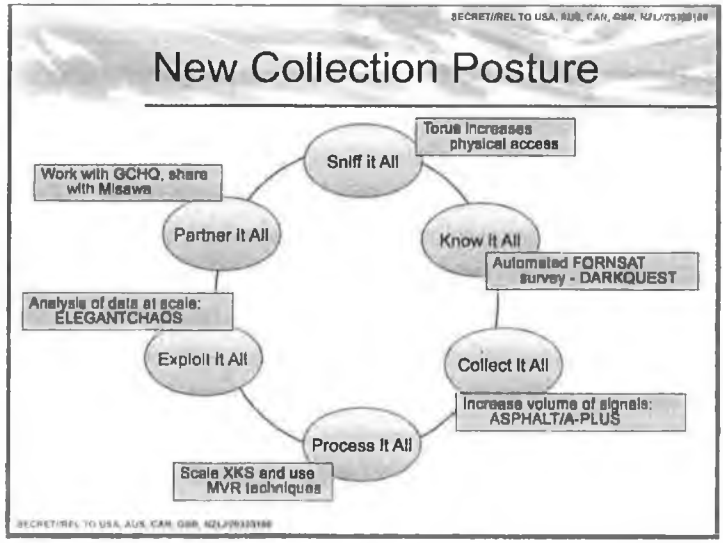
Osobiste motto Alexandra, „gromadzić wszystko", doskonale odzwierciedla główny cel NSA. Wymyślił to motto, zajmując się rozpoznaniem radioelektronicznym podczas okupacji Iraku. Jak napisał w 2013 roku „Washington Post", Alexander był niezadowolony z ograniczonego pola zainteresowań wywiadu wojskowego, który koncentrował się na podejrzanych bojownikach i innych bezpośrednich zagrożeniach dla wojsk amerykańskich. Uważał takie podejście za zbyt wąskie. „Chciał mieć wszystko: każdy iracki SMS, każdą rozmowę telefoniczną i każdy e-mail, jaki tylko dał się wessać w potężne komputery Agencji". W ten sposób rząd wykorzystał technologię do gromadzenia wszystkich danych o połączeniach całej irackiej ludności, bez wyjątków.

Po powrocie do USA w 2005 roku Alexander wymyślił, by ten sam system wszechobecnej inwigilacji, pierwotnie stworzony do kontrolowania ludności w strefie wojny, zastosować wobec obywateli amerykańskich. „I tak, jak to robił w Iraku, Alexander twardo naciskał, by dostać wszystko, co się da: narzędzia, środki i instrumenty prawne pozwalające mu ściągać i przechowywać ogromne ilości nieprzetworzonych informacji na temat amerykańskich i zagranicznych połączeń" – donosił „Washington Post". I tak „w ciągu ośmiu lat spędzonych u steru narodowej agencji zajmującej się inwigilacją elektroniczną Alexander, lat 61, po cichu rewolucjonizował zdolność rządu do gromadzenia informacji w imię bezpieczeństwa narodowego".

Opinia o Alexandrze jako o ekstremiście w dziedzinie inwigilacji jest dobrze udokumentowana. „Foreign Policy" nazwał go „kowbojem z NSA", opisując jego „nieograniczone, przebiegające na granicy prawa parcie do zbudowania największej na świecie machiny szpiegowskiej". Według magazynu nawet szefowi CIA i NSA za czasów Busha, generałowi Michaelowi Haydenowi – który sam wówczas nadzorował realizację nielegalnego programu podsłuchowego – często „robiło się niedobrze", kiedy musiał się konfrontować z poglądami Alexandra, który wyznawał zasadę „wszystkie chwyty dozwolone". Były funkcjonariusz wywiadu tak charakteryzował jego poglądy: „Nie przejmujmy się prawem. Skupiamy się jedynie na tym, jak zrobić to, co mamy do zrobienia". „Post" także zauważył: „Nawet jego obrońcy mówią, że jego agresja sprawia czasem, iż wykracza poza granice wyznaczone prawem".

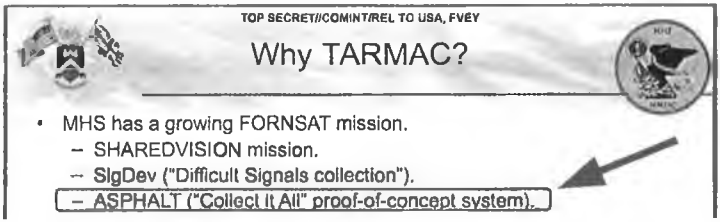
A mimo to część najbardziej ekstremalnych wypowiedzi Alexandra, tych, które znalazły potwierdzenie w materiałach ujawnionych przez Snowdena, rzecznicy Agencji zbywali, mówiąc, że to wyrwane z kontekstu żarty. Choćby ten, rzucony podczas wizyty w siedzibie brytyjskiego GCHQ w 2008 roku: „A dlaczego nie mielibyśmy bez przerwy gromadzić wszelkich

możliwych sygnałów?". Jednak dokumenty NSA wskazują, że Alexander bynajmniej nie żartował. Ściśle tajna prezentacja przygotowana na doroczną konferencję Sojuszu Pięciorga Oczu w 2011 roku świadczy o tym, że Agencja przyjęła motto Alexandra za swój główny cel.



Prezentacja (slajd powyżej) nosi tytuł *Nowa postawa wobec gromadzenia [danych]*, a kluczowymi hasłami w niej użytymi są: „wywąchaj wszystko (Sniff it All), wiedz wszystko (Know it All), gromadź wszystko (Collect it All), przetwarzaj wszystko (Process it All), wykorzystuj wszystko (Exploit it All), dziel się wszystkim z partnerami (Partner it All)".

Dokument przedstawiony rok wcześniej na konferencji Sojuszu Pięciorga Oczu przez GCHQ (slajd na stronie obok) i mówiący o wdrożonym już programie służącym do przechwytywania danych z satelity o kryptonimie TARMAC, jasno pokazuje, że brytyjska agencja szpiegowska również używa zwrotu „gromadzić wszystko" (Collect it All) , by opisać swoje cele.



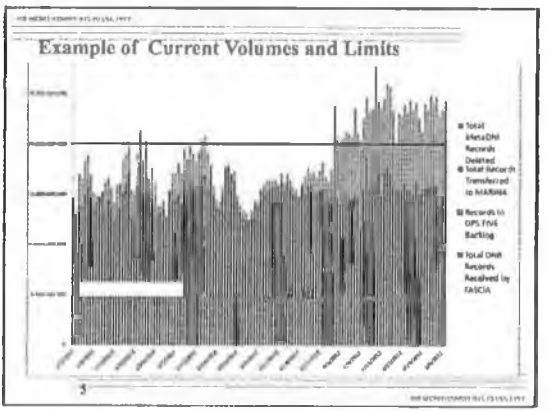
Nawet rutynowe, wewnętrzne memoranda NSA powołują się na ten zwrot, by usprawiedliwić rozszerzanie potencjału Agencji. Memorandum z 2009 roku od dyrektora technicznego zadań operacyjnych chwali niedawne usprawnienia wprowadzone w japońskiej bazie Misawa (Misawa Security Operation Center – MSOC), gdzie Agencja ma jedną z największych w swojej sieci stacji nasłuchowych i gdzie również przechowuje zgromadzone dane.

Techniczny dokument zatytułowany *Plany na przyszłość* mówi jasno:

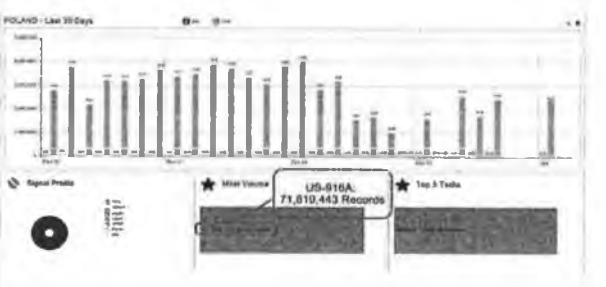
W przyszłości MSOC ma nadzieję zwiększyć liczbę platform WORD-GOPHER, by umożliwić odtwarzanie większej liczby sygnałów na niskich częstotliwościach. [...] Ponadto MSOC rozwinął zdolność automatycznego skanowania i odtwarzania sygnałów w chwili, gdy aktywują się na satelicie. Istnieje wiele możliwości zbliżających nas do celu naszego przedsięwzięcia: „gromadzenia wszystkiego".

Nie jest to bynajmniej dowcip – „gromadzić wszystko" określa aspiracje NSA i jest celem, do którego realizacji Agencja coraz bardziej się zbliża. Liczba połączeń telefonicznych, e-maili, czatów internetowych, innych czynności wykonywanych online oraz telefonicznych metadanych zebrana przez NSA wręcz oszałamia. Co więcej, Agencja często „gromadzi znacznie więcej treści, niż jest to rutynowo przydatne analitykom", jak stwierdzono w dokumencie z 2012 roku. W połowie tego samego roku *codziennie* przetwarzała ona ponad 20 miliardów połączeń (telefonicznych i internetowych) na całym świecie.

Pokazuje to poniższa prezentacja, zatytułowana *Przykład obecnej pojemności i limitów*. Liczba danych przechwyconych w ciągu miesiąca przez Global Access Operations. Skrót DNR (Dialed Number Recognition, czyli rozpoznanie numeru wybieranego) oznacza liczbę przechwytywanych rozmów telefonicznych; DNI (Digital Network Intelligence, czyli rozpoznanie w sieci cyfrowej) odnosi się do wiadomości przesyłanych przez internet, a więc e-maili.



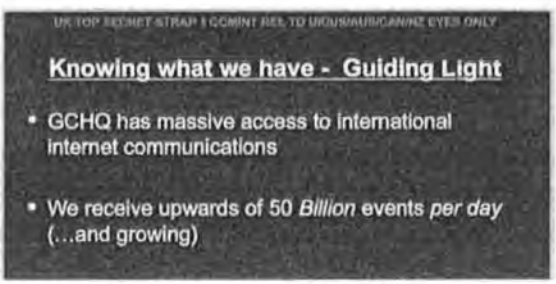
Kolejny slajd pokazuje, że dla każdego kraju z osobna NSA opracowuje codzienną analizę zebranych połączeń telefonicznych i e-maili. Wykres dotyczy Polski i pokazuje ponad 3 miliony połączeń telefonicznych zarejestrowanych w wybrane dni oraz sumę 71 milionów w ciągu miesiąca.



Równie zdumiewające są liczby dotyczące Stanów Zjednoczonych. Jeszcze przed rewelacjami Snowdena w 2010 roku „Washington Post" donosił, że „systemy gromadzenia danych w Agencji Bezpieczeństwa Narodowego dzień w dzień przechwytują i gromadzą 1,7 miliarda e-maili, połączeń telefonicznych i innego rodzaju komunikatów", które Amerykanie wymieniają między sobą. William Binney, matematyk, który pracował dla NSA przez trzydzieści lat, a zrezygnował po 11 września w proteście przeciwko działaniom Agencji, wielokrotnie wypowiadał się na temat ilości gromadzonych danych. W 2012 roku w programie *Democracy Now!* Binney powiedział, że „zgromadzili około 20 bilionów połączeń amerykańskich obywateli z innymi amerykańskimi obywatelami".

Po publikacji dokumentów ujawnionych przez Snowdena „Wall Street Journal" donosił, że system inwigilacji stworzony przez NSA „może kontrolować około 75 procent całego ruchu w amerykańskim internecie, w tym również dużą część połączeń cudzoziemców i Amerykanów". Wypowiadający się anonimowo dawni i obecni funkcjonariusze NSA powiedzieli gazecie, że w niektórych wypadkach Agencja „zachowuje treść e-maili wysyłanych między obywatelami w USA, a także filtruje krajowe połączenia telefoniczne dokonywane w technologii internetowej".

Również brytyjskie GCHQ gromadzi tak ogromne ilości danych komunikacyjnych, że ledwo może zmagazynować to, co już ma. Dokument przygotowany przez Brytyjczyków w 2011 roku omawia to planszą zatytułowaną: *Wiedząc, co mamy – światło przewodnie.*



NSA jest tak skupione na gromadzeniu wszystkiego, co się da, że po archiwum Snowdena rozsiane są wewnętrzne gratulacyjne memoranda mówiące o przekroczeniu kolejnych progów w tej dziedzinie – jak na przykład zapis z grudnia 2012, pochodzący z wewnętrznej tablicy informacyjnej Agencji, dotyczący programu SHELLTRUMPET.

21 grudnia 2012 SHELLTRUMPET przetworzył swój bilionowy zapis metadanych. SHELLTRUMPET rozpoczął pracę 8 grudnia 2007 jako działający w czasie niemal rzeczywistym analizator metadanych dla systemu gromadzenia CLASSIC. W ciągu pięciu lat jego istnienia także inne systemy Agencji zaczęły wykorzystywać możliwości SHELLTRUMPET [...]. Choć dojście do biliona zajęło pięć lat, niemal połowa z tego została przetworzona w tym roku kalendarzowym [...].

By zgromadzić tak wielką liczbę wiadomości, NSA posługuje się różnymi metodami. Obejmują one podłączanie się bezpośrednio do międzynarodowych kabli światłowodowych (także tych podmorskich) albo przekierowywanie połączeń do magazynów Agencji w trakcie ich przechodzenia przez amerykański system telekomunikacyjny (co dotyczy przeważającej części światowej łączności), albo współpracę ze służbami wywiadu różnych krajów. Coraz częściej jednak NSA opiera się także na firmach internetowych i telekomunikacyjnych, które przekazują jej informacje na temat swoich klientów.

Sama NSA jest oficjalnie agencją publiczną, jednak weszła w liczne partnerstwa z prywatnymi korporacjami i wiele swoich podstawowych funkcji zleca na zewnątrz. Sama NSA zatrudnia około 30 tysięcy osób, ale podpisuje dodatkowe kontrakty z 60 tysiącami pracowników, którzy świadczą jej usługi, choć są zatrudnieni przez prywatne firmy. Snowdena na przykład formalnie zatrudniał Dell Corporation oraz duża firma

przemysłu obronnego Booz Allen Hamilton. Jednak tak samo jak inni prywatni kontrahenci pracował on w NSA, jej biurach, przy jej podstawowych zadaniach, z dostępem do jej tajemnic.

Według Tima Shorrocka, który od dawna śledzi związki NSA z korporacjami, „70 procent naszego narodowego budżetu przeznaczonego na wywiad trafia do sektora prywatnego". Gdy Michael Hayden „powiedział, że największa koncentracja cyberwładzy na Ziemi znajduje się w stanie Maryland przy skrzyżowaniu Baltimore Parkway i drogi numer 32, [...] chodziło mu nie o samą NSA, której główna siedziba mieści się w wielkim czarnym gmachu w Fort Meade w Maryland, ale o odległy o jakąś milę *business park* – wyjaśnia Shorrock. – Tam właśnie wszyscy główni kontrahenci, od Booz, przez SAIC, po Northrop Grumman, prowadzą inwigilację i działania wywiadowcze dla Agencji".

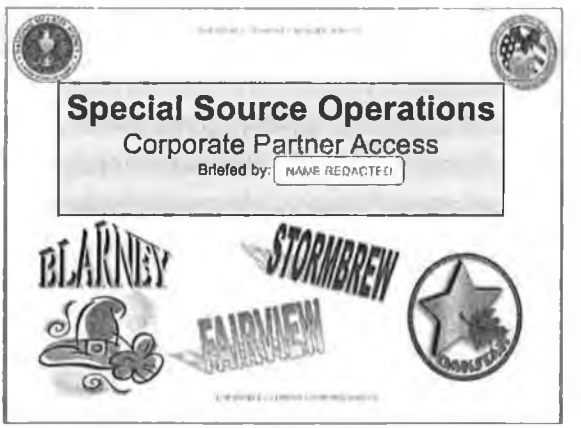
Związki NSA z korporacjami wykraczają poza kontrahentów zajmujących się wywiadem i obronnością. Obejmują także największe i najważniejsze światowe firmy internetowe i telekomunikacyjne, które przesyłają gros wiadomości na świecie. Co więcej, najistotniejszym elementem tego partnerstwa jest ułatwianie Agencji dostępu do prywatnych wiadomości.

Powyższy, ściśle tajny dokument zatytułowany *Strategiczne partnerstwa NSA* opisuje kluczowe cele defensywne i ofensywne owej współpracy, a więc „ochronę amerykańskich systemów

telekomunikacyjnych i komputerowych" oraz „przechwytywanie i wykorzystywanie sygnałów zagranicznych". Wylicza również niektóre usługi otrzymywane od tych firm. Są to między innymi: infrastruktura sieciowa, platformy hardware, desktopy/serwery, systemy operacyjne, oprogramowanie aplikacji, hardware i software zabezpieczeń.

Współpraca z korporacjami jest sterowana i nadzorowana przez należącą do Agencji ściśle tajną jednostkę SSO, czyli Centrum Operacyjne Źródeł Specjalnych. Snowden nazwał ją „klejnotem w koronie" całej organizacji.

BLARNEY, FAIRVIEW, OAKSTAR i STORMBREW to niektóre z programów nadzorowanych przez SSO i wymienionych na slajdzie z prezentacji zatytułowanej *Corporate Partner Access* (CPA, dostęp partnerów korporacyjnych).



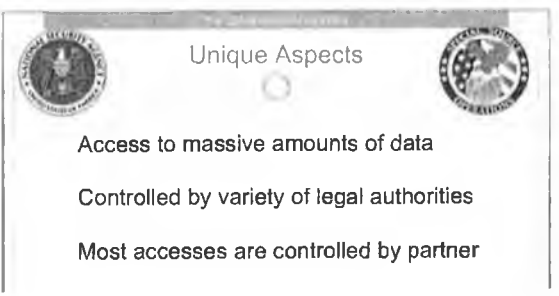
W ramach tych programów niektóre amerykańskie firmy telekomunikacyjne, które dzięki umowom z zagranicznymi firmami telekomunikacyjnymi mają dostęp do sieci międzynarodowych, wykorzystują ten dostęp do przekierowywania danych komunikacyjnych danego kraju do zasobów NSA.

Zasadniczy cel programu BLARNEY opisano w jednej z notatek Agencji. Jest ona zatytułowana *Relacje i władze* i mówi, by

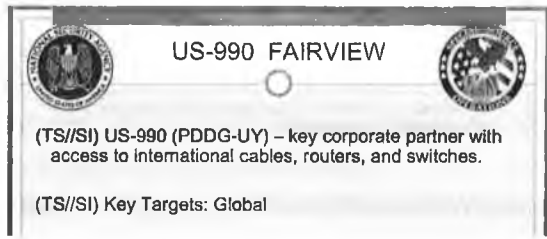
„wykorzystać kluczowe relacje z korporacjami dla uzyskania dostępu do międzynarodowych kabli światłowodowych, switchów i/lub routerów o wysokiej przepustowości na całym świecie".

Zdaniem „Wall Street Journal" projekt BLARNEY opierał się szczególnie na relacji z firmą AT&T Inc. Według danych NSA w 2010 roku lista państw, które stały się celem BLARNEY, obejmowała Brazylię, Francję, Niemcy, Grecję, Izrael, Włochy, Japonię, Meksyk, Koreę Południową i Wenezuelę, jak również Unię Europejską i Organizację Narodów Zjednoczonych.

Z kolei FAIRVIEW – jak zachwala sama NSA – gromadzi „potężne ilości danych" z całego świata. Także i ten program opiera się głównie na współpracy z jednym „partnerem korporacyjnym", a szczególnie jego dostępie do systemów telekomunikacyjnych innych państw. Wewnętrzne podsumowanie „wyjątkowych aspektów" programu FAIRVIEW jest proste i jasne: daje on dostęp „do ogromnej ilości danych", które „pozostają pod kontrolą różnych władz", a partner kontroluje dostęp do większości z nich.



Jak mówi kolejny slajd, w programie FAIRVIEW kluczowy jest jeden, niewymieniony z nazwy partner korporacyjny „z dostępem do międzynarodowych kabli, routerów i switchów", który dostarcza około 75 procent danych.
Cel programu jest prosty: „Główne obiekty: globalne".

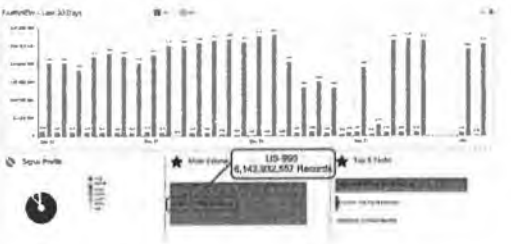


Według dokumentów NSA FAIRVIEW „jest w pierwszej piątce [programów] NSA będących źródłem danych dla serializowanej produkcji" – czyli trwającej inwigilacji – „i jednym z największych dostawców metadanych".

O gotowości do współpracy owego niewymienionego z nazwy partnera FAIRVIEW mówi ten dokument:

Partner korporacyjny od 1985 roku z dostępem do międzynarodowych kabli, routerów, switchów. Partner działa w USA, ale ma dostęp do informacji przekazywanych przez terytorium kraju, a dzięki powiązaniom korporacyjnym zapewnia wyjątkowy dostęp do sieci innych firm telekomunikacyjnych. Mocno zaangażowany w kierowanie ruchem interesujących nas sygnałów tak, by przechodziły przez nasze systemy monitorujące.

Sam program FAIRVIEW dostarcza ogromną ilość informacji na temat połączeń telefonicznych. Dowodzi tego wykres dotyczący trzydziestu dni, poczynając od 10 grudnia 2012 roku. W tym czasie dzięki FAIRVIEW gromadzono 200 milionów zapisów dziennie. Jak pokazuje slajd na sąsiedniej stronie, w ciągu 30 dni dało to dane dotyczące ponad 6 miliardów połączeń.



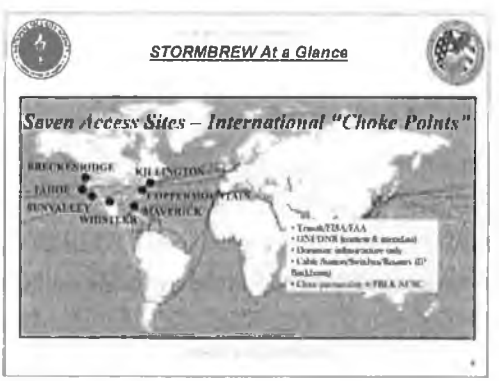
By zgromadzić te miliardy rejestrów, SSO współpracuje z partnerami korporacyjnymi oraz agencjami wywiadowczymi obcych rządów – na przykład z polską Służbą Wywiadu Wojskowego. Mówi o tym poniższy dokument:

ORANGECRUSH, część programu OAKSTAR w ramach SSO, zaczął przekazywać metadane od partnera ze Strony Trzeciej (Polska) do zasobów NSA od 3 marca, a treści od 25 marca. Program ten jest wspólnym projektem SSO, NCSC, ETC, FAD [komórki NSA – przyp. red.], korporacyjnego partnera NSA oraz agendy rządu polskiego. Polacy znają ORANGECRUSH jedynie jako BUFFALOGREEN. To wielostronne partnerstwo zaczęło funkcjonować w maju 2009 i przejęło prowadzony przez OAKSTAR projekt ORANGEBLOSSOM i jego potencjał [pozyskiwania danych na temat] DNR (dane o połączeniach telefonicznych). Dzięki nowemu dostępowi będą pozyskiwane SIGINT [Signals Intelligence – dane wywiadowcze pozyskiwane ze źródeł elektronicznych – przyp. red.] z połączeń komercyjnych prowadzonych przez partnera korporacyjnego NSA. Przewiduje się, że staną się również dostępne połączenia Narodowej Armii Afganistanu, z Bliskiego Wschodu, części kontynentu afrykańskiego i Europy.

Podobnie program OAKSTAR wykorzystuje dostęp jednego z korporacyjnych partnerów Agencji (o kryptonimie STEELKNIGHT) do zagranicznych systemów telekomunikacyjnych,

by przekierowywać dane do własnych zasobów. Inny partner, używany do działań w Ameryce Łacińskiej (kryptonim SILVERZEPHYR), pojawia się w dokumencie z 11 listopada 2009 roku opisującym współpracę, której celem było pozyskiwanie „połączeń wewnętrznych" z Brazylii i Kolumbii. Dowiadujemy się z niego, że „system [został] zainstalowany w miejscu działania partnera" i że partner „przekazał liczne próbne pliki [...], co dowiodło sprawności działania systemu. SSO będzie nadal monitorować przepływ i gromadzenie [danych], by zidentyfikować i usunąć wszelkie problemy".

I w końcu STORMBREW, program prowadzony „w bliskiej współpracy z FBI". Przekierowuje on połączenia internetowe i telefoniczne, które wchodzą do kraju przez „przewężenia" na terenie USA. Program wykorzystuje fakt, że ogromna większość światowego ruchu w internecie odbywa się za pośrednictwem amerykańskiej infrastruktury łączności, co jest efektem ubocznym kluczowej roli USA w budowaniu globalnej sieci. Gdzie znajdują się owe „przewężenia"? Można je zobaczyć na poniższym slajdzie. Jest w nich m.in. mowa o „siedmiu miejscach dostępu – międzynarodowych <<korkach>>" i „bliskiej współpracy z FBI i NCSC [National Computer Security Center, Narodowe Centrum Bezpieczeństwa Komputerowego będące częścią NSA – przyp. red.]".



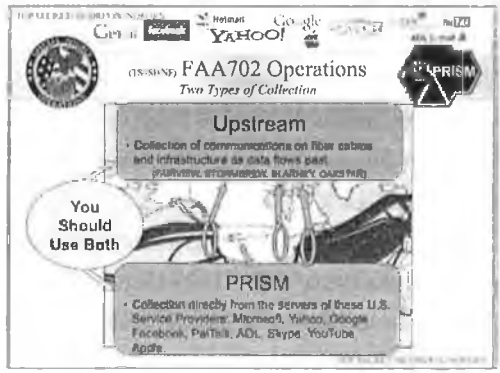
Według NSA dla STORMBREW kluczowe są „relacje z dwoma amerykańskimi dostawcami usług telekomunikacyjnych (kryptonimy ARTIFICE i WOLFPOINT)". Poza zapewnianym przez nie dostępem do przewężeń na terenie USA „program STORMBREW nadzoruje również dwa miejsca dostępu do kabli podmorskich, jedno na zachodnim wybrzeżu (kryptonim BRECKENRIDGE), drugie na wschodnim wybrzeżu USA (kryptonim QUAILCREEK)".

Obfitość kryptonimów wskazuje, że tożsamość partnerów korporacyjnych to jedna z najpilniej strzeżonych tajemnic NSA. Dokument zawierający klucz do tych kryptonimów jest ściśle tajny i Snowdenowi nie udało się rozszyfrować wielu z nich. Niemniej jednak jego odkrycia pozwoliły ujawnić niektóre firmy współpracujące z NSA. Najbardziej znany jest dokument dotyczący PRISM, którego treścią są tajne porozumienie między NSA a największymi światowymi operatorami internetowymi – Facebookiem, Yahoo!, Apple'em, Google'em. Dotyczy on także szerokiej współpracy ze strony Microsoftu, która zapewnia Agencji dostęp do jego platform komunikacyjnych takich jak Outlook.

Inaczej niż programy BLARNEY, FAIRVIEW, OAKSTAR i STORMBREW, które działają dzięki podłączeniu do kabli światłowodowych i innych form infrastruktury telekomunikacyjnej (w żargonie NSA – inwigilacja „pod prąd"), PRISM pozwala NSA na pozyskiwanie danych wprost z serwerów dziewięciu największych firm internetowych.

Dokument opatrzony logo internetowych gigantów rozróżnia „dwa rodzaje gromadzenia" metadanych: „Pod prąd", czyli „pozyskiwanie wiadomości z kabli światłowodowych i infrastruktury w chwili przepływu danych (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)", oraz „PRISM", czyli „gromadzenie bezpośrednio z serwerów tych amerykańskich dostawców internetowych: Microsoft, Yahoo!, Google,

Facebook, PalTalk, AOL, Skype, YouTube, Apple". Zalecenie jest jasne: „Należy używać obydwu metod".



Firmy wymienione na slajdzie PRISM zaprzeczyły, jakoby dały NSA dostęp do swoich serwerów. Facebook i Google twierdziły na przykład, że przesyłają tylko informacje, które Agencja wymusiła nakazem sądowym. Starały się też przedstawić PRISM jako banalny w gruncie rzeczy, techniczny detal – nieco ulepszony system przesyłu danych, które trafiają do specjalnej, dostępnej Agencji „skrytki".

Ich twierdzeniu kłam zadaje kilka rzeczy. Przede wszystkim Yahoo! energicznie walczyło w sądzie z podejmowanymi przez NSA próbami zmuszenia go do przyłączenia do PRISM. Zapewne nie robiłoby tego, gdyby program był banalną zmianą w systemie przesyłu danych (protest Yahoo! został odrzucony przez sąd FISA, a firmie nakazano uczestnictwo w PRISM). Po drugie, Bart Gellman z „Washington Post", ostro skrytykowany za „przesadę" w ocenie znaczenia PRISM, przeprowadził ponowne dochodzenie w sprawie programu i potwierdził główną tezę swoich tekstów: „Pracownicy rządu mający dostęp do PRISM mogli ze swego miejsca pracy w dowolnym punkcie na świecie «zadać pytanie» systemowi [czyli przeprowadzić wyszukiwanie – przyp. red.] i otrzymać dane od firmy internetowej bez kontaktu z personelem tej firmy".

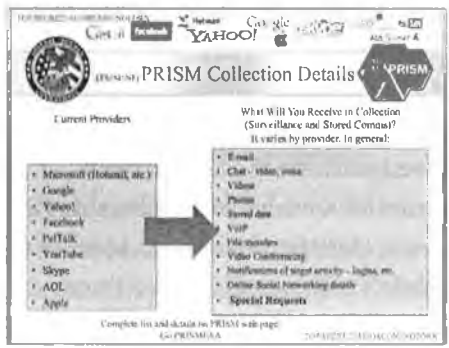
Po trzecie, zaprzeczenia firm internetowych, sformułowane wymijająco i legalistycznie, często więcej zaciemniały, niż wyjaśniały. Jak powiedział „Foreign Policy" Chris Soghoian, ekspert ACLU [American Civil Liberties Union – organizacja broniąca konstytucyjnych praw obywateli USA], Facebook, który twierdził, że nie zapewnia NSA „bezpośredniego dostępu" do danych, i Google, który zaprzeczył, jakoby utworzył „tajemne wejście" dla NSA, używały wysoce technicznych sformułowań, oznaczających bardzo konkretne sposoby pozyskania informacji. Firmy te nie zaprzeczyły jednoznacznie, że współpracowały z NSA przy instalacji systemu, dzięki któremu Agencja mogła bezpośrednio dotrzeć do ich danych.

I w końcu sama NSA wielokrotnie chwaliła PRISM za wyjątkowe możliwości pozyskiwania danych, którymi nie dysponują inne rozwiązania, i wskazywała, że program w istotny sposób zwiększa możliwość inwigilacji przez Agencję. Poniższy slajd Agencji pokazuje możliwości inwigilacji dzięki PRISM.

Zatytułowany jest *Dlaczego używać obu: PRISM kontra Pod prąd* i wymienia możliwości obu rozwiązań, takie jak gromadzenie danych DNI [internetowych], DNR [telefonicznych], dostęp do przechowywanych wiadomości, pobieranie danych w czasie rzeczywistym, w tym wiadomości głosowych,

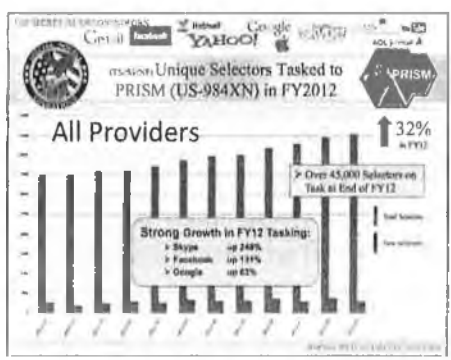
wreszcie bezpośredni kontakt z dostawcami wiadomości. W przypadku PRISM podkreśla się, że koncentruje się on na „dziewięciu dostawcach usług internetowych z siedzibami w USA", a „Pod prąd" opiera się na źródłach rozsianych po całym świecie.

Kolejny slajd pokazuje szeroki zakres wiadomości, do jakich NSA może dotrzeć dzięki PRISM.



Wynika z niego, że Agencja pozyskuje od Microsoftu, Google'a, Yahoo! czy Facebooka e-maile, czaty wideo i głosowe, zdjęcia, przesyłane pliki, wideokonferencje, powiadomienia o aktywności obiektów, takie jak loginy czy detale z internetowych serwisów społecznościowych.

Rozliczne slajdy NSA pokazują, w jak dużym stopniu PRISM zwiększył ilość danych gromadzonych przez Agencję.



Oddział Centrum Operacyjnego Źródeł Specjalnych (SSO) często chwalił się w wewnętrznych informacjach wartością informacji dostarczanych przez PRISM. Wiadomość z 19 listopada 2012 roku zatytułowana jest *PRISM rozszerza wpływy: dane za rok finansowy 2012*, i informuje, że program „jest najczęściej cytowanym źródłem danych NSA w raportach końcowych Strony Pierwszej. Więcej raportów NSA opartych było na PRISM niż na jakimkolwiek innym SIGAD [źródle danych wywiadowczych – przyp. red.]. PRISM cytowano w 13,4 procentach wszystkich raportów NSA dla Strony Pierwszej, Drugiej i Trzeciej (wzrost od 11,9 procent w stosunku do roku 2011). Liczba opartych na PRISM raportów końcowych w roku finansowym 2012 to 24 096, co oznacza wzrost o 27 procent w stosunku do poprzedniego roku finansowego".

Dokument podkreśla też, że „liczba raportów opartych na danych zgromadzonych przez PRISM i cytowanych jako źródła w Codziennych Biuletynach dla Prezydenta w roku finansowym 2012 wyniosła 1477 (to 18 procent wszystkich raportów opartych na cyfrowych danych wywiadowczych (SIGINT) cytowanych jako źródła w artykułach, które znalazły się w Codziennych Biuletynach dla Prezydenta). W roku finansowym 2011 było to odpowiednio 1152 (15 procent raportów)". Autorzy dokumentu chwalą się też „wielkim sukcesem w pozyskiwaniu i przetwarzaniu [danych] ze Skype'a: osiągnięto wyjątkowe i wartościowe cele".

Takie gratulacje nie potwierdzają tezy, że PRISM to tylko trywialne rozwiązanie techniczne, i zadają kłam zaprzeczeniom firm z Doliny Krzemowej w sprawie ich współpracy z NSA. „New York Times", który zajął się programem PRISM po ujawnieniu go przez Snowdena, opisał całe mnóstwo tajnych negocjacji między NSA a Doliną Krzemową na temat zapewnienia Agencji niczym nieskrępowanego dostępu do systemów koncernów informatycznych: „Firmy najeżyły się, gdy urzędnicy

rządowi pojawili się w Dolinie Krzemowej z żądaniem ułatwienia im dostępu do danych o ich użytkownikach w ramach tajnego programu inwigilacji [...], w końcu jednak wiele z nich zaczęło przynajmniej odrobinę współpracować".

Przykład? „Twitter odmówił ułatwień dla rządu. Według osób, które mają dostęp do informacji o negocjacjach [między NSA a firmami z Doliny Krzemowej – przyp. red.], inni okazali się jednak bardziej ulegli. Rozpoczęto rozmowy z funkcjonariuszami NSA na temat opracowania technik pozwalających wydajniej i bezpieczniej dzielić się osobistymi danymi zagranicznych użytkowników w odpowiedzi na zgodne z prawem żądania rządu. W kilku przypadkach zmieniono nawet komputery, by stało się to możliwe".

Negocjacje te, zdaniem „New York Timesa", „pokazują, jak ściśle firmy internetowe współpracują z rządem oraz jak daleko sięgają ich zakulisowe transakcje". Artykuł podważał także twierdzenie firm, że umożliwiają NSA dostęp, tylko jeśli są do tego zmuszone prawem. Wskazał bowiem, że „o ile udostępnienie danych w odpowiedzi na usankcjonowane prawnie żądania sądu FISA jest ich obowiązkiem, to już ułatwienie rządowi otrzymywania informacji takim obowiązkiem nie jest; dlatego Twitter mógł odmówić podobnych działań".

Niezbyt przekonujące jest również twierdzenie firm internetowych, że przekazują NSA jedynie te informacje, których Agencja żąda zgodnie z prawem. NSA musi bowiem pozyskiwać indywidualne nakazy w odniesieniu do konkretnych amerykańskich podmiotów. Nie musi za to mieć żadnych specjalnych zezwoleń, by otrzymywać dane o połączeniach jakichkolwiek nie-Amerykanów na terenie obcego państwa, *nawet jeśli porozumiewają się z Amerykanami.* Żadnej kontroli ani ograniczeniom nie podlega także masowe gromadzenie przez Agencję metadanych, a to dzięki rządowej interpretacji Patriot Act – tak szerokiej, że nawet twórców tej ustawy przeraził sposób, w jaki jest stosowana.

Bliska współpraca między NSA a prywatnymi korporacjami szczególnie wyraźnie rysuje się w dokumentach odnoszących się do Microsoftu. Odsłaniają one energiczne starania firmy, by umożliwić Agencji dostęp do kilku jej najpopularniejszych serwisów, w tym SkyDrive, Skype i Outlook.com.

SkyDrive, wirtualny dysk pozwalający ludziom przechowywać swoje pliki online i mieć do nich dostęp z różnych urządzeń, ma na całym świecie ponad 250 milionów użytkowników. „Wierzymy, że to ważne, byście mieli kontrolę nad tym, kto może, a kto nie może mieć dostępu do waszych osobistych danych w chmurze" – głosi SkyDrive. Jednak, jak podaje dokument NSA, Microsoft przez „wiele miesięcy" pracował nad zapewnieniem rządowi łatwiejszego dostępu do umieszczanych na nim danych. Mówi o tym dokument z 8 marca 2013 roku.

Poczynając od 7 marca 2013, PRISM gromadzi dane SkyDrive Microsoftu w ramach pakietu Standardowo Przechowywanych Zbiorów Wiadomości [...]. Oznacza to, że analitycy nie będą już musieli składać osobnych podań do SSO – to postęp, o którym wielu analityków być może nie wie. Ta nowa możliwość pozwoli znacznie pełniej i szybciej odpowiadać na zapotrzebowanie na dane ze strony SSO, jeśli chodzi o naszych niezależnych klientów. Ten sukces to rezultat wielomiesięcznej współpracy FBI z Microsoftem nad ustanowieniem tego typu rozwiązania.

Pod koniec 2011 roku Microsoft kupił Skype'a, internetowy serwis telefoniczny i czatowy. Korzysta z niego ponad 663 miliony zarejestrowanych użytkowników. W chwili zakupu Microsoft zapewniał użytkowników, że „Skype szanuje twoją prywatność i poufność twoich danych osobowych, połączeń i przekazywanych treści". W rzeczywistości jednak także i te dane wkrótce stały się dostępne dla rządu. Na początku

2013 roku w systemie NSA pojawiły się liczne wpisy chwalące usprawniony dostęp do połączeń użytkowników Skype'a.

Jeden z dokumentów opisany jako *Nowe możliwości dostępu PRISM do wiadomości przechowywanych na Skypie* wyjaśnia, że „PRISM ma teraz nową możliwość gromadzenia: wiadomości przechowywane na Skypie". Dalej podkreśla:

Wiadomości przechowywane na Skypie zawierają unikalne dane niegromadzone w normalnym procesie podsłuchiwania w czasie rzeczywistym: listy znajomych, informacje o kartach kredytowych, rejestry połączeń, informacje profilowe i inne materiały [...]. Dane gromadzone ze Skype'a dzięki PRISM w niecałe dwa lata stworzyły istotną niszę w sprawach prowadzonych przez NSA, tak ważnych jak terroryzm czy opozycja i reżim w Syrii. Od kwietnia 2011 roku na podstawie danych PRISM pochodzących ze Skype'a stworzono ponad 2000 raportów, w 76 procentach z nich dane ze Skype'a były jedynym źródłem".

W innym dokumencie NSA podkreśla: „SSO rozszerzyło dostęp PRISM do Skype'a". Jego autorzy wyjaśniają, że od 15 marca 2013 program ma dostęp do większej liczby wybranych celów:

Do tej pory PRISM nie pobierało żadnych danych ze Skype'a, jeśli użytkownik nie logował się przy pomocy nazwy użytkownika. Prowadziło to do luk w zbiorach danych. Obecne działania mają temu zapobiec. Co więcej, użytkownik Skype'a może utworzyć konto, używając dowolnego adresu e-mailowego zarejestrowanego w dowolnej domenie na świecie. UTT [Unified Target Tool – program używany przez NSA do namierzania celów inwigilacji – przyp. red.] obecnie nie pozwala analitykom namierzać tych nienależących do Microsoftu adresów, jednak SSO zamierza naprawić to jeszcze tego lata. Nie czekając na to, w ciągu ostatnich

sześciu miesięcy NSA, FBI i Departament Sprawiedliwości koordynowały działania, których celem było uzyskanie zezwoleń, by PRINTAURA [stosowany przez NSA zautomatyzowany system selekcji danych – przyp. red.], wysyłał selektory wszystkich obecnych i przyszłych celów PRISM do Microsoftu i Skype'a. W efekcie wysłano do Skype'a selektory około 980 celów i udało się pobrać dane, które w innej sytuacji by umknęły.

Współpraca z NSA była nie tylko całkowicie niejawna, ale w dodatku była sprzeczna z publicznymi oświadczeniami Skype'a. Chris Soghoian z ACLU powiedział, że ujawnienie szczegółów tej współpracy zaskoczy wielu klientów Skype'a. „W przeszłości Skype zobowiązywał się wobec użytkowników, że nie będzie pracować nad możliwością nagrywania ich rozmów – powiedział. – Trudno pogodzić tajną współpracę Microsoftu z NSA z jego publicznymi deklaracjami o konkurowaniu z Google'em pod względem ochrony prywatności".

W 2012 roku Microsoft udoskonalił Outlook, swój portal poczty elektronicznej, łącząc wszystkie usługi – w tym szeroko używany Hotmail.com – w jeden program. Firma zachwalała nowy Outlook, obiecując wysoki poziom szyfrowania w celu ochrony prywatności. NSA zaniepokoiła się, czy szyfrowanie, które Microsoft oferuje klientom Outlooka, nie zablokuje dostępu do ich połączeń. Notatka służbowa SSO z 22 sierpnia 2012 roku mówi o obawach, że „korzystanie z tego portalu oznacza, iż wychodzące z niego e-maile będą standardowo szyfrowane" i że „szyfrowane są także czaty prowadzone wewnątrz portalu, jeżeli obaj rozmówcy używają szyfrowanego przez Microsoft połączenia".

Niepokój nie trwał długo. Problem rozwiązano, wspólnie opracowując metody, dzięki którym NSA może obchodzić system szyfrowania, który Microsoft reklamował jako istotny dla ochrony prywatności.

Według dokumentu nazwanego *Microsoft udostępnia nową usługę* z 2012 roku

31 lipca wraz z wprowadzeniem nowego serwisu Outlook.com Microsoft (MS) zaczął szyfrować czaty internetowe. To nowe szyfrowanie oparte na protokole Secure Socket Layer (SSL) skutecznie odcięło Wspólnocie Wywiadów dostęp do nowej usługi dla FAA 702 i prawdopodobnie 12333 (w pewnym stopniu). MS, pracując z FBI, dostosował jednak narzędzia inwigilacji do nowego SSL. Rozwiązania przeszły udane testy i zostały wprowadzone 12 grudnia 2012". W konsekwencji *„wprowadzonych usprawnień CES odnotował wzrost liczby rejestrowanych danych.*

Inny dokument opisuje współpracę między FBI a Microsoftem, której celem było umożliwienie Biuru obchodzenie nowych zabezpieczeń Outlooka w celu umożliwienia inwigilacji:

Zespół Jednostki Technologii Przechwytywania Danych (Data Intercept Technology Unit, DITU) FBI pracuje z Microsoftem nad analizą dodatkowej funkcjonalności Outlook.com, umożliwiającej użytkownikom tworzenie pseudonimów w poczcie elektronicznej, co może wpłynąć na proces realizacji naszych zadań.

Autor prezentacji podkreśla, że prowadzone są działania mające na celu zaradzenie temu problemowi.

Wzmianka o inwigilacji prowadzonej przez FBI w dostarczonym przez Snowdena archiwum dokumentów NSA nie odnosi się do pojedynczego zdarzenia. Cała Wspólnota Wywiadów może korzystać z gromadzonych przez NSA danych. Rutynowo są one udostępniane innym agencjom, w tym CIA i FBI. Jednym z głównych celów masowego gromadzenia metadanych przez NSA było właśnie przyspieszenie procesu przekazywania ich

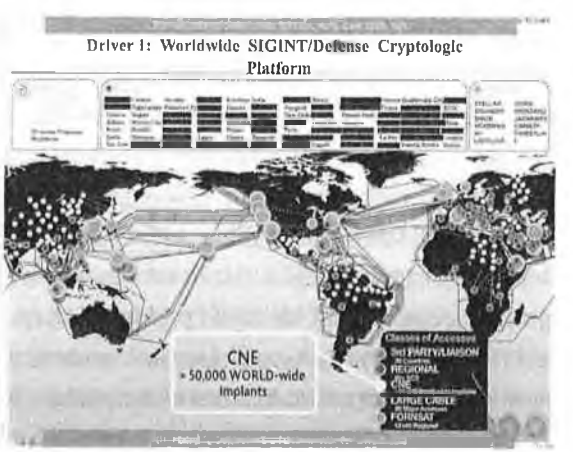
pozostałym agencjom rządowym. W niemal wszystkich dokumentach odnoszących się do różnych programów pozyskiwania danych wspomina się o włączeniu do nich innych jednostek wywiadowczych. Jeden z dokumentów SSO na temat dzielenia się danymi z PRISM deklaruje, że „PRISM to gra zespołowa!". Dokument zatytułowany został *Rozszerzenie dostępu danych z PRISM dla FBI i CIA.*

Sekcja Operacyjna Źródeł Specjalnych (SSO) rozszerzyła ostatnio dostęp do danych pozyskiwanych przez PRISM dla Federalnego Biura Śledczego (FBI) i Centralnej Agencji Wywiadowczej (CIA). Dzięki temu SSO stworzyło wspólną dla całej Wspólnoty Wywiadów możliwość dzielenia się i współpracy przy operacjach PRISM. Najpierw zespół PRINTAURA z SSO rozwiązał problem Dyrektoriatu Przekazów Wywiadowczych [Signals Intelligence Directorate, SID; odpowiada w NSA za odbiór i przetwarzanie danych od sojuszniczych agencji wywiadowczych – przyp. red.], tworząc oprogramowanie, które automatycznie co dwa tygodnie tworzy listę celów wytypowanych dla PRISM i przekazuje FBI i CIA. Dzięki temu nasi partnerzy mają możliwość sprawdzić, jakie cele NSA są monitorowane przez PRISM. FBI i CIA mogą wówczas zwrócić się o kopię danych pozyskanych przez PRISM dotyczących dowolnego celu, na co zezwala Foreign Intelligence Surveillance Act (FISA), ze zmianami z 2008 roku. Przed owymi usprawnieniami SID dostarczało FBI i CIA niekompletne i niedokładne listy celów, co uniemożliwiało naszym partnerom pełne wykorzystanie programu PRISM. Zespół PRINTAURA zaproponował, że będzie ściągać szczegółowe dane dotyczące każdego celu z wielu lokalizacji i łączyć je tak, by nadawały się do użycia. W drugim projekcie PRISM Mission Program Manager (MPM) rozpoczął niedawno wysyłanie wiadomości i wytycznych operacyjnych z PRISM do FBI i CIA, by ich analitycy mogli efektywnie wykorzystywać system PRISM, wiedzieli o przerwach i zmianach

w jego działaniu oraz optymalizowali korzystanie z niego. [...]. Te dwa działania wyraziście dowodzą, że PRISM to gra zespołowa!

