SEM LUGAR PARA SE ESCONDER

Edward Snowden, a NSA e a espionagem do governo americano

GLENN GREENWALD

SEM LUGAR PARA SE ESCONDER

SEM LUGAR PARA SE ESCONDER

GLENN GREENWALD

PRIMEIRA PESSOA

Título original: *No Place to Hide*

TRADUÇÃO: Fernanda Abreu

PREPARO DE ORIGINAIS: Taís Monteiro

REVISÃO: Hermínia Totti e Luis Américo Costa

DIAGRAMAÇÃO: Ana Paula Daudt Brandão

CAPA: David Shoemaker

ADAPTAÇÃO DA CAPA: Miriam Lerner

ADAPTAÇÃO PARA EBOOK: Marcelo Morais

CIP-BRASIL. CATALOGAÇÃO NA PUBLICAÇÃO
SINDICATO NACIONAL DOS EDITORES DE LIVROS, RJ.

G831s

Greenwald, Glenn, 1967-

Sem lugar para se esconder [recurso eletrônico] / Glenn Greenwald [tradução de

[tradução de Fernanda Abreu]; Rio de Janeiro: Sextante, 2014.
recurso digital
Tradução de: No place to hide
Formato: ePub
Requisitos do sistema: Adobe Digital Editions
Modo de acesso: World Wide Web
ISBN 978-85-431-0096-8
(recurso

(recurso eletrônico)
1. Jornalismo. 2. Reportagens investigativas. 3. Reportagens e repórteres. 4.Espionagem. 5. Livros eletrônicos. I. Título.

14-11493

CDD: 070.43
CDU: 070.4

Rua Voluntários da Pátria, 45 – Gr. 1.404
Botafogo – 22270-000 – Rio de Janeiro – RJ
Tel.: (21) 2538-4100 – Fax: (21) 2286-9244
E-mail: atendimento@esextante.com.br
www.sextante.com.br

O governo dos Estados Unidos aperfeiçoou uma capacidade tecnológica que nos permite monitorar as mensagens transmitidas pelo ar (...). A qualquer momento, ela pode ser voltada contra a população, e a capacidade de vigiar tudo – conversas telefônicas, telegramas, qualquer coisa – é tamanha que nenhum americano teria mais privacidade alguma. Não haveria onde se esconder.

Senador Frank Church, presidente do
Comitê Especial do Senado para Estudar Operações do Governo
Relacionadas a Atividades de Inteligência, 1975

Este livro é dedicado a todos aqueles que tentaram
expor os sistemas secretos de vigilância
em massa do governo dos Estados Unidos,
e principalmente aos corajosos delatores que arriscaram
a própria liberdade para fazê-lo.

INTRODUÇÃO

No outono de 2005, sem muitas expectativas grandiosas, decidi criar um blog sobre política. Na época, eu mal sabia quanto essa decisão acabaria mudando a minha vida. Minha principal motivação foi uma apreensão crescente em relação às teorias de poder radicais e extremistas adotadas pelo governo dos Estados Unidos após o 11 de Setembro, e eu esperava que escrever sobre essas questões fosse me possibilitar um impacto maior do que o proporcionado por minha carreira de advogado especializado em direito constitucional e direitos civis.

Apenas sete semanas depois de lançado o blog, o *New York Times* soltou uma bomba: segundo o jornal, em 2001 o governo Bush tinha dado uma ordem secreta à NSA – a Agência de Segurança Nacional – para espionar as comunicações eletrônicas dos norte-americanos sem obter os mandados exigidos pela legislação criminal vigente. Quando revelada, a espionagem já durava quatro anos e tivera como alvo, no mínimo, muitos milhares de cidadãos do país.

O tema era uma convergência perfeita entre minhas paixões e minha especialidade. O governo tentou justificar o programa secreto da NSA evocando exatamente o tipo de teoria extremista de poder executivo que havia me motivado a começar a escrever: a ideia de que a ameaça do terrorismo dava ao presidente autoridade praticamente ilimitada para fazer qualquer coisa de modo a "garantir a segurança da nação", inclusive violar a lei. O debate subsequente envolvia questões complexas relacionadas ao direito constitucional e à interpretação dos estatutos que minha formação jurídica me permitia abordar com conhecimento de causa.

Passei os dois anos seguintes cobrindo todos os aspectos do escândalo da espionagem não autorizada da NSA, tanto no meu blog quanto em um livro lançado em 2006, que se tornou um best-seller. Minha posição era clara: ao ordenar uma vigilância ilegal, o presidente havia cometido crimes e deveria ser responsabilizado por eles. No clima político cada vez mais opressivo e impregnado de patriotismo fanático do país, esta se revelou uma posição muito controversa.

Foi esse histórico que, muitos anos mais tarde, levou Edward Snowden a me escolher como seu primeiro contato para revelar abusos cometidos pela NSA em escala ainda mais monumental. Ele disse que acreditava poder confiar em mim para entender os perigos da vigilância em massa e do sigilo excessivo do Estado, e também para não recuar ante pressões do governo e de seus muitos aliados na mídia e em outras áreas.

O volume impressionante de documentos ultrassecretos que Snowden me transmitiu, bem como as fortes emoções dos acontecimentos relacionados à sua pessoa, gerou um interesse mundial inédito pela ameaça da vigilância eletrônica em massa e pelo valor da privacidade na era digital. Os problemas subjacentes, porém, já vinham se agravando havia muitos anos, quase sempre em segredo.

A polêmica atual em relação à NSA tem, sem dúvida, muitos aspectos singulares. A tecnologia de hoje possibilita um tipo de vigilância onipresente, antes restrita aos mais criativos autores de ficção científica. Além disso, a veneração dos Estados Unidos pela segurança acima de tudo, iniciada após o

11 de Setembro, criou um ambiente particularmente propício aos abusos de poder. Graças à coragem de Snowden e à relativa facilidade de copiar informações digitais, temos a possibilidade única de observar em primeira mão os detalhes de como o sistema de vigilância de fato funciona.

Apesar disso, as questões levantadas pelo caso da NSA remetem, sob muitos aspectos, a diversos episódios históricos ocorridos em séculos passados. Na verdade, a oposição à invasão da privacidade pelo governo foi um fator decisivo para a fundação dos próprios Estados Unidos, quando colonos norte-americanos protestaram contra leis que permitiam aos agentes do governo britânico saquear qualquer casa que quisessem. Os colonos concordavam que fosse legítimo o Estado obter mandados específicos para revistar pessoas quando os indícios estabelecessem uma causa provável para suas infrações. Mas os mandados genéricos – a prática de submeter a população inteira a revistas indiscriminadas – eram fundamentalmente ilegítimos.