Poza pozyskiwaniem danych „pod prąd" (z kabli światłowodowych) i bezpośrednio z serwerów firm internetowych (PRISM) NSA prowadzi także tak zwaną Eksploatację Sieci Komputerowych (Computer Network Exploitation, CNE), polegającą na umieszczaniu w komputerach „złośliwego oprogramowania" (*malware*) umożliwiającego śledzenie ich użytkowników. Gdy Agencji uda się umieścić takie oprogramowanie, jest w stanie – w terminologii NSA – „posiąść" komputer: widzieć każde naciśnięcie klawisza i każdą oglądaną stronę. Za te operacje odpowiada Sekcja Operacji Dostępu Dostosowanego (Tailored Access Operations, TAO). W gruncie rzeczy jest to wchodząca w skład Agencji jednostka hakerska.

Ta hakerska praktyka jest powszechna. Dowodzi tego dokument NSA mówiący, że Agencji udało się zainfekować złośliwym programem zwanym *Quantum Insertion* co najmniej 50 tysięcy komputerów osobistych. Poniższa mapa pokazuje miejsca, gdzie przeprowadzono takie operacje, oraz liczbę udanych infekcji.



Opierając się na dokumentach Snowdena, „New York Times" donosił, że NSA w rzeczywistości umieściła oprogramowanie „w niemal 100 tysiącach komputerów na świecie". Choć „złośliwe oprogramowanie" zazwyczaj instaluje się, „uzyskując dostęp do sieci komputerowych, Agencja w coraz większym stopniu wykorzystuje tajną technologię umożliwiającą jej wejście do komputera i zmianę danych, nawet jeśli nie jest on połączony z internetem".

Poza współpracą z usłużnymi firmami telekomunikacyjnymi i internetowymi NSA wspólnie z rządami innych krajów buduje ogarniający coraz większy obszar system inwigilacji. Mówiąc ogólnie, zagraniczne kontakty NSA dzielą się na trzy kategorie. Pierwsza grupa to wspomniany już Sojusz Pięciorga Oczu. USA szpieguje razem z wchodzącymi w jego skład państwami, rzadko jednak działa przeciwko nim – chyba że zwrócą się o to sami przedstawiciele tych krajów. Druga grupa to państwa, z którymi NSA współpracuje przy konkretnych projektach inwigilacji. Z drugiej strony jednak sama szpieguje je na dużą skalę. Trzecia grupa to kraje, które Stany Zjednoczone szpiegują rutynowo, za to właściwie nigdy nie współpracują.

W Sojuszu Pięciorga Oczu najbliższym współpracownikiem NSA jest brytyjska agencja GCHQ. Jak donosił „Guardian" na podstawie dostarczonych przez Snowdena dokumentów, „w ciągu ostatnich trzech lat rząd USA zapłacił co najmniej 100 milionów funtów brytyjskiej agencji wywiadu GCHQ za dostęp i wpływ na brytyjskie programy gromadzenia danych wywiadowczych". Płatności te stanowiły dla GCHQ zachętę do popierania tworzonych przez NSA planów inwigilacji. „GCHQ musi robić, co do niej należy, i pokazywać, że robi, co do niej należy" – stwierdzono w tajnych dokumentach dotyczących strategii GCHQ.

Członkowie Sojuszu Pięciorga Oczu informują się nawzajem o podejmowanych działaniach i co roku spotykają się na

konferencji Signals Development (SigDev), na której chwalą się ekspansją i odniesionymi w poprzednim roku sukcesami. Wicedyrektor NSA John Inglis powiedział o Sojuszu Pięciorga Oczu: „Pod wieloma względami prowadzimy wspólne działania wywiadowcze – pilnujemy, żeby jak najlepiej wykorzystywać swoje potencjały dla wspólnych korzyści".

Partnerzy skupieni w Sojuszu Pięciorga Oczu realizują wiele najbardziej inwazyjnych programów inwigilacji. W znacznej ich części uczestniczy GCHQ. Szczególną uwagę należy zwrócić na te wspólne działania brytyjskiej agencji oraz NSA, które mają na celu złamanie powszechnie stosowanych technik szyfrowania danych wykorzystywanych do ochrony osobistych transakcji internetowych w ramach bankowości internetowej czy blokujących wgląd w dokumentację medyczną. Agencjom udało się uzyskać dostępy do tych systemów szyfrujących, co nie tylko pozwala im śledzić działania prywatnych osób, ale także osłabia systemy ochrony danych, sprawiając, że stają się one bardziej podatne na działania hakerów i innych zagranicznych agencji wywiadowczych.

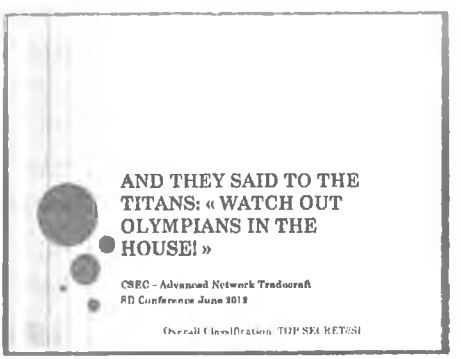
GCHQ prowadzi również masowe przechwytywanie danych z podwodnych łączy światłowodowych. Program noszący nazwę Tempora pozwolił GCHQ „podpinać się i gromadzić na okres do trzydziestu dni ogromne ilości danych pobranych z kabli światłowodowych. To czas wystarczający, by je przesiać i przeanalizować – donosił «Guardian». – GCHQ i NSA miały zatem możliwość pozyskiwania i przetwarzania ogromnych ilości połączeń między całkiem niewinnymi osobami". Przechwycone dane obejmują wszelkie formy działań online, w tym „nagrania rozmów telefonicznych, treści e-maili, wpisy na Facebooku oraz historię dostępu do stron internetowych każdego użytkownika internetu".

Inwigilacja podejmowana przez GCHQ jest równie wszechstronna – i bezkarna – jak działania NSA:

„O skali ambicji Agencji świadczą nazwy jej dwóch głównych działów: Opanowanie Internetu (Mastering the Internet) i Globalna Eksploatacja Telekomunikacji (Global Telecoms Exploitation), których celem jest dostęp do możliwie jak największej części ruchu internetowego i telefonicznego. To wszystko prowadzone jest bez żadnej publicznej świadomości czy debaty".

Bardzo aktywnym partnerem NSA, działającym także energicznie na własną rękę, jest Kanada. Podczas konferencji SigDev w 2012 roku Służba Bezpieczeństwa Łączności Kanady (Communications Security Establishment Canada, CSEC) chwaliła się wzięciem na cel brazylijskiego Ministerstwa Górnictwa i Energetyki sterującego głównymi gałęziami przemysłu tego kraju. Kanadyjskie firmy są żywotnie zainteresowane jego działaniami.

Tytuł prezentacji dotyczącej tego programu brzmi: *I powiedzieli tytanom: „Uważajcie na tych z Olimpu!"*, a podtytuł: *CSEC – zaawansowane techniki szpiegowskie w sieci.*



Na kolejnym slajdzie jednoznacznie wskazano, że „zróżnicowane źródła danych", „łańcuchowe wzbogacanie" i „zautomatyzowana analiza" mają dać wgląd w działalność „brazylijskiego Ministerstwa Kopalń i Energetyki (MME)" i że jest to nowy cel, którym trzeba się zająć na większą skalę.

OLYMPIA & THE CASE STUDY

CSEC's Network Knowledge Engine

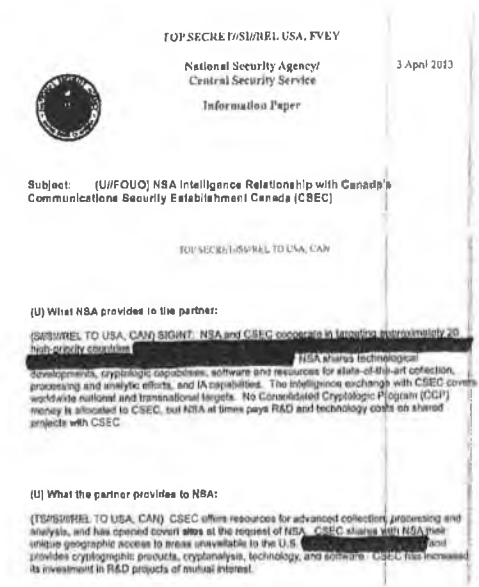
Various data sources
Chained enrichments
Automated analysis

Brazilian Ministry of Mines and Energy (MME)

New target to develop
Limited access/target knowledge

TOP SECRET//SI

Istnieją dowody na szeroką współpracę CSEC i NSA, łącznie z podjętymi przez Kanadę działaniami, by na prośbę (i korzyść)amerykańskiej agencji zakładać placówki szpiegowskie prowadzące inwigilację systemów łączności na całym świecie. A także szpiegować partnerów handlowych, którymi zainteresowana jest NSA. Jednym z tych dowodów jest kolejny dokument, zatytułowany: *Relacje wywiadowcze NSA z kanadyjskim Communications Security Establishment Canada (CSEC).*



TOP SECRET//SI//REL USA, FVEY

National Security Agency/
Central Security Service

3 April 2013

Information Paper

Subject: (U//FOUO) NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC)

TOP SECRET//SI//REL TO USA, CAN

(U) What NSA provides to the partner:

(S//SI//REL TO USA, CAN) SIGINT: NSA and CSEC cooperate in targeting approximately 20 high-priority countries [redacted] NSA shares technological developments, cryptologic capabilities, software and resources for state-of-the-art collection, processing and analytic efforts, and IA capabilities. The intelligence exchange with CSEC covers worldwide national and transnational targets. No Consolidated Cryptologic Program (CCP) money is allocated to CSEC, but NSA at times pays R&D and technology costs on shared projects with CSEC.

(U) What the partner provides to NSA:

(TS//SI//REL TO USA, CAN) CSEC offers resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the U.S. [redacted] and provides cryptographic products, cryptanalysis, technology, and software. CSEC has increased its investment in R&D projects of mutual interest.

Dokument ten informuje, że „NSA i CSEC współpracują nad celami w około dwudziestu państwach o wysokim priorytecie [...]. NSA dzieli się nowymi technologiami, zdolnościami kryptologicznymi, oprogramowaniem i pomocą w najnowocześniejszych metodach gromadzenia, przetwarzania i analizy danych [...]. Wymiana wywiadowcza z CSEC dotyczy globalnych celów krajowych i zagranicznych. CSEC nie przydzielono pieniędzy z Consolidated Cryptologic Program (CCP), ale NSA czasami pokrywa koszty badań i rozwoju oraz technologii przy projektach prowadzonych wspólnie z CSEC".

Kanadyjczycy zapewniają zaś NSA: „CSEC oferuje środki do zaawansowanego pozyskiwania, przetwarzania i analizy danych, a także na prośbę NSA otworzył tajne placówki. CSEC dzieli się z NSA swym wyjątkowym geograficznym dostępem do terenów niedostępnych dla USA [...], dostarcza również produkty kryptograficzne, kryptoanalizy, technologie i oprogramowanie. CSEC zwiększył inwestycje w przedsięwzięcia badawczo-rozwojowe interesujące dla obydwu stron".

Wzajemne związki członków Sojuszu Pięciorga Oczu są tak bliskie, że uczestniczące w sojuszu rządy nie tylko nie protestują, ale czasami nawet przedkładają życzenia NSA nad prywatność swoich obywateli. „Guardian" donosił o notatce służbowej z 2007 roku, opisującej porozumienie, „które pozwoliło Agencji «odsłonić» i przechowywać dane osobowe Brytyjczyków, do których przedtem nie miała dostępu". Co więcej, w 2007 roku zmieniono przepisy, „by NSA mogła analizować i przechowywać należące do obywateli brytyjskich numery telefonów komórkowych i faksów, e-maile i adresy IP".

W 2011 roku rząd Australii poszedł jeszcze o krok dalej i wprost zwrócił się do NSA o „rozszerzenie" partnerstwa, czyli poddanie obywateli swego kraju większemu nadzorowi. W liście z 21 lutego p.o. wicedyrektora Zarządu Łączności Ministerstwa Obrony

Australii (Defence Signals Directorate, DSD) napisał do Dyrektoriatu SID, że Australia „stoi teraz przed realnym zagrożeniem ze strony «rodzimych» ekstremistów działających i na terenie Australii, i poza nią". Prosił o nasiloną inwigilację obywateli australijskich uznanych przez rząd za niebezpiecznych:

Choć sami zainwestowaliśmy w analizę i przechwytywanie danych, by odszukać i wykorzystać interesujące nas połączenia, trudności, na jakie napotykamy w uzyskaniu regularnego i niezawodnego dostępu do nich, wpływają na naszą zdolność wykrywania i zapobiegania aktom terrorystycznym, a tym samym zmniejszają naszą zdolność ochrony życia i bezpieczeństwa obywateli Australii oraz naszych przyjaciół i sojuszników.

Długie i bardzo skuteczne partnerstwo z NSA pozwalało nam do tej pory na dostęp do niewielkiej części pozyskanych przez Stany Zjednoczone informacji o najważniejszych dla nas celach: działaniach terrorystów w Indonezji. Ten dostęp miał decydujące znaczenie w podejmowanych przez DSD działaniach zmierzających do przerwania i ograniczenia operacyjnych możliwości działania terrorystów w naszym regionie, czego dowodem jest niedawne aresztowanie ściganego zamachowca z Bali, Umara Pateka.

Z wdzięcznością przyjęlibyśmy możliwość rozszerzenia współpracy z NSA na większą liczbę Australijczyków zaangażowanych w międzynarodową działalność ekstremistyczną – szczególnie Australijczyków działających w AQAP [Al-Kaida Półwyspu Arabskiego – przyp. red.].

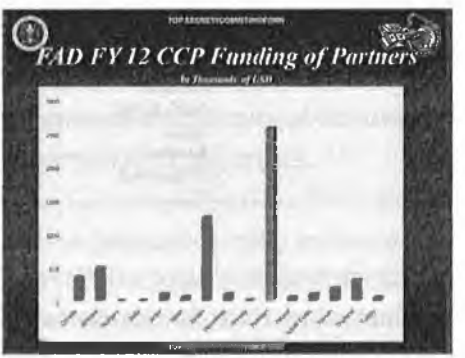
Kolejny poziom współpracy wiąże NSA z sojusznikami z „poziomu B" – państwami, które współpracują z NSA w ograniczony sposób, a same są celami agresywnej inwigilacji. NSA jasno rozdziela te dwa poziomy sojuszy: poziom A to współpraca wszechstronna, a poziom B – „współpraca ukierunkowana" (patrz wykres obok).

CONFIDENTIAL//NOFORN//20291123

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary
	Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

Niedawny dokument NSA *Foreign Partner Review (Przegląd partnerów zagranicznych* – patrz poniżej) z roku finansowego 2013, nazywając partnerów z poziomu B „Stronami Trzecimi", przedstawia rozszerzającą się listę krajów współpracujących z NSA. Obejmuje ona kraje należące do Sojuszu Pięciorga Oczu oraz między innymi Belgię, Danię, Francję, Hiszpanię, Holandię, Niemcy, Norwegię, Szwecję i Włochy, a także organizacje międzynarodowe takie jak NATO.

NSA często utrzymuje te relacje – tak jak w przypadku GCHQ – płacąc za opracowanie rozwiązań technologicznych i włączanie się w inwigilację. Oznacza to, że może kierować sposobem prowadzenia działalności szpiegowskiej. *Przegląd partnerów zagranicznych za rok finansowy 2012* (skan poniżej) ujawnia listę wielu państw, które otrzymały takie płatności, są wśród nich między innymi Polska, Kanada, Izrael, Japonia, Pakistan, Tajwan i Tajlandia.



Szczególne więzy wywiadowcze łączą NSA z Izraelem, co często oznacza współpracę tak bliską jak z członkami Sojuszu Pięciorga Oczu, a czasem może nawet bliższą. Memorandum na temat porozumienia między Agencją a wywiadem izraelskim ukazuje, że USA zdecydowały się na niezwykły krok: rutynowo dzielą się nieopracowanymi danymi, zawierającymi wiadomości amerykańskich obywateli. Wśród dostarczonych Izraelowi danych są „niepoddane ewaluacji i niezminimalizowane zapisy, podsumowania, faksymile, teleksy, nagrania i metadane, również dotyczące połączeń internetowych [DNI]".

To, co nadaje temu procesowi wyjątkowy charakter, to fakt, że materiał przekazywany Izraelowi nie przechodzi przez prawnie wymagany proces „minimalizacji". Procedura ta ma dopilnować, by w sytuacji, gdy prowadzona przez NSA

inwigilacja na szeroką skalę przynosi dane komunikacyjne, których nie wolno Agencji gromadzić nawet przy jej bardzo szerokim zakresie uprawnień, były jak najszybciej niszczone oraz nie były rozpowszechniane. W obecnym brzmieniu prawo regulujące ów proces i tak jest pełne luk prawnych. Zawiera też wyjątki dotyczące między innymi „informacji istotnych dla wywiadów zagranicznych" czy „dowodów przestępstwa". Gdy przychodzi jednak do udostępniania danych wywiadowi izraelskiemu, NSA najwyraźniej w ogóle nie uwzględnia takich zastrzeżeń prawnych.

Memorandum stwierdza wprost: „NSA rutynowo przesyła ISNU [Israeli Sigint National Unit – jednostka izraelskiego wywiadu odpowiedzialna za wywiad elektroniczny – przyp. red.] nieopracowane, zminimalizowane i niezminimalizowane zbiory".

Akcentując sposób, w jaki państwo może być równocześnie partnerem w inwigilacji i jej obiektem, dokument NSA omawiający historię współpracy z Izraelem odnotowuje „kwestie zaufania, które dotyczą dawniejszych operacji", i wskazuje, że służby Izraela należą do tych, które prowadzą najbardziej agresywną inwigilację w USA:

Jest też kilka niespodzianek... Francja namierza Departament Obrony USA za pomocą swojego wywiadu technicznego, jesteśmy również celem dla Izraela. Z jednej strony Izraelczycy są dla nas wyjątkowo dobrym partnerem, jeśli chodzi o pozyskiwanie SIGINT, z drugiej obierają sobie nas za cel, by poznać nasze stanowisko w sprawie problemów Bliskiego Wschodu. NIE [National Intelligence Estimate, sygnowany przez Dyrektora Wywiadu Narodowego dokument opisujący co roku nowe zagrożenia wywiadowcze – przyp. red.] uznał służby wywiadowcze Izraela za trzecie co do stopnia agresywności w działaniach przeciwko USA.

Ten sam raport podaje, że mimo bliskich związków między agencjami wywiadu Stanów Zjednoczonych i Izraela, i ogromna ilość informacji dostarczanych drugiej stronie przez USA nie przynosi wiele w zamian. Wywiad izraelski był zainteresowany jedynie pozyskiwaniem przydatnych dla niego danych. NSA narzekała, że współpraca była nastawiona „niemal wyłącznie" na zaspokojenie potrzeb Izraela.

Stałym wyzwaniem było wyważenie wymiany SIGINT między potrzebami USA i Izraela. W ostatniej dekadzie niewątpliwie nastąpił zdecydowany przechył w stronę potrzeb bezpieczeństwa Izraela. 11 września nadszedł i minął, a współpraca NSA w dziedzinie CT [skrót od counterterrorism, czyli działania antyterrorystyczne – przyp. red.] ze Stroną Trzecią była niemal całkowicie nakierowana na potrzeby partnera.

W skład kolejnego, trzeciego poziomu państw – poniżej Sojuszu Pięciorga Oczu i krajów z drugiego poziomu takich jak Izrael – wchodzą cele niebędące nigdy partnerami w amerykańskich programach szpiegowskich. Jak można oczekiwać, ów poziom obejmuje państwa uważane za przeciwników Ameryki, a więc Chiny, Rosję, Iran, Wenezuelę czy Syrię. Zalicza się jednak do niego również kraje uważane za względnie przyjazne lub neutralne wobec USA, jak Brazylia, Meksyk, Argentyna, Indonezja, Kenia i Republika Południowej Afryki.

W reakcji na ujawnienie dokumentów NSA rząd Stanów Zjednoczonych usiłował przekonywać, że w odróżnieniu od obywateli innych państw obywatele Stanów Zjednoczonych są chronieni przed bezprawną inwigilacją. 18 czerwca 2013 roku prezydent Obama powiedział Charliemu Rose: „Mogę jednoznacznie stwierdzić, że jeśli ktoś jest obywatelem USA, NSA nie może podsłuchiwać jego rozmów telefonicznych [...] zgodnie

z prawem i zasadami, chyba że [...] pójdzie do sądu, uzyska nakaz i poda prawdopodobne uzasadnienie, tak samo, jak to było dotychczas". Mike Rogers, republikanin, przewodniczący Komisji Wywiadu Izby Reprezentantów, tłumaczył w CNN, że NSA „nie podsłuchuje rozmów telefonicznych Amerykanów. Gdyby to robiła, byłoby to nielegalne. Oznaczałoby łamanie prawa".

To raczej dziwna linia obrony: powiadomienie reszty świata, że NSA narusza prywatność nie-Amerykanów. Wiadomość tę świat usłyszał bardzo wyraźnie: ochrona prywatności dotyczy wyłącznie obywateli amerykańskich. Wywołało to tak wielkie oburzenie, że nawet szef Facebooka Mark Zuckerberg, wcześniej nieszczególnie gorąco broniący prywatności, narzekał, iż rząd USA „schrzanił" sprawę, bowiem w reakcji na skandal NSA wystawił na szwank interesy międzynarodowych firm internetowych: „Rząd powiedział: nie przejmujcie się, nie szpiegujemy żadnych Amerykanów. Super, to naprawdę pomogło firmom, których klientami są ludzie z całego świata. Dzięki za tak jasne postawienie sprawy. Uważam, że to było naprawdę fatalne".

Ale zapewnienia, że amerykańscy obywatele nie podlegają inwigilacji, to nie tylko dziwna strategia, ale również oczywista nieprawda. Wbrew zaprzeczeniom prezydenta Obamy i jego najważniejszych urzędników NSA nieustannie i bez konkretnych nakazów przechwytuje treść połączeń obywateli amerykańskich. Nie potrzebuje do tego indywidualnych nakazów sądowych usprawiedliwiających taką inwigilację. Wystarczą „uzasadnione powody". Jak już wskazano, ustawa FISA z 2008 roku pozwala też NSA bez indywidualnych nakazów monitorować treść wiadomości wymienianych przez Amerykanów, jeżeli drugą stroną kontaktu jest namierzany cudzoziemiec. Agencja nazywa to ściąganiem „incydentalnym", jak gdyby szpiegowanie Amerykanów bez zezwolenia było jakimś niezamierzonym incydentem. To jednak fałszywy wniosek. Jameel Jaffer, wicedyrektor ACLU do spraw prawnych, wyjaśnia:

„Rząd często mówi, że inwigilacja wiadomości wymienianych przez Amerykanów jest „incydentalna", co brzmi, jak gdyby prowadzony przez NSA podsłuch rozmów telefonicznych i podglądanie e-maili Amerykanów odbywało się niechcący, a z punktu widzenia rządu były nawet godne ubolewania.

Jednak gdy urzędnicy z administracji Busha zwrócili się do Kongresu o nowe uprawnienia umożliwiające rozszerzenie możliwości inwigilacji, powiedzieli całkiem wyraźnie, że to połączenia Amerykanów zawierają najbardziej interesujące ich wiadomości. Zobaczcie na przykład wypowiedź Michaela Haydena zatytułowaną „FISA dla XXI wieku" podczas wysłuchania przed Komisją Senacką ds. Sądownictwa w 2006 roku. Powiedział, że to połączenia, „których jeden koniec znajduje się w Stanach Zjednoczonych, są dla nas najważniejsze".

Głównym celem ustawy z 2008 roku było umożliwienie rządowi gromadzenia danych o międzynarodowych połączeniach Amerykanów – i to gromadzenia niezależnie od tego, czy którakolwiek strona tego połączenia robiła coś nielegalnego. Duża część obrony rządu ma na celu zaciemnienie tego faktu, a jest on kluczowy: rząd nie musi „namierzać" konkretnych Amerykanów, by gromadzić ogromne ilości ich połączeń".

Profesor Jack Balkin ze Szkoły Prawa Uniwersytetu Yale potwierdza, że ustawa FISA z 2008 roku praktycznie rzecz biorąc daje prezydentowi władzę prowadzenia programu „podobnego w skutkach do niedozwolonego programu inwigilacji" realizowanego potajemnie przez administrację George'a W. Busha: „Te programy nieuchronnie obejmują wiele połączeń telefonicznych Amerykanów, którzy mogą nie mieć absolutnie żadnych związków z terroryzmem czy Al-Kaidą".

Zapewnienia Obamy dodatkowo dyskredytuje służalcza postawa sądu FISA wobec NSA. Sąd ten zatwierdza bowiem

niemal wszystkie wnioski o inwigilację przedstawione przez Agencję. Jej obrońcy często chwalą procedury sądowe FISA. Mają być one dowodem, że NSA znajduje się pod nadzorem. Jednak sąd powołano bardziej dla utrzymania pozorów niż dla ustanowienia rzeczywistej kontroli. Te pozorowane reformy miały złagodzić gniew społeczeństwa z powodu skandali związanych z inwigilacją w latach 70. ubiegłego wieku.

Instytucja ta ewidentnie nie sprawuje realnej kontroli nad inwigilacją, ponieważ właściwie nie ma żadnej z cech, które w oczach naszego społeczeństwa stanowią podstawowe atrybuty systemu sądowniczego. Sąd FISA spotyka się całkowicie niejawnie, jego wyroki automatycznie uznawane są za „ściśle tajne", tylko jedna strona – rząd – może przedstawiać w nim swoją sprawę. Przez wiele lat jego siedzibą był Departament Sprawiedliwości, co podkreślało jego rolę biura działającego w ramach instytucji władzy wykonawczej, a nie niezależnego sądu pełniącego funkcję kontrolną.

Rezultaty są dokładnie takie, jakich można by oczekiwać: sąd niemal nigdy nie odrzuca wniosków NSA dotyczących inwigilacji Amerykanów. Od samego początku istnienia wyroki sądu FISA były tylko ostatnią formalnością. W ciągu pierwszych dwudziestu czterech lat istnienia, od 1978 do 2002 roku, sąd odrzucił w sumie zero – zero! – wniosków rządu. Zatwierdził zaś wiele tysięcy. W ciągu kolejnych dziesięciu lat, do końca 2012 roku, sąd odrzucił zaledwie jedenaście wniosków, a zatwierdził w sumie ponad 20 tysięcy.

Jedno z postanowień ustawy FISA z 2008 roku wymaga, by władze wykonawcze co roku ujawniały Kongresowi, ile wniosków o podsłuch sąd otrzymuje, a następnie zatwierdza, modyfikuje lub odrzuca. Dane za 2012 rok ujawniły, że sąd zatwierdził wszystkie 1788 wniosków, a „zmodyfikował" – czyli zawęził zakres – zaledwie czterdzieści z nich, czyli niecałe 3 procent:

Wnioski złożone do Sądu do spraw Zagranicznej Inwigilacji Wywiadowczej w roku kalendarzowym 2012 (paragraf 107 Ustawy, 50 U.S.C. § 1907)

W roku kalendarzowym 2012 rząd złożył w Sądzie do spraw Zagranicznej Inwigilacji Wywiadowczej (FISA) 1856 wniosków o zezwolenie na prowadzenie inwigilacji elektronicznej i/lub przeszukań do celów wywiadu zagranicznego. Na 1856 wniosków składają się wnioski wyłącznie o inwigilację elektroniczną, wyłącznie o przeszukania oraz wnioski połączone, wnoszące o zezwolenie na inwigilację elektroniczną i przeszukanie. 1789 wniosków dotyczyło zezwoleń na inwigilację elektroniczną.

Z tych 1789 wniosków jeden został wycofany przez rząd. FISA nie odrzucił żadnego wniosku w całości ani w części.

To samo działo się w roku 2011 – NSA podała, że złożyła 1676 wniosków, a sąd FISA zmodyfikował trzydzieści i „nie odrzucił żadnego wniosku w całości ani w części".

Także inne statystyki wskazują na podległość sądu wobec NSA. Oto na przykład zestawienie odpowiedzi sądu FISA na wnioski składane w ciągu ostatnich sześciu lat przez Agencję z powołaniem się na Patriot Act. Dotyczą one pozyskiwania dokumentacji firm – telefonicznych, finansowych i medycznych – należących do podmiotów działających w USA. Z lewej strony znajduje się liczba wniosków złożonych przez amerykański rząd, a z prawej – odrzuconych.

A zatem nawet w tych nielicznych wypadkach, gdy wymagana jest zgoda sądu FISA, by wziąć na cel czyjeś połączenia, cały proces jest bardziej farsą niż elementem kontroli nad działaniami NSA.

Kolejny poziom nadzoru nad Agencją zapewniają rzekomo komisje do spraw wywiadu w Kongresie, także będące pokłosiem skandali szpiegowskich z lat 70. Są one jednak jeszcze bierniejsze niż sąd FISA. Wymyślone jako organy „czujnej kontroli ustawodawczej" nad działaniami agencji wywiadowczych, komisje te kierowane są obecnie przez najbardziej oddane, lojalne wobec NSA osoby w Waszyngtonie: w Senacie przez Dianne Feinstein z Partii Demokratycznej, a w Izbie Reprezentantów przez Mike'a Rogersa z Partii Republikańskiej. Zamiast zapewniać kontrolę nad operacjami NSA, Feinstein, Rogers i ich komisje istnieją głównie po to, by ich bronić i uzasadniać działania Agencji.

W artykule opublikowanym w „New Yorkerze" w grudniu 2013 roku Ryan Lizza napisał, że komisje „najczęściej traktują [...] wysokich funkcjonariuszy wywiadu jak gwiazdy sceny". Osoby obserwujące prowadzone przez senacką komisję przesłuchania na temat działalności NSA nie mogły wyjść ze zdumienia, widząc, jak senatorowie „przepytują" stających przed nimi funkcjonariuszy Agencji. Zamiast pytań najczęściej mogły wysłuchać długich monologów senatorów wspominających zamachy z 11 września i twierdzących, że najważniejsze jest zapobieżenie takim atakom w przyszłości. Nie wykorzystywali oni okazji, by przesłuchać funkcjonariuszy NSA i wypełnić obowiązki organu kontrolnego. Zamiast tego głosili propagandę wspierającą działania NSA. Doskonale oddaje to rzeczywistą funkcję komisji w ciągu ostatnich dziesięciu lat.

Co więcej, przewodniczący komisji nadzoru bronili czasami Agencji jeszcze energiczniej niż sami jej funkcjonariusze. W sierpniu 2013 dwóch kongresmanów – demokrata Alan Grayson z Florydy i republikanin Morgan Griffith z Wirginii – niezależnie od

siebie powiadomili mnie, że Komisja ds. Wywiadu blokuje przed nimi i innymi członkami Kongresu dostęp do najbardziej podstawowych informacji o NSA, by chronić Agencję przed realną kontrolą. Obaj kongresmani udostępnili mi listy, jakie pisali do sztabu przewodniczącego Rogersa, prosząc o informacje na temat opisywanych w mediach programów, ale prośby obydwu wielokrotnie ignorowano.

Gdy po ujawnieniu rewelacji Snowdena podjęto w Senacie debatę nad reformą NSA, grupa senatorów z obu partii, od dawna zaniepokojona nadużyciami związanymi z inwigilacją, podjęła starania o nowe ustawodawstwo, narzucające rzeczywiste ograniczenia władzy NSA. Reformatorzy ci, pod kierownictwem demokratycznego senatora Rona Wydena z Oregonu, natychmiast natrafili na barierę w postaci kontrofensywy obrońców NSA w Senacie. Dążyli oni do napisania ustawy tworzącej jedynie pozory reform, a realnie wręcz zwiększającej uprawnienia Agencji. Dave Wiegel z magazynu „Slate" donosił w listopadzie, 2013 roku:

Krytycy masowego gromadzenia danych i programów inwigilacji prowadzonych przez NSA nigdy nie musieli się martwić działaniami Kongresu. Słusznie oczekiwali, że przedstawi on coś, co będzie wyglądało jak reforma, ale co w rzeczywistości będzie kodyfikować i usprawiedliwiać praktyki, które dziś są ujawniane i stawiane pod pręgierzem. Zawsze tak było – każda poprawka czy nowa autoryzacja Patriot Act z 2001 roku budowała więcej ukrytych furtek niż murów.

„Będziemy musieli występować przeciwko brygadzie «nic się nie dzieje» złożonej z wpływowych członków kierownictwa wywiadu, ich sojuszników w think-tankach i świecie akademickim, emerytowanych urzędników rządowych i sympatyzujących z nimi ustawodawców – ostrzegał miesiąc temu senator Ron Wyden z Oregonu. – Ich celem jest dopilnowanie, by wszelkie reformy programów inwigilacji pozostały jedynie powierzchowne.

[...] [Zasady] ochrony prywatności, które naprawdę niczyjej prywatności nie chronią, nie są warte papieru, na którym je wydrukowano".

Frakcji pseudoreformy przewodziła Dianne Feinstein – ta sama senator, której zadaniem jest nadzór nad NSA. Od dawna jest ona bez reszty oddana interesom „bezpieczeństwa narodowego", poczynając od głośnego poparcia dla wojny w Iraku po nieugiętą obronę programów NSA w epoce Busha (jej mąż ma wielkie udziały w różnych firmach dostarczających sprzęt wojskowy). Feinstein była naturalną kandydatką na przewodniczącą komisji, która twierdzi, że sprawuje nadzór nad służbami wywiadowczymi, ale w rzeczywistości robi coś wręcz przeciwnego.

Mimo wszystkich rządowych zaprzeczeń NSA nie obowiązują żadne solidniejsze formalne ograniczenia dotyczące tego, kogo i jak może inwigilować. Nawet tam, gdzie ograniczenia rzekomo obowiązują – a więc gdy celem inwigilacji stają się Amerykanie – mamy do czynienia w gruncie rzeczy z grą pozorów. NSA to zdecydowanie zbójecka agencja: ma prawo robić, co chce, przy bardzo niewielkich oczekiwaniach w kwestiach kontroli jej działań, przejrzystości czy odpowiedzialności.

Mówiąc bardzo ogólnie, NSA gromadzi dwa rodzaje informacji: treści i metadane. „Treści" to rozmowy telefoniczne, e-maile i czaty online przechwytywane na drodze podsłuchiwania lub czytania przesyłanych treści. Treścią są także informacje pozyskane poprzez śledzenie ogólnej aktywności użytkowników sieci, takie jak historie wyszukiwań i odwiedzanych stron. „Metadane" zaś to informacje *na temat* komunikacji telefonicznej i sieciowej. NSA nazywa to „informacją o treści (ale bez samej treści)".

Na przykład metadane o e-mailach mówią, kto wysyła wiadomość i do kogo, jaki jest temat wiadomości oraz gdzie przebywała osoba ją wysyłająca. W zreprodukowanym poniżej

dokumencie NSA nakreśliła, do jakich metadanych telefonicznych uzyskuje dostęp i jakie gromadzi.


Communications Metadata Fields in ICREACH

(S//NF) NSA populates these fields in PROTON:

- Called & calling numbers, date, time & duration of call

(S//SI//REL) ICREACH users will see telephony metadata* in the following fields:

DATE & TIME
DURATION – Length of Call
CALLED NUMBER
CALLING NUMBER
CALLED FAX (CSI) – Called Subscriber ID
TRANSMITTING FAX (TSI) – Transmitting Subscriber ID
IMSI – International Mobile Subscriber Identifier
TMSI – Temporary Mobile Subscriber Identifier
IMEI – International Mobile Equipment Identifier
MSISDN – Mobile Subscriber Integrated Services Digital Network
MDN – Mobile Dialed Number
CLI – Call Line Identifier (Caller ID)
DSME – Destination Short Message Entity
OSME – Originating Short Message Entity
VLR – Visitor Location Register

Jest w nim mowa o datach i godzinach rozmów, długości połączeń, numerze dzwoniącego i odbiorcy, numerze faksu odbiorcy, numerze faksu nadawcy oraz szeregu identyfikatorów umożliwiających identyfikację rozmówców, osób wymieniających SMS-y lub wysyłających faksy (między innymi IMSI – międzynarodowy identyfikator abonenta mobilnego, TMSI – tymczasowy identyfikator abonenta mobilnego, oraz IMEI – międzynarodowy numer identyfikacyjny telefonu komórkowego, MSISDN – numer abonenta sieci komórkowej, MDN – wybrany numer telefonu komórkowego).

Rząd USA twierdzi, że znaczna część inwigilacji ujawnionej w archiwum Snowdena dotyczy gromadzenia „metadanych, nie treści", usiłując tym samym sugerować, że ten rodzaj szpiegostwa nie jest inwazyjny, a przynajmniej nie w takim samym stopniu jak przechwytywanie treści. Dianne Feinstein wyraźnie stwierdziła w programie *USA Today*, że gromadzenie metadanych wszystkich połączeń telefonicznych Amerykanów „to nie inwigilacja", ponieważ „nie oznacza to pobierania treści jakiejkolwiek wiadomości".

Te mało pomysłowe argumenty zaciemniają jednak fakt, że inwigilacja w postaci gromadzenia metadanych bywa bardziej

inwazyjna niż przechwycenie treści. Gdy rząd zna wszystkich naszych rozmówców telefonicznych i wie, kto do nas dzwoni, gdy zna wszystkich odbiorców e-maili, wszystkie miejsca, do których wysyłamy wiadomości, oraz długość trwania naszych rozmów, może sobie stworzyć niezwykle wszechstronny obraz naszego życia, naszych związków i postępowania, obejmujący także najbardziej intymne i prywatne informacje.

W zaprzysiężonym oświadczeniu złożonym przez ACLU i kwestionującym legalność programu gromadzenia metadanych przez NSA profesor Edward Felten z Centrum Komputerowego Princeton wyjaśnia, dlaczego inwigilacja przez gromadzenie metadanych może okazać się szczególnie wiele mówiąca:

„Weźmy następujący hipotetyczny przykład: młoda kobieta dzwoni do swego ginekologa, zaraz potem do matki, następnie do mężczyzny, z którym w kilku minionych miesiącach często rozmawiała przez telefon po jedenastej wieczorem; następnie dzwoni do ośrodka planowania rodziny, gdzie można dokonać także aborcji. Wynika z tego prawdopodobny zarys historii, która nie byłaby tak oczywista, gdyby podsłuchano tylko jedną rozmowę telefoniczną".

Nawet w przypadku pojedynczej rozmowy telefonicznej metadane mogą powiedzieć więcej niż jej treść. Podsłuchana rozmowa telefoniczna kobiety, która dzwoni do kliniki aborcyjnej, może nie zdradzić niczego więcej niż fakt, że umówiła się na wizytę lub ją potwierdziła w klinice o typowo brzmiącej nazwie („Klinika na East Side" czy „gabinet doktora Jonesa"). Ale metadane zdradzą więcej: tożsamość tych, do których telefonowano. To samo dotyczy telefonu do serwisu randkowego, kliniki odwykowej, lekarza specjalizującego się w leczeniu HIV, ośrodka dla gejów i lesbijek czy telefonu zaufania dla chcących popełnić samobójstwo. Metadane ujawnią także rozmowę działacza praw człowieka nawiązującego kontakt z informatorem w kraju o represyjnym reżimie albo zaufanego źródła, które

dzwoni do dziennikarza, by ujawnić przestępstwo na wysokim szczeblu. Jeśli ktoś późno w nocy często dzwoni albo wysyła e-maile do kogoś, kto nie jest jego partnerem, metadane to pokażą. Co więcej, zarejestrują nie tylko wszystkie osoby, z którymi się komunikuje, i jak często to robi, ale także wszystkie osoby, z którymi porozumiewają się jego przyjaciele i współpracownicy. W ten sposób powstanie wszechstronny obraz sieci kontaktów.

Ponadto, jak wskazuje profesor Felten, podsłuchiwanie rozmów może okazać się całkiem trudne na skutek różnic językowych, używania slangu, szyfru, konwersacji pełnej dygresji czy innych cech, które specjalnie lub przypadkowo rozmywają znaczenie. „Treść rozmów znacznie trudniej poddaje się analizie prowadzonej w sposób automatyczny, ponieważ z natury nie są one usystematyzowane" – twierdzi. Z kolei metadane są matematyczne: czyste, dokładne, a zatem łatwe do analizowania, co często „zastępuje treść".

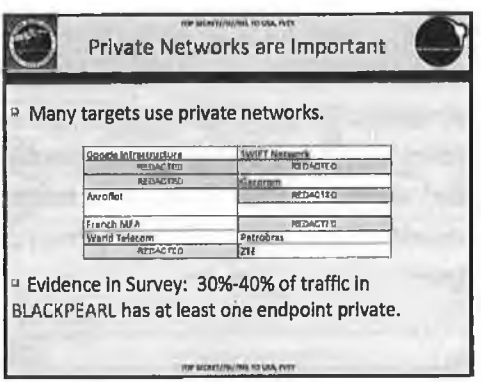
„Metadane telefoniczne mogą [...] niezwykle wiele powiedzieć o naszych przyzwyczajeniach i powiązaniach – pisze Felten. – Rozkład połączeń może pokazać, kiedy sypiamy, a kiedy nie; może zdradzić naszą religię, jeśli regularnie nie dzwonimy w soboty albo dużo dzwonimy w Boże Narodzenie; nasze przyzwyczajenia w pracy i nasze kontakty towarzyskie; liczbę przyjaciół; a nawet nasze afiliacje społeczne i polityczne".

W sumie, pisze Felten, „masowe pozyskiwanie danych nie tylko pozwala rządowi zebrać informacje o większej liczbie ludzi, ale także umożliwia mu poznanie nowych, uprzednio prywatnych faktów, do których by nie dotarł, gdyby skupiał się na szczegółach odnoszących się do konkretnych osób".

Niepokój, jaki budzi możliwość rozlicznych zastosowań tego rodzaju wrażliwych danych przez rząd, jest szczególnie uzasadniony, ponieważ wbrew powtarzanym zapewnieniom prezydenta Obamy i NSA znacząca część działań

Agencji nie ma nic wspólnego z działaniami antyterrorystycznymi, a nawet z bezpieczeństwem narodowym. Duża część archiwum Snowdena dotyczy rodzaju szpiegostwa, które można nazwać tylko w jeden sposób: wywiad gospodarczy. Bo jak inaczej określić podsłuchiwanie i przechwytywanie e-maili potężnej brazylijskiej firmy naftowej Petrobras, Organizacji Państw Amerykańskich, konferencji ekonomicznych w Ameryce Łacińskiej, firm energetycznych w Wenezueli i Meksyku oraz szpiegowanie przez sojuszników NSA (w tym Kanadę, Norwegię i Szwecję) brazylijskiego Ministerstwa Kopalń i Energetyki oraz firm energetycznych w kilku innych państwach.

W jednym z godnych uwagi dokumentów, przedstawionych przez NSA i GCHQ, wyszczególniono liczne cele inwigilacji o wyraźnie ekonomicznym charakterze: Petrobras, infrastrukturę Google'a, system służący do przelewów bankowych SWIFT, rosyjską firmę gazową Gazprom i rosyjskie linie lotnicze Aerofłot.

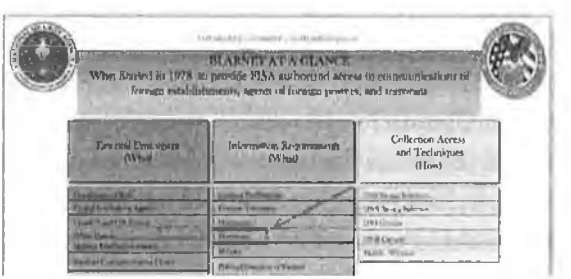


Prezydent Obama i najważniejsi urzędnicy jego administracji od lat potępiają Chiny za wykorzystywanie możliwości inwigilacji dla korzyści gospodarczych, twierdząc równocześnie, że USA i ich sojusznicy nigdy czegoś takiego nie robią.

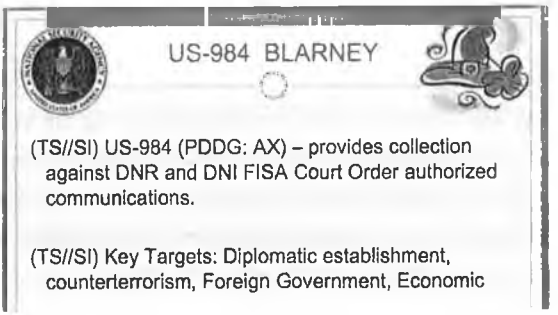
„Washington Post" cytuje wypowiedź rzecznika NSA, że Departament Obrony, do którego NSA należy, „«rzeczywiście wykorzystuje» sieci komputerowe", ale nie prowadzi szpiegostwa gospodarczego w żadnej dziedzinie, w tym «cyber»".

To, że NSA szpieguje z tych właśnie powodów, którym zaprzecza, dowodzą jej własne dokumenty takie jak prezentacja poniżej. Agencja działa na korzyść wielu, jak ich nazywa, „klientów", do których zalicza się nie tylko Biały Dom, Departament Stanu i CIA, ale także instytucje przede wszystkim ekonomiczne, takie jak Biuro Przedstawiciela Handlowego USA oraz Departamenty Rolnictwa, Skarbu i Handlu.

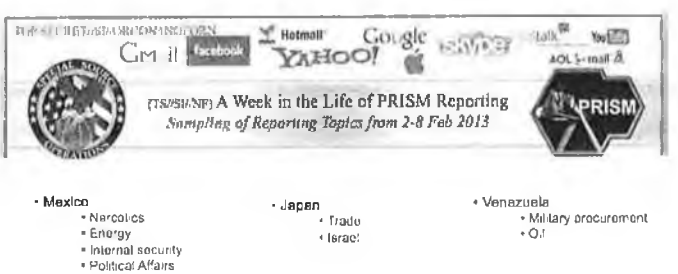
W opisie programu BLARNEY NSA wymienia zaś rodzaje informacji, które zgodnie ze swoimi uprawnieniami przekazuje „klientom", w tym dotyczące zwalczania terroryzmu, dyplomacji i gospodarki, a także sytuacji militarnej i politycznej innych krajów.



Potwierdza to kolejna plansza. Objaśnia ona, że projekt BLARNEY „zapewnia pozyskiwanie wiadomości DNI i DNR (telefonicznych i internetowych) zgodnie z nakazem sądu FISA" oraz że główne obiekty jego zainteresowania to: „kręgi dyplomatyczne, antyterroryzm, obce rządy oraz gospodarka"



Dalszym dowodem zainteresowania NSA gospodarką jest dokument o programie PRISM zawierający „próbkę" „tematów wiadomości" za okres 2-8 lutego 2013 roku. Lista typów informacji, zebranych w różnych krajach, obejmuje również kwestie ekonomiczne i finansowe, w tym „energię" i „ropę naftową".



Można się z niego dowiedzieć, że w Meksyku w obszarze zainteresowania Agencji znajdują się narkotyki, energia, bezpieczeństwo wewnętrzne i sprawy polityczne; w Japonii jest to handel; w Wenezueli zaś to zaopatrzenie militarne i ropa naftowa.

Memorandum z 2006 roku, stworzone przez członków należącej do NSA komórki zajmującej się problemami bezpieczeństwa międzynarodowego (International Security Issues, ISI), bez ogródek mówi o gospodarczym i handlowym szpiegostwie Agencji przeciwko krajom tak różnym jak Belgia, Japonia, Brazylia i Niemcy:

ISI jest odpowiedzialne za 13 państw na trzech kontynentach. Państwa te łączy istotny fakt, że wszystkie są ważne dla amerykańskich interesów ekonomicznych, handlowych i obronnych. Wydział Europy Zachodniej i Partnerstw Strategicznych skupia się głównie na polityce zagranicznej i działalności handlowej Belgii, Francji, Niemiec, Włoch i Hiszpanii, a także Brazylii, Japonii i Meksyku.

Wydział Energetyki i Bogactw Naturalnych dostarcza unikalne dane wywiadowcze na temat światowej produkcji energii i rozwoju w kluczowych państwach, mających wpływ na gospodarkę światową. Szczególnie istotne dziś państwa to Irak, Iran, Rosja i basen Morza Kaspijskiego, Wenezuela oraz Chiny. Raporty obejmowały monitoring międzynarodowych inwestycji w sektory energetyczne krajów, unowocześnianie systemów przepływu energii oraz nadzorujących przebieg procesów technologicznych, a także wspomagane komputerowo projektowanie planowanych inwestycji energetycznych.