A Quarta Emenda constitucional entronizou essa ideia no direito norte-americano. Seus termos são claros e sucintos: "O direito dos cidadãos à segurança de sua pessoa, de suas casas, de seus documentos e de seus bens contra revistas e confiscos não fundamentados não será violado, e só serão emitidos mandados mediante causa provável, sustentados por juramento ou declaração, e que descrevam em pormenores o local a ser revistado e as pessoas ou coisas a serem confiscadas." O objetivo da emenda, acima de tudo, era abolir para sempre no país o poder do governo de submeter os cidadãos a uma vigilância generalizada e sem suspeita prévia.

O desacordo relacionado à vigilância no século XVIII girava em torno de revistas domiciliares, mas, à medida que a tecnologia evoluiu, a vigilância também evoluiu. Em meados do século XIX, com a expansão das ferrovias – permitindo uma entrega de correio rápida e barata –, a abertura ilegítima de toda a correspondência pelo governo britânico provocou um forte escândalo no Reino Unido. Nas primeiras décadas do século XX, o Escritório de Investigação dos Estados Unidos – precursor do atual FBI – utilizava grampos, além de monitorar correspondências e usar informantes, para controlar quem se opusesse às políticas nacionais.

Sejam quais forem as técnicas envolvidas, a vigilância em massa apresentou várias características constantes ao longo da história. Em primeiro lugar, são sempre os dissidentes e marginalizados do país que suportam o peso maior dessa vigilância, o que leva aqueles que apoiam o governo, ou os que são simplesmente apáticos, à crença equivocada de que estão imunes. E a história mostra que a simples existência de um aparato de vigilância em massa, seja ele usado da forma que for, por si só já basta para sufocar a dissidência. Uma população consciente de estar sendo vigiada logo se torna obediente e temerosa.

Em meados dos anos 1970, uma investigação da espionagem doméstica conduzida pelo FBI fez a chocante descoberta de que a agência havia rotulado meio milhão de cidadãos norte-americanos como "subversivos" em potencial e espionava pessoas regularmente com base apenas em suas crenças políticas. (A lista de alvos ia de Martin Luther King a John Lennon, do Movimento de Liberação Feminina à anticomunista Sociedade John Birch.) Mas a praga do abuso da vigilância está longe de ser uma exclusividade da história dos Estados Unidos. Pelo contrário: ela é a tentação universal de qualquer poder inescrupuloso. E em todos os casos o motivo é sempre o mesmo: eliminar dissidências e garantir a submissão.

Assim, a vigilância une governos cujas doutrinas políticas são notavelmente divergentes em outros temas. Na virada para o século XX, tanto o Império Britânico quanto o Império Francês criaram

departamentos especializados em monitoramento para lidar com a ameaça dos movimentos anticolonialistas. Após a Segunda Guerra Mundial, o Ministério da Segurança Estatal da Alemanha Oriental, conhecido como Stasi, tornou-se um sinônimo de intromissão governamental na vida privada da população. E há pouco tempo, quando os protestos populares da Primavera Árabe ameaçaram o controle do poder pelos ditadores, os regimes da Síria, do Egito e da Líbia passaram a espionar o uso da internet por dissidentes internos.

Investigações conduzidas pelo canal de notícias Bloomberg e pelo *Wall Street Journal* mostraram que, ao serem ameaçadas pelos manifestantes, essas ditaduras literalmente foram às compras para obter dispositivos de vigilância junto a empresas de tecnologia ocidentais. Na Síria, o regime de Assad convocou funcionários da empresa de vigilância italiana Area SpA e lhes disse que precisava "rastrear pessoas com urgência". No Egito, a polícia secreta de Mubarak comprou equipamentos para quebrar a criptografia do Skype e interceptar chamadas de ativistas. E na Líbia, segundo o periódico, jornalistas e rebeldes que entraram em um centro de monitoramento do governo em 2011 encontraram "uma parede inteira de aparelhos pretos do tamanho de geladeiras" da empresa de vigilância francesa Amesys. O aparato "inspecionava o tráfego de internet" do principal provedor líbio, "abrindo e-mails, desvendando senhas, bisbilhotando chats e mapeando conexões entre vários suspeitos".

A habilidade para interceptar as comunicações das pessoas confere imenso poder a quem o faz. A menos que esse poder seja contido por uma rígida supervisão e prestação de contas, quase certamente haverá abusos. Esperar que o governo dos Estados Unidos opere uma imensa máquina de vigilância em total sigilo, sem ceder às tentações que isso representa, contraria todos os exemplos históricos e todos os indícios disponíveis sobre a natureza humana.

De fato, antes mesmo das revelações de Snowden, já estava ficando claro que tratar os Estados Unidos como um país de alguma forma excepcional no que tange à questão da vigilância é uma postura bastante ingênua. Em 2006, em uma audiência no Congresso intitulada "A internet na China: ferramenta de liberdade ou de supressão?", sucederam-se pronunciamentos condenando empresas de tecnologia norte-americanas por ajudarem a China a eliminar dissidências na internet. Christopher Smith, deputado republicano pelo estado de Nova Jersey, que presidiu a audiência, equiparou a cooperação do Yahoo com a polícia secreta chinesa a entregar Anne Frank aos nazistas. Seu discurso foi uma arenga feroz, um espetáculo típico de quando representantes do governo norte-americano discorrem sobre um regime não alinhado com os Estados Unidos.

No entanto, nem mesmo quem compareceu à audiência pôde deixar de notar que ela ocorreu coincidentemente apenas dois meses depois de o *New York Times* revelar a vasta operação de grampos não autorizados conduzida pela administração Bush. À luz dessas descobertas, denunciar outros países por realizarem a própria vigilância doméstica perdia todo o sentido. Brad Sherman, deputado democrata pela Califórnia, discursou depois de Smith e observou que as empresas de tecnologia às quais se estava aconselhando resistir ao regime chinês também deveriam tomar cuidado com seu próprio governo. "Caso contrário", afirmou ele, profético, "embora os chineses possivelmente tenham sua privacidade violada de maneira abominável, pode ser que nós, aqui nos Estados Unidos, também descubramos que talvez algum futuro presidente, em nome dessas interpretações muito genéricas da Constituição, esteja lendo nossos e-mails, e eu preferiria que isso não acontecesse sem um mandado judicial."

Nas últimas décadas, o temor relacionado ao terrorismo – intensificado pelos constantes exageros quanto ao risco real – vem sendo explorado por líderes norte-americanos para justificar uma ampla gama de políticas extremistas. Isso conduziu a guerras de agressão, a um regime de tortura com abrangência mundial e à detenção (até mesmo ao assassinato) de cidadãos estrangeiros e norte-americanos sem qualquer acusação. Mas o onipresente e sigiloso sistema de vigilância indiscriminada gerado por esse temor pode muito bem vir a se revelar seu legado mais duradouro. Isso porque, apesar de todos os paralelos históricos, o escândalo da NSA tem também uma dimensão genuinamente nova: o papel desempenhado hoje pela internet na vida cotidiana das pessoas.