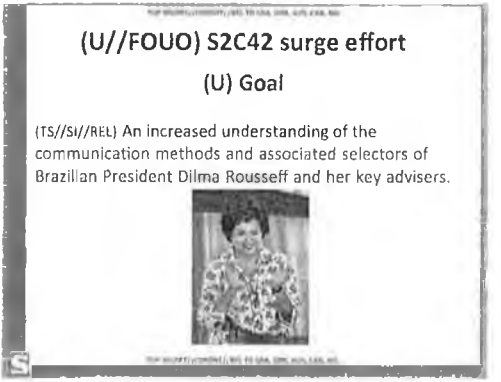
Pisząc o transzy dokumentów Brytyjczyków z GCHQ, które znalazły się w przecieku Snowdena, „New York Times" wskazał, że obiektami inwigilacji często były instytucje finansowe oraz „szefowie międzynarodowych organizacji pomocowych, zagranicznych firm energetycznych oraz urzędnik Unii Europejskiej zaangażowany w antytrustową walkę z amerykańskimi firmami technologicznymi". Dodał, że agencje

amerykańskie i brytyjskie „monitorowały połączenia wysokich urzędników Unii Europejskiej, zagranicznych przywódców, w tym głów państw afrykańskich, a czasami członków ich rodzin, dyrektorów ONZ i programów pomocowych [takich jak UNICEF], a także urzędników nadzorujących ministerstwa paliw płynnych i finansów".

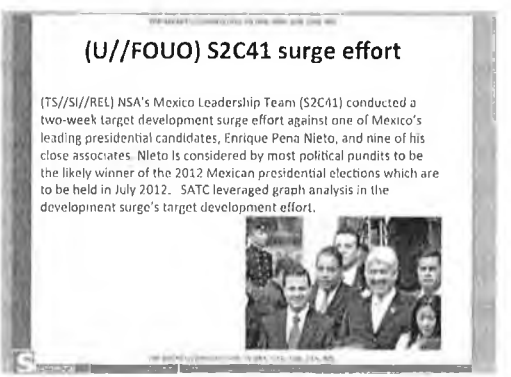
Cele wywiadu gospodarczego są jasne. Gdy USA za pomocą NSA poznają strategie innych państw na rozmowy handlowe i gospodarcze, zyskują ogromną przewagę, którą mogą wykorzystać na rzecz interesów przemysłu własnego kraju. W 2009 roku zastępca sekretarza stanu Thomas Shannon napisał list do Keitha Alexandra, „by pogratulować i wyrazić wdzięczność za wyjątkowe wsparcie ze strony wywiadu", jakie Departament Stanu otrzymał przed Piątym Szczytem Obu Ameryk, konferencją poświęconą negocjowaniu porozumień gospodarczych. W liście tym stwierdzał wyraźnie, że inwigilacja dała Amerykanom przewagę negocjacyjną:

Ponad sto otrzymanych od NSA raportów pozwoliło nam na głęboki wgląd w plany i intencje innych uczestników Szczytu oraz sprawiło, że nasi dyplomaci byli dobrze przygotowani, by doradzać prezydentowi Obamie i sekretarz stanu Clinton, jak podchodzić do kwestii spornych takich jak Kuba oraz rozmawiać z trudnymi partnerami, takimi jak prezydent Wenezueli Chávez.

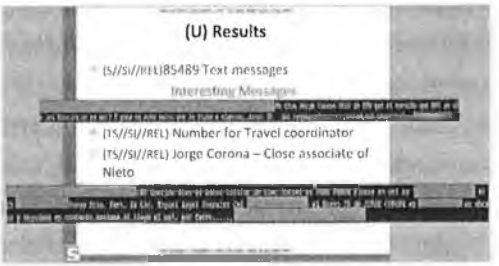
NSA zajmuje się również szpiegostwem dyplomatycznym, o czym świadczą poprzednie dokumenty, w których wspomina się o „sprawach politycznych". Jeden oczywisty przykład dotyczył szczególnie inwazyjnej inwigilacji, której celem było „lepsze zrozumienie metod porozumiewania się" i celów „brazylijskiej prezydent Dilmy Rousseff i jej najważniejszych doradców" (patrz następna strona).



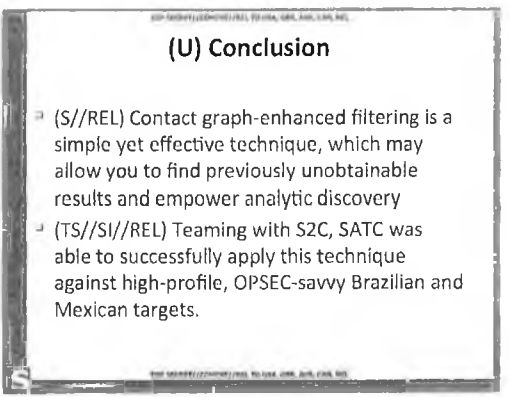
Kolejny przykład z dziedziny polityki to inwigilacyjna akcja z 2011 roku dotycząca dzisiejszego prezydenta Meksyku Enrique Peña Nieto. Związany z nią dokument stwierdza, że „przez dwa tygodnie prowadzono wzmocnione działania przeciwko jednemu z wiodących kandydatów na prezydenta Meksyku, Enrique Peña Nieto, i dziewięciu jego bliskim współpracownikom. Większość politycznych specjalistów uważa Nieto za prawdopodobnego zwycięzcę w wyborach prezydenckich w Meksyku w lipcu 2012 roku".



Dokument dotyczący tej akcji zawiera nawet kilka przechwyconych wiadomości tekstowych wysłanych i otrzymanych przez Nieto i jego bliskiego współpracownika Jorge Coronę.



Inna prezentacja (slajd poniżej) informuje o nowych technikach użytych wobec „obiektów brazylijskich i meksykańskich", podkreślając, że dzięki współpracy Departamentu Bezpieczeństwa Międzynarodowego (S2C) i Centrum Rozwijania Nowych Technik Analitycznych (SATC) „był w stanie skutecznie zastosować tę technikę przeciwko zajmującym wysokie stanowiska" i osobom „znającym kwestie bezpieczeństwa".



Można się zastanawiać, dlaczego NSA wzięło na cel przywódców politycznych Brazylii i Meksyku. Odpowiedzią zapewne jest to, że oba państwa mają bogate złoża ropy, są też dużymi krajami o znacznych wpływach w regionie. I choć niewątpliwie nie są przeciwnikami Stanów Zjednoczonych, nie można ich także zaliczyć do ich najbliższych i najbardziej zaufanych sojuszników. Co więcej, jeden z dokumentów planistycznych

NSA – zatytułowany *Identyfikacja wyzwań: tendencje geopolityczne w 2014-2019* – wymienia oba kraje pod nagłówkiem „Przyjaciele, wrogowie czy problemy?". Inne państwa na liście to Egipt, Indie, Iran, Arabia Saudyjska, Somalia, Sudan, Turcja i Jemen.

Ostatecznie jednak w tym przypadku, tak jak w większości innych, pytanie o konkretny cel opiera się na fałszywych przesłankach. NSA nie potrzebuje żadnych wyraźnych przyczyn ani uzasadnienia, żeby włamywać się do prywatnych połączeń, bo zadaniem Agencji jest wszak gromadzenie wszystkiego.

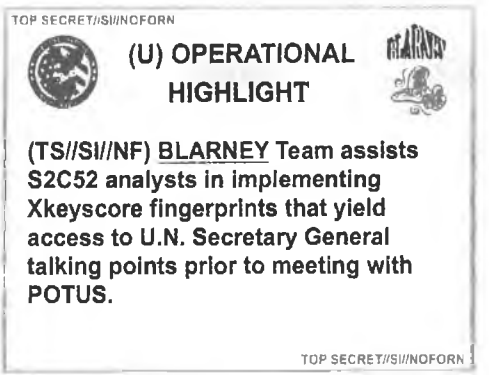
Jednakże rewelacje o szpiegowaniu zagranicznych przywódców przez NSA są mniej znaczące niż nieuprawniona, masowa inwigilacja całych populacji. Głowy państw od wieków były przedmiotem działań wywiadu, także ze strony sojuszników. Nie jest to nic niezwykłego, mimo wielkiego oburzenia wywołanego ujawnieniem, że NSA przez wiele lat podsłuchiwała rozmowy niemieckiej kanclerz Angeli Merkel prowadzone z jej prywatnego telefonu komórkowego.

Bardziej godny uwagi jest fakt, że ujawnienie, iż NSA szpiegowała setki milionów ich obywateli, w wielu krajach wywołało jedynie umiarkowane protesty ich politycznych przywódców. Prawdziwa fala oburzenia podniosła się dopiero wtedy, gdy przywódcy ci zrozumieli, że oni także byli obiektami podsłuchu.

Inwigilacja dyplomatów na skalę praktykowaną przez NSA jest i niezwykła, i godna uwagi. Stany Zjednoczone intensywnie szpiegowały na przykład międzynarodowe organizacje, takie jak ONZ, by zyskać przewagę w dyplomatycznych rozgrywkach. Typowa jest choćby notatka Sekcji Operacyjnej Źródeł Specjalnych (SSO) z kwietnia 2013 roku, która wyjaśnia użycie programów inwigilacyjnych do pozyskania danych dotyczących sekretarza generalnego ONZ przed jego spotkaniem z prezydentem Obamą.

Odnosi się ona do zespołu zajmującego się współpracą w ramach projektu BLARNEY i mówi o tym, że wspomaga on analityków S2C52, czyli Departamentu Bezpieczeństwa Międzynarodowego

NSA, w wykorzystaniu danych pozyskanych dzięki programowi NSA do wyszukiwania danych w internecie X-KEYSCORE. Dane te „dają wgląd w tematy, jakie sekretarz generalny ONZ przygotował do rozmowy z POTUS [skrót od President of the United States; prezydent Stanów Zjednoczonych – przyp. red.]".


TOP SECRET//SI//NOFORN

(U) OPERATIONAL HIGHLIGHT

(TS//SI//NF) BLARNEY Team assists S2C52 analysts in implementing Xkeyscore fingerprints that yield access to U.N. Secretary General talking points prior to meeting with POTUS.

TOP SECRET//SI//NOFORN

Wiele dokumentów wskazuje na to, że Susan Rice, ówczesna ambasador przy ONZ, a obecnie doradca prezydenta Obamy do spraw bezpieczeństwa narodowego, wielokrotnie zwracała się do NSA z prośbą o informacje dotyczące wewnętrznych dyskusji największych państw członkowskich ONZ, by poznać ich strategie negocjacyjne. Raport SSO z maja 2010 roku opisuje ten proceder w związku z rozważanym wówczas przez Narody Zjednoczone nałożeniem nowych sankcji na Iran:

Wobec zbliżającego się głosowania w ONZ na temat sankcji wobec Iranu i faktu, że kilka państw jeszcze nie podjęło decyzji [czy głosować za, czy przeciw sankcjom], ambasador Rice skierowała do NSA prośbę o SIGINT [dane wywiadowcze – przyp. red.] na temat tych państw, by na ich podstawie opracować własną strategię. Przy wymogu, by zrobić to szybko i w ramach instytucji prawa, zespół BLARNEY wciągnął do współpracy organizacje i partnerów krajowych i zagranicznych.

Podczas gdy OGC [biuro prawne NSA], SV [biuro zajmujące się dbaniem o przestrzeganie przez Agencję standardów] i TOPI [biuro zajmujące się wyznaczaniem głównych celów inwigilacji] intensywnie pracowały nad podstawami prawnymi, by szybko uzyskać cztery nowe nakazy sądu FISA dotyczące Gabonu, Ugandy, Nigerii i Bośni, Dział Operacyjny BLARNEY za kulisami zbierał dane, by stwierdzić, jakie informacje są dostępne lub mogą zostać pozyskane dzięki długoletnim kontaktom z FBI. Podczas gdy trwały prace nad zebraniem informacji o misjach [tych państw] przy ONZ i o ich ambasadach w Waszyngtonie, specjalny zespół zapewniał przyspieszony przepływ danych, wszystko po to, by informacje mogły docierać do TOPI tak szybko, jak tylko będzie to możliwe. Kilka osób, w tym jedną z zespołu prawnego i jedną z zespołu programistów, wezwano w sobotę 22 maja do wsparcia trwających non-stop przygotowań dokumentacji prawnej, by rozkazy były gotowe do podpisu przez dyrektora NSA wczesnym rankiem w poniedziałek 24 maja.

Ponieważ OGC i SV mocno naciskały na szybką wysyłkę tych czterech nakazów, w rekordowym tempie pokonały one drogę od podpisania przez dyrektora NSA do Departamentu Obrony do podpisu Sekretarza Obrony, a następnie do Departamentu Sprawiedliwości, do podpisu przez sędziego FISA. Wszystkie cztery nakazy sędzia FISA podpisał w środę 26 maja! Gdy zespół prawny BLARNEY otrzymał nakazy, natychmiast zabrał się do pracy, w ciągu jednego dnia przeprowadzając ich analizę oraz jedne „normalne" wznowienie. Analiza pięciu nakazów sądowych w jeden dzień – rekord BLARNEY! Podczas gdy zespół prawny BLARNEY pracował nad analizą nakazów sądowych, zespół kierowania dostępem BLARNEY pracował z FBI nad przekazaniem informacji o zadaniach i koordynacją współpracy z partnerami z telekomunikacji.

Podobny dokument dotyczący inwigilacji z sierpnia 2010 roku świadczy o tym, że przy okazji przygotowywania kolejnej rezolucji o sankcjach wobec Iranu USA szpiegowały ośmiu

członków Rady Bezpieczeństwa ONZ. Na liście tej znalazły się Francja, Brazylia, Japonia i Meksyk – wszystkie uważane za państwa przyjazne. Wywiad dostarczył amerykańskiemu rządowi cenne informacje na temat tego, jak kraje te zamierzają głosować, tym samym Waszyngton uzyskał przewagę w rozmowach z innymi członkami Rady Bezpieczeństwa. Dokument ten nosi znamienny tytuł: *Cichy sukces: synergia SIGINT pomaga kształtować politykę zagraniczną USA*. Dowiadujemy się z niego, że późną wiosną 2010 roku NSA i jej współpracownicy stworzyli zespół, by

dostarczać USUN [ambasador USA przy ONZ – przyp. red.] i innym klientom informacje o tym, jak członkowie Rady Bezpieczeństwa ONZ zamierzają głosować nad rezolucją w sprawie sankcji dla Iranu. Wobec tego, że Iran nadal nie respektował poprzednich rezolucji Rady Bezpieczeństwa dotyczących jego programu nuklearnego, ONZ nałożył kolejne sankcje 9 czerwca 2010 roku. Dzięki SIGINT [danym wywiadowczym] USUN był na bieżąco informowany o tym, jak będą głosować inni członkowie Rady Bezpieczeństwa.

Rezolucja została przyjęta przy dwunastu głosach za, dwóch przeciw (Brazylii i Turcji) i jednym wstrzymującym się (Liban). Według USUN SIGINT „zapewniły mi wiedzę, kiedy inni Stali Członkowie [Rady Bezpieczeństwa] mówią prawdę [...], i informowały o ich rzeczywistym stanowisku w sprawie sankcji [...], dały nam przewagę w negocjacjach [...] i dostarczyły wiedzy na temat „barier negocjacyjnych" różnych krajów.

Aby ułatwić szpiegowanie dyplomatów, NSA ustanowiła różne formy dostępu do ambasad i konsulatów swoich najbliższych sojuszników. Dokument z 10 września 2010 roku – zamieszczony tuż po usunięciu z listy niektórych państw – wymienia kraje, w których struktury dyplomatyczne na terenie USA Agencja zdołała przeniknąć; na końcu znajduje się glosariusz wyjaśniający rodzaj inwigilacji.

10 Sep 2010

CLOSE ACCESS SIGADS

CLOSE ACCESS SIGADS

All Close Access domestic collection uses the US-3136 SIGAD with a unique two-letter suffix for each target location and mission. Close Access overseas GENIE collection has been assigned the US-3137 SIGAD with a two-letter suffix.

(Note: Targets marked with an * have either been dropped or are slated to be dropped in the near future. Please check with TAO/RTD/ROS (961-1578s) regarding authorities status.)

SIGAD US-3136

SUFFIX	TARGET/COUNTRY	LOCATION	COVERTERM	MISSION
BE	Brazil/Emb	Wash,DC	KATEEL	LIFESAVER
SI	Brazil/Emb	Wash,DC	KATEEL	HIGHLANDS
VQ	Brazil/UN	New York	POCOMOKE	HIGHLANDS
HN	Brazil/UN	New York	POCOMOKE	VAGRANT
LJ	Brazil/UN	New York	POCOMOKE	LIFESAVER
YL *	Bulgaria/Emb	Wash, DC	MERCED	HIGHLANDS
QX *	Colombia/Trade Bureau	New York	BANISTER	LIFESAVER
DJ	EU/UN	New York	PERDIDO	HIGHLANDS
SS	EU/UN	New York	PERDIDO	LIFESAVER
KD	EU/Emb	Wash, DC	MAGOTHY	HIGHLANDS
IO	EU/Emb	Wash, DC	MAGOTHY	MINERALIZ
XJ	EU/Emb	Wash,DC	MAGOTHY	DROPMIRE
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX
NK *	Georgia/Emb	Wash, DC	NAVARRO	HIGHLANDS
BY *	Georgia/Emb	Wash, DC	NAVARRO	VAGRANT
RX	Greece/UN	New York	POWELL	HIGHLANDS
HB	Greece/UN	New York	POWELL	LIFESAVER
CD	Greece/Emb	Wash, DC	KLONDIKE	HIGHLANDS
PJ	Greece/Emb	Wash,DC	KLONDIKE	LIFESAVER
JN	Greece/Emb	Wash, DC	KLONDIKE	PBX
MO *	India/UN	New York	NASHUA	HIGHLANDS
QL *	India/UN	New York	NASHUA	MAGNETIC
ON *	India/UN	New York	NASHUA	VAGRANT
IS *	India/UN	New York	NASHUA	LIFESAVER
OX *	India/Emb	Wash,DC	OSAGE	LIFESAVER
CQ *	India/Emb	Wash, DC	OSAGE	HIGHLANDS
TQ *	India/Emb	Wash, DC	OSAGE	VAGRANT

CU *	India/EmbAnx	Wash, DC	OSWAYO	VAGRANT
DS *	India/EmbAnx	Wash, DC	OSWAYO	HIGHLANDS
SU *	Italy/Emb	Wash, DC	BRUNEAU	LIFESAVER
MV *	Italy/Emb	Wash, DC	HEMLOCK	HIGHLANDS
IP *	Japan/UN	New York	MULBERRY	MINERALIZ
HF *	Japan/UN	New York	MULBERRY	HIGHLANDS
BT *	Japan/UN	New York	MULBERRY	MAGNETIC
RU *	Japan/UN	New York	MULBERRY	VAGRANT
LM *	Mexico/UN	New York	ALAMITO	LIFESAVER
UX *	Slovakia/Emb	Wash, DC	FLEMING	HIGHLANDS
SA *	Slovakia/Emb	Wash, DC	FLEMING	VAGRANT
XR *	South Africa/ UN & Consulate	New York	DOBIE	HIGHLANDS
RJ *	South Africa/ UN & Consulate	New York	DOBIE	VAGRANT
YR *	South Korea/UN	New York	SULPHUR	VAGRANT
TZ *	Taiwan/TECO	New York	REQUETTE	VAGRANT
VN *	Venezuela/Emb	Wash, DC	YUKON	LIFESAVER
UR *	Venezuela/UN	New York	WESTPORT	LIFESAVER
NO *	Vietnam/UN	New York	NAVAJO	HIGHLANDS
OU *	Vietnam/UN	New York	NAVAJO	VAGRANT
GV *	Vietnam/Emb	Wash, DC	PANTHER	HIGHLANDS

SIGAD US-3137

GENERAL TERM DESCRIPTIONS

HIGHLANDS: Collection from Implants

VAGRANT: Collection of Computer Screens

MAGNETIC: Sensor Collection of Magnetic Emanations

MINERALIZE: Collection from LAN Implant

OCEAN: Optical Collection System for Raster-Based Computer Screens

LIFESAVER: Imaging of the Hard Drive

GENIE: Multi-stage operation; jumping the airgap etc.

BLACKHEART: Collection from an FBI Implant

PBX: Public Branch Exchange Switch

CRYPTO ENABLED: Collection derived from AO's efforts to enable crypto

DROPMIRE: passive collection of emanations using an antenna

CUSTOMS: Customs opportunities (not LIFESAVER)

DROPMIRE: Laser printer collection, purely proximal access (**NOT** implanted)

DEWSWEEPER USB (Universal Serial Bus): hardware host tap that provides

COVERT: link over USB link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network.

RADON: Bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-directional exploitation of

Autorzy dokumentu podkreślają, że „cele oznakowane * albo zostały zaniechane, albo mają zostać zaniechane w niedalekiej przyszłości". Przy każdym państwie znajduje się oznaczenie, czy chodzi o szpiegowanie ambasady (Emb), czy misji przy ONZ (UN) – wyjątkiem jest Tajwan, którego przedstawicielstwa na prawie całym świecie nie mają statusu ambasad, ale placówek dyplomatyczno-ekonomicznych (TECO). Inwigilacja odbywa się na kilku poziomach i przy użyciu różnych metod – na przykład HIGHLANDS to ściąganie wprost z urządzeń mających dostęp do systemów używanych przez inwigilowanych, VAGRANT to zrzuty z ekranów komputerów, MINERALIZE to pozyskiwanie danych z urządzeń lub programów monitorujących sieci LAN, LIFESAVER to szpiegowanie twardych dysków, a DROPMIRE to ściąganie informacji z drukarki laserowej, przy czym dostęp do niej uzyskuje się zdalnie, bez instalowania w niej jakichkolwiek programów czy urządzeń.

Niektóre metody szpiegowskie stosowane przez NSA służą naraz wielu rodzajom wywiadu. Pozwalają pozyskiwać informacje gospodarcze, dyplomatyczne, dotyczące kwestii bezpieczeństwa i budowania ogólnej, globalnej przewagi – i te właśnie w repertuarze Agencji należą do najbardziej inwazyjnych i zakłamanych. Przez wiele lat rząd amerykański ostrzegał świat, że chińskie routery i inny sprzęt internetowy stanowi „zagrożenie", ponieważ ma wbudowane ukryte urządzenia służące inwigilacji. Daje to władzom w Pekinie możliwość szpiegowania każdego, kto ich używa. Dokumenty NSA ujawniają jednak, że Amerykanie prowadzą dokładnie takie same działania, o jakie oskarżali Chińczyków.

Oskarżenia USA przeciwko chińskim producentom sprzętu komputerowego nie słabną. Przedstawiony w 2012 roku raport Komisji Wywiadu Izby Reprezentantów, kierowanej przez Mike'a Rogersa, stwierdzał, że dwóch największych chińskich

producentów sprzętu telekomunikacyjnego, Huawei i ZTE, „być może narusza prawo Stanów Zjednoczonych" i „nie stosuje się do prawnych regulacji obowiązujących w Stanach Zjednoczonych ani do międzynarodowych standardów postępowania w biznesie". Dlatego komisja zaleciła, by „Stany Zjednoczone nieufnie podchodziły do penetracji amerykańskiego rynku przez chińskie firmy telekomunikacyjne".

Komisja Rogersa wyraziła obawę, że firmy te umożliwiają chińskiemu rządowi inwigilację w Stanach, choć przyznała, że nie dysponuje żadnymi konkretnymi dowodami, by wbudowywały one w swoje routery czy inne urządzenia elementy służące podsłuchowi elektronicznemu. Niemniej jednak twierdziła, że firmy te nie chcą współpracować, i zachęcała podmioty amerykańskie, by nie kupowały ich produktów:

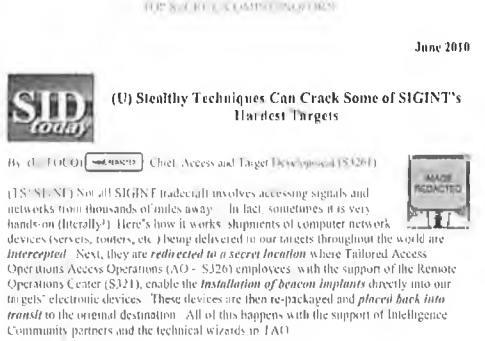
Zdecydowanie zachęcamy jednostki z sektora prywatnego w Stanach Zjednoczonych, by rozważyły dalekosiężne ryzyko dla bezpieczeństwa, związane z prowadzeniem interesów z ZTE i Huawei w dziedzinie zakupu sprzętu i usług. Amerykańskich dostawców usług sieciowych i systemów zachęca się do znalezienia innych kontrahentów handlowych. Dostępne tajne i jawne informacje wskazują, że nie można wierzyć, iż Huawei i ZTE są wolne od wpływów obcego państwa; stanowią zatem zagrożenie dla bezpieczeństwa USA i naszych systemów.

Oskarżenia tak się nasiliły, że w listopadzie 2013 roku Ren Zhengfei, 69-letni założyciel i dyrektor Huawei, ogłosił, że firma wycofuje się z amerykańskiego rynku. Jak podał magazyn „Foreign Policy", Zhengfei stwierdził: „«Jeśli Huawei znalazło się w centrum stosunków amerykańsko-chińskich» i powoduje problemy, to [obecność w USA] «nie jest tego warta»".

O ile jednak amerykańskie firmy otrzymały ostrzeżenie co do rzekomo niezasługujących na zaufanie chińskich routerów, firmy

zagraniczne powinny wystrzegać się tych, które produkowane są w Ameryce. Raport przygotowany w czerwcu 2010 roku przez Wydział Dostępu i Rozwoju NSA jest szokująco szczery. Agencja stale otrzymuje lub przechwytuje routery, serwery i pozostały sprzęt sieciowy eksportowany z USA, zanim zostanie on wysłany do zagranicznych odbiorców. Umieszcza w nim wówczas niejawne narzędzia inwigilacji, przepakowuje sprzęt z fabrycznymi pieczęciami i przesyła dalej. NSA zyskuje w ten sposób dostęp do sieci na całym świecie i wszystkich jej użytkowników:

Nie wszystkie sposoby pozyskiwania SIGINT polegają na uzyskiwaniu dostępu do sygnałów i sieci odległych o tysiące mil... Co więcej, część z nich jest bardzo poręczna (dosłownie!). Oto, jak to działa: przechwytywane są transporty sprzętu [do budowania] sieci komputerowych (serwery, routery itd.) wysyłane do naszych celów na całym świecie. Następnie kieruje się je do tajnego ośrodka, gdzie pracownicy Działu Operacji Dostępu Dostosowanego (TAO)/Operacji Dostępu (AO-S326) przy wsparciu Centrum Operacji Zdalnych (S321) umożliwiają instalację urządzeń i programów szpiegujących bezpośrednio w sprzęcie elektronicznym przeznaczonym dla naszych celów. Sprzęt ten jest następnie przepakowywany i umieszczony w przesyłce adresowanej do pierwotnego adresata. Wszystko to dzieje się przy wsparciu partnerów ze Wspólnoty Wywiadu i technicznych speców z TAO.



June 2010

SID Today

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By [redacted] Chief, Access and Target Development (S326)

IMAGE REDACTED

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away. In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations Access Operations (AO - S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

Na koniec podłączane do sieci urządzenie łączy się z infrastrukturą NSA, co Agencja opisuje w kolejnym slajdzie:

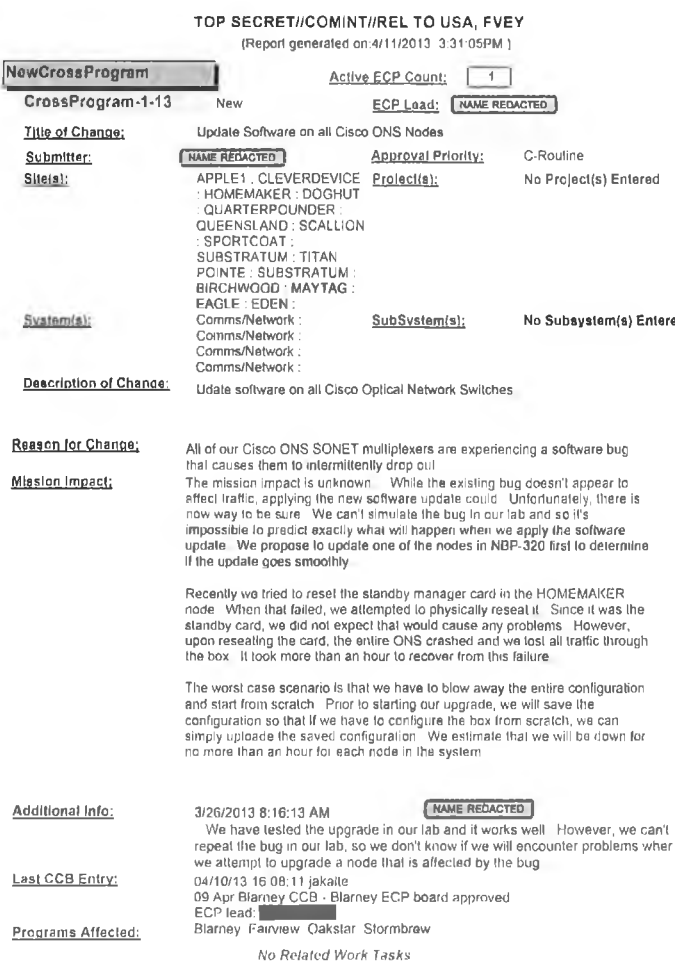
W jednym z niedawnych przypadków jedno z urządzeń zainstalowanych w ramach operacji implementowania połączyło się z tajną infrastrukturą NSA po kilku miesiącach. To połączenie zapewniło nam dostęp [umożliwiający] dalsze wykorzystanie urządzenia i przegląd sieci.

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Agencja przechwytuje między innymi routery i serwery produkowane przez firmę Cisco i majstruje przy nich, by skierować duże ilości ruchu w internecie do serwerów NSA. W dokumentach nie ma żadnych dowodów, by Cisco było tego świadome ani by akceptowało ten proceder. W kwietniu 2013 roku Agencja natrafiła na techniczne problemy w przechwyconych switchach sieciowych (to urządzenie łączące segmenty sieci komputerowej). Wpłynęło to na funkcjonowanie programów BLARNEY, FAIRVIEW, OAKSTAR i STORMBREW (dokument na następnej stronie).



TOP SECRET//COMINT//REL TO USA, FVEY

(Report generated on:4/11/2013 3:31:05PM)

NewCrossProgram — Active ECP Count: 1

CrossProgram-1-13 — New — ECP Lead: NAME REDACTED

Title of Change: Update Software on all Cisco ONS Nodes

Submitter: NAME REDACTED — Approval Priority: C-Routine

Site(s): APPLE1 : CLEVERDEVICE : HOMEMAKER : DOGHUT : QUARTERPOUNDER : QUEENSLAND : SCALLION : SPORTCOAT : SUBSTRATUM : TITAN POINTE : SUBSTRATUM : BIRCHWOOD : MAYTAG : EAGLE : EDEN : — Project(s): No Project(s) Entered

System(s): Comms/Network : Comms/Network : Comms/Network : Comms/Network : — SubSystem(s): No Subsystem(s) Entere

Description of Change: Udate software on all Cisco Optical Network Switches

Reason for Change: All of our Cisco ONS SONET multiplexers are experiencing a software bug that causes them to intermittently drop out

Mission Impact: The mission impact is unknown. While the existing bug doesn't appear to affect traffic, applying the new software update could. Unfortunately, there is now way to be sure. We can't simulate the bug in our lab and so it's impossible to predict exactly what will happen when we apply the software update. We propose to update one of the nodes in NBP-320 first to determine if the update goes smoothly.

Recently we tried to reset the standby manager card in the HOMEMAKER node. When that failed, we attempted to physically reseat it. Since it was the standby card, we did not expect that would cause any problems. However, upon reseating the card, the entire ONS crashed and we lost all traffic through the box. It took more than an hour to recover from this failure.

The worst case scenario is that we have to blow away the entire configuration and start from scratch. Prior to starting our upgrade, we will save the configuration so that if we have to configure the box from scratch, we can simply uploade the saved configuration. We estimate that we will be down for no more than an hour for each node in the system.

Additional Info: 3/26/2013 8:16:13 AM NAME REDACTED
We have tested the upgrade in our lab and it works well. However, we can't repeat the bug in our lab, so we don't know if we will encounter problems wher we attempt to upgrade a node that is affected by the bug.

Last CCB Entry: 04/10/13 16:08:11 jakaite
09 Apr Blarney CCB - Blarney ECP board approved
ECP lead: [redacted]

Programs Affected: Blarney Fairview Oakstar Stormbrew

No Related Work Tasks

Całkiem możliwe, że firmy chińskie umieszczają w swych produktach sieciowych mechanizmy inwigilacji. Stany Zjednoczone jednak z całą pewnością robią to samo.

Być może twierdząc, że chińskim urządzeniom nie można ufać, rząd USA pragnie ostrzec świat przed potencjalną chińską inwigilacją. Równie dobrze może jednak chodzić o niedopuszczenie, by urządzenia chińskie zastąpiły amerykańskie,

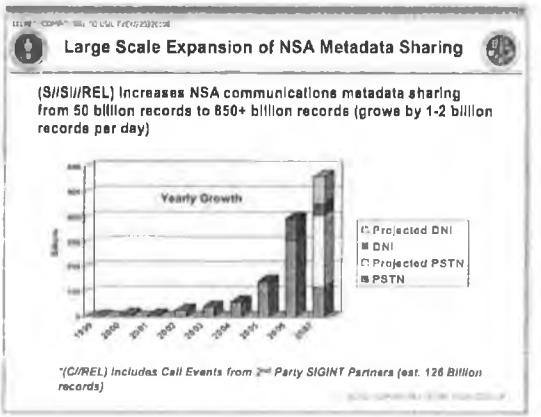
bowiem zmniejszyłoby to zasięg działań NSA. Chińskie routery i serwery nie tylko oznaczają rywalizację gospodarczą, ale i konkurencję na polu inwigilacji: gdy ktoś kupuje urządzenie chińskie zamiast amerykańskiego, NSA traci istotny środek umożliwiający szpiegowanie wielu działań w sieci.

Objętość ujawnionego przez Snowdena zakresu gromadzenia informacji wprawia w osłupienie, a dążenie NSA, by pozyskiwać bez przerwy wszelkie możliwe dane, zmusiło Agencję do ekspansji. Ilość zgromadzonych przez Agencję informacji jest tak ogromna, że głównym wyzwaniem jest obecnie ich magazynowanie. Dokument NSA nazwany *Wyzwanie*, przygotowany na konferencję SigDev Sojuszu Pięciorga Oczu, zwraca uwagę właśnie na ten, kluczowy problem: „Zbiory przerastają nasze możliwości przyjmowania, przetwarzania i magazynowania ich zgodnie z »normami«, do których przywykliśmy".

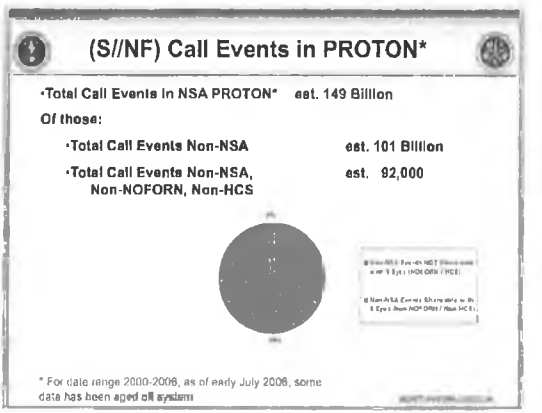
The Challenge

Collection is outpacing our ability to ingest, process and store to the "norms" to which we have become accustomed.

Sprawa sięga roku 2006, gdy Agencja rozpoczęła program nazwany *Wielka ekspansja udostępniania metadanych NSA*. Przewidywał on, że zbiory Agencji będą rosły w imponującym tempie, a rozwój ten będzie oznaczać rejestrację 1-2 miliardów więcej połączeń telefonicznych każdego dnia. Ilustruje to poniższy wykres, który pokazuje przyrost gromadzonych metadanych od 1999 do 2007 roku.



W maju 2007 roku było już wyraźnie widać, że ekspansja przyniosła owoce: liczba metadanych przechowywanych przez Agencję wzrosła do 150 miliardów, bez uwzględnienia e-maili i innych danych internetowych oraz po wyłączeniu tych, które NSA usunęła z powodu braku miejsca.



Po dodaniu do tego połączeń internetowych suma wszystkich przechowywanych „zdarzeń komunikacyjnych" wzrosła do niemal 1 biliona (należy odnotować, że te dane NSA zawdzięcza również innym agencjom wywiadowczym).

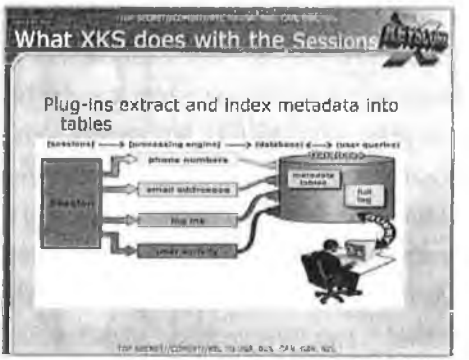
By rozwiązać problem magazynowy, Agencja rozpoczęła budowę nowego, ogromnego obiektu w Bluffdale w stanie Utah. Jego głównym przeznaczeniem jest zgromadzenie w jednym miejscu serwerów z wszystkimi danymi. Jak w 2012 roku zauważył dziennikarz James Bamford, obiekt ten zwiększy pojemność magazynów Agencji dzięki dodatkowym „czterem halom o powierzchni 25 tysięcy stóp kwadratowych [2322 metrów kwadratowych] każda, wypełnionych serwerami. Do tego dochodzi 900 tysięcy stóp kwadratowych [83 613 metrów kwadratowych] dla wsparcia technicznego i administracji". Biorąc pod uwagę wielkość budynku i fakt, że – jak mówi Bamford – „terabajt danych można teraz przechowywać na nośniku wielkości ludzkiego palca", możliwości gromadzenia danych są ogromne.

Potrzeba coraz większych obiektów wynika z inwazji Agencji na globalną aktywność internetową, wykraczającą daleko poza gromadzenie metadanych i obejmującej e-maile, wyszukiwarki i czaty. Główny program używany przez NSA do pozyskiwania, klasyfikowania i analizy tego typu danych został wprowadzony w 2007 roku i nosi nazwę X-KEYSCORE. Stanowił on radykalny krok naprzód w zakresie możliwości inwigilacji, a sama Agencja nazywa swoje dzieło „najobszerniejszym" systemem zbierania danych elektronicznych. Nie bez przyczyny.

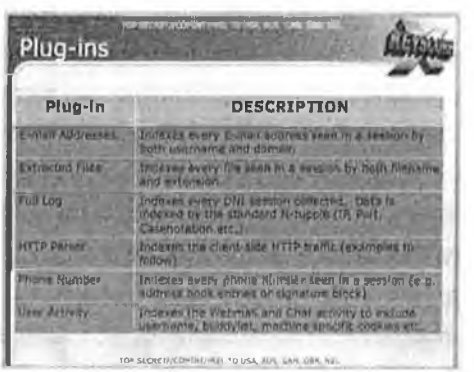
Dokument szkoleniowy przygotowany dla analityków stwierdza, że program jest w stanie kontrolować „niemal wszystko, co typowy użytkownik robi w internecie", w tym śledzić zawartość jego e-maili, historię odwiedzanych witryn internetowych i wyszukiwanie w Google'u. X-KEYSCORE pozwala nawet monitorować aktywność danej osoby online w czasie rzeczywistym, co umożliwia NSA śledzenie na bieżąco e-maili i wyszukiwań.

Poza gromadzeniem wszechstronnych danych o sieciowej aktywności setek milionów ludzi X-KEYSCORE pozwala

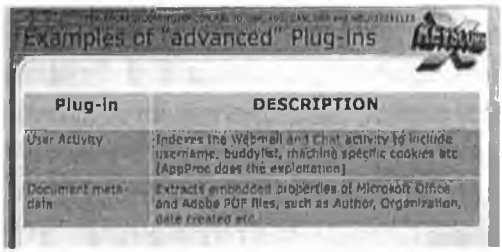
analitykom NSA przeszukiwać bazy danych według adresów e-mailowych, numerów telefonów czy innych cech identyfikacyjnych (takich jak adresy IP).



Inny slajd dotyczący X-KEYSCORE opisuje różne pola informacji, które można przeszukać dzięki „wtyczkom" programu. Obejmują one „wszystkie adresy e-mailowe widziane podczas sesji, według nazwy użytkownika i domeny", „wszystkie numery telefonów widziane podczas sesji (na przykład w książce adresowej lub w wizytówkach) i aktywność użytkownika", „aktywność poczty internetowej i czatów obejmującą nazwę użytkownika, listę kontaktów, internetowe ciasteczka itd.".



Program oferuje także możliwość szukania i odzyskiwania zaembedowanych plików z pakietu Microsoft Office i Adobe PDF, które są tworzone, wysyłane lub przyjmowane online przez użytkowników sieci.

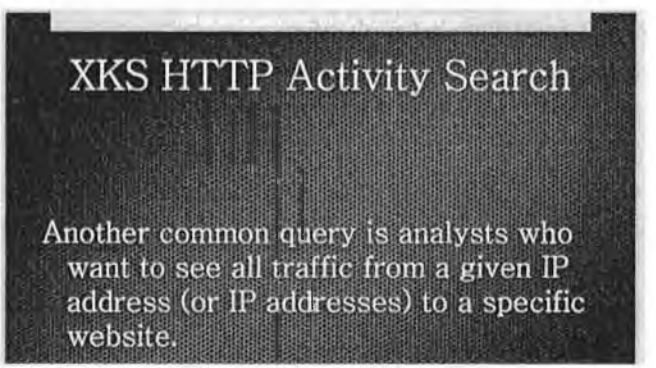


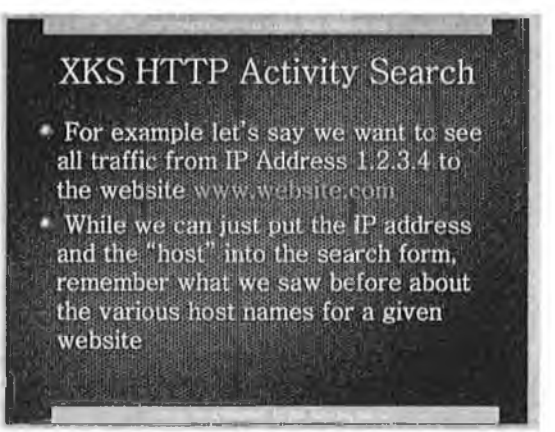
Inne slajdy NSA otwarcie mówią o nieograniczonych, globalnych ambicjach X-KEYSCORE.

Autorzy prezentacji pytają: *Dlaczego interesuje nas HTTP?*. To skrót od Hypertext Transfer Protocol, protokół przesyłania dokumentów hipertekstowych, który umożliwia publikowanie informacji w internecie. I odpowiadają: „Ponieważ niemal wszystko, co typowy użytkownik robi w internecie, wykorzystuje HTTP".

Program X-KEYSCORE umożliwia tak szczegółowe wyszukiwanie, że każdy analityk NSA nie tylko może sprawdzić, jakie witryny internetowe odwiedzała dana osoba, ale także stworzyć listę użytkowników, którzy odwiedzili konkretną witrynę.

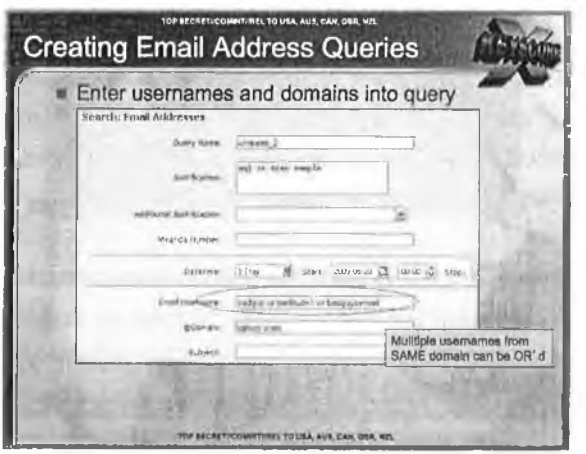
Tłumaczą to tak na slajdzie zatytułowanym *XKS wyszukuje aktywność w HTTP:*





Powiedzmy na przykład, że chcemy zobaczyć wszystkie wejścia z adresu IP 1.2.3.4 do witryny www.website.com. Wystarczy po prostu wpisać adres IP i „hosta" [chodzi o dane komputera podpiętego do sieci] do formularza wyszukiwania, ale pamiętajmy, co przedtem widzieliśmy na temat różnych nazw hostów dla danej witryny.

To niezwykłe, z jaką łatwością analitycy mogą szukać wszystkiego, czego chcą, bez żadnej kontroli. Analityk z dostępem do X-KEYSCORE nie musi zwracać się o zezwolenie do przełożonego ani nikogo innego. Wystarczy, że wypełni prosty formularz (patrz poniżej), aby uzasadnić inwigilację, a system przesyła mu żądane informacje.



W pierwszym, nagranym na wideo wywiadzie, jakiego udzielił w Hongkongu, Edward Snowden śmiało stwierdził: „Nie ruszając się zza biurka, mogłem zdobywać dane każdego, od ciebie czy twego księgowego począwszy, po sędziego federalnego, a nawet prezydenta, jeśli tylko dysponowałem ich prywatnym e-mailem". Amerykańscy politycy gwałtownie zaprzeczyli. Mike Rogers wprost oskarżył Snowdena o kłamstwo, twierdząc: „Nie miał możliwości, żeby

robić to, co twierdzi, że mógłby robić". Jednak X-KEYSCORE rzeczywiście pozwala analitykowi robić dokładnie to, co powiedział Snowden: wybrać dowolnego użytkownika jako obiekt wszechstronnego monitoringu, łącznie z treścią jego e-maili. Co więcej, program pozwala analitykowi przeszukiwać wszystkie e-maile, w których adres e-mailowy monitorowanego użytkownika pojawia się w polu „do wiadomości" albo jego nazwa wymieniona jest w treści listu.

Instrukcje wewnętrzne NSA dotyczące przeszukiwania e-maili pokazują, jak proste jest monitorowanie każdego, kogo adres już poznaliśmy. W jednej z prezentacji jej autor napisał:

Do najczęstszych zapytań należą (tak, zgadliście) zapytania według adresu e-mailowego, czyli wyszukiwanie po podanym adresie. By utworzyć zapytanie dla konkretnego adresu e-mailowego, trzeba wpisać nazwę użytkownika, uzasadnienie i zakres czasowy, a potem po prostu dodać adres/y, jakie chcecie przeszukać, oraz domenę. Będzie to wyglądać mniej więcej tak:

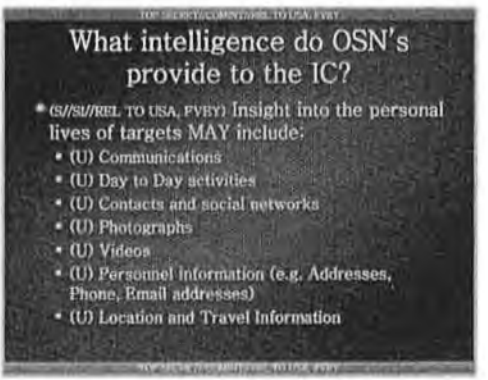
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Email Addresses Query:

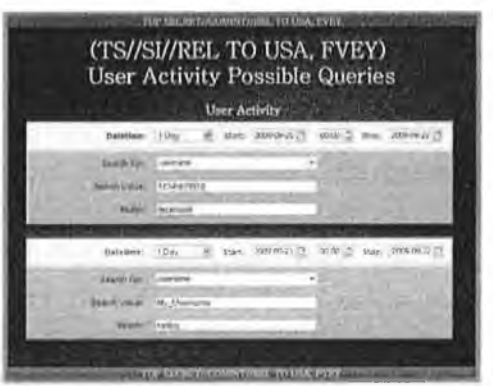
One of the most common queries is (you guessed it) an **Email Address Query** searching for an email address. To create a query for a specific email address, you have to fill in the name of the query, justify it and set a date range then you simply fill in the email address(es) you want to search on and submit.

That would look something like this...

Jedną z najcenniejszych – z punktu widzenia NSA – funkcji X-KEYSCORE jest jego zdolność śledzenia działalności w internetowych serwisach społecznościach (OSN), takich jak Facebook i Twitter, które zdaniem Agencji dostarczają bogactwa informacji i zapewniają „wgląd w życie osobiste obiektów": połączenia, codzienne działania, kontakty, zdjęcia, wideo czy informacje osobiste, takie jak telefony i adresy e-mail, wreszcie miejsce pobytu i informacje o podróżach.

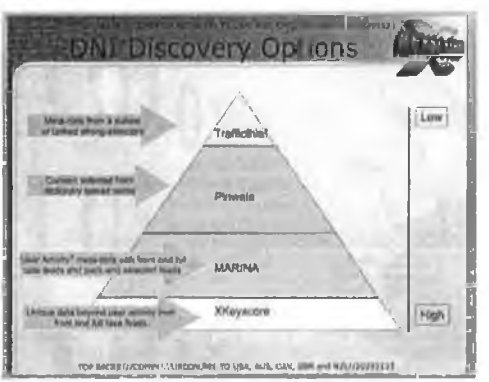


Sposób na przeszukiwanie aktywności w mediach społecznościowych jest tak samo prosty jak przeszukiwanie e-maili: analityk wprowadza nazwę użytkownika na, powiedzmy, Facebooku, do tego zakres czasowy, a X-KEYSCORE wyszukuje wszystkie informacje, w tym wiadomości, czaty i inne prywatne wpisy.



Najbardziej niezwykłą być może cechą X-KEYSCORE jest sama ilość danych, które program kataloguje i przechowuje w rozlicznych lokalizacjach na całym świecie (oczywiście pogłębiając jeszcze problemy NSA z magazynowaniem informacji). „W niektórych lokalizacjach – podaje jeden z raportów – ilość danych, które codziennie otrzymujemy (20+ terabajtów), sprawia, że przy dostępnych środkach nie możemy trzymać ich dłużej niż 24 godziny".

Jak widać na powyższym wykresie, w jednym trzydziestodniowym okresie zaczynającym się w grudniu 2012 roku liczba danych zgromadzonych przez X-KEYSCORE dla jednego tylko wydziału – SSO, czyli Centrum Operacyjnego Źródeł Specjalnych – przekraczała 41 miliardów.



Schemat na sąsiedniej stronie pokazuje, że X-KEYSCORE „przechowuje pełną zawartość przez trzy do pięciu dni, co prowadzi do «spowolnienia internetu»" – oznacza to, że „analitycy mogą wracać i odzyskiwać sesje". Następnie „treść uznaną za «interesującą» można wyciągnąć z X-KEYSCORE i przekazać do Agility lub PINWALE" – baz danych przeznaczonych do dłuższego magazynowania.

Zdolność X-KEYSCORE do przeszukiwania Facebooka i innych mediów społecznościowych zwiększają inne programy, w tym BLARNEY, co pozwala NSA monitorować „szeroki zakres danych z Facebooka drogą inwigilacji i przeszukiwania".

W dokumencie z 11 marca 2011 roku napisano, że

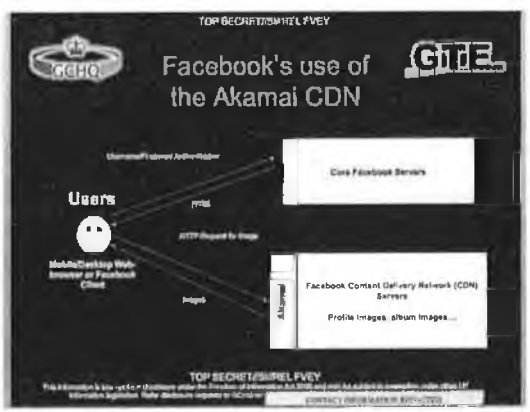
BLARNEY rozpoczął dostarczanie znacznie poprawionych i bardziej kompletnych treści z Facebooka. To duży krok naprzód w możliwościach wykorzystania Facebooka przez NSA na podstawie upoważnień FISA i FAA [FISA Amendment Acts, czyli zbiór późniejszych poprawek do ustawy FISA z 1978 roku – przyp. red.]. Działania te podjęto we współpracy z FBI sześć miesięcy temu, by usprawnić zawodny i niekompletny system gromadzenia danych z Facebooka. Dzięki aktywnej inwigilacji i przeszukiwaniu NSA ma teraz dostęp do szerokiego zakresu danych z Facebooka.

Chodzi między innymi o takie „pola treściowe" jak czaty, które można inwigilować „w sposób ciągły, podczas gdy poprzednio było to możliwe jedynie od czasu do czasu". Autorzy dokumentu podkreślają, że część treści „będzie całkiem nowa, między innymi treści wideo. Te nowe możliwości gromadzenia danych z Facebooka zapewnią solidne SIGINT [dotyczące] naszych obiektów – od miejsca lokalizacji na podstawie adresów IP i identyfikatora użytkownika po dostęp do wszystkich jego prywatnych wiadomości i informacji profilowych. Liczne komórki w całym NSA współpracowały, by zapewnić udany dostęp do tych danych".

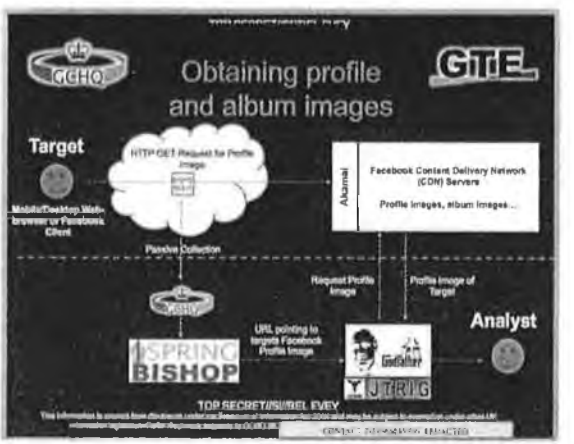
Także należący do brytyjskiego GCHQ oddział Wykorzystania Telekomunikacji Globalnej (Global Telecommunications Exploitation, GTE) przeznaczył na ten cel znaczne środki, co przedstawiono w 2011 roku na dorocznej konferencji Sojuszu Pięciorga Oczu.

GCHQ podkreśla, że Facebook to „bardzo bogate źródło informacji o obiektach: danych osobistych, sposobie życia czy znajomościach. Brytyjski wywiad elektroniczny zwrócił szczególną

uwagę na luki w zabezpieczeniach kont na Facebooku i na pozyskiwanie danych, które użytkownicy tego serwisu starają się chronić. Jak wyjaśniają autorzy jednego ze slajdów, „wiele obiektów na Facebooku blokuje swoje profile, nie można więc przeglądać wszystkich ich informacji...", ale jest „możliwość dotarcia do tych danych przez wykorzystanie wrodzonych słabości w modelu zabezpieczeń Facebooka".



GCHQ znalazło luki szczególnie w systemie służącym do przechowywania zdjęć. Okazało się, że można je wykorzystać, aby dotrzeć do profili użytkowników.



Wychodząc poza media społecznościowe, NSA i GCHQ nieustannie szukają wszelkich luk w sieci inwigilacji, wszelkich typów połączeń, które pozostają poza ich zasięgiem. Następnie opracowują programy umożliwiające objęcie ich wnikliwą obserwacją. Kwestię tę ilustruje jeden pozornie mało znaczący program.

I NSA, i GCHQ dręczyła chęć monitorowania połączeń internetowych i telefonicznych mających miejsce w trakcie komercyjnych lotów. Ponieważ połączenia te przechodzą przez niezależne systemy satelitarne, niezwykle trudno je wychwycić. Sam pomysł,

że jest takie miejsce na Ziemi, gdzie ktoś może w niewykrywalny sposób przez kilka godzin lotu korzystać z internetu w telefonie, dla agencji wywiadu jest nie do zniesienia. Dlatego też przeznaczono znaczne środki na rozwój systemów przechwytujących połączenia dokonywane w trakcie rejsów lotniczych.

Na konferencji Sojuszu Pięciorga Oczu w 2012 roku GCHQ przedstawiło program przechwytywania, nazwany *Thieving* Magpie (Sroka Złodziejka), wymierzony w coraz szerzej oferowaną możliwość korzystania z telefonów komórkowych na pokładzie samolotów.

Brytyjski wywiad proponuje, by monitorować korzystanie z sieci GSM/GPRS, tłumacząc, że „wiele linii lotniczych oferuje na pokładzie usługi telefonii komórkowej, szczególnie na długich trasach i w klasie biznes (lista się wydłuża)". I dodaje, że „na razie British Airways ogranicza usługę do przesyłu danych i SMS-ów – bez połączeń głosowych".

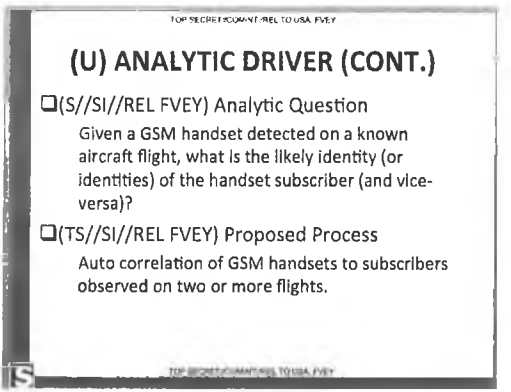
GCHQ zaproponował opracowanie systemu, który miałby w tej sferze pełen „globalny zasięg".

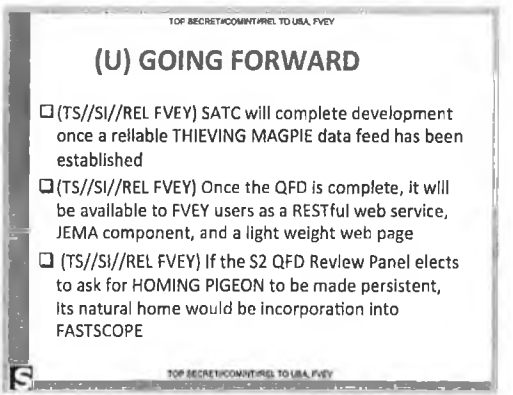
Brytyjczycy tłumaczą: „Połączenia są «odsyłane» do sieci globalnych przez terminale satelity Inmarsat BGAN [globalna łączność satelitarna oferowana przez brytyjską firmę Inmarsat]. Jeśli lot przebiega w objętym przez Inmarsat regionie Europy, Bliskiego Wschodu lub Afryki (EMEA), powinniśmy mieć kompletny dostęp (łącznie z treścią) przez Project SOUTHWINDS. Globalny zasięg przez SOUTHWINDS planowany jest w przyszłym roku".

Zaawansowane są również prace mające zapewnić możliwość podsłuchiwania niektórych urządzeń bezpośrednio na pokładzie samolotów.

Ze slajdów przedstawionych przez GCHQ wynika, że można to robić na przykład w przypadku telefonów Blackberry (chodzi o odczyt PIN-ów i związanych z nimi adresów e-mailowych). W dodatku „podczas konkretnych lotów w niedalekiej przyszłości na pokładach będzie można śledzić wybrane cele prawie non stop, co z wyprzedzeniem umożliwi sprowadzenie na miejsce zespołów inwigilujących lub aresztujących". A „jeśli używają danych, możemy także odzyskać adresy e-mailowe, ID na Facebooku, adresy w Skypie itd.". Dalej Brytyjczycy przyznają, że na razie „konkretne samoloty można śledzić podczas lotu w przybliżeniu co 2 minuty".

Podobny dokument NSA, przedstawiony na tej samej konferencji i zatytułowany *Homing Pigeon* (*Gołąb Pocztowy*), także opisuje starania, by monitorować połączenia podczas lotu. Program Agencji miał być skoordynowany z GCHQ, a cały system udostępniony członkom Sojuszu Pięciorga Oczu.





Pada w nim pytanie: „Jeśli podczas znanego połączenia lotniczego wykryjemy telefon GSM, jak poznamy tożsamość (lub tożsamości) abonenta telefonu (i vice versa)?". Odpowiedź brzmi tak: „proponowany proces" to „autodopasowanie telefonów GSM do abonentów zaobserwowanych podczas dwóch lub więcej lotów".

W niektórych działach NSA z godną uwagi szczerością mówi się o prawdziwym celu budowania tak potężnego tajnego systemu inwigilacji. Prezentacja w PowerPoincie przygotowana dla grupy funkcjonariuszy Agencji dyskutujących o perspektywie ustanowienia międzynarodowych standardów kontroli nad internetem pozwala wyrobić sobie pogląd na ten temat. Autorem prezentacji jest „NSA/SIGINT krajowy oficer wywiadu (SINIO) do spraw nauki i technologii", według jego własnego określenia „dobrze wyszkolony naukowiec i haker".

Już w tytule prezentacji autor niczego nie owija w bawełnę: *Rola interesów narodowych, pieniędzy i ego*. Jego zdaniem to owe trzy czynniki są główną przyczyną, dla której USA dążą do zachowania globalnej dominacji na polu inwigilacji.

Dokument jest bardzo bezpośredni: „Och, jasne... Połącz Pieniądze, Interes Narodowy i Ego, a będziesz mówić o kształtowaniu świata do potęgi. Jakie państwo nie chce uczynić świata lepszym miejscem... dla siebie?".

Autor prezentacji zauważa, że panowanie USA nad internetem i systemem inwigilacji dało krajowi znaczną władzę i wpływy, a także przyniosło wielkie zyski.

Jakie jest zagrożenie? Bądźmy szczerzy – świat zachodni (a USA w szczególności) zyskał wpływy i dużo zarobił na tym, że na początku określił standardy internetu. To przede wszystkim USA nadały kształt dzisiejszej sieci. Efektem jest masowy eksport amerykańskiej kultury, a także technologii. Amerykańskie przedsiębiorstwa zarobiły dzięki temu dużo pieniędzy.

Zyski i władza nieuchronnie przyniosły korzyści także samemu przemysłowi inwigilacji – co stanowi kolejną przesłankę do jego ciągłej ekspansji. Po 11 września przeznaczano na to coraz więcej środków. Większość z nich została przeniesiona z publicznych funduszy (czyli od amerykańskich podatników) do prywatnych korporacji działających w dziedzinach inwigilacji i obrony.

Takie firmy jak Booz Allen Hamilton i AT&T zatrudniają gromady byłych wysokich urzędników rządowych, natomiast gromady obecnych wysokich urzędników w resorcie obrony to byli (i prawdopodobnie przyszli) pracownicy tych korporacji. Nieustannie rozrastająca się i prowadzona przez państwo inwigilacja gwarantuje, że fundusze płyną, a drzwi między rządem a biznesem pozostają dobrze naoliwione. Gwarantuje to także, że NSA i związane z nią agencje zachowują znaczenie i wpływy w Waszyngtonie.

W miarę jak rosła skala i ambicje przemysłu inwigilacji, wyolbrzymiano rozmiary i zagrożenia ze strony rzekomego przeciwnika. Rozliczne zagrożenia podobno stojące przed Stanami Zjednoczonymi, wymienione przez NSA w dokumencie zatytułowanym *Agencja Bezpieczeństwa Narodowego: informacje przeglądowe* zawierają kilka przewidywalnych punktów: „hakerzy", „elementy kryminalne" i „terroryści". Warto jednak zauważyć, że do tej kategorii zaliczono także *technologie*, w tym „internet" jako taki.

Od dawna głosi się, że globalna sieć to bezprecedensowy instrument demokratyzacji i liberalizacji, a nawet emancypacji. Jednak w oczach amerykańskiego rządu internet i znaczna część pozostałej technologii, służącej międzyludzkiej komunikacji, stanowią zagrożenie dla potęgi Ameryki. Stosując te kategorie, ambicja NSA, by „gromadzić wszystko", nabiera sensu. To ważne, żeby Agencja monitorowała wszystkie części internetu i wszystkie inne sposoby łączności, by nic nie mogło ujść kontroli rządu USA.

W ostatecznym rozrachunku wszechobecny system inwigilacji pozwala Stanom Zjednoczonym – poza manipulacjami

dyplomatycznymi, przewagą ekonomiczną i przemysłową – gromadzić wiedzę, ta zaś przekłada się na władzę i nadzór. Gdy USA będą wiedzieć wszystko, co każdy z nas robi, mówi, myśli i planuje – a dotyczy to zarówno własnych obywateli, jak i obcych narodów, wielkich korporacji, przywódców obcych rządów – to jego władza nad tym wszystkim znacząco wzrośnie. Jest to coraz prawdziwsze stwierdzenie, bowiem rząd działa ukryty za rosnącym w górę murem tajemnicy. Mamy wtedy do czynienia z efektem lustra weneckiego: rząd Stanów Zjednoczonych widzi, co robią wszyscy ludzie na świecie, łącznie z jego własnymi obywatelami, ale nikt nie widzi, co robi rząd Stanów Zjednoczonych. Ta krańcowa nierównowaga prowadzi do najbardziej niebezpiecznej sytuacji dla ludzkości: nieograniczonej władzy bez przejrzystości czy odpowiedzialności.

To, co ujawnił Edward Snowden, osłabiło tę groźną nierównowagę, rzucając światło na system elektronicznych podsłuchów i sposób jego funkcjonowania. Po raz pierwszy ludzie na całym świecie mogli poznać prawdziwy zakres możliwości systemów inwigilacji stworzonych przeciwko nim. Informacje te wywołały intensywną i wciąż trwającą ogólnoświatową debatę właśnie dlatego, że mówią o poważnym zagrożeniu dla demokracji. Dały także początek propozycjom reformy, globalnej dyskusji na temat znaczenia wolności internetu i prywatności w epoce cyfrowej, a także skłoniły do zadania sobie zasadniczego pytania: co nieograniczona inwigilacja oznacza dla nas jako jednostek, w naszym własnym życiu.

ROZDZIAŁ 4

SZKODLIWE SKUTKI INWIGILACJI

Rządy na całym świecie robią, co mogą, by oduczyć obywateli cenienia swojej prywatności. Litania do znudzenia powtarzanych banałów przekonała ludzi, że powinni tolerować poważne naruszenia swojej sfery prywatnej; te uzasadnienia okazały się tak skuteczne, że władze gromadzą wielkie ilości danych o tym, co obywatele mówią, czytają, kupują i robią – i z kim – a oni tylko temu przyklaskują.

W ataku na prywatność władze państwowe wspierane są przez licznych magnatów internetu – nieodzownych partnerów każdego rządu w inwigilacji. Na postawiony w wywiadzie dla CNBC w 2009 roku zarzut, że jego firma przekazuje dane użytkowników, szef Google'a Eric Schmidt odpowiedział haniebnie: „Jeśli robisz coś, o czym nie chcesz, żeby inni wiedzieli, to może przede wszystkim nie powinieneś tego robić". Założyciel i dyrektor Facebooka Mark Zuckerberg z równym lekceważeniem stwierdził w wywiadzie w 2010 roku, że „ludzie dziś bez większych problemów nie tylko dzielą się większą liczbą informacji różnego rodzaju, ale czynią to bardziej otwarcie i z większą liczbą osób". Prywatność w epoce cyfrowej przestała być „normą społeczną" – oznajmił. Taka teoria doskonale służy interesom firmy internetowej wykorzystującej osobiste dane użytkowników.

Jednak prywatność wciąż ma znaczenie, co wyraźnie wynika choćby z faktu, że nawet ci, którzy podważają jej sens, którzy

ogłaszają, że jest martwa lub zbędna, sami nie wierzą w to, co mówią. Rzecznicy zaniku prywatności bardzo się starają zachować kontrolę nad stopniem jawności własnych danych. Sam rząd USA stosuje daleko posunięte środki, by chronić swoje działania przed upublicznieniem i wznosić wokół nich coraz wyższy mur tajemniczości. Raport ACLU z 2011 roku twierdzi, że „obecnie znaczna część działań rządu toczy się niejawnie". Ten tajemniczy świat jest tak pełen sekretów, „tak wielki, tak niesprawny – napisał «Washington Post» – że nikt nie wie, ile kosztuje, ilu ludzi zatrudnia, ile prowadzi programów ani dokładnie ile agencji wykonuje tę samą robotę".

Także internetowi magnaci, którzy ochoczo lekceważą naszą prywatność, zażarcie strzegą własnej. Google przestał rozmawiać z reporterami z CNET, portalu wiadomości technologicznych, gdy ten opublikował osobiste dane Erica Schmidta – w tym wysokość jego pensji, datków na kampanię i adres, (to informacje publiczne uzyskane z pomocą Google'a) – by uwydatnić niebezpieczeństwo ingerencji ze strony jego firmy.

Tymczasem Mark Zuckerberg za 30 milionów dolarów kupił cztery domy przylegające do jego posiadłości w Palo Alto, by zapewnić sobie prywatność. Jak to ujął CNET: „Twoje życie osobiste nosi teraz nazwę «dane Facebooka». Życie osobiste jego dyrektora nosi nazwę «pilnuj swojego nosa»".

Ta sama sprzeczność występuje w przypadku wielu zwykłych obywateli, którzy głośno lekceważą wartość prywatności, ale równocześnie zabezpieczają hasłami dostępu swoją pocztę elektroniczną i konta w mediach społecznościowych. Drzwi łazienki zamykają na haczyk, koperty z listami zaklejają. Gdy nikt nie widzi, zachowują się w sposób, w jaki nigdy nie zachowaliby się publicznie. Przyjaciołom, psychologom i prawnikom mówią rzeczy, których nie chcieliby ujawnić nikomu innemu. Zamieszczają w internecie wypowiedzi, pod którymi nie chcieliby się podpisać imieniem i nazwiskiem.

Wielu zwolenników inwigilacji, z którymi rozmawiałem od czasu, gdy Snowden ujawnił cały problem, popierało pogląd Erica Schmidta, że prywatność jest dla tych, którzy mają coś do ukrycia. Żaden z nich jednak nie chciał podać mi hasła do swojej poczty internetowej ani pozwolić na zainstalowanie kamery wideo w domu.

Gdy przewodnicząca senackiej Komisji Wywiadu Dianne Feinstein twierdziła, że zbieranie metadanych przez NSA nie oznacza inwigilacji – ponieważ nie zawiera treści przekazów – protestujący internauci zażądali, by poparła słowa czynem: czy pani senator zgodzi się co miesiąc publikować pełną listę osób, do których dzwoniła i pisała, podawać długość rozmowy telefonicznej i miejsca, gdzie znajdowała się i ona, i jej rozmówcy? Oczywiście wiadomo było, że nie wyrazi zgody, właśnie dlatego, że takie informacje bardzo wiele ujawniają i publikowanie ich rzeczywiście stanowiłoby naruszenie sfery prywatnej.

Nie chodzi tu o hipokryzję tych, którzy pogardliwie odnoszą się do wartości sfery prywatnej, a równocześnie pilnie strzegą własnej – choć jest ona dość uderzająca. Chodzi natomiast o to, że cechujące wszystkich pragnienie prywatności to integralny – a nie drugorzędny – element tego, co oznacza być człowiekiem. Wszyscy instynktownie rozumiemy, że to właśnie w sferze prywatnej możemy działać, myśleć, mówić, pisać, eksperymentować i wybierać, jacy jesteśmy naprawdę, z dala od osądzających oczu innych. Prywatność to podstawowy warunek bycia wolnym człowiekiem.

Najbardziej być może znaną definicję tego, co oznacza prywatność i dlaczego jest ona tak powszechnie i wysoce pożądana, sformułował sędzia Sądu Najwyższego USA Louis Brandeis w sprawie Olmstead przeciw USA z 1928 roku: „Prawo do tego, by inni zostawili nas w spokoju, jest ze wszystkich praw najwszechstronniejsze i najwyżej cenione przez wolny naród". Wartość prywatności, napisał, „ma znacznie szerszy zakres"

niż zwykłe swobody obywatelskie. Jego zdaniem prywatność jest prawem fundamentalnym:

Twórcy naszej Konstytucji postanowili zapewnić warunki sprzyjające dążeniu do szczęścia. Uznali znaczenie duchowej natury człowieka, jego uczuć i myśli. Wiedzieli, że nie wszystkie życiowe cierpienia, przyjemności i satysfakcje wynikają z rzeczy materialnych. Pragnęli chronić przekonania, myśli, uczucia i doznania Amerykanów. Przyznali im prawo do tego, by rząd zostawił ich w spokoju.

Zanim jeszcze Brandeisa mianowano sędzią Sądu Najwyższego, dał się poznać jako gorący zwolennik prawa do prywatności. Razem z prawnikiem Samuelem Warrenem napisał wpływowy artykuł *Prawo do prywatności*, opublikowany w 1890 roku w „Harvard Law Review". Twierdził w nim, że odebranie komuś prywatności to przestępstwo całkiem innej natury niż kradzież własności materialnej. „Zasada chroniąca prywatne pisma i wszelkie inne wytwory człowieka nie przed kradzieżą i fizycznym przywłaszczeniem, ale przed ogłoszeniem w dowolnej formie w rzeczywistości nie odnosi się do własności prywatnej, tylko do nienaruszalności osobistej".

Prywatność jest niezbędna dla wolności i szczęścia człowieka z przyczyn, o których rzadko się mówi, ale które większość ludzi instynktownie rozumie; zresztą świadczy o tym fakt, że są gotowi na wiele, byle tylko własną prywatność chronić. Przede wszystkim ludzie zachowują się zupełnie inaczej, gdy wiedzą, że ktoś ich obserwuje. Starają się wtedy postępować tak, jak się od nich oczekuje, bo chcą uniknąć wstydu i potępienia. Dlatego też przestrzegają społecznych konwencji, nie przekraczają wyznaczonych granic i unikają działań, które mogłyby być postrzegane jako odbiegające od normy.

Zakres wyborów rozważanych przez osoby przekonane, że inni na nie patrzą, jest zatem znacznie węższy niż zakres zachowań w sferze prywatnej. Odmowa prywatności poważnie ogranicza więc wolność wyboru.

Kilka lat temu uczestniczyłem w bat micwie córki przyjaciela. Podczas uroczystości rabin podkreślał, że dziewczyna powinna „w każdej chwili pamiętać, że jest obserwowana i osądzana". Powiedział jej, że Bóg zawsze wie, co człowiek robi, zna każdy wybór, każde działanie, a nawet każdą, choćby najtajniejszą myśl. „Nigdy nie jesteś sama" – stwierdził, co oznaczało, że powinna zawsze postępować zgodnie z wolą Boga.

Rabin ujął to jasno: skoro nie sposób uniknąć czujnych oczu najwyższej władzy, nie ma się wyboru – trzeba stosować się do zasad narzucanych przez tę władzę. Nie można nawet rozważać ruszenia własną drogą poza tymi zasadami: kto wierzy, że jest zawsze obserwowany i osądzany, w gruncie rzeczy nie jest wolną jednostką.

Na tej istotnej prawdzie opiera się wszelka władza oparta na dominacji – polityczna, religijna, społeczna, rodzicielska – i wykorzystuje ją jako główne narzędzie narzucania ortodoksji, zmuszania do wierności i tłumienia protestów. To w interesie owej władzy leży przekonanie wszystkich, że nic, co zrobią poddani, nie umknie oczom władzy. Pozbawienie prywatności zdusi wszelką pokusę odejścia od norm i zasad znacznie skuteczniej niż siły policyjne.

Zburzenie sfery prywatnej pociąga za sobą utratę wielu atrybutów zazwyczaj kojarzonych z jakością życia. Większość ludzi wie z doświadczenia, że prywatność umożliwia odrzucenie ograniczeń. Z drugiej strony wszyscy przeżyliśmy sytuację, w której sądziliśmy, że jesteśmy sami, zachowywaliśmy się więc w sposób prywatny – tańcząc, spowiadając się, eksperymentując w dziedzinie seksu, dzieląc się spontanicznymi

pomysłami – a potem ogarniał nas wstyd i zażenowanie, gdy okazywało się, że widzieli nas inni.

Tylko wtedy, gdy wierzymy, że nikt nas nie widzi, czujemy się wolni – bezpieczni – na tyle, by eksperymentować, badać granice, wypróbowywać nowe sposoby myślenia i bycia, sprawdzać, co to znaczy być sobą. Internet okazał się tak bardzo atrakcyjny właśnie dzięki możliwości anonimowego wypowiadania się i działania. Dlatego też to w sferze prywatnej kiełkują kreatywność, odmienne zdania i kwestionowanie dominujących poglądów. Społeczeństwo, w którym każdy wie, że państwo może go obserwować – gdzie sfera prywatna praktycznie przestała istnieć – to społeczeństwo, w którym te cechy zanikają tak na poziomie wspólnotowym, jak indywidualnym.

Powszechna inwigilacja przez państwo jest zatem z natury opresyjna, nawet w tym mało prawdopodobnym przypadku, gdy mściwi urzędnicy nie wykorzystują jej na przykład do pozyskiwania prywatnych informacji o przeciwnikach politycznych. Niezależnie od tego, czy inwigilacja jest używana, czy nadużywana, jej nieuchronnym skutkiem jest ograniczenie wolności.

Przywoływanie *Roku 1984* George'a Orwella jest dość banalne, ale w obsługiwanym przez NSA inwigilującym państwie nie sposób nie słyszeć echa świata, przed jakim autor ostrzegał: oba opierają się na istnieniu systemu technologicznego zdolnego do monitorowania działań i słów każdego obywatela. Podobieństwu temu zaprzeczają zwolennicy inwigilacji – *nie zawsze* jesteśmy obserwowani, mówią – ale ten argument mija się z istotą sprawy. W *Roku 1984* obywatele niekoniecznie byli cały czas monitorowani; w gruncie rzeczy nie mieli pojęcia, czy w ogóle ktoś ich rzeczywiście obserwuje. Jednak państwo dysponowało odpowiednimi środkami, by cały czas sprawować kontrolę.

To niepewność i możliwość wszechobecnej inwigilacji sprawiała, że nikt się nie wychylał:

Teleekrany były aparatami odbiorczo-nadawczymi. Najlżejszy głos, jaki wydałby Winston, o natężeniu nieco większym niż najcichszy szept, był automatycznie przekazywany. Również jak długo znajdował się w zasięgu wizji tele-ekranu, można go było zarówno podsłuchiwać, jak i obserwować. Oczywiście nikt nie wiedział, czy w tym momencie jest śledzony, czy nie. Jak często policja myśli włącza czyjś aparat w celu obserwacji, mogło być tylko przedmiotem domysłów. Nie można było wykluczyć, że obserwowali wszystkich i o każdym czasie. W każdym razie mogli włączyć podsłuch i podgląd do każdego mieszkania, kiedy tylko chcieli.

Trzeba było żyć w przeświadczeniu – z nawykiem, który stawał się instynktem – że każde słowo czy dźwięk jest podsłuchiwane i każdy ruch (z wyjątkiem w ciemnościach) śledzony.

Nawet NSA, przy całym swoim potencjale, nie jest w stanie czytać wszystkich e-maili, słuchać wszystkich rozmów telefonicznych i śledzić działań każdej jednostki. Skuteczność systemu inwigilacji bierze się z przekonania ludzi, że to, co mówią i robią, *może* być monitorowane.

Ta zasada leżała u podstaw koncepcji Panoptykonu stworzonej przez XVIII-wiecznego brytyjskiego filozofa Jeremy'ego Benthama – projektu budowli, w której jego zdaniem można by skutecznie kontrolować ludzkie zachowania. Według opisu Benthama budynek ten miałby zastosowanie do „wszystkich instytucji, gdzie na niezbyt rozległej przestrzeni trzeba utrzymać pod nadzorem pewną liczbę osób". Główną architektoniczną innowacją Panoptykonu była wysoka centralna wieża, z której strażnicy mogli cały czas monitorować każde pomieszczenie – celę, klasę czy salę. Przebywające w tych pomieszczeniach osoby nie były jednak w stanie dostrzec,

co znajduje się w wieży, nigdy więc nie wiedziały, czy są obserwowane, czy nie.

Ponieważ żadna instytucja nie może przez cały czas obserwować wszystkich, Bentham proponował stworzyć „pozorną wszechobecność nadzorcy" w umysłach osób kontrolowanych. „Osoby nadzorowane powinny zawsze czuć się tak, jakby były pod nadzorem, a w każdym razie powinny wierzyć, że jest to bardzo prawdopodobne". W takiej sytuacji będą się zachowywać, jak gdyby ktoś je ciągle obserwował, nawet jeśli w rzeczywistości tak nie będzie. To doprowadzi do uległości, posłuszeństwa i postępowania według reguł. Bentham przewidywał, że jego projekt znajdzie zastosowanie nie tylko w więzieniach i szpitalach psychiatrycznych, ale i w innych instytucjach. Jego zdaniem takie uwarunkowanie myślenia obywateli zrewolucjonizuje zachowanie się ludzi.

W latach 70. zeszłego wieku Michel Foucault wskazał, że zasada Panoptykonu Benthama stanowi jeden z podstawowych mechanizmów współczesnego państwa. W *Słowach i rzeczach* napisał, że panoptyzm to „typ władzy stosowanej w odniesieniu do jednostek w postaci ciągłego indywidualnego nadzoru, kary i nagrody, i w postaci korekcji, czyli kształtowania i przekształcania jednostek w kategoriach pewnych norm".

W książce *Nadzorować i karać. Narodziny więzienia* Foucault wyjaśniał dalej, że wszechobecna inwigilacja nie tylko zwiększa władzę rządzących i wymusza przystosowanie się do niej, ale także skłania jednostki do internalizacji strażników. Ci, którzy wierzą, że są obserwowani, instynktownie wybiorą takie działanie, jakiego się od nich oczekuje, nie zdając sobie nawet sprawy, że to czynią. „To główny efekt Panoptykonu: wzbudzić w uwięzionym świadome i trwałe przeświadczenie o widzialności, które daje gwarancję automatycznego funkcjonowania władzy". Przy internalizacji kontroli zanika otwarte stosowanie represji, ponieważ przestają być konieczne:

„[...] władza zewnętrzna może pozbyć się nieco fizycznej ociężałości; zmierza ku niecielesności, a im bardziej zbliża się do tej granicy, tym trwalsze, głębsze, ustalone raz na zawsze i bez przerwy odnawiane są jej efekty – ustawiczna wiktoria, która unika wszelkiej konfrontacji fizycznej i gdzie wszystko przesądzone jest z góry".

Co więcej, ten model kontroli ma wielki plus: równocześnie tworzy iluzję wolności. Przymus posłuszeństwa istnieje w umyśle jednostki. Jednostki same postanawiają, że się dostosują, ze strachu, że są obserwowane. To eliminuje potrzebę wszystkich widocznych oznak przymusu, a zatem umożliwia kontrolę nad ludźmi, którzy fałszywie uważają się za wolnych.

Z tego powodu każde państwo oparte na ucisku wykorzystuje powszechną inwigilację jako jeden z najważniejszych instrumentów kontroli. Gdy zazwyczaj opanowana kanclerz Niemiec Angela Merkel dowiedziała się, że NSA od lat podsłuchuje jej rozmowy prowadzone przez prywatny telefon komórkowy, w rozmowie z prezydentem Obamą gniewnie przyrównała amerykańską inwigilację do działań Stasi, niesławnej służby bezpieczeństwa we wschodnich Niemczech. Merkel nie chodziło o to, że Stany Zjednoczone są porównywalne z reżimem komunistycznym, tylko że istotą państwa stosującego groźną inwigilację – czy to w postaci NSA, Stasi, Wielkiego Brata czy Panoptykonu – jest świadomość, iż niewidzialna władza może nas w każdym momencie obserwować.

Nietrudno zrozumieć, dlaczego władze Stanów Zjednoczonych i innych krajów Zachodu kusiło zbudowanie wszechobecnego systemu szpiegowania własnych obywateli. Pogłębiające się nierówności gospodarcze, które na skutek załamania się finansów w 2008 roku przerodziły się w pełen kryzys, spowodowały poważne wewnętrzne rozchwianie. Nawet w stosunkowo stabilnych demokracjach, takich jak Hiszpania i Grecja, doszło

do otwartych niepokojów. W 2011 roku wybuchły krótkotrwałe zamieszki w Londynie. W Stanach Zjednoczonych protesty obywatelskie organizowała i prawica (protesty Tea Party w 2008 i 2009 roku), i lewica (ruch Occupy). Badania opinii publicznej w tych krajach wykazały uderzająco wysoki poziom niezadowolenia z klasy politycznej i kierunku rozwoju społeczeństwa.

Władze, które spotykają się z niezadowoleniem, zazwyczaj mają dwie opcje: udobruchać społeczeństwo symbolicznymi ustępstwami albo wzmocnić kontrolę, by zminimalizować szkody, jakie protesty mogą przynieść ich interesom. Elity na Zachodzie wydają się uważać opcję drugą – umocnienie władzy – za lepsze, być może jedyne możliwe rozwiązanie pozwalające im chronić swoją pozycję. Odpowiedzią na ruch Occupy było zdławienie go siłą, przy użyciu gazu pieprzowego, gazu łzawiącego i procesów sądowych. W amerykańskich miastach dało się zauważyć paramilitaryzację sił policyjnych, gdy policjanci wyciągnęli broń widywaną przedtem na ulicach Bagdadu, by okiełznać legalnie zgromadzonych i przeważnie spokojnych protestujących. W tej strategii chodziło o to, by ludzie zaczęli się bać uczestnictwa w marszach i protestach, i najczęściej okazywała się ona skuteczna. W ogólniejszym sensie celem było wpojenie ludności przekonania, że taki rodzaj oporu jest nieskuteczny w starciu z potężną i nieprzeniknioną władzą establishmentu.

System wszechobecnej inwigilacji służy temu samemu, ale z jeszcze większą siłą. Samo organizowanie ruchów protestu staje się trudne, jeśli rząd śledzi wszystko, co ludzie robią. Jednak powszechna inwigilacja zabija niezgodę także w miejscu głębszym i ważniejszym: w umyśle. Jednostka uczy się wtedy myśleć jedynie w taki sposób, jakiego się od niej oczekuje i wymaga.

Historia nie pozostawia wątpliwości, że zamiarem i skutkiem inwigilacji przez państwo jest zbiorowy przymus i kontrola. Hollywoodzki scenarzysta Walter Bernstein, który w epoce

makkartyzmu znalazł się na czarnej liście i był kontrolowany przez państwo i zmuszony do pisania pod pseudonimem, by w ogóle móc pracować, opisał dynamikę autocenzury, która rodzi się z poczucia bycia obserwowanym:

Wszyscy byli ostrożni. To nie była pora na podejmowanie ryzyka [...] Byli pisarze, którzy nie znaleźli się na czarnej liście, którzy robili – nie wiem, jak byście to nazwali – „nowatorskie" rzeczy, ale nie polityczne. Trzymali się z daleka od polityki [...]. Myślę, że panowało takie ogólne przekonanie, żeby „nie nadstawiać karku".

To nie jest atmosfera, która sprzyjałaby twórczości czy pozwalała swobodnie myśleć. Zawsze istnieje niebezpieczeństwo autocenzury, powiedzenia: „Nie, tego nie spróbuję, bo wiem, że nic z tego nie będzie albo to się nie spodoba rządowi", albo czegoś w tym rodzaju.

Obserwacje Bernsteina znalazły niesamowite echo w raporcie sporządzonym przez PEN America w listopadzie 2013 roku, zatytułowanym *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self Censor (Przygnębiający efekt: inwigilacja przez NSA skłania amerykańskich pisarzy do autocenzury).* Organizacja ta przeprowadziła sondaż mający na celu zbadanie wpływu rewelacji o NSA na jej członków i stwierdziła, że wielu pisarzy „zakłada, że ich połączenia są monitorowane", wobec czego zmienia swoje zachowanie w sposób, który „ogranicza ich wolność słowa i swobodny przepływ informacji". Konkretnie zaś „24 procent specjalnie unikało niektórych tematów w rozmowach telefonicznych lub w e-mailach".

Szkodliwy kontrolny wpływ wszechobecnej inwigilacji i wynikająca z niego autocenzura znalazły potwierdzenie w rozlicznych eksperymentach socjologicznych i wykraczają daleko poza polityczny aktywizm. Liczne badania pokazują, jak ta dynamika funkcjonuje na najgłębszych poziomach osobistych i psychologicznych.

Grupa badaczy opublikowała w czasopiśmie „Evolutionary Psychology" wyniki doświadczenia, w którym respondentom przedstawiono moralnie wątpliwe działania, takie jak zatrzymanie sobie znacznej sumy pieniędzy ze znalezionego na ulicy portfela lub świadomość, że przyjaciel dodał do życiorysu nieprawdziwe informacje. Respondentów poproszono o ocenę stopnia wykroczenia. Badanie wskazało, że osoby, którym wpierw pokazano obrazy sugerujące kontrolę, takie jak duże, szeroko otwarte oczy, oceniały te działania jako bardziej „karygodne" niż te, którym pokazano obraz neutralny. Badacze stwierdzili, że nadzór zachęca osoby obserwowane do „potwierdzania poparcia dla istniejących norm społecznych", ponieważ starają się „aktywnie kształtować swoją reputację".

Wszechstronny eksperyment przeprowadzony w 1975 roku przez psychologów z Uniwersytetu Stanforda, Gregory'ego White'a i Philipa Zimbardo, zatytułowany *Szkodliwe skutki nadzoru*, starał się ocenić, czy bycie obserwowanym miało wpływ na głoszenie kontrowersyjnych opinii politycznych. Bodźcem do doświadczenia był niepokój Amerykanów z powodu kontroli ze strony rządu:

Skandal Watergate, ujawnienie podsłuchów w Białym Domu i dochodzenie Kongresu w sprawie szpiegowania przez Centralną Agencję Wywiadowczą (CIA) w kraju posłużyły do wzmocnienia rozwijającej się paranoi w amerykańskim życiu: może Wielki Brat ci się przygląda! Propozycje utworzenia krajowych banków danych, wykorzystanie helikopterów obserwacyjnych przez miejskie siły policyjne, obecność kamer w bankach i supermarketach oraz przeszukania osób i własności na lotniskach z powodów bezpieczeństwa to zaledwie niektóre oznaki, że nasze prywatne życie znalazło się pod narastającą kontrolą.

Uczestnicy badania, monitorowani w różnym stopniu, mieli przedstawić swoje poglądy na kwestię legalizacji marihuany. Okazało się, że respondenci „zagrożeni" – ci, którym powiedziano, że ich wypowiedź zostanie udostępniona policji „dla celów szkoleniowych" – w większym stopniu potępiali używanie marihuany, a mówiąc, częściej posługiwali się zaimkami w drugiej i trzeciej osobie („wy", „oni", „ludzie"). Tylko 44 procent obserwowanych osób opowiedziało się za legalizacją, w porównaniu do 77 procent w grupie „niezagrożonej". Wiele zdradza także fakt, że 31 procent osób w grupie monitorowanej spontanicznie szukało aprobaty u badaczy (na przykład pytając: „Czy tak jest w porządku?"), podczas gdy w drugiej grupie uczyniło tak tylko 7 procent respondentów. Uczestnicy „zagrożeni" cechowali się także wyraźnie wyższym poziomem niepokoju i zahamowań.

White i Zimbardo odnotowali we wnioskach, że „zagrożenie kontrolą lub istniejąca kontrola ze strony rządu może psychologicznie zahamować swobodę wypowiedzi". Dodali, że choć ich „projekt badawczy nie przewidywał możliwości «unikania zgromadzeń»", to przypuszczają, iż „niepokój wywołany perspektywą kontroli skłoniłby wiele osób do całkowitego unikania takich sytuacji", w których mogłyby być monitorowane. „Ponieważ takie założenia ogranicza jedynie ludzka wyobraźnia, a codziennie wzmacniają je rewelacje na temat inwazji w prywatność ze strony rządu i instytucji – napisali – granice między paranoicznymi urojeniami a uzasadnioną ostrożnością stają się wątłe".

To prawda, że nadzór może czasami wspierać takie zachowanie, jakie niektórzy uważają za pożądane. W pewnym badaniu stwierdzono, że liczba burd na szwedzkich stadionach piłkarskich – rzucanie butelek i rac na boisko – spadła o 65 procent po wprowadzeniu kamer bezpieczeństwa. W publicznie dostępnej literaturze na temat konieczności mycia rąk wielokrotnie

potwierdzono, że prawdopodobieństwo mycia rąk znacznie wzrasta, jeśli ktoś stoi obok.

W sumie jednak skutkiem obserwacji jest poważne ograniczenie osobistych wyborów. Nawet w bardzo kameralnym otoczeniu, na przykład w rodzinie, kontrola zmienia mało znaczące działania w źródło samooceny i niepokoju, wynikające z samego faktu bycia obserwowanym. W doświadczeniu, przeprowadzonym w Wielkiej Brytanii, badacze dali respondentom urządzenia umożliwiające sprawdzanie, gdzie w danej chwili znajdują się inni członkowie rodziny. Każdy mógł ustalić dokładne położenie pozostałych. Osoba, której lokalizację sprawdzono, była o tym powiadamiana, sprawdzający zaś otrzymywał ankietę z pytaniami, dlaczego to zrobił i czy otrzymane informacje potwierdzały jego/jej przypuszczenia.

Omawiając wyniki, uczestnicy stwierdzili, że choć czasami świadomość, iż ich miejsce pobytu jest znane, działała uspokajająco, to jeśli znaleźli się w nieoczekiwanym miejscu, czuli również niepokój, że członkowie rodziny „wysnują pochopne wnioski" co do ich zachowania. Niepokoju tego nie zmniejszała również opcja „stania się niewidocznym" – zablokowania możliwości przesyłania danych lokalizacyjnych. Wielu uczestników stwierdziło, że samo unikanie nadzoru w ten sposób budziłoby podejrzenia. Badacze podsumowali:

W naszym codziennym życiu są ślady, których nie potrafimy wyjaśnić i które mogą być kompletnie bez znaczenia. Jednak śledzenie ich na lokalizatorze [...] nadaje im znaczenie, pozornie wymagając rozliczania się w bardzo wielkim stopniu. To generuje niepokój, szczególnie w bliskich związkach, w których ludzie być może czują większą presję, by rozliczać się z rzeczy, z których rozliczyć się po prostu nie potrafią.

W eksperymencie fińskim przeprowadzono jedną z najbardziej radykalnych symulacji nadzoru – kamery umieszczono w domach badanych (poza sypialniami i łazienkami) i śledzono wszystkie połączenia elektroniczne uczestników. Choć ogłoszenie o badaniu umieszczono w wielu mediach społecznościowych, badacze mieli trudności ze znalezieniem choćby dziesięciu chętnych gospodarstw domowych.

Ci, którzy zdecydowali się uczestniczyć, uskarżali się przede wszystkim na ingerencję w zwykłe elementy ich codziennego życia. Jedna osoba źle się czuła, gdy chodziła po domu nago; inną krępowały kamery, gdy czesała się po kąpieli; ktoś inny myślał o kontroli, gdy wstrzykiwał sobie lekarstwo. Niewinne czynności nabierały dodatkowych znaczeń.

Badani początkowo opisywali nadzór jako „drażniący"; wkrótce jednak „przyzwyczaili się". To, co zaczęło się jako głęboka ingerencja, z czasem znormalizowało się, przekształciło w coś zwyczajnego i przestało być dostrzegane.

Jak wykazały eksperymenty, jest bardzo wiele rzeczy, które ludzie robią i chcą zachować jako prywatne, mimo że te rzeczy nie są „niczym złym". Prywatność jest niezbędna dla szerokiego zakresu ludzkich działań. Kiedy ktoś dzwoni do telefonu zaufania dla samobójców, odwiedza klinikę aborcyjną, wchodzi na stronę serwisu seksu online, zamawia wizytę w klinice rehabilitacyjnej lub leczy się z jakiejś choroby albo jeśli sygnalista dzwoni do dziennikarza, ma wiele powodów, dla których chce zachować takie działania dla siebie, ale nie ma to nic wspólnego z nielegalnością czy wykroczeniem.

W sumie – każdy ma coś do ukrycia. Dziennikarz Barton Gellman ujął to następująco:

Prywatność zależy od relacji. Zależy od publiczności. Nie chcesz, by twój pracodawca wiedział, że szukasz pracy. Nie opowiadasz szczegółów życia uczuciowego mamie ani dzieciom. Nie zdradzasz

tajemnic handlowych konkurentom. Nie odsłaniamy się w sposób nieograniczony i na tyle przejmujemy się odsłanianiem, by automatycznie kłamać. Badacze wielokrotnie stwierdzali, że uczciwi obywatele kłamią w ramach „zwykłych stosunków międzyludzkich" (studenci dwa razy dziennie, w świecie rzeczywistym raz dziennie). [...] Wszechstronna przejrzystość to koszmar. [...] Każdy ma coś do ukrycia.