Sobretudo para as gerações mais jovens, a grande rede não é um universo isolado, separado, no qual são realizadas algumas das funções da vida. A internet não é apenas nosso correio e nosso telefone. Ela é a totalidade do nosso mundo, o lugar onde quase tudo acontece. É lá que se faz amigos, se escolhe livros e filmes, se organiza o ativismo político, e é lá que são criados e armazenados os dados mais particulares de cada um. É na internet que desenvolvemos e expressamos nossa personalidade e individualidade.

Transformar *essa* rede em um sistema de vigilância em massa tem implicações muito diferentes das de quaisquer outros programas semelhantes anteriores do governo. Todos os antigos sistemas de espionagem eram obrigatoriamente mais limitados e propensos a serem driblados. Permitir que a vigilância crie raízes na internet significaria submeter quase todas as formas de interação, planejamento e até mesmo pensamento humanos ao escrutínio do Estado.

Desde que começou a ser usada de forma ampla, a internet foi vista por muitos como detentora de um potencial extraordinário: o de libertar centenas de milhões de pessoas graças à democratização do discurso político e ao nivelamento entre indivíduos com diferentes graus de poder. A liberdade na rede – a possibilidade de usá-la sem restrições institucionais, sem controle social ou estatal, e sem a onipresença do medo – é fundamental para que essa promessa se cumpra. Converter a internet em um sistema de vigilância, portanto, esvazia seu maior potencial. Pior ainda: a transforma em uma ferramenta de repressão, e ameaça desencadear a mais extrema e opressiva arma de intrusão estatal já vista na história humana.

É isso que torna as revelações de Snowden tão estarrecedoras e lhes confere uma importância tão vital. Quando se atreveu a expor a capacidade espantosa de vigilância da NSA e suas ambições mais espantosas ainda, ele deixou bem claro que estamos em uma encruzilhada histórica. Será que a era digital vai marcar o início da liberação individual e da liberdade política que só a internet é capaz de proporcionar? Ou ela vai criar um sistema de monitoramento e controle onipresentes, que nem os maiores tiranos do passado foram capazes de conceber? Hoje, os dois caminhos são possíveis. São as nossas ações que irão determinar nosso destino.

1

CONTATO

Recebi minha primeira comunicação de Edward Snowden no dia 1º de dezembro de 2012, embora na época não tivesse a menor ideia de que viesse dele.

O contato foi feito por um e-mail assinado Cincinnatus, em referência a Lucius Quinctius Cincinnatus, agricultor romano que, no século V a.C., foi nomeado ditador da cidade para defendê-la dos ataques que sofria. Ele é mais lembrado pelo que fez após derrotar os inimigos da cidade: voluntariamente, abriu mão na mesma hora do poder político e voltou à vida de agricultor. Aclamado como "modelo de virtude cívica", Cincinnatus virou um símbolo do uso do poder político em prol do interesse público, e do valor de limitar ou mesmo abandonar o poder individual em nome do bem maior.

O e-mail começava dizendo: "A segurança das comunicações das pessoas é muito importante para mim", e seu objetivo declarado era me convencer a adotar o padrão de criptografia PGP, para que Cincinnatus pudesse me transmitir informações nas quais tinha certeza que eu estaria interessado. Inventado em 1991, o PGP – que em inglês significa *pretty good privacy* , "privacidade bastante razoável" – foi aprimorado até se tornar uma sofisticada ferramenta de proteção para e-mails e outras formas de contato on-line contra vigilância e hackers.

Basicamente, o programa envolve cada mensagem em um escudo de proteção formado por um código composto por centenas, ou até milhares, de números aleatórios e letras com distinção entre caixa alta e baixa. As agências de inteligência mais avançadas do mundo – grupo que sem dúvida inclui a NSA – têm so wares de quebra de senhas com capacidade de um bilhão de tentativas por segundo, mas os códigos PGP são tão compridos e aleatórios que mesmo o mais sofisticado dos so wares precisa de muitos anos para quebrá-los. As pessoas que mais temem ter suas comunicações monitoradas, como agentes de inteligência, espiões, ativistas dos direitos humanos e hackers, confiam nesse padrão de criptografia para proteger suas mensagens.

No e-mail, "Cincinnatus" dizia que tinha procurado por toda parte minha "chave pública" de PGP, um código único que permite às pessoas receberem e-mails criptografados, mas que não havia encontrado. Isso o levara a concluir que eu não usava o programa, e ele então continuou: "Isso põe em risco qualquer pessoa que se comunique com o senhor. Não estou dizendo que todas as suas comunicações precisam ser criptografadas, mas seria bom pelo menos dar essa opção a quem deseja entrar em contato com o senhor."

A seguir, "Cincinnatus" citou o escândalo sexual do general David Petraeus, cujo caso extraconjugal com a jornalista Paula Broadwell, que pôs fim à sua carreira, foi revelado quando investigadores descobriram e-mails do Google entre os dois. Se Petraeus tivesse criptografado as mensagens antes de enviá-las pelo Gmail ou salvá-las em sua pasta de rascunhos, escreveu ele, os investigadores não teriam conseguido lê-las. "A criptografia é importante, e não só para espiões e adúlteros." Instalar um programa de e-mail criptografado, segundo Cincinnatus, "é uma medida de

segurança crucial para qualquer um que deseje se comunicar com o senhor". Para me motivar a seguir seu conselho, ele acrescentou: "Há pessoas por aí com quem o senhor adoraria conversar, mas que nunca vão poder entrar em contato a menos que saibam que suas mensagens não poderão ser lidas em trânsito."

Ele então se ofereceu para me instruir na instalação do programa. "Se precisar de alguma ajuda, por favor, me avise, ou então peça auxílio no Twitter. O senhor tem muitos seguidores versados em tecnologia dispostos a oferecer assistência imediata." E assinou assim: "Obrigado. C."

Eu já pretendia usar um so ware de criptografia havia bastante tempo. Fazia anos que escrevia sobre o WikiLeaks, delatores, o coletivo ativista cibernético conhecido como Anonymous e assuntos relacionados, além de me comunicar de vez em quando com membros do establishment de segurança nacional norte-americana. A maioria dessas pessoas se preocupa muito com a segurança de suas comunicações e com impedir qualquer monitoramento indesejado. Só que o programa é complicado, sobretudo para alguém como eu, que tinha muito pouca habilidade em programação e informática. Assim, essa era uma das coisas que eu nunca chegara a fazer.