Podstawowe uzasadnienie inwigilacji – że chodzi o dobro społeczeństwa – opiera się na wizji świata, w której obywatele podzieleni są na kategorie ludzi dobrych i ludzi złych. Zgodnie z takim poglądem władze wykorzystują swoje możliwości inwigilacji jedynie przeciwko złym ludziom, tym, którzy „robią coś złego", i tylko oni mają się czego obawiać w związku z ingerencją w ich prywatność. To znana taktyka. W artykule zamieszczonym w magazynie „Time" w 1969 roku, dotyczącym rosnącego niepokoju Amerykanów z powodu możliwości inwigilacji, jakimi dysponował rząd, prokurator generalny w administracji Nixona John Mitchell zapewniał czytelników, że „żaden obywatel Stanów Zjednoczonych, który nie jest zamieszany w nielegalne działania, nie musi się niczego obawiać".

Ten sam temat podjął w 2005 roku rzecznik Białego Domu, odpowiadając na zarzuty o wprowadzony przez Busha nielegalny program podsłuchowy: „Nie chodzi tu o monitorowanie rozmów telefonicznych na temat treningów Małej Ligi czy tego, co przynieść na składkowy obiad. Chodzi o monitorowanie telefonów od bardzo złych ludzi do bardzo złych ludzi". A gdy w *The Tonight Show* w sierpniu 2013 roku prezydent Obama odpowiadał na pytania Jaya Leno na temat ujawnionych programów NSA, stwierdził: „Nie mamy programu krajowego szpiegostwa. To, co mamy, to pewne mechanizmy umożliwiające wyśledzenie numeru telefonu albo adresu e-mailowego osób związanych z atakiem terrorystycznym".

Ten argument przemawia do wielu osób. Przekonanie, że inwigilacja ingerująca w prywatność ograniczona jest do marginalnej, zasługującej na to grupy, która „źle postępuje" – czyli złych ludzi – sprawia, że większość przystaje na podobne nadużywanie władzy, a nawet je popiera.

Ten pogląd wyrasta jednak z podstawowego braku zrozumienia, jakimi celami kierują się wszystkie instytucje władzy. „Złe postępowanie" w oczach takich instytucji obejmuje znacznie więcej niż nielegalne działania, zachowania pełne przemocy i spiski terrorystyczne. Rozciąga się także na znaczące akty protestu i wszelkie prawdziwe wyzwania. Władza ze swej natury stawia znak równości między niezgodą a występkiem, a co najmniej zagrożeniem.

Historia pełna jest przykładów grup i jednostek poddanych przez rząd inwigilacji z powodu ich rewolucyjnych poglądów i działań – należeli do nich między innymi Martin Luther King, ruch na rzecz praw obywatelskich, ruchy antywojenne, ekolodzy. W oczach rządu i FBI J. Edgara Hoovera wszyscy oni „źle postępowali", prowadzili bowiem działalność polityczną zagrażającą istniejącemu porządkowi.

Nikt lepiej niż Hoover nie rozumiał siły inwigilacji w tłumieniu sprzeciwów politycznych, miał bowiem do rozstrzygnięcia dylemat: jak zapobiec realizacji prawa do wolności słowa i stowarzyszania się, zagwarantowanych w pierwszej poprawce do konstytucji, skoro państwu nie wolno aresztować ludzi za głoszenie niepopularnych poglądów. W latach 60. ubiegłego wieku mieliśmy do czynienia w Sądzie Najwyższym USA z wielką liczbą spraw, które doprowadziły do ustanowienia rygorystycznej ochrony wolności słowa; ich kulminacją był jednogłośny werdykt wydany w 1969 roku w sprawie Brandenburg przeciw stanowi Ohio, uchylający wyrok skazujący na działacza Ku Klux Klanu, który w przemówieniu groził użyciem przemocy wobec przedstawicieli władz politycznych. Sąd orzekł, że gwarancje wolności słowa i prasy ujęte w pierwszej

poprawce są tak mocne, że „żaden stan nie może zakazać ani potępić głoszonego poparcia dla użycia siły".

W obliczu takich gwarancji Hoover wprowadził system, który miał po prostu nie dopuścić do powstania jakiegokolwiek aktu sprzeciwu.

Istnienie stosowanego przez FBI programu krajowego kontrwywiadu, COINTELPRO, ujawniła grupa antywojennych aktywistów, którzy nabrali przekonania, że ruch antywojenny jest infiltrowany, poddany inwigilacji i atakowany przy użyciu różnych brudnych chwytów. Ponieważ brakowało im dowodów na poparcie swojego przekonania, a nie udało im się skłonić dziennikarzy do napisania o tych podejrzeniach, w 1971 roku włamali się do oddziału FBI w Pensylwanii i wynieśli stamtąd tysiące dokumentów.

Te, które odnosiły się do COINTELPRO, pokazywały, jak FBI namierzało grupy polityczne i jednostki, które uznawało za wywrotowe i niebezpieczne, w tym Krajowe Stowarzyszenie na rzecz Awansu Ludności Kolorowej (National Association for the Advancement of Colored People, NAACP), ruchy czarnych nacjonalistów, organizacje socjalistyczne i komunistyczne, osoby protestujące przeciwko wojnie i liczne grupy prawicowe. Biuro wprowadzało do nich agentów, którzy między innymi starali się tak manipulować członkami, by ci zgadzali się popełniać przestępstwa, a wtedy FBI mogło ich aresztować i stawiać przed sądem.

FBI udało się przekonać „New York Timesa", by nie ujawniał tych dokumentów, a nawet je zwrócił, ale „Washington Post" opublikował serię opartych na nich artykułów. To z kolei doprowadziło do powołania komisji senackiej pod przewodnictwem senatora Churcha. Komisja doszła do wniosku, że:

[W ciągu piętnastu lat] Biuro prowadziło wyrafinowane operacje nadzoru mające na celu zapobieganie realizacji prawa do

wolności słowa i stowarzyszania się, zagwarantowanych w pierwszej poprawce do konstytucji, wychodząc z założenia, że zapobieganie rozrostowi niebezpiecznych ugrupowań i propagowaniu niebezpiecznych idei służy ochronie bezpieczeństwa narodowego i zapobiega aktom przemocy.

Wiele zastosowanych technik byłoby nie do zaakceptowania w społeczeństwie demokratycznym, nawet gdyby wszystkie podmioty były zaangażowane w agresywne działania, ale COINTELPRO posunęło się znacznie dalej. Nieujętą w słowa, główną przesłanką programu było to, że agencja zajmująca się egzekwowaniem prawa ma obowiązek robić wszystko, co konieczne, by zwalczać dostrzegane zagrożenia dla systemu społecznego i politycznego.

Jeden z kluczowych dokumentów COINTELPRO wyjaśniał, że wśród działaczy antywojennych można szerzyć „paranoję", pozwalając im wierzyć, że „za każdą skrzynką pocztową czai się agent FBI". W ten sposób dysydenci, przekonani, że znajdują się pod nieustanną obserwacją, tak się przerażą, że zaprzestaną działalności.

Trudno się dziwić, że ta taktyka była skuteczna. W wyprodukowanym w 2013 roku filmie dokumentalnym zatytułowanym *1971* kilku działaczy ruchu praw obywatelskich opowiadało, jak FBI Hoovera nieustannie infiltrowało i nadzorowało ich środowisko dzięki ludziom, którzy przychodzili na spotkania, a potem na nich donosili. Monitoring utrudniał możliwości organizacji i rozwoju ruchu.

W tamtym czasie nawet najmocniej zakorzenione instytucje w Waszyngtonie rozumiały, że samo istnienie rządowej inwigilacji, niezależnie jak stosowanej, zmniejsza możliwość protestu. W artykule z marca 1975 roku na temat włamania „Washington Post" ostrzegał przed tą właśnie ujarzmiającą dynamiką:

FBI nigdy nie wykazywało szczególnej wrażliwości na trujący wpływ, jaki prowadzona przez nie inwigilacja, a szczególnie poleganie na anonimowych informatorach, wywiera na procesy demokracji i korzystanie z wolności słowa. Musi być jednak oczywiste, że dyskusje i spory na temat polityki i programów rządu ulegną zahamowaniu, jeśli będzie wiadomo, że Wielki Brat w przebraniu słucha ich i o nich donosi.

COINTELPRO dalece wykraczał jednak poza to jedyne nadużycie, jakie znalazła komisja Churcha. Końcowy raport Komisji Specjalnej stwierdzał, że „miliony prywatnych telegramów wysyłanych z, do lub przez Stany Zjednoczone w latach 1945-1975 trafiały do Agencji Bezpieczeństwa Narodowego na skutek niejawnego porozumienia z trzema amerykańskimi firmami telegraficznymi". Ponadto podczas jednej tylko operacji CIA o kryptonimie CHAOS (1967-1973) „około 300 tysięcy osób wpisano do systemu komputerowego CIA, a osobne pliki utworzono dla około 7200 Amerykanów i ponad 100 krajowych ugrupowań".

Co więcej, „około 100 tysięcy Amerykanów znalazło się w kartotekach wywiadu armii Stanów Zjednoczonych, utworzonych między połową lat 60. a rokiem 1971", razem z blisko 11 tysiącami osób i ugrupowań, które zostały sprawdzone przez urząd skarbowy (Internal Revenue Service, IRS) „na podstawie kryteriów raczej politycznych niż podatkowych". Biuro posługiwało się także podsłuchami, by odkryć słabe punkty obiektów inwigilacji, na przykład ich aktywność seksualną, co później wykorzystywano do ich „zneutralizowania".

Te wydarzenia nie były aberracją tamtej epoki. Na przykład w latach prezydentury Busha dokumenty pozyskane przez ACLU ujawniły – jak to określiło stowarzyszenie w 2006 roku – „nowe szczegóły prowadzonej przez Pentagon inwigilacji Amerykanów sprzeciwiających się wojnie w Iraku, w tym kwakrów

i ugrupowań studenckich". Pentagon „miał na oku uczestników biernych protestów, gromadził informacje i przechowywał je w wojskowej antyterrorystycznej bazie danych". ACLU wskazało, że jeden dokument, „oznaczony jako «potencjalna działalność terrorystyczna», wymienia takie wydarzenia, jak wiec «Stop the War NOW!» w Akron w stanie Ohio".

Dowody wskazują, że zapewnienia, iż inwigilacją objęte są wyłącznie osoby, które „zrobiły coś złego", nie powinny uspokajać, ponieważ państwo postrzega każde wystąpienie przeciwko swojej władzy jako przestępstwo.

Jak się wielokrotnie okazywało, osoby sprawujące władzę nie potrafią się powstrzymać przed charakteryzowaniem przeciwników politycznych jako „zagrożenia dla bezpieczeństwa narodowego" czy nawet „terrorystów". W ostatniej dekadzie rząd, naśladując FBI Hoovera, formalnie użył tego określenia w stosunku do działaczy na rzecz środowiska, szerokiego wachlarza antyrządowych grup prawicowych, aktywistów antywojennych i stowarzyszeń zajmujących się prawami Palestyńczyków. Niektóre osoby w ramach tych szerokich kategorii być może zasługują na takie określenie, niewątpliwie jednak większość nie, a ich jedyna wina polega na głoszeniu przeciwnych poglądów politycznych. Jednak takie właśnie ugrupowania są rutynowo inwigilowane przez NSA i jej partnerów.

Co więcej, gdy władze brytyjskie zatrzymały na lotnisku Heathrow mojego partnera Davida Mirandę, powołując się na ustawę antyterrorystyczną, rząd Wielkiej Brytanii dosłownie postawił znak równości między moimi doniesieniami na temat NSA a terroryzmem, twierdząc, że ujawnienie dokumentów Snowdena „miało na celu wywarcie wpływu na rząd i zostało dokonane w celu promowania kwestii politycznej lub ideologicznej. Mieści się zatem w definicji terroryzmu". To najbardziej

jednoznaczne ze wszystkich sformułowanie łączące zagrożenie dla interesów władzy z terroryzmem.

Nic z tego nie jest niespodzianką dla amerykańskiej społeczności muzułmańskiej, w której strach przed inwigilacją z tytułu terroryzmu jest głęboki i wszechobecny, i nie bez przyczyny. W 2012 roku Adam Goldman i Matt Apuzzo z Associated Press ujawnili wspólny projekt CIA i policji nowojorskiej przewidujący objęcie całych społeczności muzułmańskich w Stanach Zjednoczonych inwigilacją fizyczną i elektroniczną bez choćby cienia sugestii, że popełniono jakieś przestępstwo. Amerykańscy muzułmanie regularnie opisują wpływ szpiegowania na ich życie: każda nowa osoba pojawiająca się w meczecie traktowana jest podejrzliwie, jako informator FBI; przyjaciele i rodziny tłumią rozmowy ze strachu, że są kontrolowani, i dlatego, że wiedzą, iż każda wyrażona przez nich opinia, uznana za wrogą wobec Ameryki, może zostać wykorzystana jako pretekst do wszczęcia dochodzenia, a nawet wysunięcia oskarżenia.

Jeden z dokumentów Snowdena, datowany na 3 października 2012 roku, dobitnie podkreśla tę kwestię. Ujawnia, że NSA monitorowała działalność internetową osób, które jej zdaniem wyrażają „radykalne" idee i wywierają „radykalizujący" wpływ na innych. Notatka mówi o sześciu konkretnych osobach, wyłącznie muzułmanach, choć podkreślono, że to jedynie „przykłady".

Agencja stwierdza wyraźnie, że żadna z tych osób nie jest członkiem organizacji terrorystycznej ani nie jest zamieszana w terrorystyczny spisek. Ich przestępstwem są wyrażane opinie, uważane za „radykalne", a słowo to uzasadnia wszechstronną kontrolę i destrukcyjne kampanie w celu „wykorzystania słabych stron".

Wśród informacji zgromadzonych na temat tych osób, z których co najmniej jedna jest „podmiotem amerykańskim", znajdują się szczegóły o ich aktywności seksualnej online

i „rozwiązłości online" – witrynach pornograficznych, jakie odwiedzają, i seksualnych czatach z kobietami niebędącymi ich żonami. Agencja rozważa, w jaki sposób wykorzystać te informacje do zniszczenia reputacji i wiarygodności tych osób.

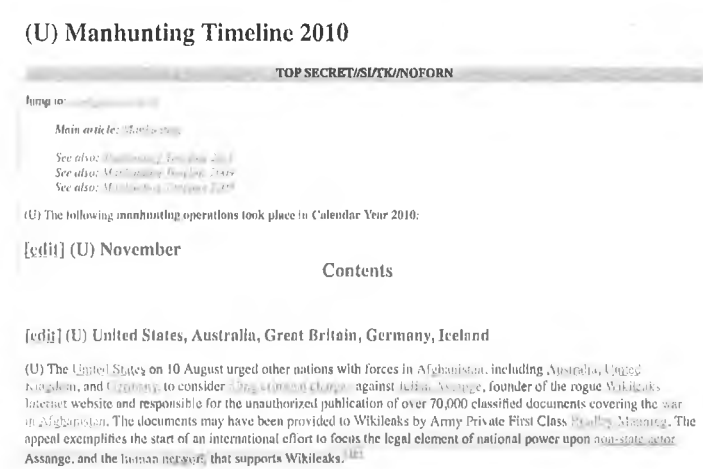
Uprzedni raport na podstronie SIGINT oceniający radykalizację odnotowywał, że autorytet radykałów najłatwiej podważyć, wskazując na rozbieżność ich postępowania w sferze publicznej i prywatnej. (A) Niektóre słabe punkty, gdyby zostały ujawnione, prawdopodobnie spowodowałyby zakwestionowanie oddania radykała sprawie dżihadu, co prowadziłoby do potępienia go lub utraty autorytetu. Niektóre przykłady tych słabych punktów to:

- *Oglądanie online materiałów erotycznych lub używanie jednoznacznie seksualnego, perswazyjnego języka w rozmowach z młodymi dziewczętami;*
- *Wykorzystanie części datków, jakie otrzymują od podatnych na jego argumenty osób, na pokrycie własnych osobistych wydatków;*
- *Żądanie niezwykle wysokich honorariów za wystąpienia i chętne wykorzystywanie okazji do podwyższenia swego statusu; albo*
- *Opinia, że ich publiczne wystąpienia opierają się na wątpliwych źródłach albo że posługują się językiem pełnym sprzeczności, co sprawia, że ich wiarygodność bywa kwestionowana.*

Jak zauważył Jameel Jaffer, zastępca dyrektora do spraw prawnych ACLU, bazy danych NSA „zawierają historię medyczną, informacje o twoich poglądach politycznych, bliskich związkach i działaniach online". Agencja twierdzi, że te osobiste dane nie będą nadużywane, „ale te dokumenty pokazują, że NSA prawdopodobnie bardzo wąsko definiuje słowo «nadużywane»". Jaffer zauważył, że zdarzało się już, iż na prośbę prezydenta NSA „wykorzystywała owoce inwigilacji do zdyskredytowania przeciwnika politycznego, dziennikarza lub działacza na rzecz praw człowieka". Naiwnością byłoby sądzić

– powiedział – że Agencja nie mogłaby „wciąż wykorzystywać tej władzy w ten sam sposób".

Inne dokumenty pokazują, że rząd skupiał się nie tylko na WikiLeaks i jego założycielu Julianie Assange'u, ale też na tym, co Agencja nazywa „ludzką siecią wspierającą WikiLeaks". W sierpniu 2010 roku administracja Obamy namawiała kilku sojuszników do postawienia Assange'owi zarzutów kryminalnych za to, że grupa ta opublikowała dzienniki wojenne z Afganistanu. Dyskusja dotycząca nacisków wywieranych na inne państwa, by oskarżyły Assange'a, występuje w pliku NSA, który agencja nazwała *Manhunting Timeline* („harmonogramem obławy"). Przedstawia on, kraj po kraju, podjęte przez Stany Zjednoczone i sojuszników starania, by zlokalizować, ścigać, ująć i/albo zabić różne osoby, w tym uznane za terrorystów, handlarzy narkotyków i przywódców palestyńskich. Harmonogram taki istnieje dla wszystkich lat od 2008 do 2012 roku.



(U) Manhunting Timeline 2010

TOP SECRET//SI/TK//NOFORN

Jump to:

Main article:

See also:
See also:
See also:

(U) The following manhunting operations took place in Calendar Year 2010:

[edit] (U) November

Contents

[edit] (U) United States, Australia, Great Britain, Germany, Iceland

(U) The United States on 10 August urged other nations with forces in Afghanistan, including Australia, United Kingdom, and Germany, to consider bringing criminal charges against Julian Assange, founder of the rogue Wikileaks Internet website and responsible for the unauthorized publication of over 70,000 classified documents covering the war in Afghanistan. The documents may have been provided to Wikileaks by Army Private First Class Bradley Manning. The appeal exemplifies the start of an international effort to focus the legal element of national power upon non-state actor Assange, and the human network that supports Wikileaks.

10 sierpnia Stany Zjednoczone nalegały na inne państwa zaangażowane wojskowo w Afganistanie, w tym Australię, Wielką Brytanię i Niemcy, by rozważyły ściganie za przestępstwo kryminalne Juliana Assange'a, założyciela bandyckiego portalu internetowego

WikiLeaks, odpowiedzialnego za niedozwoloną publikację ponad 70 tysięcy tajnych dokumentów dotyczących wojny w Afganistanie. Możliwe, że WikiLeaks otrzymało te dokumenty od żołnierza wojsk lądowych Bradleya Manninga. Apel ten jest przykładem rozpoczęcia międzynarodowych starań koncentracji władz państwowych na bezpaństwowym aktywiście Assange'u i sieci osób wspierających WikiLeaks.

Osobny dokument zawiera podsumowanie odbytej w lipcu 2011 roku dyskusji na temat tego, czy WikiLeaks, a także portal Pirate Bay, pozwalający udostępniać pliki, można „w celach namierzenia określić jako «złośliwi zagraniczni aktywiści»". Takie określenie pozwoliłoby na szeroką elektroniczną inwigilację tych portali, w tym także ich amerykańskich użytkowników. Dyskusja ta pojawia się w długiej liście „Pytań i odpowiedzi", w której funkcjonariusze z Biura Nadzoru i Zgodności (Oversight and Compliance Office, NOC), należącego do Narodowego Centrum Operacyjnego ds. Zagrożeń (National Threat Operations Center, NTOC), oraz z Biura Prawnego NSA (Office of General Counsel, OGC) udzielają odpowiedzi na zadane pytania:

Czy zagraniczny serwer, który przechowuje, a potencjalnie rozsiewa dane amerykańskie z przecieku lub kradzieży, można bez ryzyka traktować jako „szkodliwego zagranicznego działacza" w celu namierzenia go? Przykłady: WikiLeaks, thepiratebay.org itp.

Odpowiedź noc/ogc: Porozumiemy się z tobą.

Pewna taka wymiana zdań, z 2011 roku, ukazuje, jak obojętnie NSA traktuje łamanie reguł inwigilacji.

Dałem plamę... – pisze operator Agencji – wiele cech wybranego celu świadczyło, że jest zagraniczny, ale okazał się amerykański... co teraz?

Odpowiedź: Jeśli po sprawdzeniu wszystkiego odkryjesz, że to USA, musisz złożyć raport, który trafi do kwartalnego sprawozdania OGC... „ale nie ma się czym przejmować".

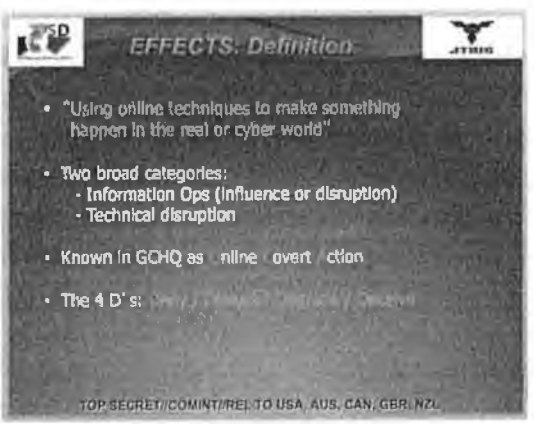
Szczególny niepokój budzi ekstremalne traktowanie Anonymous i niezbyt precyzyjnie opisywanej grupy ludzi zwanych „haktywistami". To dlatego, że Anonymous nie ma określonej struktury, ale jest grupą luźno związaną wokół jednej idei; stowarzyszenie się z Anonymous następuje dzięki głoszonym poglądom. Jeszcze gorzej, kategoria „haktywistów" w ogóle nie ma jednej definicji – może oznaczać kogoś, kto dzięki umiejętnościom programowania osłabia bezpieczeństwo i funkcjonowanie internetu, ale może też odnosić się do każdej osoby, która wykorzystuje internetowe narzędzia do promocji idei politycznych. To, że NSA bierze na cel tak szerokie kategorie ludzi, jest równoznaczne z zezwoleniem Agencji na szpiegowanie każdego i wszędzie, także w Stanach Zjednoczonych, jeśli tylko rząd uzna jego/jej idee za niebezpieczne.

Gabriella Coleman, specjalizująca się w sprawach Anonymous na uniwersytecie McGill w Montrealu, mówi, że ta grupa to „niezdefiniowana" jednostka, a bardziej „idea mobilizująca aktywistów do podejmowania wspólnych działań i dawania wyrazu niezadowoleniu politycznemu. To oparty na szerokich podstawach globalny ruch społeczny niemający żadnej scentralizowanej ani oficjalnie zorganizowanej struktury i przywództwa. Niektórzy pod tą nazwą zajmują się cyfrowym nieposłuszeństwem obywatelskim, ale w żadnej mierze nie przypomina to terroryzmu". Większością osób, które przyciągnęła ta idea, kierowała „przede wszystkim zwykła chęć wyrażenia poglądów politycznych. Branie na cel Anonymous i haktywistów to tyle, co branie na cel obywateli za to, że wyrażają swoje przekonania polityczne,

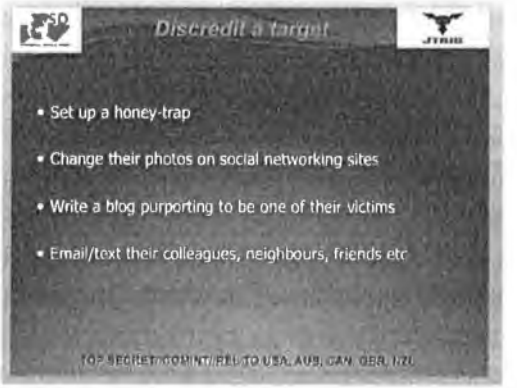
a to prowadzi do zduszenia uprawnionej różnicy zdań" – wyjaśniła Coleman.

Jednak Anonymous stał się celem działań brytyjskiego wywiadu elektronicznego GCHQ, stosującego niezwykle kontrowersyjne i radykalne taktyki rozpoznawcze: „operacje pod fałszywą flagą", „słodkie pułapki", wirusy i inne ataki, strategie oszustwa i „operacje informacyjne w celu popsucia opinii".

Jeden ze slajdów prezentacji przedstawionej na konferencji SigDev w 2012 roku przez funkcjonariuszy GCHQ zajmujących się inwigilacją opisuje dwie formy ataku: „operacje informacyjne (wpływu lub zakłócania)" oraz „zakłócenia techniczne". GCHQ nazywa te środki „Tajnym Działaniem Online" mającym na celu osiągnięcie tego, co dokument określa jako „The 4 D's: Deny/Disrupt/Degrade/Deceive" („zaprzeczyć/zakłócić/pogorszyć/oszukać").



Kolejny slajd opisuje techniki używane do „zdyskredytowania obiektu". Obejmują one: „zastawienie słodkiej pułapki", „zmianę fotografii na portalach społecznościowych", „pisanie bloga rzekomo przez jedną z ich ofiar" oraz „e-maile/SMS-y do współpracowników, sąsiadów, znajomych itd.".



W towarzyszących temu notatkach GCHQ wyjaśnia, że „słodka pułapka" – stara zimnowojenna technika, w której atrakcyjne kobiety wciągały mężczyzn w kompromitujące i dyskredytujące ich sytuacje – została dostosowana do epoki cyfrowej: obiekt jest kuszony do wejścia na kompromitującą stronę lub do spotkania online. Dodano tu komentarz: „Bardzo skuteczna, jeśli się uda". Podobnie online stosuje się też tradycyjne metody infiltracji.

Kolejna technika dotyczy „odcięcia łączności". W tym celu agencja będzie: „bombardować telefon SMS-ami", „bombardować telefon połączeniami", „usuwać obecność online" oraz „blokować faks".

GCHQ także lubi stosować techniki „utrudniania" zamiast tego, co nazywa „tradycyjnym egzekwowaniem prawa", a więc gromadzeniem dowodów i procesami. W dokumencie nazwanym *Sesja cyberofensywy. Przesuwanie granic i działania przeciwko haktywizmowi* GCHQ rozważa celowanie w „haktywistów", paradoksalnie, atakami „odmowy usługi", czyli taktyką powszechnie kojarzoną z hakerami.

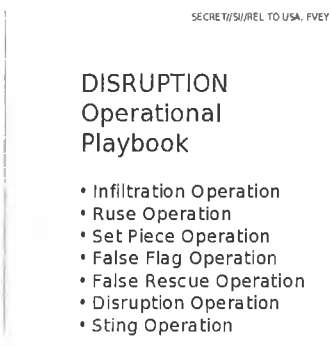
Brytyjska agencja inwigilacyjna zatrudnia także zespół specjalistów nauk społecznych, w tym psychologów, do opracowania technik „online HUMINT" (human intelligence) oraz „strategicznego utrudniania wpływu". Tym taktykom poświęcony jest dokument *Sztuka podstępów. Szkolenie do celów nowej generacji tajnych operacji online.* Przygotowany przez należącą do agencji komórkę operacyjną wykorzystującą nauki o człowieku (Human Science Operation Cell, HSOC) dokument opiera się między innymi na socjologii, psychologii, antropologii, neurobiologii i biologii, by zmaksymalizować umiejętności podstępów online stosowanych przez GCHQ.

Jeden ze slajdów pokazuje, jak się zajmować „Dysymulacją – ukrywaniem rzeczywistości", przy równoczesnym propagowaniu „Symulacji – pokazywania fałszu". Bada „psychologiczne klocki budujące podstęp" oraz „mapę technologii" używanych do przeprowadzenia podstępów, w tym Facebooka, Twittera, LinkedIn oraz stron WWW".

Podkreślając, że „ludzie podejmują decyzje z powodów emocjonalnych, nie racjonalnych", GCHQ twierdzi, że zachowaniami w sieci kieruje zasada „lustrzanego odbicia" („ludzie nawiązujący społeczne interakcje nawzajem się naśladują"), „przystosowania" i „mimikry" („przyjęcie przez jednostkę konkretnych cech społecznych od pozostałych uczestników komunikacji").

Dokument wykłada następnie to, co nazywa „Zbiorem operacyjnych strategii zakłócania". Obejmuje on „operacje infiltracji", „podstępy", „operacje pod fałszywą flagą" i „prowokacje".

Obiecuje „pełne rozwinięcie" programu zakłócania „do początku 2013 roku", ponieważ „personel liczący 150+ osób [jest] w pełni przeszkolony".


SECRET//SI//REL TO USA, FVEY

DISRUPTION
Operational
Playbook

- Infiltration Operation
- Ruse Operation
- Set Piece Operation
- False Flag Operation
- False Rescue Operation
- Disruption Operation
- Sting Operation

Pod tytułem *Magiczne techniki i doświadczenie* dokument omawia: „legitymizację przemocy", „budowanie w umysłach obiektów doświadczeń, które powinny być akceptowane, tak by obiekty nie zdawały sobie [z tego] sprawy" oraz „optymalizację kanałów oszukiwania".

Takie rodzaje planów rządu, mające na celu monitorowanie i wpływanie na połączenia internetowe oraz rozsiewanie fałszywych informacji online, od dawna były przedmiotem spekulacji. Cass Sunstein, profesor prawa na Harvardzie i bliski doradca Obamy, były szef Biura Informacji i Spraw Regulacyjnych Białego Domu, członek panelu mianowanego przez Biały Dom do przeglądu działalności NSA, w 2008 roku napisał kontrowersyjny artykuł proponujący, by rząd USA zatrudnił zespoły tajnych agentów i pseudoniezależnych rzeczników, którzy mieliby „poznawczo infiltrować" grupy internetowe, czaty, sieci społecznościowe i portale internetowe, a także grupy aktywistów offline.

Dokumenty GCHQ po raz pierwszy poświadczają, że takie kontrowersyjne techniki, używane do oszukiwania i psucia opinii, przeszły z etapu propozycji do etapu realizacji.

Wszystkie te dowody podkreślają niejawną umowę oferowaną obywatelom: jeśli nie będziecie się niczemu sprzeciwiać, nie macie się o co martwić. Pilnujcie swego nosa, wspierajcie – a przynajmniej tolerujcie – to, co robimy, a nic wam nie będzie. Inaczej mówiąc, jeśli chcecie cieszyć się opinią niewinnych, musicie unikać prowokowania władz, które dysponują możliwościami inwigilacji. To umowa, która zakłada bierność, posłuszeństwo i konformizm. Najbezpieczniejszą drogą, sposobem, by „zostawiono nas w spokoju", jest siedzieć cicho, niczemu nie zagrażać i się przystosowywać.

Pogląd, że inwigilacja jest łagodna, a nawet korzystna, jest dla wielu osób atrakcyjny, a dla większości przekonujący. Jesteśmy zbyt nudni, by zwracać uwagę rządu – myślą. „Naprawdę wątpię, by NSA się mną interesowało" – to słowa, które często słyszałem w rozmowie. „Jeśli chcą słuchać o moim nudnym życiu, to niech sobie słuchają". Albo: „NSA nie interesuje twoja babcia opowiadająca o przepisach kuchennych ani dziadek umawiający się na golfa".

Tak mówią ludzie, którzy są przekonani, że oni sami nie staną się obiektem zainteresowania – ponieważ nikomu nie zagrażają i przystosowują się do zarządzeń – a zatem albo zaprzeczają, że coś takiego się dzieje, albo ich to nie obchodzi, albo wręcz są gotowi wprost to wspierać.

Lawrence O'Donnell, który dla MSNBC prowadził ze mną wywiad wkrótce po ujawnieniu sprawy NSA, kpił sobie z pomysłu, że Agencja to „wielki, przerażający, inwigilujący potwór". Podsumowując swoją opinię, stwierdził:

Jak dotychczas [...] nie boję się [...] Fakt, że rząd gromadzi [dane] na tak gigantycznym, potężnym szczeblu, oznacza, że rządowi jest jeszcze trudniej mnie znaleźć [...] i nie ma absolutnie żadnego powodu, by mnie znajdować. Więc ja, na tym etapie, w ogóle nie czuję się zagrożony.

Hendrik Hertzberg z „New Yorkera" wygłaszał podobnie lekceważące poglądy na temat niebezpieczeństwa inwigilacji. Przyznawał, że „są powody, by niepokoić się przekraczaniem granic przez agencję wywiadu, jej nadmierną tajemniczością i brakiem przejrzystości, ale są także powody, by zachować spokój", a szczególnie, że zagrożenie dla „swobód obywatelskich, takie jak się nam rysuje, jest abstrakcyjne, hipotetyczne, nieokreślone". Felietonistka „Washington Post" Ruth Marcus ogłosiła zaś – absurdalnie – że „moich metadanych niemal na pewno nikt nie analizował".

W pewnym znaczącym sensie O'Donnell, Hertzberg i Marcus mają rację. Chodzi o to, że rząd USA „nie ma absolutnie żadnego powodu", by brać na cel ludzi takich jak oni, czyli osoby, dla których zagrożenie ze strony nadzoru państwa jest „abstrakcyjne, hipotetyczne, nieokreślone". To dlatego, że dziennikarze, którzy swoje kariery poświęcają czczeniu najpotężniejszego urzędnika kraju – prezydenta, będącego także naczelnym dowódcą NSA – i bronieniu jego partii politycznej, rzadko, jeśli w ogóle, ryzykują, że urażą kogoś u władzy.

Oczywiście posłuszni, lojalni zwolennicy prezydenta i jego polityki, dobrzy obywatele, którzy nic nie robią, by skupić na sobie niechęć potężnych osób, nie mają powodu, by obawiać się nadzorującego państwa. Tak jest w każdym społeczeństwie: ci, którzy nie stanowią zagrożenia, rzadko stają się celem prześladowań, więc ze swojej perspektywy mogą przekonać samych siebie, że żadna opresja w rzeczywistości nie istnieje. Jednak prawdziwą miarą wolności społeczeństwa jest to, jak traktuje dysydentów i inne marginalizowane grupy, a nie jak traktuje lojalistów. Nawet w najgorszych tyraniach posłuszni zwolennicy nie padają ofiarą nadużyć ze strony władzy. W Egipcie za rządów Mubaraka to ci, którzy wyszli na ulice, by manifestować na rzecz jego obalenia, byli aresztowani, torturowani i zabijani; zwolennicy Mubaraka i ci, którzy siedzieli cicho w domu – nie. W Stanach Zjednoczonych to przywódcy NAACP,

komuniści, działacze na rzecz praw obywatelskich i aktywiści antywojenni stawali się celem inwigilacji ze strony FBI Hoovera, a nie grzeczni obywatele, którzy nie protestowali przeciwko społecznej niesprawiedliwości.

Nie powinno tak być, że jedynie lojaliści wierni władzom mogą czuć się bezpieczni od nadzoru ze strony państwa. Ceną nietykalności nie powinno być powstrzymanie się od kontrowersyjnych lub prowokacyjnych wypowiedzi i działań. Nie powinniśmy pragnąć społeczeństwa, któremu daje się do zrozumienia, że nikt nie będzie się nikogo czepiał jedynie wówczas, gdy ludzie zgodzą się naśladować posłuszne zachowanie się i opinie związanego z establishmentem publicysty.

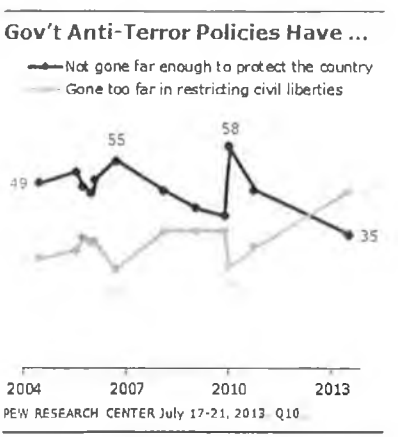
Poza tym poczucie nietykalności odczuwane przez konkretną grupę obecnie sprawującą władzę musi być iluzoryczne. To jasne, gdy widzimy, jak przynależność partyjna kształtuje w ludziach poczucie zagrożenia ze strony nadzoru państwa. Wczorajsi przywódcy szybko stają się dzisiejszymi dysydentami.

Podczas sporu na temat nieuprawnionych podsłuchów NSA w 2005 roku liberałowie i członkowie Partii Demokratycznej powszechnie uważali program inwigilacji za zagrożenie. Oczywiście częściowo chodziło o typową partyjną przepychankę: prezydentem był George W. Bush, więc dostrzegli szansę, by zaszkodzić jemu i jego partii. W dużej mierze ich obawy były jednak prawdziwe – ponieważ uważali Busha za złośliwego i niebezpiecznego, twierdzili, że inwigilacja przez państwo pod jego kierownictwem stanowi zagrożenie, szczególnie dla nich jako politycznych oponentów. Republikanie natomiast głosili łagodniejszy, a nawet przychylny pogląd na temat działań NSA. W grudniu 2013 roku natomiast demokraci i postępowcy przeszli na stronę czołowych obrońców NSA.

Przesunięcie to odzwierciedlają dane z sondaży. Pod koniec lipca 2013 roku Pew Research Center opublikowało wyniki

badania opinii publicznej wskazujące, że większość Amerykanów nie wierzy w argumenty broniące działań NSA. Szczególnie „większość Amerykanów – 56 procent – mówi, że sądy federalne nie ograniczają we właściwy sposób gromadzenia danych telefonicznych i komputerowych przez rząd w ramach jego działań antyterrorystycznych". Ponadto „jeszcze większy odsetek (70 procent) uważa, że rząd wykorzystuje te dane do celów innych niż ściganie terrorystów". Co więcej, „63 procent jest zdania, że rząd gromadzi także informacje dotyczące treści wiadomości".

Szczególnie warto zwrócić uwagę, że Amerykanie są obecnie przekonani, iż zagrożenie ze strony inwigilacji jest bardziej niepokojące niż zagrożenie ze strony terroryzmu:



W sumie 47 procent mówi, że w stosunku do antyterrorystycznej polityki rządu bardziej ich niepokoi to, że poszła ona za daleko w ograniczaniu swobód obywatelskich przeciętnej osoby, a 35 procent uważa, że polityka ta nie poszła wystarczająco daleko w ochronie kraju. Od kiedy w 2004 roku zaczęto zadawać to pytanie w sondażach Pew Research, pierwszy raz zdarzyło się, że więcej osób wyraża niepokój o swobody obywatelskie niż o ochronę przed terroryzmem.

Te dane sondażowe stanowią dobrą wiadomość dla każdego, kogo niepokoi nadmierna władza rządu i chroniczne wyolbrzymianie zagrożenia terroryzmem. Uwypuklają też znaczącą inwersję: republikanie, którzy bronili NSA za prezydentury Busha, ustąpili miejsca demokratom, gdy system inwigilacji przeszedł pod zarząd prezydenta Obamy, członka Partii Demokratycznej. „Ogólnie w kraju program gromadzenia danych przez rząd ma większe poparcie ze strony demokratów (57 procent za) niż wśród republikanów (44 procent za)".

Podobne dane sondażowe z „Washington Post" wskazały, że konserwatyści są znacznie bardziej zaniepokojeni szpiegowaniem NSA niż liberałowie. Na pytanie: „Jak bardzo – jeśli w ogóle – niepokoi was gromadzenie i wykorzystanie osobistych informacji o was przez Agencję Bezpieczeństwa Narodowego?", 48 procent konserwatystów było „bardzo zaniepokojonych" w porównaniu do zaledwie 26 procent liberałów. Jak zauważył profesor prawa Orin Kerr, oznaczało to zasadniczą zmianę: „To interesujące odwrócenie sytuacji z 2006 roku, gdy prezydentem był republikanin, a nie demokrata. W tamtym roku badanie opinii publicznej przeprowadzone przez Pew wskazało, że 75 procent republikanów aprobuje inwigilację NSA w porównaniu do zaledwie 37 procent demokratów".

Wykres zatytułowany *Przesunięcie w poglądach na temat programów inwigilacji NSA w zależności od partii politycznej* jasno to obrazuje:

Partisan Shifts in Views of NSA Surveillance Programs

	Views of NSA surveillance programs (See previous table for differences in question wording)			
	January 2006		June 2013	
	Acceptable %	Unacceptable %	Acceptable %	Unacceptable %
Total	51	47	56	41
Republican	75	23	52	47
Democrat	37	61	64	34
Independent	44	55	53	44

PEW RESEARCH CENTER June 6-9, 2013. Figures read across. Don't know/Refused responses not shown.

Argumenty za i przeciw inwigilacji bezwstydnie zamieniają się miejscami, zależnie od tego, która partia sprawuje władzę. W 2006 roku pewien senator w programie *The Early Show* gwałtownie zaatakował hurtowe gromadzenie metadanych przez NSA:

Nie muszę wysłuchiwać twoich rozmów telefonicznych, by wiedzieć, co robisz. Jeśli znam każde twoje połączenie, jestem w stanie określić każdą osobę, z jaką rozmawiałeś, potrafię odtworzyć wzorzec twojego życia, a to jest wielka, ogromna ingerencja. [...] Jednak kluczowe pytanie brzmi: co oni robią z tymi informacjami, które gromadzą, a które nie mają nic wspólnego z al-Kaidą? [...] I my mamy zawierzyć prezydentowi i wiceprezydentowi Stanów Zjednoczonych, że postępują słusznie? Mnie do tego nie włączajcie.

Senatorem, który tak ostro krytykował gromadzenie metadanych, był Joe Biden, który potem, jako wiceprezydent, został częścią administracji demokratów wysuwającej dokładnie te same argumenty, które wcześniej wyszydzał.

Istotny jest tu nie tylko fakt, że wielu partyjnych lojalistów to pozbawieni pryncypiów hipokryci, niekierujący się żadnymi przekonaniami poza żądzą władzy – choć niewątpliwie to także jest prawda. Ważniejsze jest to, co takie stwierdzenia mówią o podejściu do inwigilacji przez państwo. Jak w przypadku licznych niesprawiedliwości ludzie ignorują strach przed nadużyciami ze strony rządu, gdy wierzą, że ci, którzy akurat sprawują władzę, są życzliwi i wiarygodni. Uznają inwigilację za niebezpieczną lub budzącą niepokój tylko wówczas, gdy sami czują się przez nią zagrożeni.

Często w ten właśnie sposób następuje radykalne poszerzenie zakresu władzy – przez wmawianie ludziom, że dotyczy to tylko konkretnej, wyodrębnionej grupy. Rządy od dawna

skłaniały społeczeństwa do przymykania oczu na represyjne postępowanie czołowych obywateli i do wiary, słusznej lub nie, że celem są jedynie niektórzy ludzie z marginesu, a wszyscy inni mogą się na represje zgadzać, a nawet je popierać, bez obawy, że dotkną także i ich. Pomijając oczywiste moralne niedostatki takiego stanowiska – nie lekceważymy rasizmu, choć dotyczy mniejszości, ani nie wzruszamy ramionami, słysząc o głodzie, tylko dlatego, że sami mamy co jeść – niemal zawsze jest ono błędne także z powodów pragmatycznych.

Obojętność lub poparcie dla rządu ze strony tych, którzy uważają, że to ich nie dotyczy, nieodmiennie pozwala nadużywaniom władzy rozlewać się daleko poza pierwotne potrzeby, aż w końcu sytuacja wymyka się spod kontroli. Zbyt wiele jest przykładów, by je wyliczać, ale warto zwrócić uwagę na najnowszy i mający największe znaczenie – jest nim powoływanie się na Patriot Act. Kongres niemal jednogłośnie zatwierdził ogromny wzrost możliwości inwigilacji i zatrzymywania po 11 września, przekonany argumentem, że dzięki temu zapobiegnie się planowanym atakom, ponieważ zostaną odkryte z wyprzedzeniem.

Domyślne założenie mówiło, że władza ta będzie wykorzystywana zasadniczo przeciwko muzułmanom powiązanym z terroryzmem. To klasyczne rozszerzenie uprawnień ograniczono do konkretnej grupy zajmującej się konkretnym rodzajem działań, i między innymi dlatego właśnie propozycja ta zyskała tak powszechne poparcie. Jednak stało się coś zupełnie innego: stosowanie Patriot Act znacznie wykroczyło poza rzekomy cel ustawy. Co więcej, od samego początku używano jej w przypadkach niemających nic wspólnego z terroryzmem czy bezpieczeństwem narodowym. Czasopismo „New York" donosiło, że w latach 2006-2009 punkt tej ustawy zezwalający na „wejście i sprawdzenie" (uprawnienie do przeprowadzenia przeszukania bez informowania o tym osoby będącej przedmiotem

dochodzenia) został wykorzystany 1618 razy w sprawach handlu narkotykami, w 122 sprawach związanych z oszustwem, a tylko 15 razy w sprawach wiążących się z terroryzmem.

Jednak gdy obywatele raz już zgodzą się na nowe uprawnienia władz w przekonaniu, że sami od nich nie ucierpią, uprawnienia te nabierają charakteru zinstytucjonalizowanego i usankcjonowanego. Nie sposób więc przeciwko nim protestować. Główną nauką, jaką Frank Church wysnuł w 1975 roku, był zakres niebezpieczeństw wynikających z powszechnej inwigilacji. W wywiadzie w programie *Meet the Press* powiedział:

Ten potencjał może być w każdej chwili zwrócony przeciwko narodowi amerykańskiemu i żaden Amerykanin nie będzie już cieszył się prywatnością, taki bowiem jest potencjał monitorowania wszystkiego – rozmów telefonicznych, telegramów, nie ma znaczenia czego. Nie sposób będzie się ukryć. Jeśli ten rząd kiedykolwiek stanie się tyranem [...] technologiczne możliwości, jakie wspólnota wywiadów daje rządowi, mogą mu umożliwić narzucenie pełnej tyranii, i nie sposób będzie z tym walczyć, ponieważ nawet najostrożniejsze próby zorganizowanego oporu [...] rząd będzie mógł poznać z wyprzedzeniem. Taki jest potencjał tej technologii.

Pisząc w 2005 roku w „New York Timesie", James Bamford zauważył, że zagrożenie ze strony państwowej inwigilacji jest dziś znacznie większe niż w latach 70.: „Gdy ludzie dają wyraz najskrytszym myślom w wiadomościach e-mailowych, ujawniają w internecie swoje dane medyczne i finansowe, nieustannie rozmawiają przez telefony komórkowe, to Agencja ma de facto możliwość wejścia w umysł każdego człowieka".

Wyrażony przez Churcha niepokój, że wszelkie aspekty inwigilacji „mogą być w każdej chwili zwrócone przeciwko narodowi amerykańskiemu", okazał się uzasadniony właśnie przez to, co NSA zrobiła po 11 września. Mimo działania ograniczonego przez

Ustawę o nadzorowaniu zagranicznych wywiadów (FISA) i mimo zakazu szpiegowania wewnątrz kraju, obowiązującego Agencję od chwili powstania, inwigilacja w znacznej mierze dotyczy teraz obywateli amerykańskich na amerykańskiej ziemi.

Nawet wówczas, gdy nie dochodzi do nadużyć, i wówczas, gdy inwigilacja nie jest wymierzona w nikogo osobiście, sam fakt, że państwo stosuje takie metody, szkodzi społeczeństwu i ogólnie wolności politycznej. Postęp – i w Stanach Zjednoczonych, i w innych krajach – zawsze napędzany był wyzwaniami rzucanymi władzy i dominującym poglądom, wytyczaniem nowych szlaków myślenia i nowych sposobów życia. Każdy – nawet ci, którzy nie włączają się w ruchy protestu czy działalność polityczną – cierpi, jeśli te swobody są tłumione przez strach przed obserwacją. Hendrik Hertzberg, który tak lekko traktował niepokoje wywołane programami NSA, przyznał jednak, że „krzywda się stała. Krzywda jest obywatelska. Krzywda jest zbiorowa. Krzywdę wyrządzono architekturze zaufania i odpowiedzialności, która wspiera otwarte społeczeństwo i państwo".

Entuzjaści inwigilacji wysuwają właściwie tylko jeden argument za powszechną kontrolą: jedynym jej celem jest położenie kresu terroryzmowi i zapewnienie bezpieczeństwa ludziom. Niewątpliwie odwoływanie się do zewnętrznego zagrożenia to taktyka często wybierana w historii, by utrzymać społeczeństwo w posłuszeństwie wobec władzy. Od ponad dziesięciu lat rząd USA zagrożeniem ze strony terroryzmu usprawiedliwia mnóstwo radykalnych działań – od zmuszania do wyrzekania się różnych rzeczy, przez tortury, po zabójstwa i inwazję na Irak. Od ataków z 11 września amerykańscy urzędnicy automatycznie rzucają słowo „terroryzm". Stało się ono w większej mierze sloganem i taktyką niż rzeczywistym argumentem czy przekonującym uzasadnieniem działania. W przypadku inwigilacji zaś zdecydowana większość dowodów wskazuje, jak wątpliwe jest to uzasadnienie.

Przede wszystkim znaczna część danych gromadzonych przez NSA w zupełnie oczywisty sposób nie ma nic wspólnego z terroryzmem ani bezpieczeństwem narodowym. Przechwytywanie łączności wielkiej brazylijskiej firmy naftowej Petrobras, szpiegowanie sesji negocjacji na szczycie ekonomicznym, podsłuchiwanie rozmów demokratycznie wybranych przywódców sojuszniczych państw czy gromadzenie rejestrów wszystkich połączeń Amerykanów w żaden sposób nie wiąże się z terroryzmem. Biorąc pod uwagę obecny zakres inwigilacji NSA, zapobieżenie terroryzmowi jest wyraźnie jedynie pretekstem.

Co więcej, argument, że powszechna inwigilacja zapobiegła spiskom terrorystycznym – jak twierdził prezydent Obama i wiele postaci związanych z bezpieczeństwem narodowym – okazał się fałszywy. W grudniu 2013 roku w artykule zatytułowanym *Obrona programu telefonicznego NSA przez urzędników może obrócić się wniwecz* „Washington Post" cytował sędziego federalnego, który powiedział, że program gromadzenia metadanych telefonicznych jest „niemal na pewno" sprzeczny z konstytucją. I dodał, że Departament Sprawiedliwości nie przedstawił „ani jednego przypadku, w którym analiza zbiorów metadanych NSA rzeczywiście zapobiegła grożącemu atakowi terrorystycznemu".

W tym samym miesiącu starannie dobrany przez Obamę panel doradców (w skład którego weszli między innymi były zastępca dyrektora CIA i były doradca Białego Domu, a który badał program NSA, korzystając z dostępu także do informacji niejawnych) przedstawił wniosek, że program metadanych „nie był istotny dla zapobieżenia atakom i można było [te dane] pozyskać bez problemu i na czas, wykorzystując konwencjonalne nakazy [sądowe]".

Kolejny cytat z „Washington Post": „Składając wyjaśnienia przed Kongresem, [szef NSA Keith] Alexander przypisał

programowi pomoc w wykryciu kilkudziesięciu spisków w Stanach Zjednoczonych i za granicą", jednak raport panelu doradców „zdecydowanie podważył wiarygodność tych twierdzeń".

Ponadto, jak wprost powiedzieli „New York Timesowi" demokratyczni senatorowie Ron Wyden, Mark Udall i Martin Heinrich – wszyscy są członkami Komisji Wywiadu – powszechne gromadzenie rejestrów telefonicznych nie zwiększyło ochrony Amerykanów przed zagrożeniem terroryzmem.

Przydatność hurtowego programu gromadzenia została znacznie wyolbrzymiona. Nie widzieliśmy jeszcze ani jednego dowodu, że ma rzeczywistą, wyjątkową wartość dla ochrony bezpieczeństwa narodowego. Mimo wielokrotnie powtarzanych próśb, NSA nie przedstawiła dowodów na ani jeden przypadek wykorzystania tego programu do przejrzenia rejestrów rozmów telefonicznych, których nie dałoby się uzyskać dzięki zwykłemu nakazowi sądowemu lub autoryzacji drogą alarmową.

Analiza przeprowadzona przez centrową New America Foundation w celu zbadania prawdziwości oficjalnych uzasadnień dla hurtowego gromadzenia danych potwierdziła, że program „nie ma żadnego dostrzegalnego wpływu na zapobieganie aktom terrorystycznym". Zamiast tego, jak wskazał „Washington Post", w większości wypadków, w których odkryto spiski, badanie sprawy ujawniło, że to „tradycyjne metody egzekwowania prawa i dochodzenia przyniosły wskazówki lub dowody pozwalające rozpocząć śledztwo".

Rzeczywiście, osiągnięcia są bardzo skromne. System „gromadzenia wszystkiego" w żaden sposób nie przyczynił się do wykrycia – nie mówiąc już o zapobieżeniu – ataku podczas maratonu w Bostonie w 2013 roku. Nie wykrył próby wybuchu w samolocie lecącym z Europy do Detroit w dzień Bożego Narodzenia 2009 roku ani planu wysadzenia w powietrze

samochodu z ładunkiem wybuchowym na Times Square w Nowym Jorku w 2010 roku, ani planowanego ataku na system nowojorskiego metra – wszystkim zapobiegli czujni obywatele lub tradycyjne siły policyjne. Niewątpliwie też w żaden sposób nie uniemożliwił masowych zamachów od Aurory po Newtown (szaleńcy z karabinami dokonali tam masakry widzów w kinie oraz dzieci w szkole podstawowej). Duże międzynarodowe zamachy, od Londynu, przez Bombaj, po Madryt, nie zostały wcześniej odkryte, mimo że pracowało przy tym co najmniej kilkunastu agentów.

I mimo wszystkich twierdzeń NSA masowa inwigilacja nie zapewniłaby służbom wywiadu lepszych narzędzi do zapobieżenia atakom 11 września. Keith Alexander powiedział senackiemu panelowi, że „woli być tutaj i rozmawiać [o programie], niż próbować wyjaśnić, dlaczego nie zapobiegliśmy kolejnemu 11 września" (ten sam argument, słowo w słowo, umieszczono w pouczeniach, jakie NSA rozdała pracownikom, by ich używali, odpowiadając na pytania).

Widać tu wyraźnie, że chodzi o wzbudzenie strachu, a poza tym mamy obrzydliwe oszustwo. Analityk kwestii bezpieczeństwa CNN Peter Bergen udowodnił, że CIA dysponowała wieloma raportami na temat spisku al-Kaidy i „całkiem sporą ilością informacji na temat dwóch z porywaczy i ich obecności w Stanach Zjednoczonych, [ale] Agencja nie powiadomiła innych agend rządowych, aż było za późno, by cokolwiek z tym zrobić".

Lawrence Wright, ekspert do spraw al-Kaidy z „New Yorkera", także obalił twierdzenie NSA, że gromadzenie metadanych mogło zapobiec atakom z 11 września, wyjaśniając, że „CIA nie przekazała istotnych informacji wywiadu FBI, które jako jedyne ma najwyższą władzę dochodzenia w sprawach terroryzmu na terenie USA i ataków przeciwko Amerykanom za granicą". To FBI mogłoby nie dopuścić do ataków – twierdził.

[FBI] miało prawo prowadzić inwigilację każdego, kto w Ameryce był związany z al-Kaidą. Mogło go śledzić, założyć podsłuch na telefonach, klonować komputery, czytać e-maile, zażądać dostępu do dokumentacji medycznej, bankowej i kredytowej. Miało prawo zażądać billingów od firm telefonicznych. Nie było żadnej potrzeby uruchamiania programu gromadzenia metadanych. Istniała natomiast potrzeba współpracy z innymi agencjami federalnymi, tylko że z przyczyn tak małostkowych jak niejasnych agencje te postanowiły ukryć istotne wskazówki przed tymi śledczymi, którzy z największym prawdopodobieństwem zdołaliby zapobiec atakom.

Zatem rząd dysponował koniecznymi informacjami, ale albo ich nie zrozumiał, albo zaniedbał działań. Rozwiązanie, które wówczas przyjął – gromadzić wszystko, masowo – w żaden sposób tego zaniedbania nie naprawiło.

Wielokrotnie, z wielu stron, udowadniano, że uzasadnianie inwigilacji zagrożeniem terrorystycznym to fikcja.

Co więcej, powszechna inwigilacja ma wręcz przeciwny skutek: utrudnia wykrycie terroryzmu i zapobieganie mu. Rush Holt, kongresman z Partii Demokratycznej, fizyk i jeden z niewielu naukowców w Kongresie, wskazał, że gromadzenie wszystkiego na temat wszystkich połączeń tylko przysłania rzeczywiste spiski, omawiane przez prawdziwych terrorystów. Inwigilacja ukierunkowana zamiast powszechnej przyniosłaby bardziej konkretne i przydatne informacje. Obecnie agencje wywiadu zalewane są taką ilością danych, że w żaden sposób nie są w stanie ich skutecznie posortować.

Programy inwigilacji prowadzone przez NSA nie tylko przynoszą zbyt wiele informacji, ale też w efekcie zwiększają podatność kraju na atak: podejmowane przez agencje próby łamania metod szyfrowania chroniących zwykłe transakcje internetowe – takie jak bankowość i handel – czy dostęp do

dokumentacji medycznej sprawiają, że systemy te zostają otwarte przed hakerami i innymi wrogimi jednostkami.

Bruce Schneider, ekspert do spraw bezpieczeństwa, napisał w „Atlantic" w styczniu 2014:

Wszechobecna inwigilacja nie tylko jest nieefektywna, ale też niezwykle kosztowna. [...] Łamie nasze systemy techniczne, więc same protokoły internetowe stają się niegodne zaufania. [...] Musimy się martwić nie tylko o krajowe nadużycia; dotyczy to także reszty świata. Im bardziej chcemy prowadzić podsłuch w internecie i innych technologiach łączności, tym mniej jesteśmy zabezpieczeni przed podsłuchiwaniem przez innych. Wybór, jaki stoi przed nami, nie jest wyborem między cyfrowym światem, gdzie NSA może podsłuchiwać, a takim, w którym nie dopuszcza się podsłuchiwania przez NSA. To wybór między światem podatnym na wszelkie ataki a takim, który jest bezpieczny dla wszystkich użytkowników.

Być może najbardziej godną uwagi rzeczą w tym nieskończonym eksploatowaniu groźby terroryzmu jest fakt, że jest ona tak ewidentnie wyolbrzymiona. Ryzyko, że jakiś Amerykanin zginie w ataku terrorystycznym, jest nieskończenie małe, zdecydowanie mniejsze niż trafienie przez piorun. John Mueller, profesor na uniwersytecie stanowym w Ohio, który wiele napisał na temat wyważenia między zagrożeniem a wydatkami na walkę z terroryzmem, wyjaśnił w 2011 roku: „Liczba ludzi na całym świecie zabitych przez terrorystów typu muzułmańskich naśladowców al-Kaidy sięga może kilkuset, poza strefami działań wojennych. Mniej więcej tyle samo ludzi rocznie ginie na skutek utonięcia we własnej wannie".

Więcej obywateli amerykańskich „niewątpliwie" zginęło „za granicą w wypadkach drogowych lub na skutek zatrucia pokarmowego niż w atakach terrorystycznych" – poinformowała agencja prasowa McClatchy.

Pomysł, że dla takiego właśnie ryzyka powinniśmy zdemontować zasadnicze zabezpieczenia naszego ustroju politycznego, by zbudować system wszechobecnej państwowej inwigilacji, to szczyt irracjonalności. Jednak to niebezpieczeństwo nieustannie się rozdmuchuje. Niedługo przed igrzyskami olimpijskimi w Londynie w 2012 roku wybuchł spór na temat rzekomego braku bezpieczeństwa. Firma, która miała zapewnić ochronę, nie zatrudniła tylu strażników, ile przewidywał kontrakt, więc na całym świecie podniosły się głosy, że igrzyska są podatne na atak terrorystyczny.

Po zakończeniu olimpiady, podczas której nie wydarzyło się nic niebezpiecznego, Stephen Walt napisał w „Foreign Policy", że jak zwykle alarm napędzało wyolbrzymione wyobrażenie zagrożenia. Zacytował artykuł Johna Muellera i Marka G. Stewarta w „International Security", do którego autorzy przeprowadzili analizę pięćdziesięciu przypadków rzekomych „islamskich spisków terrorystycznych" wymierzonych w Stany Zjednoczone, dochodząc do wniosku, że „właściwie wszyscy wykonawcy byli «niekompetentni, nieskuteczni, nieinteligentni, bezmyślni, niedouczeni, niezorganizowani, zagubieni, otumanieni, amatorscy, gamoniowaci, nierealistyczni, kretyńscy, irracjonalni i głupi»". Mueller i Stewart cytowali Glenna Carle'ego, byłego zastępcę krajowego oficera wywiadu do spraw zagrożeń ponadnarodowych, który powiedział: „Musimy widzieć dżihadystów takimi, jakimi są: małymi, zabójczymi, chaotycznymi i nieszczęsnymi przeciwnikami", i dodawali, że jeśli chodzi o al-Kaidę, jej „możliwości są znacznie mniejsze niż jej ambicje".

Problem polega jednak na tym, że we władzach istnieje zbyt wiele grup mających swój ukryty interes w podtrzymywaniu lęku przed terroryzmem: rząd, szukający w nim uzasadnienia dla swoich działań; producenci sprzętu do inwigilacji i przemysł zbrojeniowy, zalewane funduszami publicznymi; i stale walczące o władzę frakcje w Waszyngtonie, pragnące bez przeszkód promować swoje priorytety. Wskazał na to Stephen Walt:

Mueller i Stewart szacują, że wydatki na bezpieczeństwo kraju (tzn. nie licząc wojen w Iraku i Afganistanie) wzrosły od 11 września o ponad bilion, choć roczne ryzyko śmierci na skutek ataku terrorystycznego w kraju wynosi około 1 do 3,5 miliona. Posługując się ostrożnymi założeniami i konwencjonalną metodologią szacowania ryzyka, oceniają, że aby te wydatki okazały się opłacalne, „musiałyby corocznie przeciwdziałać, zapobiegać, niweczyć lub chronić przed 333 bardzo wielkimi, skutecznymi atakami". Obawiają się także, że to nakręcone poczucie zagrożenia zostało już „zinternalizowane": nawet jeśli politycy i „specjaliści do spraw terroryzmu" nie wyolbrzymiają niebezpieczeństwa, społeczeństwo i tak uważa zagrożenie za wielkie i bliskie.

Tak jak manipuluje się strachem przed terroryzmem, tak samo poważnie pomniejsza się udowodnione niebezpieczeństwa wynikające z pozwolenia państwu na prowadzenie ogromnego tajnego systemu inwigilacji.

Nawet gdyby poziom zagrożenia terroryzmem był tak wielki, jak twierdzi rząd, i tak nie uzasadniałoby to programów inwigilacyjnych NSA. Wartości inne niż fizyczne bezpieczeństwo są co najmniej tak samo ważne, jeśli nie ważniejsze. Uznanie tego faktu od samego początku zostało wbudowane w amerykańską kulturę polityczną, a w innych państwach jest nie mniej istotne.

Narody i jednostki nieustannie dokonują wyborów, które wartość prywatności, a domyślnie – wolności stawiają nad innymi, w tym nad bezpieczeństwem fizycznym. Co więcej, czwarta poprawka do amerykańskiej konstytucji ma na celu niedopuszczenie do niektórych działań policji, nawet jeśli mogłyby one prowadzić do spadku przestępczości. Gdyby policji wolno było wpadać do każdego domu bez nakazu sądowego, być może łatwiej ujmowano by morderców, gwałcicieli i porywaczy. Gdyby państwu wolno było umieścić w naszych domach kamery, przestępczość prawdopodobnie znacząco by spadła

(niewątpliwie sprawdziłoby się to w przypadku włamań do mieszkań, ale większość ludzi zareagowałaby na taką propozycję obrzydzeniem). Gdyby FBI pozwolono słuchać naszych rozmów i czytać naszą korespondencję, prawdopodobnie dałoby się zapobiec wielu przestępstwom, a w innych znaleźć sprawcę.

Jednak konstytucję napisano po to, by nie dopuścić do takiej pozbawionej podstaw ingerencji państwa. Stawiając barierę przed tego rodzaju działaniami, świadomie dopuszczamy możliwość większej przestępczości. Mimo to ją stawiamy, ryzykując większe zagrożenie, ponieważ dążenie do absolutnego bezpieczeństwa fizycznego nigdy nie było dla nas jedynym, przewyższającym wszystko inne priorytetem.

Nasz fizyczny dobrobyt ustępuje potrzebie utrzymania państwa poza naszą sferą prywatną – potrzebie „nietykalności osobistej, mieszkania, dokumentów i mienia", jak to ujęto w czwartej poprawce. Wynika to z tego, że ta strefa jest podstawą tak wielu cech nieodmiennie kojarzonych z jakością życia – kreatywnością, emocjami, intymnością.

Wyrzeczenie się prywatności w pogoni za absolutnym bezpieczeństwem jest szkodliwe i dla zdrowia psychicznego, i życia jednostki, i dla jakości kultury politycznej. Dla jednostki stawianie bezpieczeństwa na pierwszym miejscu oznacza życiowy paraliż i strach – nigdy nie wsiadać do samochodu ani samolotu, nigdy nie angażować się w nic, co wiąże się z ryzykiem, nigdy nie przedkładać jakości życia nad ilość i płacić każdą cenę, byle tylko uniknąć niebezpieczeństwa.

Władze bardzo lubią posługiwać się taktyką strachu właśnie dlatego, że strach tak przekonująco racjonalizuje ekspansję władzy i ograniczanie praw. Od początku wojny z terrorem Amerykanom często mówiono, że jeśli chcą uniknąć katastrofy, muszą wyrzec się podstawowych praw. Oto na przykład wypowiedź Pata Robertsa, przewodniczącego senackiej Komisji Wywiadu:

„Zdecydowanie popieram pierwszą poprawkę, czwartą poprawkę i swobody obywatelskie. Nie masz jednak żadnych swobód obywatelskich, jeśli jesteś martwy". Zaś republikański senator John Cornyn, który w ramach kampanii o reelekcję w Teksasie pokazywał wideo z sobą samym jako twardym facetem w kowbojskim kapeluszu, wygłosił tchórzliwy pean na rzecz wyrzeczenia się praw: „Żadne swobody obywatelskie nie mają znaczenia, gdy jesteś martwy".

Wtórował im autor popularnego programu radiowego Rush Limbaugh, odsłaniając swą historyczną ignorancję pytaniem do wielkiej publiczności: „Kiedy ostatni raz słyszeliście, by prezydent wypowiadał wojnę, argumentując, że musimy chronić nasze swobody obywatelskie? Nic mi nie przychodzi do głowy. [...] Nasze swobody obywatelskie są bezwartościowe, jeśli jesteśmy martwi! Jeśli jesteś martwy i wąchasz kwiatki od spodu, jeśli gryziesz ziemię, to wiesz, ile warte są twoje swobody obywatelskie? Nic, zero".

Społeczeństwo czy kraj, które przedkładają fizyczne bezpieczeństwo nad wszystkie inne wartości, w końcu wyrzekną się wolności i usankcjonują każdą siłą wziętą władzę w zamian za obietnicę – choćby całkowicie iluzoryczną – totalnego bezpieczeństwa. Jednak absolutne bezpieczeństwo to chimera, coś, do czego można dążyć, ale czego nigdy nie można osiągnąć. Dążenie takie poniża tych, którzy je podejmują, i każdy naród, który jest przez nie definiowany.

Niebezpieczeństwo wynikające z faktu, że państwo prowadzi masowy tajny system inwigilacji, jest teraz znacznie groźniejsze niż kiedykolwiek przedtem. Podczas gdy rząd dzięki inwigilacji wie coraz więcej, co robią obywatele, ci wiedzą coraz mniej, co robi rząd, ponieważ kryje się za murem tajemnicy.

Nie da się wystarczająco mocno powiedzieć, jak radykalnie ta sytuacja odwraca dynamikę zdrowego społeczeństwa albo jak fundamentalnie przesuwa ciężar władzy na państwo.

Panoptykon Benthama zaprojektowany tak, by władza dysponowała niepodważalną siłą, opierał się dokładnie na tym właśnie odwróceniu: „Istotą rzeczy – pisał – jest centralne położenie nadzorcy [w połączeniu z] najskuteczniejszymi urządzeniami pozwalającymi widzieć bez bycia widzianym".

W zdrowej demokracji sytuacja jest odwrotna. Demokracja wymaga odpowiedzialności i zgody rządzonych możliwej jedynie wówczas, gdy obywatele są świadomi, co robi się w ich imieniu. Założenie jest takie, że – z nielicznymi wyjątkami – będą wiedzieć o wszystkim, co czynią ich polityczni przedstawiciele, którzy dlatego nazywani są pracownikami służby cywilnej, pracującymi w sektorze publicznym, w służbie publicznej, dla agend publicznych. Z drugiej strony zakłada się, że rząd – z nielicznymi wyjątkami – nie będzie wiedział o niczym, co robi obywatel, o ile przestrzega prawa. Dlatego jesteśmy prywatnymi jednostkami funkcjonującymi w sferze prywatnej. Przejrzystość obowiązuje tych, którzy wypełniają obowiązki publiczne i sprawują władzę publiczną.

Prywatność jest dla wszystkich innych.

ROZDZIAŁ 5

CZWARTA WŁADZA

Jedną z głównych instytucji, rzekomo powołanych do patrzenia władzy państwowej na ręce, są media. W teorii czwarta władza ma pilnować przejrzystości działań rządu i nie dopuszczać, by nadużywał swoich uprawnień. Sekretna inwigilacja całych populacji niewątpliwie jest jednym z najskrajniejszych przykładów takiego nadużycia. Kontrola ze strony prasy jest jednak skuteczna jedynie wówczas, gdy dziennikarze występują jako adwersarze tych, którzy sprawują władzę polityczną. Media amerykańskie często rezygnują jednak z pełnienia tej roli, podporządkowując się interesom rządu, wręcz nagłaśniając jego działania, zamiast się im uważnie przyglądać, i wykonując za rząd brudną robotę.

W takim kontekście wiedziałem, że nie uniknę wrogiej reakcji mediów na moje teksty o odkryciach Snowdena. 6 czerwca, dzień po ukazaniu się w „Guardianie" pierwszego artykułu na temat NSA, „New York Times" wspomniał o możliwości śledztwa. „Glenn Greenwald, który od lat intensywnie, nawet obsesyjnie pisze o rządowej inwigilacji i prześladowaniu dziennikarzy, postawił się nagle dokładnie na skrzyżowaniu tych dwóch spraw, a być może także na celowniku prokuratury federalnej" – napisano w artykule nakreślającym moją sylwetkę. Dodano jeszcze, że moje teksty na temat NSA „niewątpliwie spowodują dochodzenie ze strony Departamentu Sprawiedliwości, który

energicznie ściga źródła przecieków". W artykule zacytowano neokonserwatystę Gabriela Schoenfelda z Hudson Institute, który od dawna opowiada się za ściganiem dziennikarzy publikujących tajne informacje, mnie zaś nazwał „wysoce profesjonalnym apologetą wszelkiego rodzaju antyamerykanizmu, nawet najbardziej skrajnego".

Szczególnie dobitne dowody intencji „New York Timesa" dostarcza cytowana w tym samym artykule wypowiedź dziennikarza Andrew Sullivana: „Gdy człowiek raz wda się z nim [Greenwaldem] w dyskusję, trudno mieć ostatnie słowo", oraz: „Wydaje mi się, że nie całkiem zdaje sobie sprawę, co to naprawdę znaczy rządzić krajem czy prowadzić wojnę". Zdenerwowany wykorzystaniem jego wyrwanych z kontekstu uwag, Andrew przysłał mi później całą swoją rozmowę z reporterką „New York Timesa" Leslie Kaufman. Wyrażał w niej pochwałę dla mojej pracy, czego gazeta jednak nie zamieściła. Jeszcze więcej mówiące były pytania, które Kaufman mu pierwotnie wysłała:

Najwyraźniej ma zdecydowane poglądy, ale jaki jest jako dziennikarz? Wiarygodny? Uczciwy? Cytuje wiernie rozmówcę? Dokładnie opisuje jego stanowisko? Czy też jest bardziej rzecznikiem niż dziennikarzem?

Mówi, że jest pana przyjacielem, czy rzeczywiście? Mam wrażenie, że to raczej samotnik, który głosi tak bezkompromisowe opinie, że utrudnia to utrzymanie przyjaźni, ale mogę się mylić.

Drugie pytanie – o to, czy jestem „raczej samotnikiem", który nie potrafi utrzymywać przyjaźni – było w pewnym sensie jeszcze bardziej znaczące niż pierwsze. Dyskredytowanie posłańca jako nieudacznika, by pomniejszyć znaczenie przyniesionej przez niego wiadomości, to stara zagrywka wobec sygnalistów, i często bywa skuteczna.

Staranie, by zdyskredytować mnie osobiście, stało się jeszcze wyraźniejsze, gdy otrzymałem e-mail od reportera z „New York Daily News". Napisał, że zajmuje się różnymi aspektami mojej przeszłości, w tym długami, zobowiązaniami podatkowymi i udziałami pewnej prywatnej korporacji, której akcje osiem lat temu posiadałem, w firmie rozpowszechniającej filmy wideo dla dorosłych. Ponieważ „Daily News" to tabloid często uciekający się do oszczerczych ataków osobistych, uznałem, że nie ma co reagować, bo zwróciłoby to tylko większą uwagę na wyciągane przez nich sprawy.

Tego samego dnia otrzymałem jednak e-mail także od reportera „New York Timesa" Michaela Schmidta, również zainteresowanego moimi dawnymi zaległościami podatkowymi. Jak dwie gazety równocześnie dowiedziały się o tak mało znanych szczegółach, pozostawało tajemnicą – „New York Times" jednak najwyraźniej uznał, że warto napisać o moim dawnym długu, choć odmawiał sensownego wyjaśnienia dlaczego.

Te kwestie, wyraźnie trywialne, miały mnie oczernić. „New York Times" w końcu nic nie opublikował, inaczej niż „Daily News", gdzie opisano nawet szczegóły konfliktu w budynku, w którym mieszkałem dziesięć lat temu – chodziło o to, że mój pies jakoby ważył więcej niż limit określony przez regulamin kondominium.

O ile spodziewałem się kampanii oszczerstw, o tyle nie byłem przygotowany na podważanie mego statusu dziennikarza – to zaś mogło mieć potencjalnie drastyczne konsekwencje. Także i tę kampanię rozpoczął „New York Times" w artykule z 6 czerwca. Już w tytule gazeta bardzo się starała, by nie nazywać mnie dziennikarzem: *W centrum tej debaty jest bloger zajmujący się inwigilacją.* Choć tytuł był okropny, jego pierwsza wersja była jeszcze gorsza: *W centrum nowego przecieku jest aktywista przeciwny inwigilacji.*

Margaret Sullivan, redaktor publiczny „New York Timesa" (odpowiada za standardy dziennikarskie), skrytykowała tytuł,

stwierdzając, że jest „lekceważący". Dodała: „Oczywiście nie ma niczego złego w byciu blogerem – sama jestem blogerką. Jednak kiedy słowa tego używają media, sugeruje to, że mówią: «nie jesteś jednym z nas»".

W artykule cały czas unikano określenia mnie jako „dziennikarza" czy „reportera". Stwierdzano, że jestem „prawnikiem i wieloletnim blogerem" (od sześciu lat nie działam jako prawnik, a od lat pracuję jako publicysta w znaczących mediach, poza tym wydałem cztery książki). W sensie „pracy dziennikarskiej", pisano, moje doświadczenie jest „niezwykłe" nie ze względu na moje „zdecydowane opinie", ale dlatego, że „rzadko byłem podporządkowany redaktorowi".

Potem media zaangażowały się w debatę, czy rzeczywiście jestem „dziennikarzem", czy kimś innym. Najczęściej mówiono o „aktywiście". Nikt nie zadawał sobie trudu, żeby zdefiniować któreś z tych słów; zamiast tego opierano się na mało konkretnych banałach, jak to bywa w mediach, szczególnie gdy celem jest demonizacja. Od tamtej pory rutynowo stosowano tę pustą, jałową etykietkę.

To określenie jest jednak ważne, i to w kilku aspektach. Przede wszystkim usunięcie określenia „dziennikarz" pomniejsza wiarygodność reportera. Ponadto uczynienie ze mnie „aktywisty" może mieć prawne – czyli karne – konsekwencje. Dziennikarze objęci są i formalną, i umowną (niepisaną) ochroną prawną, która nie przysługuje nikomu innemu. Choć na ogół uważa się, że dziennikarz ma prawo publikować na przykład rządowe sekrety, to nie dotyczy to nikogo, kto działa w innym charakterze.

W sposób zamierzony czy nie ci, którzy twierdzili, że nie jestem dziennikarzem – mimo że pisałem dla jednej z najstarszych i największych gazet w świecie zachodnim – ułatwiali rządowi uznanie moich tekstów za przestępstwo. Gdy „New York Times" uznał mnie za „aktywistę", Sullivan przyznała,

że „te sprawy w obecnym klimacie nabrały większego znaczenia i mogą być kluczowe dla pana Greenwalda".

Aluzja do „obecnego klimatu" to skrótowe nawiązanie do dwóch znaczących sporów, które podzieliły Waszyngton w kwestii traktowania dziennikarzy przez administrację rządową. Pierwszy spór odnosił się do tajnego przejęcia przez Departament Sprawiedliwości e-maili i rejestrów rozmów telefonicznych reporterów i redaktorów Associated Press w celu zidentyfikowania źródła pewnej wiadomości.

Drugi, jeszcze skrajniejszy incydent, dotyczył podjętych przez Departament Sprawiedliwości działań zmierzających do odkrycia tożsamości innego źródła przecieku tajnych informacji. W tym celu departament złożył zaprzysiężone oświadczenie w sądzie federalnym, wnioskując o nakaz udostępnienia e-maili Jamesa Rosena, szefa waszyngtońskiego biura telewizji Fox News.

We wniosku prawnicy rządowi nazwali Rosena „współwinnym" w przestępstwie popełnionym przez informatora, dlatego że otrzymał tajne materiały. Oświadczenie było szokujące, ponieważ – jak sformułował to „New York Times" – „żaden amerykański dziennikarz nigdy nie był prześladowany za zbieranie i publikację poufnych informacji, więc użyty język pozwala przypuszczać, że administracja Obamy przenosi ściganie przecieków na nowy poziom".

Departament Sprawiedliwości uzasadniał nazwanie Rosena „współwinnym", powołując się na jego postępowanie – współpracę z informatorem w celu uzyskania dokumentów, ustanowienie „tajnego planu porozumiewania się", by rozmawiać bez wykrycia, oraz „stosowanie pochlebstw i granie na próżności i ego [informatora]", by przekonać go do przecieku. To wszystko jednak należy do rutynowego postępowania dziennikarza śledczego.

Jak to ujął doświadczony waszyngtoński reporter Olivier Knox, Departament Sprawiedliwości „oskarżył Rosena,

że złamał prawo przeciwko szpiegostwu, postępując w sposób, który – według opisu w zaprzysiężonym oświadczeniu agenta – doskonale mieści się w granicach tradycyjnego dziennikarstwa". Uznanie postępowania Rosena za przestępstwo oznacza uznanie za przestępstwo samego dziennikarstwa.

Takie postępowanie departamentu nie było może szczególnie zaskakujące, jeśli weźmie się pod uwagę szerszy kontekst: ataki administracji Obamy na sygnalistów i informatorów. W 2010 roku „New York Times" ujawnił, że Departament Sprawiedliwości, starając się znaleźć źródło artykułu napisanego przez Jima Risena, „uzyskał obszerne dane na temat jego połączeń telefonicznych, finansów i podróży", w tym „dane o kartach kredytowych i rachunkach bankowych, pewne dane o jego podróżach samolotem oraz trzy raporty z jego rozliczeniami finansowymi".

Departament Sprawiedliwości próbował także zmusić Risena do ujawnienia tożsamości jego informatora, sugerując, że jeśli odmówi, może go czekać więzienie. Takie potraktowanie Risena przeraziło dziennikarzy w całym kraju: skoro jeden z najbardziej zasłużonych i chronionych przez instytucję dziennikarzy śledczych stał się celem tak agresywnego ataku, to może to także dotknąć każdego reportera.

Prasa zareagowała niepokojem. Typowy dla tej reakcji artykuł z „USA Today" wskazywał, że „prezydent Obama musi teraz odpierać zarzuty, iż jego administracja w gruncie rzeczy wydała wojnę dziennikarzom", i cytował wypowiedź byłego dziennikarza „Los Angeles Timesa" specjalizującego się w sprawach bezpieczeństwa narodowego Josha Meyera: „Istnieje czerwona linia, której żadna poprzednia administracja nie przekroczyła, a administracja Obamy po prostu nad nią przemknęła". Jane Mayer, powszechnie szanowana dziennikarka śledcza „New Yorkera", ostrzegała w „New Republic", że atak prowadzony przez Departament Sprawiedliwości Obamy przeciwko

sygnalistom jest w gruncie rzeczy atakiem przeciwko dziennikarstwu jako takiemu: „To ogromne utrudnienie w pracy reportera; ochłodzenie nie jest wystarczająco mocnym słowem, mówmy raczej o zamrożeniu całego procesu".

Sytuacja ta do tego stopnia poruszyła Komitet Ochrony Dziennikarzy – międzynarodową organizację monitorującą zagrożenia dla wolności prasy ze strony państwa – że wydał on pierwszy w historii raport na temat Stanów Zjednoczonych. Opublikowany w październiku 2013 roku i napisany przez Leonarda Downiego Jr., byłego redaktora naczelnego „Washington Post", podsumowywał:

Wojna wydana przez administrację przeciekom i inne próby kontroli informacji przybrały formę najbardziej agresywną [...] od czasów administracji Nixona [...]. Żaden z trzydziestu doświadczonych dziennikarzy z Waszyngtonu, związanych z różnymi organizacjami prasowymi [...], którzy wypowiadali się na potrzeby tego raportu, nie przypominał sobie żadnego precedensu.

Dynamika tego procesu wykroczyła poza kwestie bezpieczeństwa narodowego i – jak powiedział jeden z szefów biur – objęła próby „utrudnienia dziennikarzom pisania o odpowiedzialności *agencji* rządowych".

Dziennikarze amerykańscy, od lat zakochani w Baracku Obamie, powszechnie zaczęli mówić, że stanowi poważne zagrożenie dla wolności prasy i pod tym względem jest najbardziej represyjnym przywódcą od czasów Richarda Nixona. To godna uwagi zmiana tonu w stosunku do polityka, który doszedł do władzy, obiecując „najbardziej przejrzystą administrację w historii USA".

Próbując zdusić rosnący skandal, Obama kazał prokuratorowi generalnemu Erikowi Holderowi spotkać się z przedstawicielami mediów i przedyskutować zasady kierujące traktowaniem dziennikarzy przez Departament Sprawiedliwości.

Obama deklarował „zaniepokojenie możliwością, że dochodzenie w sprawie przecieków zmrozi dziennikarstwo śledcze, które służy do rozliczania rządu" – zupełnie jak gdyby podczas pięciu lat właśnie takich ataków na proces zbierania informacji to nie on stał na czele rządu.

Podczas przesłuchania w Senacie 6 czerwca 2013 roku (dzień po publikacji pierwszego artykułu o NSA w „Guardianie") Holder przyrzekał, że Departament Sprawiedliwości nigdy nie będzie ścigał „żadnego reportera za to, że wykonuje swoją pracę". Celem departamentu, dodał, jest jedynie „zidentyfikowanie i ukaranie urzędników rządowych, którzy łamiąc przysięgę, wystawiają na szwank bezpieczeństwo narodowe, a nie ściganie przedstawicieli prasy czy też odwodzenie od wykonywania istotnego zadania".

Niewątpliwie była to pożądana reakcja – administracja najwyraźniej poczuła tak silny sprzeciw, że stworzyła przynajmniej pozory, iż podejmuje temat wolności prasy. W przyrzeczeniach Holdera znalazła się jednak ogromna, wyraźna luka: Departament Sprawiedliwości uznał, w przypadku Jamesa Rosena z Fox News, że współpraca z informatorem, mająca na celu „kradzież" poufnych informacji, wykracza poza zakres „zadań reportera". Zatem udzielona przez Holdera gwarancja zależała od tego, co Departament Sprawiedliwości uzna za dziennikarstwo i co jego zdaniem wykracza poza granice uprawnionego informowania.

Na tym tle podjęte przez niektóre osoby z mediów starania, by wyrzucić mnie z „dziennikarstwa" twierdzeniem, że to, co robię, to „aktywizm", a nie publicystyka – czyli że popełniam przestępstwo – były potencjalnie niebezpieczne.

Pierwsze wyraźne wezwanie do oskarżenia mnie padło z ust republikańskiego kongresmana z Nowego Jorku Petera Kinga, który uprzednio pełnił funkcję przewodniczącego Podkomisji Izby Reprezentantów do spraw Terroryzmu i prowadził utrzymane

w stylu McCarthy'ego przesłuchania w sprawie „wewnętrznego" zagrożenia terrorem ze strony muzułmańskiej społeczności w Ameryce (paradoksalne jest to, że King przez wiele lat popierał Irlandzką Armię Republikańską, IRA). King oświadczył Andersonowi Cooperowi z CNN, że reporterzy pracujący przy artykułach o NSA powinni być ścigani, „jeśli byli świadomi, że są to informacje tajne [...] szczególnie tak doniosłe". Dodał: „To obowiązek moralny, ale moim zdaniem także prawny, by wystąpić przeciwko reporterowi, który ujawnia coś tak poważnie wystawiającego na szwank bezpieczeństwo narodowe".

King wyjaśnił później w Fox News, że mówił konkretnie o mnie:

Mówię o Greenwaldzie [...] nie tylko ujawnił informacje, ale powiedział też, że zna nazwiska agentów CIA i jej aktywa na całym świecie, i groził, że je ujawni. Ostatnim razem, gdy w naszym kraju do tego doszło, szef placówki w Grecji został zamordowany [...]. Uważam, że [ściganie dziennikarzy] powinno być bardzo wybiórcze, ściśle wymierzone, i oczywiście stanowić rzadki wyjątek. Jednak w tym wypadku, gdy jest ktoś, kto ujawnia takie tajemnice i grozi, że ujawni więcej – tak, przeciwko niemu należy podjąć działania prawne.

To, że groziłem ujawnieniem nazwisk i aktywów CIA, było bezczelnym kłamstwem wymyślonym przez Kinga. Niemniej jednak jego słowa otworzyły śluzy i komentatorzy ruszyli falą. Marc Thiessen z „Washington Post", były autor przemówień Busha i książki usprawiedliwiającej amerykański program tortur, bronił Kinga pod nagłówkiem: *Tak, publikacja tajemnic NSA to przestępstwo.* Oskarżając mnie o „naruszenie 18 USC 798, gdzie określono, że przestępstwem jest publikowanie tajnych informacji ujawniających rządowe dane wywiadu z kryptografii lub łączności", dodał: „Greenwald wyraźnie pogwałcił to prawo (zresztą tak samo jak «Post», gdy opublikował tajne

szczegóły prowadzonego przez NSA programu PRISM)".

Alan Dershowitz oznajmił w programie CNN: „Greenwald – moim zdaniem – niewątpliwie popełnił przestępstwo". Dershowitz, choć znany jako obrońca swobód obywatelskich i wolności prasy, uznał jednak, że moje artykuły „nie stoją na granicy przestępstwa – one znajdują się dokładnie w sercu przestępstwa".

Do tego rosnącego chóru dołączył generał Michael Hayden, były szef NSA, a potem CIA za prezydentury George'a W. Busha, który wprowadził nielegalny, realizowany bez nakazu sądowego program podsłuchów. „Edward Snowden – napisał na CNN.com – prawdopodobnie okaże się najbardziej kosztownym źródłem przecieku amerykańskich tajemnic w historii republiki", a następnie dodał: „Glenn Greenwald [...] znacznie bardziej zasługuje, by Departament Sprawiedliwości nazwał go współwinnym, niż James Rosen z Fox".

Chór głosów podnoszących kwestię oskarżenia – początkowo ograniczony głównie do przedstawicieli prawicy, po których można spodziewać się traktowania dziennikarstwa jako zbrodni – przybrał na sile podczas niesławnego wystąpienia w programie *Meet the Press*.

Sam Biały Dom chwalił *Meet the Press* jako wygodne miejsce, gdzie politycy waszyngtońscy i inni członkowie elit mogą wygłaszać swoje opinie bez ryzyka, że zostaną one podważone. Catherine Martin, dyrektor do spraw komunikacji byłego wiceprezydenta Dicka Cheneya, chwaliła ten cotygodniowy program NBC jako „nasz najlepszy format", ponieważ Cheney był w stanie „kontrolować informacje". Udział wiceprezydenta w *Meet the Press*, powiedziała, był „często stosowaną przez nas taktyką". Rzeczywiście, film wideo, na którym prowadzący program David Gregory tańczy niezgrabnie, choć entuzjastycznie na scenie za rapującym Karlem Rove'em podczas obiadu korespondentów prasowych w Białym Domu, rozprzestrzeniał się jak wirus, ponieważ tak żywo obrazował to, czym jest

ten program: miejscem, do którego możni świata polityki idą, by im kadzono i pochlebiano, gdzie słyszy się tylko najbardziej obiegowe sądy, gdzie dopuszcza się jedynie bardzo wąski zakres poglądów.

Zaproszono mnie do programu w ostatniej chwili i tylko z konieczności. Parę godzin wcześniej podano wiadomość, że Snowden opuścił Hongkong i znajduje się na pokładzie samolotu lecącego do Moskwy. Tak niespodziewany rozwój wydarzeń niewątpliwie musiał zdominować programy informacyjne. *Meet the Press* nie miało innego wyjścia, jak podjąć ten temat, zaproszono mnie więc jako głównego gościa, ponieważ należałem do tych nielicznych, którzy mieli ze Snowdenem kontakt.

Od lat ostro krytykowałem Gregory'ego, oczekiwałem więc, że wywiad będzie miał napastliwy charakter. Nie spodziewałem się jednak, że Gregory zapyta: „Na tyle, na ile udzielił pan pomocy Snowdenowi w popełnieniu przestępstwa, a nawet w jego obecnych ruchach, dlaczego pan nie miałby zostać oskarżony o przestępstwo, panie Greenwald?". W tym pytaniu zawierało się tyle błędów, że chwilę trwało, zanim do mnie dotarło, że rzeczywiście je zadał.

Najjaskrawszym problemem były zawarte w tym pytaniu pozbawione podstaw założenia. „Na tyle, na ile udzieliłem pomocy Snowdenowi, nawet w jego obecnych ruchach" nie różni się niczym od powiedzenia: „Na tyle, na ile pan Gregory zamordował swoich sąsiadów...". Był to klasyczny przykład pytania typu: „Kiedy przestał pan bić żonę?".

Pomijając jednak tę retoryczną zwodniczość, dziennikarz telewizyjny właśnie wyraził przekonanie, że jego koledzy po fachu mogą i powinni być ścigani za wykonywanie swego zawodu. To niezwykłe stwierdzenie. Pytanie Gregory'ego sugerowało, że każdy reporter śledczy w Stanach Zjednoczonych, który korzysta z informatorów i otrzymuje tajne informacje, jest przestępcą. To właśnie ta teoria i ten klimat sprawiały, że dziennikarstwo śledcze stało się tak ryzykowne.

Jak można było się spodziewać, Gregory cały czas przedstawiał mnie jako kogoś innego niż dziennikarza. We wstępie do jednego z pytań oświadczył: „Jest pan tu polemistą, ma pan własny punkt widzenia, jest pan publicystą". I ogłosił: „W odniesieniu do tego, co pan robi, można się spierać, kto właściwie jest dziennikarzem".

Jednak Gregory nie był jedyną osobą, która wysuwała takie argumenty. Żaden z panelistów w *Meet the Press*, mających dyskutować o mojej wymianie zdań z Gregorym, nie zaprotestował przeciwko poglądowi, że dziennikarz może zostać pociągnięty do odpowiedzialności za współpracę z informatorem. Chuck Todd z NBC wsparł tę teorię, niepokojąco podnosząc „kwestię" tego, co nazwał moją „rolą w akcji":

Glenn Greenwald [...] jak bardzo był zaangażowany w tę akcję? [...] Czy odegrał jakąś rolę poza tym, że był po prostu osobą otrzymującą informacje? I czy będzie musiał odpowiedzieć na te pytania? Bo przecież istnieje – istnieje – aspekt prawny.

Podczas *Reliable Sources*, jednego z programów CNN, na ekranie cały czas widniała grafika z napisem: „Czy Glenn Greenwald powinien zostać oskarżony?".

Walter Pincus z „Washington Post" – który w latach 60. ubiegłego wieku szpiegował przebywających za granicą amerykańskich studentów dla CIA – napisał artykuł zawierający sugestię, że Laura, Snowden i ja należymy do spisku, którym potajemnie kieruje założyciel WikiLeaks Julian Assange. W artykule znalazło się tak wiele błędów rzeczowych (które udokumentowałem w liście otwartym do Pincusa), że „Post" poczuł się zmuszony zamieścić nieprzeciętnie długie, składające się z trzech paragrafów i dwustu słów sprostowanie, w którym przyznał, że popełniono błędy.

Komentator finansowy „New York Timesa" Andrew Ross Sorkin powiedział we własnym programie w CNBC:

Moim zdaniem: A – spieprzyliśmy sprawę, pozwalając [Snowdenowi] dostać się do Rosji. B – Chińczycy muszą nas nienawidzić, skoro wypuścili go z kraju. [...] Ja bym go aresztował, a teraz niemal aresztowałbym Glenna Greenwalda, dziennikarza, który najwyraźniej pragnie pomóc mu dostać się do Ekwadoru.

Fakt, że dziennikarz „New York Timesa", który aż po Sąd Najwyższy USA walczył o publikację Pentagon Papers, teraz opowiada się za aresztowaniem mnie, dobitnie świadczy, jak bardzo wielu należących do establishmentu dziennikarzy jest oddanych amerykańskiemu rządowi: ostatecznie uznanie aspektów dziennikarstwa śledczego za przestępstwo miałoby poważny wpływ na tę gazetę i jej pracowników. Sorkin mnie później przeprosił, ale jego uwagi ukazywały, w jakim tempie i z jaką łatwością takie stwierdzenia się rozchodzą.

Na szczęście amerykański korpus prasowy bynajmniej nie był jednomyślny w tych poglądach. Co więcej, widmo kryminalizacji sprawiło, że wielu dziennikarzy ruszyło w obronie moich działań, a gospodarzy licznych znaczących programów telewizyjnych bardziej interesowały ujawnione treści niż demonizowanie zaangażowanych w to osób. W tygodniu po mojej rozmowie z Gregorym jego pytanie dość powszechnie potępiano. Z *Huffington Post*: „Wciąż nie możemy uwierzyć w to, o co David Gregory zapytał Glenna Greenwalda". Toby Harnden, szef waszyngtońskiego biura brytyjskiego „Sunday Timesa", tweetował: „Byłem więziony w Zimbabwe Mugabego za «praktykowanie dziennikarstwa». Czy David Gregory mówi, że Ameryka Obamy powinna robić to samo?". Wielu dziennikarzy i publicystów z „New York Timesa", „Washington Post" i innych broniło mnie publicznie i prywatnie. Jednak największe nawet poparcie nie mogło zmienić faktu, że sami dziennikarze usankcjonowali perspektywę odpowiedzialności karnej.