O e-mail de C. não me levou a agir. Como eu tinha ficado conhecido por cobrir histórias que o restante da imprensa em geral ignorava, era procurado com frequência por todo tipo de gente me oferecendo um "grande furo" que em geral acabava não sendo nada. Além disso, sempre trabalho em mais reportagens do que consigo administrar, e portanto preciso de algo concreto para me obrigar a largar o que estou fazendo e correr atrás de uma nova pista. Apesar da vaga alusão a "pessoas por aí" com quem eu "adoraria conversar", não havia nada suficientemente tentador no e-mail de C. Eu o li, mas não respondi.

Três dias depois, recebi uma nova mensagem dele pedindo-me que confirmasse o recebimento do primeiro e-mail. Dessa vez respondi depressa: "Recebi e vou cuidar do assunto. Não tenho código PGP e não sei como arranjar um, mas vou tentar encontrar alguém para me ajudar."

Mais tarde no mesmo dia, ele me respondeu com um passo a passo claro sobre o sistema PGP, uma espécie de manual de criptografia para iniciantes. Ao final das instruções – que considerei complexas e confusas, sobretudo devido à minha própria ignorância –, ressaltou que aquilo era só "o básico do básico. Se não conseguir alguém para guiá-lo na instalação, geração e utilização do programa, por favor, me avise. Posso facilitar o contato com pessoas que entendem de cripto em quase qualquer lugar do mundo".

Esse e-mail terminava com uma assinatura mais reveladora: "Criptograficamente, Cincinnatus."

Apesar das minhas intenções, não pude arrumar tempo para me dedicar à criptografia. Sete semanas se passaram, e o fato de eu não conseguir resolver aquilo não me saiu da cabeça. E se aquela pessoa tivesse mesmo uma revelação importante a fazer e eu fosse perdê-la só por ter deixado de instalar um programa de computador? Tirando todo o resto, mesmo que Cincinnatus no final das contas não tivesse nada de interessante a dizer, eu sabia que a criptografia poderia me ser útil no futuro.

No dia 28 de janeiro de 2013, mandei-lhe um e-mail dizendo que iria arrumar alguém para me ajudar com a criptografia, e que esperava estar com tudo pronto dali a um ou dois dias.

Ele respondeu no dia seguinte: "Que ótima notícia! Se precisar de mais alguma ajuda ou surgirem outras perguntas, estarei sempre à disposição. Queira aceitar meus mais sinceros agradecimentos pelo seu apoio à privacidade nas comunicações! Cincinnatus."

Mais uma vez, porém, não tomei nenhuma atitude. Além de estar envolvido em outras matérias, eu ainda não me convencera de que C. tivesse qualquer coisa interessante a dizer. Não fazer nada não foi uma decisão consciente. O que aconteceu foi que, na minha lista sempre comprida demais de coisas a fazer, instalar um programa de criptografia a pedido daquele desconhecido nunca se tornou urgente o bastante para que eu interrompesse outras atividades e me concentrasse nisso.

C. e eu, portanto, nos vimos em um impasse: ele não queria me dizer nada específico sobre o que tinha, ou mesmo sobre quem era e onde trabalhava, a menos que eu instalasse a criptografia. No entanto, sem o atrativo de algum detalhe, atender ao seu pedido e encontrar tempo para isso não era uma prioridade para mim.

Diante da minha inércia, C. intensificou seus esforços: produziu um vídeo de dez minutos chamado "PGP para jornalistas". Usando um so ware que gera vozes computadorizadas, o vídeo me ensinava a instalar o programa, passo a passo, de um modo fácil, que incluía gráficos e imagens.

Mesmo assim, continuei sem fazer nada. Nesse momento, como ele me contou mais tarde, C. ficou frustrado. "Aqui estou eu", pensou, "prestes a arriscar minha liberdade e talvez até minha vida para entregar a esse cara milhares de documentos ultrassecretos do mais secreto órgão público desta nação – um vazamento que vai gerar dezenas, se não centenas, de enormes furos jornalísticos, e ele não é capaz nem de se dar ao trabalho de instalar um programa de criptografia."

Eis quão perto cheguei de ignorar um dos maiores e mais influentes vazamentos de segurança nacional da história dos Estados Unidos.

A notícia seguinte que tive do assunto veio dez semanas mais tarde. Em 18 de abril, peguei um avião do Rio de Janeiro, onde moro, até Nova York, onde tinha algumas palestras marcadas sobre os perigos do sigilo governamental e da violação das liberdades civis em nome da Guerra ao Terror.

Ao aterrissar no aeroporto JFK, vi que tinha recebido um e-mail da documentarista Laura Poitras, que dizia: "Alguma chance de você estar nos Estados Unidos nesta próxima semana? Adoraria trocar umas ideias sobre um assunto, mas seria melhor pessoalmente."

Eu levo a sério qualquer mensagem de Laura Poitras. Uma das pessoas mais focadas, destemidas e independentes que já conheci, ela fez vários filmes em circunstâncias arriscadíssimas, sem equipe nem apoio de qualquer organização de mídia, com orçamentos modestos, munida apenas de uma câmera e da própria determinação. No auge da pior onda de violência da Guerra do Iraque, aventurou-se no Triângulo Sunita para filmar *My Country, My Country* (Meu país, meu país), um retrato inflexível da vida sob a ocupação norte-americana que tinha sido indicado ao Oscar.

Para seu filme seguinte, *e Oath* (O juramento), Poitras foi até o Iêmen, onde passou meses acompanhando dois iemenitas – o guarda-costas de Osama bin Laden e seu motorista. Desde então, vem trabalhando em um documentário sobre a vigilância da NSA. Esses três filmes, pensados como uma trilogia sobre a conduta norte-americana durante a Guerra ao Terror, tornaram-na um alvo constante de intimidação por parte das autoridades dos Estados Unidos toda vez que ela entrava no país ou saía dele.

Graças a Laura, aprendi uma valiosa lição. Em 2010, quando nos conhecemos, ela já havia sido detida em aeroportos mais de trinta vezes pelo Departamento de Segurança Interna ao chegar ao país; fora interrogada, ameaçada e tivera seu material apreendido, inclusive seu laptop, sua câmera e seus cadernos de anotações. Mesmo assim, em todas as ocasiões decidira não ir a público denunciar esse

assédio implacável por temer que as repercussões tornassem seu trabalho impossível. Isso mudou após um interrogatório particularmente agressivo no aeroporto de Newark. Laura havia chegado ao seu limite. "O fato de eu ficar calada está fazendo a situação piorar, não melhorar." Ela estava pronta para que eu escrevesse a respeito.

A matéria que publiquei na revista on-line *Salon*, com detalhes sobre os constantes interrogatórios aos quais ela fora submetida, atraiu atenção significativa e produziu declarações de apoio e denúncias de intimidação. Na vez seguinte em que Laura saiu do país e retornou de avião após a publicação do texto, não houve interrogatório e seu material não foi confiscado. Ao longo dos meses seguintes, ela não sofreu qualquer assédio. Pela primeira vez em anos, pôde viajar livremente.