Prawnicy i inni doradcy zgadzali się, że w razie powrotu do USA naprawdę mogę zostać aresztowany. Starałem się znaleźć choć jedną osobę, której bym ufał, a która powiedziałaby mi, że nie ma takiego ryzyka, że to niemożliwe, by Departament Sprawiedliwości się do tego posunął. Nie znalazłem. Powszechnie uważano, że Departament Sprawiedliwości nie wystąpi przeciwko mnie za moje reportaże, by nie stwarzać wrażenia, że ściga dziennikarzy; obawiano się natomiast, że rząd przedstawi teorię, iż rzekomo popełnione przeze mnie przestępstwa leżą poza dziennikarstwem. Inaczej niż Barton Gellman z „Washington Post" przed publikacją pojechałem do Hongkongu na spotkanie ze Snowdenem; rozmawiałem z nim regularnie po jego przybyciu do Rosji, a także publikowałem artykuły o NSA jako niezależny dziennikarz w gazetach na całym świecie. Departament Sprawiedliwości mógł próbować twierdzić, że „pomagałem Snowdenowi w przestępstwie" przecieku lub że pomogłem „ściganemu" umknąć przed sprawiedliwością albo że moja praca dla zagranicznych gazet stanowi jakiś rodzaj szpiegostwa.

Ponadto moje komentarze na temat NSA i rządu amerykańskiego specjalnie były agresywne i wyzywające. Niewątpliwie rząd desperacko pragnął ukarać kogoś za to, co nazwano najbardziej szkodliwym przeciekiem w historii kraju – jeśli nie po to, by rozładować wściekłość instytucji, to przynajmniej by zniechęcić innych. Skoro człowiek, którego głowę najchętniej nabito by na pal, znalazł się bezpiecznie pod ochroną politycznego azylu w Moskwie, Laura i ja staliśmy się pożądanym celem w drugiej kolejności.

Przez kilka miesięcy paru prawników mających kontakty z wysoko postawionymi osobami w Departamencie Sprawiedliwości próbowało uzyskać nieoficjalne zapewnienie, że nie zostanę oskarżony. W październiku, pięć miesięcy po publikacji pierwszego artykułu, kongresman Alan Grayson napisał do prokuratora generalnego Holdera, wskazując, że znaczący

politycy nalegali na moje aresztowanie i że musiałem odmówić zaproszenia do złożenia zeznań przed Kongresem na temat NSA z obawy przed możliwym oskarżeniem. Na zakończenie listu stwierdził:

Uważam to za godne pożałowania, ponieważ: 1 – wykonywanie zawodu dziennikarza nie jest przestępstwem; 2 – wręcz przeciwnie, jest wyraźnie chronione zgodnie z pierwszą poprawką do konstytucji; 3 – artykuły pana Greenwalda na te tematy poinformowały mnie, innych członków Kongresu i społeczeństwo o poważnych, wielokrotnych naruszeniach prawa i praw konstytucyjnych przez agentów rządowych.

Kongresman pytał w liście, czy Departament Sprawiedliwości zamierza postawić mi zarzuty i czy, gdybym próbował wjechać na teren Stanów Zjednoczonych, „Departament Sprawiedliwości, Departament Bezpieczeństwa Krajowego czy jakikolwiek inny urząd rządu federalnego zamierzają zatrzymać, przepytywać, aresztować [mnie] lub wysunąć zarzuty" przeciwko mnie. Jak w grudniu donosił „Orlando Sentinel", gazeta z rodzinnego miasta Graysona, kongresman nie otrzymał odpowiedzi na swój list.

Pod koniec 2013 i na początku 2014 roku groźba oskarżenia mnie wzrosła, ponieważ urzędnicy rządowi wciąż przypuszczali wyraźnie skoordynowane ataki mające na celu uznanie mojej pracy za przestępstwo. Pod koniec października szef NSA Keith Alexander, jednoznacznie nawiązując do mojej pracy niezależnego dziennikarza na całym świecie, narzekał, że „reporterzy prasowi mają te wszystkie dokumenty, te pięćdziesiąt tysięcy czy ile tam mają, i sprzedają", a także groźnie twierdził, że „powinniśmy" – czyli rząd – „znaleźć sposób, jak to powstrzymać". Mike Rogers, przewodniczący Komisji Wywiadu Izby Reprezentantów, podczas wysłuchania w styczniu cały czas

powtarzał dyrektorowi FBI Jamesowi Corneyowi, że niektórzy dziennikarze „sprzedają kradzioną własność", co czyni z nich „paserów" albo „złodziei" – a potem sprecyzował, że mówi o mnie. Gdy w CBC/Radio-Canada zacząłem informować o szpiegostwie kanadyjskim, rzecznik parlamentu w prawicowym rządzie Stephena Harpera nazwał mnie „pornoszpiegiem" i oskarżył CBC o kupowanie ode mnie ukradzionych dokumentów. W Stanach Zjednoczonych dyrektor Wywiadu Narodowego (Director of National Intelligence, DNI) James Clapper zaczął posługiwać się prawnym określeniem „współwinnych w przestępstwie" w odniesieniu do dziennikarzy piszących o NSA.

Moim zdaniem prawdopodobieństwo, że zostanę aresztowany w chwili powrotu do USA, było mniejsze niż 50 procent, choćby ze względu na wizerunek i ogólnoświatową dyskusję. Potencjalna plama na wizerunku Obamy jako pierwszego prezydenta, który ścigał dziennikarza za wykonywanie swojej pracy, stanowiła – jak zakładałem – wystarczający hamulec. Z drugiej strony, jeśli sądzić po niedawnej przeszłości, widać, że rząd USA był skłonny postępować w różny godny potępienia sposób i nie przejmować się tym, jak postrzega go reszta świata, jeśli tylko mógł powołać się na bezpieczeństwo narodowe. Konsekwencje błędnej decyzji – czyli skończenie w kajdankach z oskarżeniem opartym na paragrafach dotyczących szpiegostwa oraz proces przed sądem federalnym, który w takich sprawach okazywał się bezwstydnie usłużny wobec Waszyngtonu – były zbyt poważne, by je lekceważyć. Byłem zdecydowany powrócić do USA, ale dopiero wtedy, gdy jasno zrozumiem ryzyko. Na razie rodzina, przyjaciele i rozliczne ważne okazje, by w Stanach Zjednoczonych mówić o wykonywanej przeze mnie pracy, pozostawały dla mnie niedostępne.

Prawnicy i jeden kongresman uważali, że samo ryzyko jest nienormalne i dobitnie świadczy o erozji wolności prasy. Natomiast fakt, że także i niektórzy dziennikarze zgodzili się

uważać moje artykuły za przestępstwo, stanowił godny uwagi triumf propagandy strony rządowej. Mogła ona liczyć, że wykształceni profesjonaliści wykonają za nią robotę i postawią znak równości między bezkompromisowym dziennikarstwem śledczym a przestępstwem.

Ataki przeciwko Snowdenowi były oczywiście znacznie bardziej zajadłe, a ich wydźwięk – zadziwiająco podobny. Czołowi komentatorzy, którzy nic w ogóle o Snowdenie nie wiedzieli, natychmiast przyjęli ten sam zestaw banałów, by go poniżyć. Zaledwie kilka godzin po tym, jak poznali jego nazwisko, pomaszerowali ramię w ramię, by oczernić jego charakter i motywy. Kierowało nim – mówili chórem – nie żadne prawdziwe przekonanie, ale „pragnienie sławy i narcyzm".

Bob Schieffer, prowadzący *CBS News*, potępił Snowdena jako „narcystycznego młodego człowieka", który uważa, że „jest mądrzejszy od nas wszystkich". Jeffrey Toobin z „New Yorkera" zdiagnozował, że jest on „napuszonym narcyzem, który powinien znaleźć się w więzieniu". Richard Cohen z „Washington Post" oświadczył, że Snowden „nie jest paranoikiem; jest po prostu narcyzem", co miało odnosić się do informacji, że Snowden przykrywał się kocem, by kamery w suficie nie mogły wyłapać wpisywanych do komputera haseł. Cohen dodał, niezrozumiale, że Snowden „zapisze się jako transwestycki Czerwony Kapturek", a jego rzekome pragnienie sławy „spali na panewce".

Taka charakterystyka była w oczywisty sposób absurdalna. Snowden powiedział, że zniknie z widoku i nie zamierza udzielać wywiadów. Rozumiał, że media uwielbiają personalizować każdą historię, on zaś chciał, by skupiono się na fakcie inwigilacji prowadzonej przez NSA, a nie na nim samym. Odmawiał więc zaproszeń do wystąpienia w mediach. Przez wiele miesięcy codziennie otrzymywałem e-maile i odbierałem telefony z niemal wszystkich amerykańskich programów

telewizyjnych, od prowadzących wiadomości i publicystykę po znanych dziennikarzy, błagających o szansę rozmowy ze Snowdenem. Gospodarz *Today Show* Matt Lauer dzwonił kilkakrotnie, bym się za nim wstawił; *60 Minutes* tak mnie prześladowało prośbami, że przestałem odbierać od nich telefony; Brian Williams wysłał kilku przedstawicieli, by nalegali w jego imieniu. Gdyby Snowden tylko chciał, mógłby występować przez całą dobę w najbardziej opiniotwórczych programach telewizyjnych, a świat by go słuchał.

On jednak pozostał nieporuszony. Przekazywałem mu prośby, a on je odrzucał, by nie odwracać uwagi od tego, co ujawnił. Dziwne zachowanie jak na szukającego sławy narcyza.

Potem przyszła kolej na inne oskarżenia pod adresem Snowdena. Publicysta „New York Timesa" David Brooks kpił z niego, twierdząc, że „nie udało mu się nawet skończyć szkoły". Snowden, zawyrokował Brooks, jest „człowiekiem w najwyższym stopniu bez powiązań", symbolem „rosnącej fali nieufności, niszczycielskiego rozprzestrzeniania się cynizmu, rozpadu tkanki społecznej i awansu ludzi, których poglądy są tak indywidualistyczne, że naprawdę nie rozumieją, jak łączyć innych w grupy i strzec wspólnego dobra".

Roger Simon z serwisu Politico uznał, że Snowden to „nieudacznik", ponieważ „nie skończył szkoły średniej". Demokratyczna kongresmanka Debbie Wasserman-Schultz, pełniąca także funkcję przewodniczącej Krajowego Komitetu Partii Demokratycznej, potępiła Snowdena, który właśnie zrujnował sobie życie, by ujawnić to, co robi NSA, jako „tchórza".

Jak można było się spodziewać, zakwestionowano patriotyzm Snowdena. Pojechał do Hongkongu, twierdzono więc, że zapewne pracował jako szpieg dla chińskiego rządu. „Nietrudno sobie wyobrazić, że Snowden był chińskim podwójnym agentem i wkrótce tam ucieknie" – oświadczył doświadczony republikański konsultant kampanijny Mark Mackowiak.

Gdy Snowden opuścił Hongkong, by przez Rosję dotrzeć do Ameryki Łacińskiej, w oskarżeniach gładko wymieniono szpiega chińskiego na rosyjskiego. Tacy ludzie jak kongresman Mike Rogers wysuwali to oskarżenie całkowicie bezpodstawnie, mimo oczywistego faktu, że Snowden został w Rosji tylko dlatego, iż Stany Zjednoczone unieważniły jego paszport, a potem groźbami zmusiły takie kraje jak Kuba do odwołania obietnicy bezpiecznego tranzytu. Co więcej, jaki rosyjski szpieg pojechałby do Hongkongu czy pracował z dziennikarzami i publicznie się przedstawił, zamiast po prostu przekazać swoją zdobycz szefom w Moskwie? Ten zarzut nigdy nie miał sensu i nie opierał się na żadnych faktach, ale nie przeszkodziło to w jego rozpowszechnianiu.

Do najbardziej bezczelnych i pozbawionych podstaw insynuacji posunął się „New York Times", twierdząc, że na wyjazd z Hongkongu pozwoliły Snowdenowi władze chińskie, a nie hongkońskie. Gazeta dodała do tego obrzydliwą, szkodzącą mu sugestię: „Dwaj zachodni eksperci do spraw wywiadu, którzy pracowali dla dużych rządowych agencji wywiadowczych, powiedzieli, że ich zdaniem rządowi chińskiemu mogło udać się przejęcie treści czterech laptopów, które pan Snowden, jak mówi, przywiózł do Hongkongu".

„New York Times" nie miał ani cienia dowodu, że chiński rząd zdołał wejść w posiadanie tych plików. Gazeta po prostu pozwoliła czytelnikom wnioskować, że tak było, na podstawie wypowiedzi dwóch anonimowych „ekspertów", których zdaniem „mogło" do tego dojść.

W dniu, w którym opublikowano ten artykuł, Snowden utknął na lotnisku w Moskwie i nie mógł podłączyć się do internetu. Gdy tylko znów się pojawił, zdecydowanie odrzucił zarzut, jakoby przekazał jakieś dane Chinom lub Rosji, w artykule, który opublikowałem w „Guardianie". „Nigdy nie przekazałem żadnych informacji żadnemu z tych rządów, oni zaś nigdy nie ściągnęli niczego z moich laptopów" – stwierdził.

Dzień po publikacji zaprzeczenia Snowdena Margaret Sullivan skrytykowała „New York Timesa" za artykuł. Przeprowadziła wywiad z Josephem Kahnem, redaktorem działu zagranicznego, który powiedział: „Ważne, żeby ten fragment artykułu odczytać właściwie: jako rozważanie, co mogło się zdarzyć, na podstawie wypowiedzi ekspertów, którzy nie twierdzili, że dysponują bezpośrednią wiedzą". Sullivan skomentowała, że „dwa zdania w środku artykułu «New York Timesa» na tak drażliwy temat – choć być może nie dotyczą głównego wątku – mogą skierować dyskusję na inne tory lub zaszkodzić czyjejś opinii". W zakończeniu zgodziła się z czytelnikiem, który poskarżył się na artykuł, pisząc: „Czytam «New York Timesa», żeby znać prawdę. Spekulacje mogę czytać niemal wszędzie".

Redaktor naczelna „New York Timesa" Jill Abramson podczas spotkania mającego na celu przekonanie „Guardiana" do współpracy przy niektórych artykułach o NSA przekazała mi przez Janine Gibson następującą wiadomość: „Chcę osobiście powiedzieć Glennowi Greenwaldowi, że całkowicie się z nim zgadzam, iż nie powinniśmy byli pisać o możliwości «ściągnięcia» zawartości laptopów Snowdena przez Chiny. To było nieodpowiedzialne".

Gibson wydawała się oczekiwać, że będę zadowolony, ale wcale tak się nie czułem. Jak redaktor naczelna gazety może mówić, że wyraźnie szkodliwy artykuł jest nieodpowiedzialny i nie powinien być opublikowany, a potem go nie odwołać ani nawet nie opublikować sprostowania od redaktora?

Pomijając brak dowodów, twierdzenie, że z laptopów Snowdena „ściągnięto" zawartość, nie miało sensu. Ludzie od lat nie używają laptopów do przewożenia wielkich ilości danych. Jeszcze zanim laptopy się rozpowszechniły, dokumenty przechowywano na dyskietkach, teraz zaś na przenośnych pamięciach USB. To prawda, że Snowden wziął ze sobą do Hongkongu

cztery laptopy, każdy służący innemu celowi bezpieczeństwa, ale nie miały one związku z zakresem przechowywanych przez niego dokumentów. Te znajdowały się na pendrive'ach, zaszyfrowane przy użyciu skomplikowanych metod kryptograficznych. Snowden, który pracował w NSA jako haker, wiedział, że nie odszyfruje ich nawet NSA, nie mówiąc już o chińskich czy rosyjskich agencjach wywiadu.

Ogłaszanie liczby laptopów Snowdena było zwodniczym sposobem grania na ignorancji i strachu ludzi – *zabrał tyle dokumentów, że potrzebował aż czterech laptopów, żeby je wszystkie zmagazynować.* A Chińczycy, gdyby nawet udało im się ściągnąć ich zawartość, nie pozyskaliby niczego przydatnego.

Równie nonsensowny był pomysł, że Snowden będzie próbował się ratować, ujawniając tajemnice inwigilacji. Zniszczył sobie życie i zaryzykował przyszłość w więzieniu, żeby poinformować świat o tajnym systemie inwigilacji, który jego zdaniem należało przerwać. Sugestia, że przeszedłby na drugą stronę, by pomóc Chinom lub Rosji w usprawnieniu ich zdolności inwigilacji, po prostu nie miała sensu.

A jednak, choć twierdzenie to było absurdalne, wyrządzona przez nie szkoda okazała się i znaczna, i łatwa do przewidzenia. Podczas wszystkich dyskusji na temat NSA nieodmiennie ktoś stwierdzał – nie spotykając się z żadnym sprzeciwem – że przez Snowdena Chiny znalazły się teraz w posiadaniu najbardziej wrażliwych sekretów USA. Pod tytułem *Dlaczego Chiny wypuściły Snowdena* „New Yorker" informował czytelników: „Jego przydatność niemal się wyczerpała. Eksperci do spraw wywiadu, cytowani przez «New York Timesa», uważają, że rządowi chińskiemu «mogło udać się przejęcie treści czterech laptopów, które pan Snowden, jak mówi, przywiózł do Hongkongu»".

Demonizowanie osobowości każdego, kto rzuca wyzwanie sile politycznej, to stara strategia Waszyngtonu, w tym mediów. Jednym z pierwszych i być może najjaskrawszych przykładów

tej taktyki było potraktowanie przez administrację Nixona Pentagon Papers i sygnalisty Daniela Ellsberga; rząd posunął się wówczas do włamania do biura jego psychoanalityka w celu kradzieży dokumentacji Ellsberga i grzebania w jego historii seksualnej. Choć taktyka ta może wydawać się absurdalna – dlaczego ujawnienie krępujących osobistych informacji miałoby niweczyć dowody oszustw rządu? – Ellsberg doskonale ją rozumiał: ludzie nie chcą, by kojarzono ich z kimś, kto został zdyskredytowany lub publicznie upokorzony.

Tę samą taktykę zastosowano do zniszczenia reputacji Juliana Assange'a na długo przedtem, zanim został oskarżony o przestępstwa seksualne przez dwie kobiety ze Szwecji. Warto zauważyć, że Assange'a atakowały te same gazety, które przedtem z nim współpracowały i dzięki WikiLeaks korzystały z materiałów ujawnionych przez Chelsea Manning (wówczas Bradleya Manninga).

Gdy „New York Times" opublikował to, co nazywał *Dziennikami wojny w Iraku*, tysiące tajnych dokumentów opisujących okrucieństwa i inne wykroczenia amerykańskich wojskowych i ich irackich sojuszników, równocześnie na pierwszej stronie zamieścił artykuł – zajmujący tyle samo miejsca co same dokumenty – napisany przez popierającego wojnę dziennikarza Johna Burnsa. Jego jedynym celem było przedstawienie Assange'a jako dziwaka i paranoika mającego słabe pojęcie o rzeczywistości.

Artykuł opisywał, jak Assange „melduje się w hotelach pod fałszywymi nazwiskami, farbuje włosy, śpi na kanapach i na podłodze, używa gotówki zamiast kart kredytowych, często pożycza pieniądze od przyjaciół". Wskazywał na, jak to ujęto, jego „nieobliczalne, władcze zachowanie" i „manię wielkości"; cytował również jego krytyków, którzy „oskarżają go o wendetę przeciwko Stanom Zjednoczonym", a także przytaczał słowa niezadowolonego wolontariusza WikiLeaks, który postawił

psychologiczną diagnozę: „On nie jest przy zdrowych zmysłach".

Przedstawianie Assange'a jako żyjącego złudzeniami wariata stało się niezmiennym elementem amerykańskiego dyskursu politycznego w ogóle, a taktyki „New York Timesa" w szczególności. W jednym z artykułów Bill Keller cytował reportera „New York Timesa", który opisał Assange'a następująco: „Zaniedbany, jak bezdomna żebraczka wprost z ulicy, w poplamionej jasnej sportowej marynarce i workowatych spodniach, brudnej białej koszuli, znoszonych adidasach i strasznie brudnych białych skarpetkach, które wałkowały mu się wokół kostek. Śmierdział, jakby się od wielu dni nie mył".

„New York Times" przewodził również w artykułach na temat Chelsea Manning, twierdząc, że do zostania sygnalistą skłoniły ją/jego nie przekonania czy sumienie, ale zaburzenia osobowości i niestabilność psychiczna. W licznych artykułach bezpodstawnie dopatrywano się głównych motywów decyzji o ujawnieniu tak ważnych dokumentów w całym zestawie problemów osobistych – od borykania się z tożsamością płciową, przez prześladowanie gejów w wojsku, po konflikty z ojcem.

Przypisywanie źródeł sprzeciwu zaburzeniom osobowości nie jest bynajmniej wynalazkiem amerykańskim. Radzieckich dysydentów regularnie zamykano w szpitalach psychiatrycznych, a chińskich dysydentów wciąż często leczy się przymusowo jako chorych psychicznie. Istnieją oczywiste cele personalnych ataków na krytyków status quo. Jak wskazano, jednym z nich jest ograniczenie skuteczności krytyki: mało kto chce być kojarzony z wariatem lub dziwakiem. Kolejny to zniechęcanie – gdy dysydentów wyrzuca się poza nawias społeczeństwa i poniża oskarżeniami o niestabilność emocjonalną, inni otrzymują silny bodziec, by nie postępować podobnie.

Kluczowym motywem jest jednak logiczna konieczność. Strażnicy status quo nie dostrzegają niczego rzeczywiście czy zasadniczo niewłaściwego w istniejącym porządku i jego

głównych instytucjach uważanych za sprawiedliwe. Dlatego też każdego, kto twierdzi inaczej – a szczególnie każdego, kogo takie przekonania skłoniły do podjęcia zdecydowanych działań – z definicji traktują jako emocjonalnie niestabilnego i psychicznie zaburzonego.

Inaczej mówiąc, ogólnie istnieją dwie możliwości: posłuszeństwo wobec władzy instytucjonalnej albo radykalna z nią niezgoda. Pierwsza możliwość jest zdrowa i sensowna tylko wtedy, gdy druga jest szalona i bezprawna. Dla obrońców status quo sama korelacja między chorobą psychiczną a radykalną opozycją wobec dominującej ortodoksji to za mało. Radykalna niezgoda to świadectwo, a nawet dowód poważnego zaburzenia osobowości.

W sercu takiego sformułowania leży istotne przekłamanie – że sprzeciw wobec władzy instytucjonalnej wymaga wyboru moralnego czy ideologicznego, a posłuszeństwo – nie. Przy takim fałszywym założeniu społeczeństwo zwraca wielką uwagę na motywy dysydentów, ale żadnej na motywy tych, którzy się instytucjom podporządkowują – czy to pilnując, by ich działania pozostawały niejawne, czy w jakiś inny sposób. Posłuszeństwo wobec władzy jest bez zastrzeżeń uważane za stan naturalny.

W rzeczywistości moralnego wyboru dokonuje się i przestrzegając zasad, i je łamiąc; obie ścieżki działania mówią coś ważnego o osobie, której to dotyczy. Wbrew przyjętemu założeniu – że radykalna niezgoda oznacza zaburzenie osobowości – prawdą może być sytuacja przeciwna: w obliczu poważnej niesprawiedliwości odmowa sprzeciwu oznacza słabość charakteru lub brak poczucia moralności.

Profesor filozofii Peter Ludlam, piszący w „New York Timesie" o tym, co nazywa „przeciekami, sygnalizowaniem i haktywizmem, drażniącymi amerykańskie wojsko oraz prywatne i rządowe wspólnoty wywiadów" – czyli o działaniach kojarzonych z grupą, którą nazywa „Generacją W", a której

głównymi przykładami są Snowden i Manning – porusza tę właśnie kwestię:

Dość naturalne jest okazywane przez media pragnienie psychoanalizowania członków Generacji W. Media chcą wiedzieć, dlaczego ludzie działają w sposób, w jaki oni, członkowie korporacyjnych mediów, nigdy by nie działali. Ale zasady są takie same dla wszystkich; skoro istnieje psychologiczna motywacja do zostania sygnalistą, do powodowania przecieków czy haktywizmu, istnieją także psychologiczne motywacje do identyfikowania się ze strukturą władzy w ramach systemu – w tym wypadku systemu, w którym korporacyjne media odgrywają ważną rolę.

Tak samo istnieje możliwość, że to sam system jest chory, choć aktorzy wewnątrz organizacji zachowują się zgodnie z organizacyjną etykietą i przestrzegają wewnętrznych więzów zaufania.

To właśnie takiej dyskusji władze instytucjonalne najbardziej pragną uniknąć. Odruchowa demonizacja sygnalistów jest sposobem, w jaki należące do establishmentu media w Stanach Zjednoczonych chronią interesy osób dzierżących władzę. Ta podległość jest tak głęboka, że wiele reguł dziennikarskich przykrawa się tak – a przynajmniej tak się stosuje – by popierać to, co rząd ma do powiedzenia.

Weźmy na przykład pogląd, że przecieki tajnych informacji to działanie złośliwe i przestępcze. Waszyngtońscy dziennikarze, którzy tę opinię stosują do Snowdena czy do mnie, nie potępiają ujawniania tajnych informacji, a jedynie ujawnianie tego, co się nie podoba rządowi lub go osłabia.

Rzeczywistość jest bowiem taka, że Waszyngton zawsze tonie w przeciekach. Najsławniejsi i najbardziej szanowani reporterzy waszyngtońscy, na przykład Bob Woodward, osiągnęli swoją pozycję dzięki temu, że regularnie otrzymywali poufne informacje od źródeł na wysokich stanowiskach,

a następnie je publikowali. Urzędnicy Obamy wielokrotnie chodzili do „New York Timesa", żeby serwować poufne informacje o takich sprawach, jak zabijanie przez drony czy zabójstwo Osamy bin Ladena. Były sekretarz obrony, a wcześniej szef CIA Leon Panetta i funkcjonariusze CIA karmili tajnymi informacjami reżyserkę filmu *Wróg numer jeden* w nadziei, że film nagłośni największy triumf Obamy (równocześnie zaś Departament Sprawiedliwości mówił sądom federalnym, że nie może udostępnić informacji o ataku na bin Ladena ze względu na ochronę bezpieczeństwa narodowego).

Żaden dziennikarz związany z establishmentem nie zaproponowałby, żeby oskarżyć funkcjonariuszy odpowiedzialnych za te przecieki ani reporterów, którzy je otrzymali, a następnie o nich napisali. Rozbawiłaby ich sugestia, że Bob Woodward, który od lat ujawnia ściśle tajne dane, i jego wysokie źródła rządowe są przestępcami.

Tak się dzieje, ponieważ te przecieki są sankcjonowane przez Waszyngton i służą interesom rządu USA, a zatem uważa się je za właściwe i pożyteczne. Jedyne przecieki, jakie spotykają się z potępieniem waszyngtońskich mediów, to te informujące o sprawach, które urzędnicy woleliby ukryć.

Zastanówcie się, co się wydarzyło, tuż zanim David Gregory zasugerował w programie *Meet the Press*, że powinienem zostać aresztowany za artykuły o NSA. Na początku wywiadu wspomniałem ściśle tajną decyzję sądu FISA, wydaną w 2011 roku, która uznawała znaczną część krajowego programu inwigilacji NSA za niekonstytucyjną i naruszającą statuty regulujące szpiegostwo. Wiedziałem o tym wyroku tylko dlatego, że przeczytałem o nim w dokumentach Agencji, które dał mi Snowden. Podczas *Meet the Press* wezwałem do ujawnienia go społeczeństwu.

Gregory jednak twierdził, że sąd FISA powiedział coś innego:

Jeśli chodzi o tę konkretną opinię FISA, to nie jest tak, na podstawie tego, co mi mówili ludzie, że opinia FISA w odpowiedzi na wniosek rządu mówi: „No, możecie dostać to, ale nie możecie dostać tamtego. Tamto wykraczałoby poza zakres tego, co wam wolno robić" – a to znaczy, że wniosek został zmieniony albo odrzucony, i o tym właśnie mówi rząd, że mamy tu rzeczywisty nadzór sądowy, a nie nadużycie.

Ważna tu jest nie tyle konkretna treść opinii sądu FISA (choć gdy osiem tygodni później została ujawniona, stało się jasne, że zdaniem sądu NSA naprawdę działała nielegalnie). Ważniejsze jest to, że Gregory twierdził, iż zna to orzeczenie, ponieważ jego informatorzy mu o nim powiedzieli, i podał te informacje publicznie.

A zatem tuż zanim Gregory poruszył kwestię aresztowania mnie za artykuły, sam ujawnił coś, co uważał za ściśle tajną informację ze źródeł rządowych. Nikt nigdy nie zasugerowałby jednak uznania pracy Gregory'ego za przestępstwo. Zastosowanie tej samej logiki do gospodarza *Meet the Press* i jego informatora uznano by za absurdalne.

Co więcej, Gregory zapewne nie byłby w stanie zrozumieć, że można porównać to, co ujawnił, i to, co ujawniłem ja, ponieważ on działał na życzenie rządu, starającego się bronić i usprawiedliwiać swoje działanie, ja natomiast postępowałem wbrew życzeniom biurokracji rządowej.

To oczywiście jest dokładnie sprzeczne z zamierzonymi celami wolności prasy. Zgodnie z ideą czwartej władzy powinna ona kontrolować sprawujących rządy i naciskać na przejrzystość ich działań; zadaniem prasy jest wskazywanie kłamstw, jakie władza nieodmiennie rozpowszechnia, by się chronić. Bez takiego rodzaju dziennikarstwa nadużycia są nieuniknione. Nikt nie potrzebuje konstytucyjnych gwarancji wolnej prasy po to, by dziennikarze przyjaźnili się z liderami politycznymi,

rozwodzili się nad ich działalnością i wychwalali; gwarancje są potrzebne, by dziennikarze mogli robić coś wręcz przeciwnego.

Podwójny standard stosowany przy publikacji poufnych informacji jest jeszcze wyraźniejszy, gdy chodzi o niepisany wymóg „dziennikarskiego obiektywizmu". To domniemane naruszenie tej zasady uczyniło ze mnie „aktywistę", a nie „dziennikarza". Nieustannie się nam powtarza, że dziennikarze nie wyrażają opinii, podają jedynie fakty.

To oczywisty pozór, zarozumialstwo zawodu. Percepcja i wypowiedzi istot ludzkich są z natury rzeczy subiektywne. Każdy artykuł prasowy jest produktem rozlicznych, wysoce subiektywnych założeń kulturowych, narodowych i politycznych. I każde dziennikarstwo służy interesom jakiejś frakcji.

Nie istnieje podział na dziennikarzy, którzy mają własne opinie, i tych, którzy ich nie mają, bo ta druga kategoria nie istnieje. Można ich natomiast dzielić na tych, którzy jasno wyrażają swoje opinie, i tych, którzy je ukrywają.

Sama idea, że dziennikarze nie powinni mieć opinii, jest daleka od niektórych od dawna respektowanych wymogów zawodu; co więcej, jest ona tworem stosunkowo nowym, skutkującym – nawet niezamierzenie – neutralizacją dziennikarstwa.

Jak zauważył Jack Shafer, publicysta Reutersa zajmujący się mediami, ten niedawno zrodzony amerykański pogląd odzwierciedla „smutne oddanie korporacyjnemu ideałowi tego, jakie dziennikarstwo być powinno", a także „bolesny brak zrozumienia historii". Od powstania USA najlepsze, powodujące największe konsekwencje dziennikarstwo często uprawiali reporterzy prowadzący krucjaty, będący rzecznikami spraw, zwalczający niesprawiedliwości. Pozbawione opinii, bezbarwne, bezduszne i szablonowe korporacyjne dziennikarstwo wyssało z zawodu jego najwartościowsze cechy, sprawiając, że związane z establishmentem media straciły znaczenie – nie stanowią zagrożenia dla władzy, dokładnie tak, jak zamierzono.

Pomijając jednak wrodzoną niemożność obiektywnego reportażu, reguły tej niemal nigdy nie stosują konsekwentnie ci, którzy twierdzą, że w nią wierzą. Dziennikarze establishmentu nieustannie wyrażają opinie na temat rozlicznych kontrowersyjnych kwestii, a nikt im nie odmawia zawodowego statusu. Chodzi o to, że głoszone przez nich opinie mają poparcie waszyngtońskiej biurokracji, a zatem uważane są za uprawnione.

Od początku sporu na temat NSA Bob Schieffer, prowadzący program *Face the Nation,* oskarżał Snowdena i bronił inwigilacji NSA. To samo robił Jeffrey Toobin, publikujący w dziale prawnym „New Yorkera" i wypowiadający się na tematy prawne w CNN. John Burns, korespondent „New York Timesa", piszący o wojnie w Iraku, przyznał po fakcie, że był zwolennikiem inwazji, a żołnierzy amerykańskich opisywał jako „moich wyzwolicieli" i „troskliwych aniołów". Christiane Amanpour z CNN przez całe lato 2013 roku nalegała na wysłanie amerykańskiego wojska do Syrii. A jednak ich działalności nie określano mianem „aktywizmu", ponieważ mimo całego szacunku dla obiektywizmu w gruncie rzeczy nie istnieje zakaz głoszenia własnych opinii przez dziennikarzy.

Tak samo jak rzekoma reguła przeciwko przeciekom, „reguła" obiektywności nie jest żadną regułą, a jedynie sposobem na promowanie interesów dominującej klasy politycznej. Dlatego też „inwigilacja przez NSA jest legalna i konieczna", „wojna w Iraku jest słuszna", a „USA powinny dokonać inwazji na ten kraj" – to opinie, które dziennikarzom wolno głosić, i cały czas to czynią.

„Obiektywizm" to nic więcej jak odzwierciedlenie uprzedzeń i służenie interesom tych, którzy umocnili się w Waszyngtonie. Opinie stają się problematyczne dopiero wtedy, gdy odchodzą od akceptowanego zakresu waszyngtońskiej ortodoksji.

Nietrudno było wyjaśnić wrogość wobec Snowdena. Wrogość wobec dziennikarzy ujawniających tę sprawę – wobec

mnie – jest być może kwestią bardziej złożoną, wynikającą częściowo z rywalizacji, częściowo z odwetu za lata zawodowej krytyki, jakiej nie szczędziłem amerykańskim gwiazdom mediów. Wydaje mi się, że dochodził do tego gniew, a nawet wstyd z powodu prawdy ujawnionej przez bezkompromisowe dziennikarstwo. Publicystyka, która wywołuje gniew rządu, odsłania prawdziwą rolę dziennikarzy sankcjonowanych przez Waszyngton – fakt, że służą wzmacnianiu władzy.

Zdecydowanie najbardziej znaczącym powodem wrogości było to, że przedstawiciele związanych z establishmentem mediów przyjęli na siebie rolę posłusznych rzeczników władzy politycznej, szczególnie tam, gdzie chodzi o bezpieczeństwo narodowe. Dlatego też tak samo jak politycy z pogardą odnoszą się do osób podważających lub kwestionujących waszyngtońskie centra władzy.

Dawniej ikoną dziennikarstwa był reporter, który pozostawał całkowitym outsiderem. Wiele osób, które podjęło ten zawód, miało skłonność raczej się władzy przeciwstawiać, niż jej służyć – nie tylko ze względu na ideologię, ale także osobowość i usposobienie. Wybór zawodu dziennikarza właściwie gwarantował status outsidera: reporterzy zarabiali niewiele, nie cieszyli się szczególnym prestiżem i najczęściej pozostawali w cieniu.

To się zmieniło. Gdy największe światowe korporacje kupiły firmy mediowe, większość gwiazd mediów stała się wysoko opłacanymi pracownikami konglomeratów, niczym nieróżniącymi się od innych pracowników. Zamiast w imieniu tych korporacji sprzedawać usługi bankowe lub instrumenty finansowe, wciskają społeczeństwu produkty mediowe. Ich drogę kariery określają te same cechy, które prowadzą do sukcesu w takim środowisku: stopień, do jakiego zadowalają swych korporacyjnych szefów i dbają o interesy firmy.

Ci, którzy znakomicie funkcjonują w strukturach wielkich korporacji, zazwyczaj lepiej potrafią zadowalać instytucjonalną władzę, niż ją kwestionować. Dlatego też reporterzy odnoszący sukcesy w korporacyjnym dziennikarstwie są przyzwyczajeni iść na rękę władzy. Identyfikują się z kierownictwem, wiedzą, jak mu służyć, a nie jak z nim walczyć.

Dowodów jest wiele. Wiemy, że w 2004 roku na prośbę Białego Domu „New York Times" zgodził się nie pisać o odkryciu Jamesa Risena dotyczącym nielegalnego programu podsłuchowego NSA. Ówczesny redaktor publiczny gazety określił wyjaśnienia jej kierownictwa jako „żałośnie nieadekwatne". W podobnym przypadku w 2006 roku redaktor Dean Baquet z „Los Angeles Timesa" uśmiercił tekst swoich reporterów na temat tajnej współpracy między AT&T a NSA oparty na informacjach dostarczonych przez sygnalistę Marka Kleina. Klein przedstawił ogromną liczbę dokumentów ujawniających budowę przez AT&T tajnego pomieszczenia w biurze w San Francisco, gdzie NSA mogło zainstalować splitery do przekierowywania połączeń telefonicznych i internetowych klientów tej firmy telekomunikacyjnej do zasobów Agencji.

Jak to ujął Klein, dokumenty świadczyły o tym, że NSA „przeczesywało prywatne życie milionów niewinnych Amerykanów". W *ABC News* w 2007 roku powiedział, że Baquet zablokował publikację tego artykułu „na prośbę ówczesnego dyrektora Wywiadu Narodowego Johna Negroponte i ówczesnego dyrektora NSA generała Michaela Haydena". Wkrótce potem Baquet został szefem waszyngtońskiego biura „New York Timesa", a następnie awansował na stanowisko sekretarza redakcji tej gazety.

Fakt, że „New York Times" awansował tak oddanego sługę interesów rządu, nie powinien dziwić. Redaktor publiczna Margaret Sullivan zauważyła, że gdyby redaktorzy gazety chcieli zrozumieć, dlaczego informatorzy ujawniający ważne sprawy dotyczące bezpieczeństwa narodowego – tacy jak

Manning i Snowden – to nie do nich przynoszą swoje rewelacje, „New York Times" powinien popatrzeć w lustro. To prawda, że „New York Times" publikował dużą część dokumentów we współpracy z WikiLeaks, ale wkrótce potem były redaktor naczelny Bill Keller bardzo się starał, by gazeta zdystansowała się od swego partnera – publicznie zestawił gniew administracji Obamy przeciwko WikiLeaks z uznaniem tejże administracji dla „New York Timesa" i jego „odpowiedzialnej" publicystyki.

Także i przy innych okazjach Keller chwalił się związkami gazety z Waszyngtonem. Występując w 2011 roku w BBC w dyskusji o depeszach pozyskanych przez WikiLeaks, Keller wyjaśnił, że w sprawach podobnych publikacji „New York Times" przyjmuje wskazówki od rządu USA. Prowadzący program dziennikarz BBC spytał niedowierzająco: „Czy chce pan powiedzieć, że idziecie wcześniej do rządu i mówicie: a co z tym czy z tamtym, czy możemy zrobić to albo tamto, i wtedy dostajecie zgodę albo nie?". Drugi gość, brytyjski ambasador Carne Ross, powiedział, że po komentarzu Kellera pomyślał, iż nie powinno się szukać informacji o tych depeszach w „New York Timesie". „To niezwykłe, że «New York Times» uzgadnia z amerykańskim rządem, co może na ten temat publikować".

W tego rodzaju współpracy mediów z Waszyngtonem nie ma jednak niczego niezwykłego. Dziennikarze stale przyjmują na przykład oficjalne stanowisko Ameryki w sporach z zagranicznymi adwersarzami i podejmują decyzje redakcyjne, opierając się na tym, co według definicji rządu najlepiej „zabezpiecza interesy Stanów Zjednoczonych". Prawnik z Departamentu Sprawiedliwości w administracji Busha Jack Goldsmith chwali „niedocenione zjawisko: patriotyzm amerykańskiej prasy", rozumiejąc przez to, że krajowe media zazwyczaj okazują lojalność wobec programu rządu. Cytował dyrektora CIA i NSA w administracji Busha Michaela Haydena, który wskazywał, że dziennikarze wykazują „chęć współpracy z nami", natomiast

w wypadku prasy zagranicznej, dodawał, „jest to bardzo, bardzo trudne".

Identyfikowanie się głównych mediów z rządem umacniają różne czynniki, w tym społeczno-ekonomiczny. Wielu wpływowych dziennikarzy w Stanach Zjednoczonych jest teraz multimilionerami. Mieszkają w tych samych dzielnicach co politycy i elity finansowe, czyli osoby, którym powinni patrzeć na ręce. Bywają na tych samych uroczystościach, obracają się w tych samych kręgach towarzyskich, mają tych samych współpracowników, ich dzieci chodzą do tych samych elitarnych prywatnych szkół.

To jeden z powodów, dlaczego dziennikarze i urzędnicy rządowi tak gładko mogą wymieniać się stanowiskami. Czołowe postaci mediów przechodzą na wysokie stanowiska w Waszyngtonie, urzędnicy rządowi często opuszczają swoje z lukratywnym kontraktem z mediami w kieszeni. Jay Carney i Richard Stengel z magazynu „Time" pracują teraz dla rządu, natomiast doradcy Obamy David Axelrod i Robert Gibbs są komentatorami w MSNBC. Są to raczej przesunięcia poprzeczne niż zmiany zawodu – przychodzą tak gładko właśnie dlatego, że ludzie ci wciąż służą tym samym interesom.

Dziennikarstwo amerykańskie związane z establishmentem bynajmniej nie jest niezależne. Stało się w pełni zintegrowane z dominującą w kraju siłą polityczną. Pod względem kulturowym, emocjonalnym i społeczno-ekonomicznym są jednym i tym samym. Bogaci, sławni dziennikarze cieszący się dostępem do właściwych kręgów nie chcą naruszyć status quo, które przynosi im tak hojne nagrody. Podobnie jak wszyscy dworzanie, chętnie bronią systemu, który zapewnia im przywileje, i z pogardą traktują każdego, kto ten system podważa.

Już tylko mały krok dzieli ich od pełnego identyfikowania się z potrzebami funkcjonariuszy politycznych. Stąd przekonanie, że przejrzystość jest zła, a antagonistyczne dziennikarstwo

– szkodliwe, może nawet przestępcze. Przywódcom politycznym należy pozwolić sprawować władzę w ciemnościach.

We wrześniu 2013 roku te kwestie bardzo dobitnie podniósł Seymour Hersh, zdobywca Nagrody Pulitzera, dziennikarz, który odkrył i masakrę w My Lai podczas wojny wietnamskiej, i skandal z traktowaniem irackich więźniów w Abu Ghraib. W udzielonym „Guardianowi" wywiadzie Hersh wystąpił przeciwko „lękliwości dziennikarzy w Ameryce, ich niezdolności do podważania słów Białego Domu i występowania w charakterze niepopularnych posłańców prawdy". Powiedział, że „New York Times" poświęca bardzo dużo czasu „wyręczaniu Obamy". Administracja systematycznie kłamie, twierdził, „ale żaden z lewiatanów amerykańskich mediów, sieci telewizyjnych czy wielkonakładowych tytułów" nie stanowi dla niej zagrożenia.

Wysunięta przez Hersha propozycja, „jak naprawić dziennikarstwo", brzmiała: „zamknąć działy wiadomości w NBC i ABC, wyrzucić 90 procent redaktorów w wydawnictwach i wrócić do podstawowej funkcji dziennikarzy", czyli działania z zewnątrz. „Zacznijcie awansować tych dziennikarzy, których nie jesteście w stanie kontrolować" – radził Hersh. – Ci, co robią zamieszanie, nie dostają promocji" – powiedział. Natomiast „bojaźliwi redaktorzy" i dziennikarze niszczą zawód, ponieważ dominująca mentalność sprawia, że ludzie obawiają się być outsiderami.

Gdy raz nazwie się reportera aktywistą, gdy jego reputacja zostanie nadszarpnięta przez oskarżenie o przestępczą działalność, a on sam wyrzucony poza krąg ochrony należnej dziennikarzom, staje się podatny na traktowanie jako przestępca. Zrozumiałem to bardzo szybko po nagłośnieniu sprawy NSA.

Ledwo wróciłem z Hongkongu do domu w Rio, David powiedział mi, że zniknął jego laptop. Podejrzewał, że to zniknięcie

było związane z rozmową, jaką odbyliśmy podczas mojej nieobecności – przypomniał, że dzwoniłem do niego przez Skype'a, by porozmawiać o dużym zaszyfrowanym pliku dokumentów, który zamierzałem mu przesłać drogą elektroniczną. Wyjaśniłem mu wtedy, że gdy już go dostanie, ma go gdzieś bezpiecznie umieścić. Zdaniem Snowdena ktoś, komu bezwarunkowo ufam, powinien dostać na przechowanie komplet dokumentów na wypadek, gdyby moje własne archiwum zaginęło, zostało uszkodzone lub skradzione.

– Może okazać się, że nie będzie dużo dłużej dostępne – powiedział. – A nigdy nie wiesz, jak się rozwinie twoja współpraca z Laurą. Ktoś powinien mieć komplet, żebyś nie stracił dostępu, niezależnie co się stanie.

Oczywistym wyborem był David. Nigdy jednak nie wysłałem tego pliku. Była to jedna z tych rzeczy, których nie zdążyłem zrobić w Hongkongu.

– Nie minęło 48 godzin od naszej rozmowy, gdy laptop został skradziony z domu – twierdził David. Nie chciałem wierzyć, że kradzież laptopa mogła wynikać z kontaktu przez Skype'a. Powiedziałem Davidowi, że nie wolno nam wpaść w taką paranoję jak ci, co każde niespodziewane wydarzenie w swoim życiu przypisują CIA. Może laptop gdzieś się zapodział albo zabrał go jakiś gość, a może został skradziony zupełnie niezależnie od sprawy NSA.

David po kolei obalał moje teorie: nigdy nie wychodził z domu z laptopem; przewrócił dom do góry nogami i nigdzie laptopa nie znalazł; nic poza tym nie zginęło i nie zmieniło miejsca. Jego zdaniem odmowa rozważenia jedynego możliwego wyjaśnienia była z mojej strony irracjonalna.

Do tamtej pory sporo reporterów zdążyło już zauważyć, że NSA właściwie nie ma pojęcia, co Snowden zabrał albo co mi dał – nie tylko jeśli chodzi o konkretne dokumenty, ale też o ich zakres. Nie byłoby nic dziwnego w tym, że rząd amerykański

(a może także inne rządy) chce się pilnie dowiedzieć, co posiadam. Skoro mogliby zdobyć tę informacje, kradnąc komputer Davida, to dlaczego nie mieliby tego zrobić?

Wiedziałem już wówczas także, że rozmowa z Davidem przez Skype bynajmniej nie była bezpieczna; Skype jest tak samo podatny na monitoring NSA jak każdy inny rodzaj połączeń. Rząd zatem mógł usłyszeć, że zamierzam wysłać dokumenty Davidowi, miał więc silny motyw, by zabrać jego laptop.

Od Davida Schultza, prawnika do spraw mediów w „Guardianie", usłyszałem, że istnieją podstawy, by wierzyć w przedstawioną przez Davida teorię kradzieży. Kontakty w amerykańskim wywiadzie pozwoliły mu stwierdzić, że obecność CIA w Rio jest silniejsza niż niemal gdziekolwiek indziej na świecie, a szef tamtejszej placówki jest „znany z agresywnego działania". Opierając się na tym, Schultz ostrzegał: „Powinieneś właściwie zakładać, że wszystko, co mówisz, wszystko, co robisz, i wszystkie miejsca, do których chodzisz, podlegają ścisłemu monitoringowi".

Pogodziłem się z faktem, że moja zdolność do porozumiewania się będzie teraz poważnie ograniczona. Starałem się nie używać telefonu, chyba że do najbardziej niejasnych i banalnych rozmów. Wysyłałem i otrzymywałem e-maile jedynie przez skomplikowany system szyfrowania. Ograniczyłem dyskusje z Laurą, Snowdenem i różnymi źródłami do szyfrowanych czatów online. Byłem w stanie pracować nad artykułami z redaktorami „Guardiana", jedynie jeśli przyjeżdżali do Rio, by spotkać się ze mną osobiście. Ważyłem słowa w rozmowach z Davidem w domu i samochodzie. Kradzież laptopa uświadomiła mi, że nawet te najbardziej prywatne miejsca mogą być pod obserwacją.

Gdybym potrzebował dalszych dowodów na groźny klimat, w jakim teraz pracowałem, to pojawiły się one w formie doniesienia o rozmowie zasłyszanej przez Steve'a Clemonsa, szanowanego i mającego dobre powiązania analityka polityki waszyngtońskiej, a także niezależnego publicystę magazynu „Atlantic".

Clemons opowiadał, że 8 czerwca znajdował się w poczekalni United Airlines na waszyngtońskim lotnisku Dullesa, gdzie usłyszał głośną rozmowę czterech amerykańskich agentów wywiadu, którzy twierdzili, że osobę odpowiedzialną za przeciek i dziennikarza zajmującego się programami NSA „należy zniknąć". Clemons nagrał telefonem fragment rozmowy. Jego zdaniem brzmiała jak „przechwałki", ale i tak postanowił ją opublikować.

Nie potraktowałem tego doniesienia poważnie, choć Clemons jest całkiem wiarygodny. Niepokojący był jednak sam fakt takiej publicznej pogawędki ludzi z establishmentu o „spowodowaniu zniknięcia" Snowdena i dziennikarzy, z którymi pracował.

W kolejnych miesiącach możliwość nadania publicystyce o NSA charakteru przestępstwa zmieniła się z abstrakcyjnej idei w rzeczywistość. Tę drastyczną zmianę wywołały działania brytyjskiego rządu.

W szyfrowanej rozmowie z Janine Gibson po raz pierwszy usłyszałem o niezwykłym wydarzeniu, które miało miejsce w londyńskim biurze „Guardiana" w połowie lipca. Nazwała to „radykalną zmianą" w tonie rozmów między „Guardianem" a GCHQ, jaka zaszła w kilku minionych tygodniach. To, co początkowo miało formę „bardzo cywilizowanych kontaktów" na temat zamieszczanych przez gazetę artykułów, przekształciło się w serię coraz bardziej wojowniczych żądań, a potem otwartych gróźb ze strony tej brytyjskiej agencji wywiadu elektronicznego.

A potem, jak opowiadała Gibson, GCHQ dość nagle oświadczyło, że nie będzie gazecie dłużej „pozwalać" na publikowanie artykułów opartych na ściśle tajnych dokumentach. Zażądało, żeby londyński „Guardian" oddał wszystkie kopie plików otrzymanych od Snowdena. Gdyby „Guardian" odmówił, wyrok sądu zakazałby wszelkich dalszych doniesień na ten temat.

Nie była to czcza pogróżka. W Wielkiej Brytanii nie ma konstytucyjnej gwarancji wolności prasy. Brytyjskie sądy tak dalece szanują żądania rządu dotyczące „powstrzymywania",

że mediom można z wyprzedzeniem zakazać publikacji czegokolwiek, co uznaje się za zagrożenie dla bezpieczeństwa narodowego.

W latach 70. ubiegłego wieku Duncan Campbell, dziennikarz, który pierwszy odkrył istnienie GCHQ, a potem o tym napisał, został nawet aresztowany i skazany. Sąd brytyjski mógł w dowolnym momencie zamknąć „Guardiana", przejąć wszystkie materiały i sprzęt. „Żaden sędzia nie odmówi, jeśli zostanie poproszony – powiedziała Janine. – My to wiemy, a oni wiedzą, że my wiemy".

Dokumenty będące w posiadaniu „Guardiana" stanowiły ułamek całego archiwum, jakie Snowden przekazał nam w Hongkongu. Uważał, że autorami artykułów odnoszących się konkretnie do GCHQ powinni być dziennikarze brytyjscy, więc jednego z ostatnich dni w Hongkongu dał kopie tych dokumentów Ewenowi MacAskillowi.

Janine powiedziała mi, że w miniony weekend ona, redaktor naczelny Alan Rusbridger i kilkoro innych członków redakcji wyjechali odpocząć poza Londyn. Nagle zawiadomiono ich, że funkcjonariusze GCHQ są w drodze do redakcji „Guardiana" w Londynie, skąd zamierzają zabrać twarde dyski, na których przechowywane były dokumenty. „Już dość się bawiliście – powiedzieli Rusbridgerowi, jak później wspominał – a teraz chcemy odzyskać te materiały". Gdy GCHQ się z nim porozumiało, grupa redaktorów przebywała na wsi od zaledwie dwóch i pół godziny. „Musieliśmy natychmiast wrócić do Londynu, by bronić budynku. Zrobiło się naprawdę niebezpiecznie" – powiedziała Janine.

GCHQ zażądało, by „Guardian" oddał wszystkie egzemplarze dokumentów. Gdyby gazeta to uczyniła, rząd dowiedziałby się, co Snowden przekazał, a jego sytuacja prawna stałaby się jeszcze bardziej niebezpieczna. Zamiast tego „Guardian" zgodził się zniszczyć wszystkie wskazane twarde dyski pod nadzorem funkcjonariuszy GCHQ, którzy pilnowali, by zniszczenie

przeprowadzono zgodnie z ich wymogami. Przebieg wydarzeń Janine określiła jako „bardzo skomplikowany taniec przeciągania, dyplomacji, szmuglowania, a potem współpracy przy «poświadczonej destrukcji»".

Wyrażenie „poświadczona destrukcja" zostało właśnie wymyślone przez GCHQ na określenie tego, co zaszło. Funkcjonariusze towarzyszyli redaktorom „Guardiana", łącznie z redaktorem naczelnym, do sutereny w budynku redakcji i przyglądali się rozbijaniu na kawałki twardych dysków, a nawet żądali, by niektóre fragmenty posiekać jeszcze drobniej. „Żeby mogli być pewni, iż w pokiereszowanych kawałkach metalu nie zostało nic, co mogłoby zainteresować przechodzących przypadkiem chińskich agentów" – kpił później Rusbridger. Jeden z ekspertów do spraw bezpieczeństwa zażartował: „Możemy już odwołać helikoptery", a członkowie redakcji „zmiatali resztki MacBook Pro".

Wizerunek rządu, który wysyła agentów do gazety, by zmusić ją do zniszczenia komputerów, jest sam w sobie szokujący; mieszkańcom Zachodu mówi się, że podobne rzeczy zdarzają się jedynie w takich krajach jak Chiny, Iran czy Rosja. Z drugiej strony zdumiewa, że szanowana gazeta z własnej woli i pokornie poddała się takiemu rozkazowi.

Skoro rząd zagroził zamknięciem gazety, dlaczego nie złapać go za słowo i nie zmusić do wyrażenia tej groźby jasno i otwarcie? Gdy Snowden usłyszał o akcji GCHQ, powiedział: „Jedyna właściwa odpowiedź to: no dobra, dalej, zamknijcie nas!". Zgoda wyrażona w sekrecie i z własnej woli umożliwia rządowi ukrycie przed światem swego prawdziwego charakteru – państwa, które po bandycku nie pozwala dziennikarzom informować o jednej z najbardziej znaczących dla interesu publicznego historii.

Co gorsza, akt zniszczenia materiałów, które informator przekazał, narażając własną wolność, a nawet życie, był całkowitą antytezą celu dziennikarstwa.

Niezależnie od potrzeby ujawnienia tak despotycznego postępowania, fakt, że rząd wmaszerowuje do redakcji i zmusza gazetę do zniszczenia informacji, sam w sobie jest wart ujawnienia. Jednak „Guardian" najwyraźniej zamierzał zachować milczenie, co bardzo mocno podkreśla, jak krucha jest wolność prasy w Wielkiej Brytanii.

Tak czy inaczej, Gibson zapewniła mnie, że „Guardian" wciąż ma kopie dokumentów w biurze w Nowym Jorku. A potem powiedziała coś zaskakującego: kolejna kopia była teraz także w posiadaniu „New York Timesa"; Alan Rusbridger dał ją Jill Abramson, by gazeta ta miała dostęp do dokumentów na wypadek, gdyby brytyjski sąd próbował zmusić również amerykańskie biuro „Guardiana" do ich zniszczenia.

Także i to nie było dobrą wiadomością. „Guardian" nie tylko zgodził się, potajemnie, zniszczyć własne dokumenty, ale również bez konsultacji czy nawet powiadomienia Snowdena lub mnie dał je tej właśnie gazecie, którą Snowden wykluczył, bo nie darzył jej zaufaniem z powodu bliskich, podległych stosunków z amerykańskim rządem.

Z punktu widzenia „Guardiana" nie mógł on sobie pozwolić na nonszalancję w obliczu gróźb ze strony rządu Wielkiej Brytanii, musiał bowiem liczyć się z brakiem konstytucyjnej ochrony, a także koniecznością chronienia setek pracowników i liczącej sobie blisko dwieście lat gazety, zniszczenie komputerów było zaś lepsze niż przekazanie archiwum w ręce GCHQ. Mnie jednak niepokoiła gotowość zastosowania się do żądań rządu, a jeszcze bardziej ich wyraźna decyzja, by o tym nie informować.

Trzeba jednak przyznać, że i przed zniszczeniem twardych dysków, i po tym wydarzeniu „Guardian" twardo i nieugięcie pisał o odkryciach Snowdena – moim zdaniem nie zdobyłaby się na to żadna gazeta o porównywalnej wielkości i reputacji. Mimo stosowanej przez władze taktyki zastraszania, która przybierała na sile, redaktorzy nie przestawali publikować

jednego artykułu o NSA i GCHQ za drugim, i z tego powodu należy im się szacunek.

Jednak Laura i Snowden byli bardzo źli – że „Guardian" ugiął się przed groźbami rządu i że później milczał na temat tego, co się stało. Snowdena zaś szczególnie rozwścieczyło, że archiwum GCHQ znalazło się w rękach „New York Timesa". Postrzegał to jako złamanie jego porozumienia z „Guardianem" i naruszenie jego życzenia, by tylko brytyjscy dziennikarze zajmowali się brytyjskimi dokumentami, a szczególnie, by dokumentów nie dostał „New York Times". Jak się miało okazać, podobna reakcja Laury doprowadziła do dramatycznych konsekwencji.

Od samego początku naszej pracy stosunki Laury z „Guardianem" były niełatwe, a teraz konflikt stał się jawny. Pracując razem przez tydzień w Rio, odkryliśmy, że część jednego z archiwów NSA, które Snowden dał mi w Hongkongu tego dnia, gdy zaczął się ukrywać (ale nie miał okazji dać Laurze), jest uszkodzona. Laura nie potrafiła naprawić tego w Rio, ale sądziła, że być może uda jej się to zrobić w Berlinie.

Tydzień po powrocie do Berlina Laura zawiadomiła mnie, że może mi już przekazać dokumenty. Uzgodniliśmy, że pracownik „Guardiana" poleci do Berlina, zabierze archiwum i przywiezie mi do Rio. Jednak pracownik „Guardiana", najwyraźniej w strachu po sprawie z GCHQ, powiedział Laurze, że zamiast osobiście dawać mu archiwum, powinna mi je wysłać FedExem.

Laura była tak wzburzona i wściekła jak nigdy wcześniej.

– Nie widzisz, co oni robią? – spytała mnie. – Chcą móc powiedzieć: nie mieliśmy nic wspólnego z przewożeniem tych dokumentów, to Glenn i Laura przesyłali je sobie tam i z powrotem.

Dodała, że korzystanie z FedExu do wysyłki ściśle tajnych dokumentów przez pół świata – i to w dodatku wysyłki od niej z Berlina do mnie do Rio, co byłoby głośnym obwieszczeniem

dla wszystkich zainteresowanych stron – tak dalece naruszało bezpieczeństwo naszego działania, że trudno sobie wyobrazić większe zagrożenie.

– Nigdy im już nie zaufam – oświadczyła.

Ja jednak potrzebowałem tego archiwum. Znajdowały się w nim dokumenty istotne dla tekstów, nad którymi pracowałem, a także wiele innych, jeszcze nieopublikowanych.

Janine twierdziła, że problem wyniknął z nieporozumienia – pracownik źle zinterpretował komentarz przełożonego, że część kierownictwa w Londynie niepokoi się faktem, przewożenia dokumentów między Laurą a mną.

– Nie ma problemu – powiedziała. – Ktoś z „Guardiana" tego samego dnia poleci do Berlina po archiwum.

Było za późno.

– Nigdy więcej nie dam żadnych dokumentów „Guardianowi" – oświadczyła Laura. – Po prostu już im nie ufam.

Wielkość i znaczenie archiwum sprawiało, że nie chciała wysyłać go drogą elektroniczną. Musiał je osobiście przewieźć ktoś, komu ufaliśmy. Tym kimś był David, który, usłyszawszy o problemie, natychmiast zaoferował, że pojedzie do Berlina. Oboje uznaliśmy, że to doskonałe rozwiązanie. David rozumiał całą sprawę, Laura go znała i miała do niego zaufanie, a on i tak zamierzał ją odwiedzić, by porozmawiać o potencjalnych nowych przedsięwzięciach. Janine chętnie się zgodziła, a „Guardian" miał pokryć koszty jego podróży.

Dział podróży „Guardiana" zarezerwował Davidowi bilet w British Airways, a potem przysłał mu marszrutę. Nie przyszło nam do głowy, że z podróżą mogą się wiązać jakieś kłopoty. Dziennikarze „Guardiana", którzy pisali artykuły o archiwach Snowdena, a także członkowie personelu gazety, którzy w charakterze kurierów przewozili dokumenty tam i z powrotem, wielokrotnie wylatywali z Heathrow i lądowali tam bez żadnych problemów. Sama Laura też kilka tygodni wcześniej

poleciała do Londynu. Skąd komuś miałoby przyjść do głowy przypuszczenie, że David – postać znacznie bardziej na obrzeżach sprawy – wystawia się na ryzyko?

David wyleciał do Berlina w niedzielę 11 sierpnia i miał wrócić tydzień później z archiwum od Laury. Jednak w dzień, w którym miał wylądować w Rio, obudził mnie wczesny telefon. Ktoś mówiący z ciężkim brytyjskim akcentem przedstawił się jako „agent bezpieczeństwa na lotnisku Heathrow" i spytał, czy znam Davida Mirandę.

– Dzwonimy, by pana powiadomić – mówił dalej – że zatrzymaliśmy pana Mirandę zgodnie z Ustawą o terroryzmie z 2000 roku, załącznik 7.

Słowo „terroryzm" nie od razu do mnie dotarło – przede wszystkim czułem się zagubiony. Najpierw zadałem pytanie, od jak dawna go trzymają, a gdy mi powiedzieli, że od trzech godzin, wiedziałem, że nie jest to żadna rutynowa kontrola. Mój rozmówca wyjaśnił, że Wielka Brytania ma „legalne prawo" przetrzymać go do dziewięciu godzin, a czas ten może zostać przedłużony wyrokiem sądu. David może też zostać aresztowany.

– Nie wiemy jeszcze, co zamierzamy zrobić – powiedział agent bezpieczeństwa.

I Stany Zjednoczone, i Wielka Brytania jasno mówiły, że wtedy, kiedy ich zdaniem działają przeciwko terroryzmowi, nie zamierzają przestrzegać żadnych ograniczeń – etycznych, prawnych ani politycznych. Teraz David został zatrzymany, a władze powoływały się na ustawę o terroryzmie. Nie wkroczył nawet na teren Wielkiej Brytanii, korzystał jedynie z tranzytu na lotnisku. Władze Wielkiej Brytanii sięgnęły na terytorium, które technicznie rzecz biorąc, nie było nawet brytyjskie, i go capnęły, powołując się przy tym na przerażające i bardzo mętne podstawy.

Prawnicy „Guardiana" i brazylijscy dyplomaci natychmiast zaczęli działać na rzecz zwolnienia Davida. Nie martwiłem się,

jak David przeżyje to zatrzymanie. Niezwykle trudne dzieciństwo sieroty w jednej z najbiedniejszych faveli w Rio de Janeiro sprawiło, że jest bardzo silny, uparty i cwany. Wiedziałem, że doskonale rozumie, co się dzieje i dlaczego, nie miałem też wątpliwości, że ci, którzy go przesłuchują, mają twardy orzech do zgryzienia. Jednak zdaniem prawników „Guardiana" rzadko zdarza się, by kogokolwiek przetrzymywano tak długo.

Badając historię stosowania Ustawy o terroryzmie, dowiedziałem się, że zatrzymuje się jedynie trzy osoby na tysiąc, a znakomita większość przesłuchań – ponad 97 procent – nie trwa nawet godziny. Jedynie 0,06 procent zatrzymań trwa ponad sześć godzin. Wyglądało na to, że należy liczyć się z możliwością aresztowania Davida po upływie dziewięciu godzin.

Celem Ustawy o terroryzmie, jak nazwa wskazuje, jest dochodzenie w sprawie powiązań różnych osób z terroryzmem. Rząd Wielkiej Brytanii twierdzi, że wykorzystuje ją „do stwierdzenia, czy dana osoba jest lub była zaangażowana w zlecanie, przygotowywanie lub podburzanie do aktów terroryzmu". Według takiego prawa zatrzymanie Davida nie miało najsłabszych nawet podstaw, chyba że stawiano teraz znak równości między moją publicystyką a terroryzmem – a jak się wydaje, tak właśnie było.

Z każdą mijającą godziną sytuacja wydawała się coraz poważniejsza. Wiedziałem jedynie, że brazylijscy dyplomaci i prawnicy „Guardiana" bez skutku starają się zlokalizować Davida na lotnisku i do niego dotrzeć. W końcu, dwie minuty przed upływem dziewiątej godziny, e-mail od Janine przyniósł wiadomość, na którą czekałem, w jednym słowie: „UWOLNIONY".

Oburzające zatrzymanie Davida natychmiast potępiono na całym świecie jako brutalną próbę zastraszenia. Reuters potwierdził w swoim doniesieniu, że taki rzeczywiście był zamiar rządu brytyjskiego: „Amerykański funkcjonariusz bezpieczeństwa powiedział Reutersowi, że jednym z głównych

celów [...] zatrzymania i przesłuchania Mirandy było danie do zrozumienia odbiorcom materiałów Snowdena, w tym «Guardianowi», iż rząd brytyjski poważnie traktuje próbę powstrzymania wszelkich przecieków".

Jednak, jak powiedziałem tłumowi dziennikarzy zebranych na lotnisku w Rio i czekających na powrót Davida, siłowa taktyka Wielkiej Brytanii nie przeszkodzi mojej publicystyce, a może nawet doda jej odwagi. Władze Wielkiej Brytanii udowodniły, że postępują skrajnie napastliwie; jedyną właściwą odpowiedzią, moim zdaniem, było stosowanie silniejszych nacisków, żądanie większej przejrzystości i odpowiedzialności. To podstawowe zadanie dziennikarstwa. Na pytanie, jak – według mnie – ta sprawa zostanie przyjęta, odparłem, że sądzę, iż rząd Wielkiej Brytanii w końcu pożałuje tego, co zrobił, ponieważ przedstawił się jako represyjny i agresywny.

Zespół Reutersa zniekształcił i źle przetłumaczył moją wypowiedź – udzieloną po portugalsku – zabrzmiała więc, jakbym w odpowiedzi na postępowanie brytyjskich władz wobec Davida zamierzał teraz opublikować dokumenty dotyczące Wielkiej Brytanii, które przedtem zamierzałem zataić. Jako wiadomość przesłana przez agencję informacyjną w tej zniekształconej formie szybko rozeszła się po świecie.

Przez następne dwa dni media gniewnie donosiły, że zamierzam prowadzić „mściwe dziennikarstwo". Było to absurdalne i nieprawdziwe – chodziło mi o to, że agresywne zachowanie rządu Wielkiej Brytanii jedynie umocniło mnie w decyzji kontynuowania pracy. Jednak, jak wielokrotnie miałem okazję się przekonać, twierdzenie, że komentarz wyrwano z kontekstu, nie pomaga zatrzymać medialnej maszynerii.

Reakcja na moje uwagi, zniekształcone czy nie, okazała się wymowna: Wielka Brytania i USA od lat zachowywały się jak zbiry, na wszelką krytykę odpowiadając groźbami – i nie tylko. Władze brytyjskie dopiero co zmusiły „Guardiana" do

zniszczenia komputerów i właśnie zatrzymały mego partnera, powołując się na Ustawę o terroryzmie. Sygnalistów ścigano, a dziennikarzom grożono więzieniem. Jednak nawet zapowiedź zdecydowanej reakcji na taką agresję spotyka się z oburzeniem ze strony lojalistów i apologetów rządu: „Mój Boże! On mówi o odwecie!". Potulne poddanie się zastraszaniu przez rządową biurokrację postrzega się jako obowiązek; opór potępia się jako niesubordynację.

W końcu David i ja uciekliśmy sprzed kamer i mogliśmy porozmawiać. Przez całe dziewięć godzin stawiał opór, przyznał jednak, że się bał.

Jasne było, że został namierzony już wcześniej – podróżnym z tego samolotu kazano pokazać paszporty czekającym na zewnątrz agentom. Gdy pokazał swój, został zatrzymany z powołaniem na Ustawę o terroryzmie. David powiedział, że „grożono mu od pierwszej do ostatniej sekundy", iż trafi do więzienia, jeśli nie będzie „w pełni współpracować". Zabrano mu cały sprzęt elektroniczny, łącznie z telefonem komórkowym zawierającym osobiste fotografie, kontakty i czaty z przyjaciółmi; grożąc aresztowaniem, zmuszono także do podania hasła do komórki.

– Czuję się, jakby wtargnęli w moje życie, jakbym był nagi – powiedział. Cały czas myślał o tym, co w minionym dziesięcioleciu rządy amerykański i brytyjski robiły pod pretekstem zwalczania terroryzmu. – Porywają ludzi, wsadzają do więzienia bez oskarżenia i bez prawnika, powodują ich zniknięcie, zamykają w Guantanamo, zabijają. Właściwie nie ma nic bardziej przerażającego, niż usłyszeć od tych dwóch rządów, że jesteś terrorystą.

To, co powiedział, nie przychodzi do głowy większości obywateli brytyjskich i amerykańskich: „Zdajesz sobie sprawę, że mogą z tobą zrobić wszystko".

Kontrowersje co do zatrzymania Davida ciągnęły się tygodniami. W Brazylii stanowiły główną wiadomość dnia,

a społeczeństwo brazylijskie dawało wyraz niemal powszechnemu oburzeniu. Brytyjscy politycy zaczęli wzywać do reformy Ustawy o terroryzmie. Oczywiście cieszyło nas, że ludzie uważali działanie Wielkiej Brytanii za nadużycie, równocześnie jednak trzeba pamiętać, że ta skandaliczna ustawa obowiązuje od lat – tyle że stosowano ją głównie wobec muzułmanów, więc mało kto się nią przejmował. To nie w porządku, że dopiero zatrzymanie współmałżonka znanego białego zachodniego dziennikarza zwróciło uwagę na jej nadużywanie – ale tak było.

Nie budziło zdziwienia ujawnienie, że przed zatrzymaniem Davida rząd brytyjski rozmawiał z Waszyngtonem. Na pytanie zadane podczas konferencji prasowej rzecznik Białego Domu odpowiedział: „Zostaliśmy uprzedzeni... więc mieliśmy zapowiedź, że coś takiego może się wydarzyć". Biały Dom odmówił potępienia zatrzymania i przyznał, że nie zrobił nic, by do niego nie dopuścić czy nawet choćby je odradzić.

Większość dziennikarzy rozumiała, jak niebezpieczny był ten krok. „Dziennikarstwo to nie terroryzm" – powiedziała oburzona Rachel Maddow w prowadzonym w MSNBC programie, trafiając w sedno sprawy. Nie wszyscy jednak podzielali jej opinię. Jeffrey Toobin chwalił rząd brytyjski w programie telewizyjnym nadawanym w paśmie największej oglądalności, równocześnie porównując Davida do „kuriera narkotykowego". Toobin dodał, że David powinien być wdzięczny, iż nie został aresztowany i postawiony przed sądem.

To zagrożenie stało się nieco bardziej prawdopodobne po ogłoszeniu przez rząd brytyjski, że rozpoczyna formalne dochodzenie w sprawie przewożonych przez Davida dokumentów (sam David wytoczył sprawę władzom brytyjskim, twierdząc, że zatrzymanie było bezprawne, ponieważ nie miało nic wspólnego z jedynym celem ustawy, na którą się powoływano: zbadania powiązań danej osoby z terroryzmem). Trudno się dziwić, że władze ośmieliły się tak postępować, skoro wybitny dziennikarz

porównuje publicystykę prowadzoną w interesie publicznym do z gruntu nielegalnych działań handlarzy narkotyków.

Niedługo przed śmiercią w 2005 roku ceniony korespondent wojenny z Wietnamu David Halberstam wygłosił wykład do studentów Szkoły Dziennikarstwa na Uniwersytecie Columbia. Powiedział, że tym momentem jego kariery, który napawa go największą dumą, była groźba ze strony amerykańskich generałów w Wietnamie, iż zażądają od redakcji „New York Timesa" odwołania go z funkcji korespondenta. Jak powiedział Halberstam, „rozwścieczyłem Waszyngton i Sajgon, pisząc pesymistyczne depesze o wojnie". Generałowie uznali go za „wroga", ponieważ przerywał ich konferencje prasowe oskarżeniami o kłamstwa.

Halberstam uważał, że doprowadzanie rządu do wściekłości jest powodem do dumy, prawdziwym celem i powołaniem dziennikarstwa. Wiedział, że bycie dziennikarzem oznacza podejmowanie ryzyka, występowanie przeciwko nadużywaniu władzy, a nie poddawanie się jej.

Dzisiaj dla wielu osób wykonujących ten zawód powodem do dumy jest pochwała od rządu za „odpowiedzialną" publicystykę – za stosowanie się do wskazówek, o czym należy pisać, a o czym nie. Ten fakt właśnie jest prawdziwą miarą, jak nisko upadło dziennikarstwo w Stanach Zjednoczonych.

EPILOG

Edward Snowden podczas naszej pierwszej rozmowy przez internet powiedział mi, że jedyną rzeczą, jakiej się obawia w związku z ujawnieniem swojej tożsamości, jest to, że jego rewelacje spotkają się z apatią i obojętnością – to zaś będzie oznaczać, że na próżno zmarnował sobie życie i zaryzykował więzienie. Stwierdzenie, że ta obawa się nie sprawdziła, byłoby znacznym niedopowiedzeniem.

W rzeczywistości skutki tej rozwijającej się wciąż historii są znacznie potężniejsze i trwalsze, mają także większy zasięg, niż kiedykolwiek uważaliśmy za możliwe. Świat zwrócił uwagę na niebezpieczeństwa wynikające z wszechobecnej inwigilacji przez państwo i zachowywanej przez rządy tajemniczości. Rozpoczęła się pierwsza globalna debata na temat wartości prywatnego życia jednostek w epoce cyfrowej, co doprowadziło do kwestionowania roli Ameryki jako hegemona w internecie. Zmienił się sposób, w jaki ludzie na całym świecie traktują wiarygodność wszelkich wypowiedzi amerykańskich urzędników rządowych. Transformacji uległy relacje między państwami. Radykalnie zmieniły się poglądy na właściwą rolę dziennikarstwa w odniesieniu do władzy, jaką dysponuje rząd. A w samych Stanach Zjednoczonych powstała zróżnicowana pod względem ideologicznym, ponadpartyjna koalicja domagająca się znaczącej reformy inwigilujących instytucji państwowych.

Głębokie przemiany wywołane przez rewelacje Snowdena ilustruje szczególnie jeden przypadek. Zaledwie kilka tygodni po pierwszym artykule dotyczącym programu potężnego

gromadzenia metadanych przez NSA, który napisałem dla „Guardiana", opierając się na dostarczonych przez Snowdena materiałach, dwaj członkowie Kongresu wspólnie zgłosili projekt ustawy zakładającej koniec finansowania tego programu Agencji. Godny uwagi jest fakt, że projekt zgłosili wspólnie John Conyers, liberał z Detroit, mający za sobą dwadzieścia kadencji w Izbie Reprezentantów, oraz Justin Amash, konserwatywny członek Tea Party, służący dopiero drugą kadencję. Trudno sobie wyobrazić dwóch bardziej różniących się kongresmanów, a jednak obu połączył sprzeciw wobec szpiegowania prowadzonego w kraju przez NSA. Ich propozycja szybko zyskała kilkudziesięciu zwolenników wywodzących się z całego spektrum ideologicznego, od najbardziej liberalnych po najbardziej konserwatywnych oraz licznych odcieni pośrednich – a to w Waszyngtonie jest bardzo rzadkim zjawiskiem.

Gdy projekt ustawy trafił pod głosowanie, debatę transmitowała telewizja C-SPAN (Cable-Satellite Public Affairs Network). Oglądałem ją, rozmawiając przez internet ze Snowdenem, który również śledził ją na komputerze w Moskwie. Obaj byliśmy pod wrażeniem. Wydaje mi się, że właśnie wówczas po raz pierwszy Snowden naprawdę zdał sobie sprawę z ogromu tego, co osiągnął. Kolejni członkowie Izby Reprezentantów wstawali, by gwałtownie zaatakować program, szydzili z pomysłu, że gromadzenie danych o połączeniach każdego Amerykanina jest konieczne do położenia kresu terroryzmowi. Było to zdecydowanie najmocniejsze zakwestionowanie polityki państwa w dziedzinie bezpieczeństwa narodowego przez Kongres od ataków z 11 września.

Aż do ogłoszenia rewelacji Snowdena po prostu trudno było sobie wyobrazić, by jakikolwiek projekt ustawy mającej osłabić znaczący program bezpieczeństwa narodowego zebrał więcej niż garstkę głosów. Jednak wynik głosowania nad projektem ustawy Conyersa-Amasha zaszokował waszyngtońskich

oficjeli: ustawa przepadła niewielką tylko liczbą głosów, 205 do 217. Poparcie dla niej nie zależało od partii politycznej: 111 demokratów sprzymierzyło się w tym wypadku z 94 republikanami. Takie przełamanie tradycyjnych podziałów partyjnych było dla mnie i Snowdena tak samo podniecające, jak wyraźne poparcie dla powściągnięcia działań NSA. Oficjalny Waszyngton jest uzależniony od ślepych podziałów plemiennych zrodzonych w sztywnych ramach walki partyjnej. Jeśli można naruszyć, a następnie wykroczyć poza pole walki niebieskich z czerwonymi, to rodzi się nadzieja na działania polityczne mające na celu prawdziwy interes obywateli.

W kolejnych miesiącach na całym świecie pojawiało się coraz więcej publikacji na temat NSA, a wielu mędrków przepowiadało, że społeczeństwa szybko stracą zainteresowanie tematem. W rzeczywistości jednak zainteresowanie dyskusją o inwigilacji narastało, nie tylko w kraju, ale i na arenie międzynarodowej. Wydarzenia z jednego zaledwie tygodnia w grudniu 2013 roku – ponad sześć miesięcy po publikacji w „Guardianie" mojego pierwszego artykułu – pokazują, jak bardzo ujawnione przez Snowdena fakty wciąż odbijają się echem i jak bardzo stanowisko NSA jest na dłuższą metę nie do utrzymania.

Tydzień rozpoczął się od głośnego orzeczenia sędziego federalnego Richarda Leona, który stwierdził, że gromadzenie metadanych przez NSA może zostać uznane za naruszenie czwartej poprawki do konstytucji USA, i nazwał zakres tego programu „niemal orwellowskim". Co więcej, ten mianowany przez Busha prawnik wskazał celnie, że „rząd nie przytacza ani jednego przypadku, w którym analiza masowego gromadzenia metadanych przez NSA rzeczywiście pomogła zapobiec grożącemu atakowi terrorystycznemu". Zaledwie dwa dni później panel doradców powołany przez prezydenta Obamę po wybuchu skandalu z NSA wydał liczący 308 stron raport na ten temat. Także i ten dokument zdecydowanie odrzucał

argumenty NSA mówiące o ogromnym znaczeniu prowadzonej przez Agencję inwigilacji. „Nasz przegląd wskazuje, że informacje na temat metadanych telefonicznych, jakie zasiliły śledztwa w sprawie terroryzmu dzięki zastosowaniu Paragrafu 215 [Patriot Act], nie były istotne dla zapobieżenia atakom" – napisali członkowie panelu, potwierdzając, że w ani jednym wypadku wynik nie byłby inny „bez programu metadanych telefonicznych z Paragrafu 215".

Poza Stanami Zjednoczonymi ten tydzień też nie był dobry dla NSA. Zgromadzenie Ogólne ONZ jednogłośnie opowiedziało się za rezolucją – zaproponowaną przez Niemcy i Brazylię – stwierdzającą, że prywatność w internecie jest podstawowym prawem człowieka; jeden z ekspertów określił ją jako „mocny komunikat dla Stanów Zjednoczonych, że pora zmienić kierunek i skończyć z całościową inwigilacją przez NSA". Tego samego dnia Brazylia ogłosiła, że nie podpisze długo oczekiwanego, wartego 4,5 miliarda dolarów kontraktu na samoloty myśliwskie z amerykańskim Boeingiem, ale kupi je od szwedzkiej firmy Saab. Kluczowym czynnikiem w zaskakującej decyzji Brazylii niewątpliwie było oburzenie, że NSA szpieguje jej przywódców, jej firmy i jej obywateli. „Amerykanów załatwił problem z NSA" – powiedział Reutersowi informator z brazylijskiego rządu.

Nie oznacza to oczywiście, że bitwa została wygrana. System bezpieczeństwa państwowego jest niezwykle potężny, prawdopodobnie nawet potężniejszy niż nasi najwyżsi wybieralni urzędnicy, i może liczyć na szerokie grono wpływowych lojalistów, gotowych bronić go za wszelką cenę. Nic więc dziwnego, że także i ta strona odnotowała kilka zwycięstw. Dwa tygodnie po opinii sędziego Leona inny sędzia federalny w innej sprawie ogłosił, odwołując się do pamięci o 11 września, że program NSA jest zgodny z konstytucją. Europejscy sojusznicy, po pierwszych wybuchach gniewu, wycofali się i potulnie

stanęli u boku Ameryki, jak to często robią. Poparcie ze strony społeczeństwa amerykańskiego również nie było stałe: sondaże wskazują, że większość Amerykanów, choć sprzeciwia się programom NSA ujawnionym przez Snowdena, chce jednak, by stanął on za to przed sądem. A wysocy amerykańscy urzędnicy państwowi zaczęli nawet argumentować, że nie tylko sam Snowden zasługuje na osądzenie i karę więzienia, ale także niektórzy dziennikarze, z którymi współpracował – w tym ja.

A jednak zwolennicy NSA wyraźnie stracili pewność siebie, a ich argumenty przeciwko reformie są coraz słabsze. Obrońcy niejawnej masowej inwigilacji często twierdzą na przykład, że pewna miara szpiegostwa jest nieodzowna. Ale to argument pozorny, bo nikt temu nie przeczy. Alternatywą masowej inwigilacji nie jest jej całkowity brak, tylko inwigilacja wymierzona, skierowana przeciwko tym, których można w uzasadniony sposób podejrzewać, że naprawdę zajmują się działalnością przestępczą. Tak „dopasowana" inwigilacja z większym prawdopodobieństwem zapobiegnie spiskom terrorystów niż obecne podejście pod hasłem „gromadzić wszystko", które zalewa agencje wywiadowcze taką ilością danych, że analitycy nie są w stanie skutecznie niczego wyłapać. Co więcej, inaczej niż ślepa inwigilacja masowa, byłaby ona zgodna z amerykańskimi wartościami konstytucyjnymi i podstawowymi założeniami zachodniej sprawiedliwości.

To właśnie na skutek skandalu z nadużywaniem inwigilacji ujawnionego przez komisję Churcha w latach 70. ta zasada – że rząd musi przedstawić jakieś dowody na możliwe wykroczenie lub status obcego agenta, zanim wolno mu będzie podsłuchiwać czyjeś rozmowy – doprowadziła do powołania sądu FISA. Niestety, sąd ten stał się zwykłym pionkiem i nie dokonuje żadnych znaczących analiz prawnych wniosków rządu o inwigilację. Zasadnicza jego idea jest jednak rozsądna i wskazuje drogę postępowania. Przekształcenie sądu FISA w prawdziwy

system prawny, zamiast obecnego jednostronnego układu, w którym tylko rząd może przedstawiać sprawę, oznaczałoby pozytywne działanie reformatorskie.

Podobne zmiany legislacyjne w kraju same w sobie zapewne nie wystarczą, by rozwiązać problem inwigilacji, ponieważ agencje bezpieczeństwa narodowego często współpracują z ciałami, które powinny je kontrolować (jak widzieliśmy na przykładzie Komisji Wywiadu w Kongresie, które już są całkowicie opanowane). Jednak ten rodzaj zmian legislacyjnych może przynajmniej wzmocnić zasadę, że dla prowadzonej na ślepo masowej inwigilacji nie ma miejsca w demokracji głoszącej, iż kieruje się ona konstytucyjnymi gwarancjami prywatności.

Możliwe są także inne kroki w celu odzyskania prywatności w internecie i ograniczenia inwigilacji przez państwo. Międzynarodowe wysiłki – którym obecnie przewodzą Niemcy i Brazylia – na rzecz zbudowania nowej struktury internetu, tak by większość ruchu w sieci nie musiała iść tranzytem przez Stany Zjednoczone, mogą przyczynić się do znacznego osłabienia kontroli Ameryki nad internetem. Także i jednostki mogą odegrać rolę w odzyskiwaniu własnej prywatności online. Odmowa korzystania z usług firm technologicznych, które współpracują z NSA i jej sojusznikami, przyczyni się do nacisku na te firmy, by zaprzestały współpracy, ich rywali skłoni zaś do poświęcenia większej uwagi ochronie prywatności. Już w tej chwili pewna liczba europejskich firm promuje usługi poczty elektronicznej i czaty jako alternatywę dla ofert Google'a i Facebooka, podkreślając, że nie dostarczają – i nie będą dostarczać – danych użytkowników do NSA.

Co więcej, wszyscy użytkownicy mogą stosować szyfrowanie i narzędzia umożliwiające anonimowe wyszukiwanie, by w ten sposób nie pozwolić rządom na wgląd w prywatną korespondencję i śledzenie sposobu korzystania z internetu. Jest to szczególnie istotne dla osób pracujących we wrażliwych

dziedzinach: dziennikarzy, prawników czy działaczy praw człowieka. Natomiast społeczność informatyków powinna starać się rozwijać skuteczniejsze i przyjazne dla użytkowników programy szyfrujące i zapewniające anonimowość.

Na wszystkich tych frontach wiele pozostało do zrobienia. Jednak nie upłynął jeszcze rok od mego spotkania ze Snowdenem w Hongkongu, a już nie ma wątpliwości, że jego rewelacje przyniosły zasadnicze, nieodwracalne zmiany w wielu krajach i wielu dziedzinach. Poza konkretnymi rozwiązaniami dotyczącymi reformy NSA Snowden znacznie przyczynił się do przejrzystości działań rządu i reform jako takich. Stał się wzorem i inspiracją dla innych, przyszli aktywiści zaś zapewne pójdą w jego ślady i udoskonalą zastosowane przez niego metody.

Administracja Obamy, która wniosła więcej oskarżeń przeciwko winnym przecieków niż wszystkie poprzednie administracje razem wzięte, starała się stworzyć klimat strachu, który wszelkich sygnalistów zniechęciłby do działania. Snowden jednak rozbił ten wzorzec. Udało mu się pozostać na wolności, poza zasięgiem USA. Co więcej, odmówił działania w ukryciu, tylko dumnie wystąpił i się przedstawił. W rezultacie społeczeństwo nie wyobraża go sobie jako skazańca w pomarańczowym kombinezonie i kajdankach, ale jako niezależną postać, która przemawia we własnym imieniu i wyjaśnia, co zrobiła i dlaczego. Rząd USA nie ma już możliwości osłabiania przekazu przez samą demonizację posłańca. To potężna nauka dla przyszłych sygnalistów: mówienie prawdy nie musi niszczyć życia.

Jeśli zaś chodzi o nas, pozostałych, to inspiratorski wpływ Snowdena także jest głęboki – po prostu przypomniał on wszystkim o niezwykłej zdolności każdej istoty ludzkiej do zmieniania świata. Ktoś pod wszelkimi względami zwyczajny – wychowany przez rodziców niedysponujących ani pieniędzmi, ani władzą, ktoś, kto nawet nie ukończył szkoły średniej, ktoś, kto pracuje jako mało znany pracownik ogromnej korporacji – jednym

działaniem zmienił bieg historii, bo kierował się sumieniem.

Nawet najbardziej oddani aktywiści czasami mają ochotę ulec defetyzmowi. Największe instytucje wydają się zbyt potężne, by je zmienić; ortodoksyjne przekonania wydają się zbyt mocno zakorzenione, by je usunąć. Istnieje zawsze wiele stron mających ukryty interes w zachowaniu status quo. Jednak to ludzie wspólnie mogą zadecydować, w jakim świecie chcą żyć – a nie tylko nieliczne, działające w sekrecie elity. Popieranie ludzkiej zdolności do rozumnego myślenia i podejmowania decyzji to cel sygnalistów, aktywistów i politycznego dziennikarstwa. I z tym właśnie mamy teraz do czynienia – dzięki temu, co ujawnił Edward Snowden.

PODZIĘKOWANIA

Podejmowane w ostatnich latach wysiłki zachodnich rządów, by ukrywać przed własnymi obywatelami niosące poważne konsekwencje działania, wielokrotnie natrafiały na przeszkody w postaci godnych uwagi przedsięwzięć odważnych sygnalistów, którzy te działania ujawniali. Ludzie pracujący w agencjach rządowych lub wojskowych Stanów Zjednoczonych i ich sojuszników, którzy odkrywają poważne nadużycia, raz za razem uznają, że nie mogą zachować milczenia. Zamiast tego występują publicznie, mówiąc o wykroczeniach władzy. Czasami oznacza to świadome łamanie prawa, a zawsze – narażenie się na wielkie koszty osobiste, ryzykują oni bowiem karierę, osobiste związki i wolność. Każdy, kto żyje w demokracji, każdy, kto ceni sobie przejrzystość i odpowiedzialność, ma wobec tych sygnalistów ogromny dług wdzięczności.

Długa liczba poprzedników, będących inspiracją dla Edwarda Snowdena, zaczyna się od człowieka, który ujawnił Pentagon Papers – Daniela Ellsberga, przez wiele lat mego osobistego bohatera, a teraz przyjaciela i współpracownika. To jego przykładem staram się kierować we wszystkim, co robię. Inni odważni sygnaliści, którzy podejmowali ryzyko prześladowania, by ujawnić światu ważne prawdy, to między innymi Chelsea Manning, Jesselyn Radack i Thomas Tamm, jak również byli pracownicy NSA Thomas Drake i Bill Binney. Także i oni w znaczący sposób zainspirowali Snowdena.

Ujawnienie wszechobecnego systemu niepodejrzewanej przez nikogo inwigilacji, budowanego przez Stany Zjednoczone i ich sojuszników, było osobistym aktem sumienia i poświęceniem się Snowdena. Niezwykły był widok tego dwudziestodziewięciolatka,

który świadomie ryzykuje życie w więzieniu w imię obrony zasad i podstawowych praw człowieka. Nieugięty charakter Snowdena i jego niewzruszony spokój – wyrastający z przekonania, że postępuje słusznie – kierowały wszystkimi moimi doniesieniami w tej sprawie i niewątpliwie wywrą głęboki wpływ na resztę mego życia.

Ta sprawa nie mogłaby się odbić tak szerokim echem bez działań mojej niezwykle dzielnej i znakomitej dziennikarskiej partnerki i przyjaciółki Laury Poitras. Mimo że rząd USA przez lata nękał ją za kręcone przez nią filmy, ani przez chwilę nie zawahała się przed ostrym przedstawieniem sprawy NSA. Jej uparte zachowywanie prywatności, jej niechęć do znajdowania się w świetle reflektorów czasami uniemożliwiały dostrzeżenie, jak nieodzowny był jej wkład w całą naszą pracę reporterską. Niemniej jednak to właśnie jej doświadczenie, jej geniusz strategiczny, jej rozsądek i odwaga były sercem i duszą wszystkich naszych działań. Rozmawialiśmy niemal codziennie i każdą znaczącą decyzję podejmowaliśmy razem. Nie mógłbym sobie życzyć doskonalszego partnerstwa ani bardziej dodającej odwagi i inspirującej przyjaźni.

Odwaga Snowdena – jak Laura i ja się spodziewaliśmy – okazała się zaraźliwa. Wielu dziennikarzy niezłomnie prowadziło tę sprawę, w tym redaktorzy „Guardiana" Janine Gibson, Stuart Millar i Alan Rusbridger oraz kilku dziennikarzy tej gazety, z Ewenem MacAskillem na czele. Snowdenowi udało się pozostać na wolności, a zatem mógł uczestniczyć w wywołanej przez siebie debacie dzięki śmiałemu i nieodzownemu poparciu ze strony WikiLeaks i ich pracownicy Sarah Harrison, która pomogła mu wyjechać z Hongkongu, a potem pozostała z nim przez kilka miesięcy w Moskwie, co sprawiło, że nie może teraz bezpiecznie wrócić do Wielkiej Brytanii, swojej ojczyzny.

Liczni przyjaciele i koledzy udzielali mi mądrych rad i wspierali w trudnych sytuacjach, w tym Ben Wizner i Jameel Jaffer z ACLU, mój od zawsze najlepszy przyjaciel Norman Fleisher, jeden z najodważniejszych i najlepszych dziennikarzy śledczych na

świecie Jeremy Scahill, silna i przedsiębiorcza brazylijska reporterka Sonia Bridi z TV Globo oraz dyrektor zarządzający fundacji Freedom of the Press Trevor Timm. Członkowie mojej rodziny, w tym moi rodzice, mój brat Mark i moja bratowa Christine, którzy często martwili się tym, co się działo (jak tylko członkowie rodziny potrafią), i cały czas zdecydowanie okazywali mi wsparcie (jak tylko członkowie rodziny potrafią).

Nie było mi łatwo pisać tę książkę, szczególnie w istniejących okolicznościach, dlatego jestem naprawdę wdzięczny Metropolitan Books: Connorowi Guyowi za sprawne zarządzanie, Grigory'emu Tovbisowi za przenikliwe uwagi redakcyjne i techniczną skuteczność, a przede wszystkim Rivie Hocherman, której inteligencja i wysokie standardy uczyniły ją najlepszą z możliwych redaktorką tej książki. To już moja druga książka, której wydawcą jest Sara Bershtel; jej wielka mądrość i twórczy umysł sprawiają, że nie wyobrażam sobie, żebym kiedykolwiek chciał coś publikować bez niej. Mój agent literacki Dan Conaway raz jeszcze okazał się stabilizującym, mądrym głosem podczas całego procesu pisania. Wielkie dzięki także dla Taylor Barnes za jej krytyczną pomoc w pisaniu tej książki; jej talenty dokumentalistki i intelektualna energia nie pozostawiają wątpliwości, że czeka ją znakomita kariera dziennikarska.

Jak zawsze w centrum wszystkiego, co robię, jest mój partner życiowy, od dziewięciu lat mąż, moja bratnia dusza David Miranda. Ciężka próba, jaką przeszedł na skutek naszej publicystyki, była ogromnie denerwująca i groteskowa, ale dzięki temu świat zobaczył, jakim jest niezwykłym człowiekiem. Przez cały czas dodawał mi odwagi, umacniał mnie w decyzjach, doradzał w wyborach, oferował wnikliwe uwagi i bez wahania stał u mego boku, okazując mi bezwarunkowe wsparcie i miłość. Takie partnerstwo nie da się porównać z niczym innym, ponieważ gasi strach, burzy przeszkody i sprawia, że wszystko staje się możliwe.

O AUTORZE

GLENN GREENWALD jest pisarzem, autorem niedawno wydanych książek *With Liberty and Justice for Some* oraz *A Tragic Legacy*. Był prawnikiem specjalizującym się w prawie konstytucyjnym i do października 2013 roku publicystą „Guardiana". Wielokrotnie nagradzany za komentarze i artykuły śledcze, w 2013 roku otrzymał między innymi prestiżową nagrodę za dziennikarstwo śledcze od Online News Association, nagrodę Esso za wybitne osiągnięcia reporterskie (Prêmio Esso de Reportagem, brazylijski odpowiednik Nagrody Pulitzera) oraz Pioneer Award przyznawaną przez Electronic Frontier Foundation. Przyznano mu również 2013 George Polk Award for National Security Reporting, zaś czasopismo „Foreign Policy" uznało go za jednego ze stu najważniejszych myślicieli na świecie (100 Top Global Thinkers). Teksty Greenwalda zamieszczało wiele gazet i czasopism o tematyce politycznej, w tym „New York Times", „Los Angeles Times" i „American Conservative". Na początku 2014 roku Greenwald został współzałożycielem nowej organizacji mediowej The Intercept.

SPIS TREŚCI