A lição para mim foi clara: os agentes de segurança nacional não gostam de ser expostos. Só agem de forma abusiva e truculenta quando acreditam estar seguros, escondidos. Descobrimos que o sigilo é a chave do abuso de poder, a força que o possibilita. O único antídoto verdadeiro é a transparência.

Ao ler o e-mail de Laura no aeroporto, respondi na mesma hora: "Na verdade, acabei de chegar aos Estados Unidos hoje de manhã... Onde você está?" Combinamos nos encontrar no dia seguinte, no lobby do Marriott em Yonkers no qual eu estava hospedado, e nos acomodamos no restaurante do hotel. Por insistência de Laura, mudamos de mesa duas vezes antes de começar a conversa, para ter certeza de que ninguém poderia nos escutar. Ela foi bem direta. Disse que tinha "um assunto extremamente importante e delicado" a discutir e que a segurança era fundamental.

Como eu estava com meu celular, ela me pediu para tirar a bateria ou então deixá-lo no quarto. "Parece paranoia", falou, mas o governo consegue ativar celulares e laptops remotamente para usá-los como escutas. Desligar o telefone ou o laptop não impede essa utilização: apenas a remoção da bateria a evita. Eu já tinha escutado a mesma coisa de ativistas defensores da transparência e de hackers, mas minha tendência era considerar aquilo uma cautela excessiva. Dessa vez, porém, por se tratar de Laura, levei a sério. Depois de constatar que a bateria do meu celular não saía, levei o aparelho para o quarto e voltei ao restaurante.

Só nesse momento Laura começou a falar. Tinha recebido uma série de e-mails anônimos de um indivíduo que parecia honesto e sério. Ele alegava ter acesso a documentos ultrassecretos e incriminadores sobre a espionagem dos próprios cidadãos e do resto do mundo conduzida pelo governo norte-americano. Estava decidido a fazer vazar o conteúdo desses documentos, e lhe pedira especificamente que trabalhasse comigo na liberação e divulgação desse material. Não liguei isso a nenhum dos e-mails já esquecidos que recebera de Cincinnatus meses antes. Eles estavam armazenados no fundo da minha mente, fora do meu campo de visão.

Laura, então, tirou da bolsa várias folhas de papel, parte de dois dos e-mails enviados pelo delator anônimo, e eu as li ali mesmo, à mesa, de cabo a rabo. Eram fascinantes.

O segundo desses e-mails, enviado semanas depois do primeiro, começava tranquilizando-a: "Ainda estou aqui." Em relação à dúvida que mais atormentava Laura – quando ele estaria pronto para fornecer os documentos –, ele dizia: "Tudo o que posso responder é: em breve."

Depois de instruí-la a sempre remover a bateria do celular antes de falar sobre assuntos delicados – ou pelo menos a colocar o aparelho no congelador, o que o impediria de funcionar como escuta –, o delator dizia a Laura que ela deveria trabalhar comigo nos tais documentos. E então chegava ao cerne

daquilo que considerava sua missão:

> O choque desse período inicial [após a primeira revelação] irá proporcionar o apoio necessário à construção de uma internet mais igualitária, mas isso só vai funcionar para o indivíduo comum se a ciência for mais rápida que a legislação.
>
> Ao entender os mecanismos pelos quais nossa privacidade é violada, conseguiremos vencer. Por meio de leis universais, poderemos garantir a todos a mesma proteção contra buscas indiscriminadas, mas só se a comunidade tecnológica estiver disposta a encarar essa ameaça e a se comprometer com a implementação de soluções mais sofisticadas. Por fim, precisamos aplicar um princípio segundo o qual a única forma de os poderosos terem privacidade será quando ela for do mesmo tipo compartilhado pelo homem comum: aquela garantida pelas leis da natureza, não pelas políticas humanas.

– Esse cara está falando sério – comentei, ao terminar a leitura. – Não sei explicar por quê, mas minha intuição me diz que isso é importante, que ele é exatamente quem diz ser.

– Também acho – disse Laura. – Não tenho quase nenhuma dúvida.

De um ponto de vista sensato e racional, nós dois sabíamos que a nossa fé na veracidade do delator poderia estar equivocada. Não tínhamos a menor ideia de quem estava escrevendo para ela. Poderia ser qualquer um. Ele poderia estar inventando a história toda. Aquilo podia também ser algum tipo de complô montado pelo governo para nos enganar e nos fazer colaborar com um vazamento criminoso. Ou talvez a mensagem tivesse sido mandada por alguém com a intenção de prejudicar nossa credibilidade transmitindo documentos fraudulentos para publicação.

Debatemos todas essas possibilidades. Sabíamos que, em 2008, um relatório secreto do exército norte-americano havia declarado o WikiLeaks inimigo de Estado e sugerido maneiras de causar "danos e a potencial destruição" da organização. O relatório (vazado, por ironia, pelo próprio WikiLeaks) discutia a possibilidade de fazer circular documentos falsos. Se o WikiLeaks os publicasse como autênticos, sua confiabilidade sofreria um sério revés.

Laura e eu conhecíamos todas as armadilhas, mas as ignoramos e resolvemos confiar na nossa intuição. Algo intangível, mas poderoso, naqueles e-mails nos convenceu de que seu autor era legítimo. Ele escrevia por acreditar de fato nos perigos do sigilo e da espionagem generalizada praticados pelo governo; reconheci instintivamente sua paixão política. Senti uma identificação com aquele correspondente, com sua visão de mundo e com a sensação de urgência que sem dúvida o consumia.

Ao longo dos últimos sete anos, movido pela mesma convicção, escrevi quase todos os dias sobre a perigosa tendência do sigilo de Estado nos Estados Unidos, sobre as teorias de poder executivo radical, os abusos na detenção e na vigilância, o militarismo e a violação das liberdades civis. Existe um tom específico que une jornalistas, ativistas e meus leitores, todos alarmados na mesma medida por essas tendências. Seria difícil para alguém que não acreditasse naquele alarme e não o sentisse de verdade, ponderei, reproduzi-lo de forma tão exata, com tamanha autenticidade.

Em um dos últimos trechos dos e-mails que Laura me mostrou, o remetente dizia que estava concluindo os últimos passos necessários para nos encaminhar os documentos. Precisava de mais quatro a seis semanas, e nós deveríamos aguardar notícias. Ele nos garantiu que entraria em contato.

Três dias depois, Laura e eu tornamos a nos encontrar, dessa vez em Manhattan, e com outro e-mail do delator anônimo nas mãos, no qual ele explicava por que estava disposto a arriscar a própria liberdade, a enfrentar a alta probabilidade de uma longa sentença de prisão para divulgar aqueles documentos. Então fiquei ainda mais convencido: nossa fonte estava falando sério. No entanto, como disse a meu companheiro, David Miranda, durante nosso voo de volta para o Brasil, resolvi tirar aquela história da cabeça.

– Pode ser que não aconteça. Ele pode mudar de ideia. Pode ser pego.

Dono de uma poderosa intuição, David se mostrou estranhamente seguro.

– É tudo verdade. Ele existe. Isso vai acontecer – afirmou. – E vai ser uma bomba.

De volta ao Rio, passei três semanas sem notícias. Quase não pensei na história da fonte, porque tudo o que podia fazer era esperar. Então, em 11 de maio, recebi o e-mail de um especialista em tecnologia com quem Laura e eu já havíamos trabalhado. Apesar das palavras cifradas, o significado de sua mensagem foi claro: "Oi, Glenn, estou escrevendo para continuar a lhe ensinar a usar o PGP. Você tem um endereço de e-mail para onde eu possa enviar uma coisa que o ajude a começar na semana que vem?"

Tive certeza de que aquela "coisa" a que ele se referia era o que eu precisava para começar a trabalhar nos documentos do delator. Isso, por sua vez, significava que Laura tinha sido contatada por nosso remetente anônimo e recebido o que aguardávamos.

Então o especialista em tecnologia me mandou uma encomenda pela Federal Express, agendada para ser entregue dali a dois dias. Eu não sabia o que esperar: um programa, os documentos em si? Passei 48 horas sem conseguir me concentrar em mais nada. No dia marcado para a entrega, porém, nada tinha aparecido até as cinco e meia da tarde. Liguei para a FedEx e fui informado de que a encomenda estava retida na alfândega por "motivos desconhecidos". Dois dias se passaram. Depois, cinco. Em seguida, uma semana inteira. A empresa sempre dizia a mesma coisa: que a encomenda estava retida na alfândega por motivos desconhecidos.

Passou-me pela cabeça que alguma autoridade do governo – americano, brasileiro ou outro qualquer – estivesse por trás daquele atraso por saber alguma coisa, mas me aferrei à explicação bem mais provável de que aquilo era apenas uma daquelas chateações burocráticas, uma mera coincidência.

Àquela altura, Laura já não queria mais conversar sobre o assunto por telefone nem pela internet, de modo que eu não sabia exatamente o que o pacote continha.

Por fim, cerca de dez dias após ter sido expedida, a encomenda me foi entregue pela FedEx. Rasguei o envelope e encontrei dois pen drives USB acompanhados de um bilhete datilografado com instruções detalhadas sobre como usar diversos programas de computador destinados a proporcionar segurança máxima, além de várias frases de acesso a contas de e-mail criptografadas e outros programas dos quais eu jamais ouvira falar.

Não fazia a menor ideia do que significava tudo aquilo. Nunca tinha ouvido falar naqueles programas específicos, embora conhecesse o termo "frases de acesso": basicamente, eram senhas compridas, formadas de maneira aleatória por letras tanto em caixa alta quanto em caixa baixa e sinais de pontuação, com o objetivo de torná-las difíceis de decifrar. Como Laura estava relutando muito em falar por telefone ou pela internet, continuei frustrado: enfim recebera o que estava

esperando, mas não tinha como saber aonde aquilo iria me levar.

Estava prestes a descobrir, com o melhor guia possível.

No dia seguinte à chegada da encomenda, na semana de 20 de maio, Laura me disse que precisávamos conversar com urgência, mas só por chat OTR, um instrumento de criptografia que possibilita conversas seguras on-line. Eu já tinha usado o OTR, e consegui instalar, pelo Google, o programa de chat; criei uma conta e adicionei o nome de Laura à minha lista de contatos. Ela apareceu na hora.

Eu quis saber se teria acesso aos documentos secretos. Eles viriam da fonte, respondeu Laura, não dela. Então acrescentou uma informação surpreendente: talvez tivéssemos de ir a Hong Kong de imediato para encontrar nossa fonte.

Fiquei pasmo. O que alguém com acesso a documentos ultrassecretos do governo norte-americano estava fazendo em Hong Kong? Tinha imaginado que nossa fonte anônima fosse estar em Maryland ou na parte norte da Virgínia. O que Hong Kong tinha a ver com aquilo? É claro que eu estava disposto a viajar para qualquer lugar; só queria mais informações sobre por que precisava ir até lá. Mas o fato de Laura não poder falar livremente nos forçou a adiar essa conversa. Ela me perguntou se eu estaria disposto a ir até Hong Kong nos próximos dias. Eu queria ter certeza de que aquilo valeria a pena, ou seja, se ela tinha conseguido alguma prova concreta de que aquela fonte era real. Ela retrucou de forma cifrada: "É claro que sim, caso contrário não pediria a você que fosse a Hong Kong." Imaginei que isso significasse que ela havia recebido alguns documentos sérios da fonte.

Mas Laura também me falou sobre um problema em potencial. A fonte estava chateada com o andamento das coisas até ali, sobretudo com um fato novo: o possível envolvimento do jornal *The Washington Post*. Segundo Laura, era fundamental que eu conversasse diretamente com a fonte, para tranquilizá-la e apaziguar suas preocupações crescentes.

Em menos de uma hora, a própria fonte me mandou um e-mail.

O remetente era Verax@ INFORMAÇÃO OMITIDA . "Verax", em latim, significa "aquele que diz a verdade". A mensagem dizia: "Precisamos conversar".

"Estou trabalhando em um projeto importante com uma amiga que temos em comum", começava a mensagem, informando-me ser mesmo ele a fonte anônima, em uma clara referência a seus contatos com Laura.

"Há pouco tempo, o senhor teve de recusar uma viagem curta para se encontrar comigo. Mas o senhor precisa estar envolvido diretamente nesta história", escreveu ele. "Existe alguma forma de conversarmos logo? Sei que o senhor não dispõe de muita infraestrutura em termos de segurança, mas posso me virar com o que tiver." Ele sugeriu que falássemos pelo OTR, e informou seu nome de usuário.

Não entendi muito bem o que ele quis dizer com "recusar uma viagem curta": eu havia expressado certa incompreensão em relação ao fato de ele estar em Hong Kong, mas de forma alguma tinha me recusado a viajar. Atribuí isso a uma falha de comunicação e respondi na mesma hora: "Eu quero fazer o que for possível para me envolver nisso", escrevi, sugerindo que nos falássemos no mesmo instante pelo OTR. Adicionei o nome dele à minha lista de contatos e aguardei.

Quinze minutos depois, meu computador emitiu um alerta parecido com um sino, mostrando que a fonte havia se conectado. Um pouco nervoso, cliquei no nome dele e digitei "oi". Ele respondeu, e me peguei conversando diretamente com um indivíduo que àquela altura, segundo entendi, revelara

diversos documentos secretos sobre programas norte-americanos de vigilância e queria revelar ainda mais.

Já de saída, disse-lhe que meu comprometimento com aquela reportagem era total. "Estou disposto a fazer o que for preciso para dar essa notícia", escrevi. A fonte – cujo nome, local de trabalho, idade e todas as outras características eu ainda desconhecia – perguntou se eu poderia ir encontrá-lo em Hong Kong. Não perguntei por que ele estava lá; não quis dar a impressão de estar tentando lhe arrancar informações.

De fato, desde o início decidi que o deixaria tomar a iniciativa. Se ele quisesse que eu soubesse por que estava em Hong Kong, me diria. Se quisesse que eu soubesse que documentos tinha e quais planejava me entregar, também me diria. Essa postura passiva foi difícil para mim. Como ex-advogado de contencioso e atual jornalista, estou acostumado a questionar de maneira veemente quando quero respostas, e tinha centenas de perguntas que desejava fazer.

No entanto, parti do princípio de que a situação dele era delicada. Fossem quais fossem as outras circunstâncias, sabia que aquela pessoa decidira fazer algo que o governo dos Estados Unidos consideraria um crime muito sério. Por sua preocupação com a segurança da nossa comunicação, estava claro que discrição era fundamental. Além do mais, como eu tinha muito poucas informações sobre a pessoa com quem estava conversando – como pensava, quais eram suas motivações e seus temores –, cautela e restrição eram imperativas para mim. Eu não queria afugentá-lo. Assim, forcei-me a deixar a informação chegar a mim em vez de tentar agarrá-la.

"É claro que posso ir a Hong Kong", digitei, ainda sem ter a menor ideia de por que ele estava lá, dentre todos os lugares possíveis, ou por que desejava que eu fosse encontrá-lo.

Passamos duas horas no chat nesse dia. Sua principal preocupação era o que estava acontecendo com o que Laura, com o consentimento dele, tinha dito a respeito de alguns documentos da NSA a um jornalista do *Washington Post* chamado Barton Gellman. Os documentos se referiam a uma reportagem específica sobre um programa chamado PRISM, que permitia à NSA coletar comunicações pessoais das maiores empresas de internet do mundo, entre as quais Facebook, Google, Yahoo! e Skype. Em vez de publicar a matéria de forma rápida e agressiva, o *Post* convocara uma grande equipe de advogados, que estava fazendo todo tipo de exigência e emitindo toda a sorte de alerta severo. Para a fonte, isso mostrava que, diante do que ele considerava uma oportunidade jornalística sem precedentes, o periódico estava se deixando levar não pela convicção ou pela determinação, mas pelo medo. Ele também estava furioso com o fato de o *Post* ter envolvido tantas pessoas, e temia que essas conversas pudessem ameaçar sua segurança.

"Não gosto do rumo que isto está tomando", disse-me ele. "Eu queria que outra pessoa trabalhasse na reportagem sobre o PRISM, de modo que o senhor pudesse se concentrar no arquivo maior, sobretudo naquele sobre a espionagem doméstica em massa, mas agora prefiro realmente que seja o senhor a publicar essa matéria. Há muito tempo venho lendo o que escreve, e sei que vai ser agressivo e destemido na condução deste assunto", afirmou.

"Estou pronto e animado", escrevi para ele. "Vamos decidir agora o que preciso fazer."

"A primeira coisa da lista é vir até Hong Kong", instruiu-me. Ele não parava de bater nessa tecla: *venha a Hong Kong o mais rápido possível.*

O outro tópico importante que discutimos nessa primeira conversa pela internet foram os seus objetivos. Pelos e-mails que Laura havia me mostrado, eu sabia de sua propensão para revelar ao

mundo o imenso aparato de espionagem que o governo norte-americano estava montando em segredo. Mas o que ele esperava conseguir?

"Quero iniciar um debate mundial sobre privacidade, liberdade na internet e os perigos da vigilância estatal", esclareceu ele. "Não tenho medo do que vai acontecer comigo. Já aceitei que a minha vida provavelmente vai terminar se eu fizer isso. Estou em paz. Sei que é a coisa certa a fazer."

Ele então disse algo surpreendente: "Quero me identificar como o responsável por essas revelações. Acredito que tenho a obrigação de explicar por que estou agindo assim e o que espero conseguir." Ele me contou que havia preparado um documento que desejava postar na internet quando se revelasse como a fonte, um manifesto pró-privacidade e antivigilância a ser assinado por pessoas do mundo todo, para mostrar que o apoio à proteção da privacidade era mundial.

Apesar do custo quase certo de se revelar – uma longa sentença de prisão, no melhor dos casos –, a fonte afirmou várias vezes que estava "em paz" com essas consequências. "Meu único medo é que as pessoas vejam esses documentos, deem de ombros e digam: 'Já imaginávamos que isso estivesse acontecendo, e não estamos nem aí.' A única coisa que me preocupa é fazer isso a troco de nada."

"Duvido muito que isso vá acontecer", ponderei, embora não estivesse tão convicto disso. Depois de tantos anos escrevendo sobre os abusos da NSA, tinha consciência de que pode ser difícil gerar uma preocupação séria em relação à vigilância secreta do governo: invasão de privacidade e abuso de poder podem ser vistos como abstrações, coisas com as quais é difícil fazer as pessoas se importarem de forma visceral. Além do mais, a questão da vigilância é invariavelmente complexa, o que dificulta ainda mais um envolvimento abrangente da população.

Mas aquilo parecia diferente. Um vazamento de documentos ultrassecretos atrai a atenção da mídia. O fato de o alerta vir de alguém de dentro do aparato de segurança nacional – e não de um advogado da ACLU (União Norte-Americana pelas Liberdades Civis) ou de algum outro defensor das liberdades civis – com certeza lhe conferiria mais importância ainda.

Nessa noite, conversei com David sobre ir a Hong Kong. Ainda relutava em largar todo o meu trabalho para voar até o outro lado do mundo ao encontro de alguém sobre quem nada sabia – nem sequer o nome –, especialmente sem ter nenhuma prova concreta de que ele era mesmo quem dizia ser. Aquilo poderia ser uma total perda de tempo – ou ainda uma armadilha, ou algum outro complô bizarro.

– Você deveria dizer a ele que quer ver alguns documentos primeiro, para saber que ele está falando sério e que isso vale a pena para você – sugeriu David.

Como de hábito, segui seu conselho. Ao me logar no OTR na manhã seguinte, falei que planejava viajar para Hong Kong dali a poucos dias, mas que primeiro queria ver alguns documentos, para entender o tipo de revelação que ele estava disposto a fazer.

Para atender ao meu pedido, ele mais uma vez me disse para instalar diversos programas. Em seguida, passei mais alguns dias on-line enquanto a fonte me guiava pelo passo a passo da instalação e do uso de cada um deles, incluindo, enfim, a criptografia PGP. Sabendo que eu era iniciante, ele demonstrou grande paciência, literalmente a ponto de dar instruções do tipo "Clique no botão azul, agora dê OK, agora passe para a tela seguinte".

Eu não parava de me desculpar por minha falta de conhecimento, por ele ter de gastar horas do seu tempo me ensinando os aspectos mais básicos da comunicação segura. "Não tem problema nenhum", afirmou. "A maioria dessas coisas é difícil de entender mesmo. E eu estou com muito

tempo livre no momento."

Quando todos os programas estavam instalados, recebi um arquivo com mais ou menos 25 documentos. "Isso é só uma provinha: a ponta do iceberg", explicou ele, de forma provocativa.

Descompactei o arquivo, olhei a lista de itens e cliquei em um qualquer. No alto da página, em letras vermelhas, apareceu um código: "TOP SECRET//COMINT/NOFORN/".

Isso significava que o documento tinha sido oficialmente considerado ultrassecreto (*top secret*), que estava relacionado à inteligência de comunicações (*communications intelligence,* COMINT) e que não deveria ser distribuído para cidadãos estrangeiros, nem mesmo para organizações internacionais ou parceiros de coalizão (*no foreign nationals*, NOFORN). Ali estava, com uma clareza incontestável: uma comunicação altamente confidencial da NSA, uma das agências mais sigilosas do governo mais poderoso do mundo. Nada com aquele grau de importância jamais tinha vazado da NSA durante as seis décadas de história da agência. Eu agora tinha nas mãos mais de vinte documentos desse tipo. E a pessoa com quem havia passado horas conversando no chat nos últimos dois dias tinha muitos, muitos outros para me entregar.

Esse primeiro documento era um manual de treinamento para agentes da NSA destinado a ensinar aos analistas novas técnicas de vigilância. Discorria, em termos genéricos, sobre o tipo de informação que os analistas podiam solicitar (endereços de e-mail, dados de localização do IP, números de telefone) e o tipo de dados que receberiam de volta (conteúdo dos e-mails, "metadados" telefônicos, logs de chat). Basicamente, eu estava espionando as instruções dos agentes da NSA a seus analistas sobre como vigiar seus alvos.

Meu coração disparou. Tive que parar de ler e circular pela casa algumas vezes para absorver o que acabara de ver e me acalmar o suficiente para conseguir me concentrar na leitura dos arquivos. Voltei ao laptop e cliquei de forma aleatória em mais um documento, uma apresentação de PowerPoint ultrassecreta intitulada "PRISM/US-984XN Overview" (*overview* significa "visão geral"). Todas as páginas traziam os logotipos de nove das maiores empresas de internet do mundo, incluindo Google, Facebook, Skype e Yahoo!.

O primeiro slide explicava um programa graças ao qual a NSA obtinha o que chamava de "coleta direta dos servidores dos seguintes provedores de serviço norte-americanos: Microso , Yahoo!, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple". Um gráfico indicava as datas nas quais cada uma dessas empresas havia entrado no programa.

Mais uma vez, fiquei tão empolgado que tive de interromper a leitura.

A fonte disse também que iria me enviar um arquivo grande que eu não conseguiria acessar até o momento certo. Decidi, por ora, deixar passar essas afirmações cifradas, embora significativas, sempre de acordo com minha postura de permitir que ele decidisse quando me passar as informações, mas também por estar tão entusiasmado com o que via.

Pela primeira olhada que dei apenas nesses poucos documentos, entendi duas coisas: tinha de ir a Hong Kong quanto antes, e precisaria de um respaldo institucional significativo para dar aquela notícia. Isso queria dizer envolver o *Guardian*, o jornal e site de notícias para o qual começara a trabalhar como colunista diário apenas nove meses antes. Eu agora estava prestes a fazê-los embarcar no que já sabia que seria uma reportagem importante e explosiva.

Pelo Skype, liguei para Janine Gibson, editora-chefe britânica da edição norte-americana do jornal. Meu acordo com a empresa era que eu tinha independência editorial completa, ou seja,

ninguém podia editar, nem mesmo revisar, minhas matérias antes da publicação. Eu escrevia meus textos e os publicava direto na internet. A única exceção a esse acordo é que eu deveria avisá-los quando a matéria pudesse ter implicações jurídicas para o jornal ou apresentar um dilema jornalístico extraordinário. Como isso havia acontecido muito poucas vezes nos últimos nove meses, uma ou duas, no máximo, eu tivera pouquíssima interação com os editores do periódico.

Naturalmente, se havia uma reportagem que merecia esse aviso, era aquela. Além do mais, eu sabia que precisaria dos recursos e do apoio do jornal.

– Janine, estou com um furo incrível nas mãos – comecei, sem rodeios. – Tenho uma fonte com acesso ao que parece ser uma quantidade enorme de documentos ultrassecretos da NSA. Ele já me passou alguns, e são bombásticos. Mas ele diz que tem muitos, muitos outros. O que já me mandou e eu acabei de ver tem algumas informações bem chocantes sobre...

– Como você me ligou? – interrompeu ela.

– Pelo Skype.

– Não acho que devamos falar sobre isso pelo telefone, e com certeza não pelo Skype – disse ela, com sensatez, e propôs que eu pegasse um avião para Nova York o mais rápido possível para podermos conversar pessoalmente sobre a reportagem.

Meu plano, que eu comuniquei a Laura, era voar até Nova York, mostrar os documentos ao *Guardian*, deixá-los empolgados com a reportagem e então fazer com que me mandassem a Hong Kong. Laura topou me encontrar em Nova York, e de lá planejávamos ir juntos para a Ásia.

No dia seguinte, peguei um voo noturno do Rio de Janeiro para o JFK, e às nove horas da manhã do outro dia, sexta-feira, 31 de maio, já tinha feito o check-in no meu hotel em Manhattan e encontrado Laura. Nossa primeira providência foi ir a uma loja e comprar um laptop que me serviria de *air gap*, ou "brecha de ar": um computador que nunca se conecta à internet. É muito mais difícil submeter a vigilância um equipamento que não acessa a rede. Para monitorar um *air gap*, um serviço de inteligência como a NSA teria de utilizar métodos bem mais complexos, tais como obter acesso físico à máquina e instalar um mecanismo de vigilância no disco rígido. Manter o computador consigo em todos os momentos impede esse tipo de invasão. Eu usaria esse laptop novo para trabalhar com todo o material que não quisesse que fosse monitorado, como os documentos secretos da NSA, sem medo de ser detectado.

Enfiei o computador recém-comprado na mochila e percorri a pé com Laura os cinco quarteirões de Manhattan até a redação do *Guardian*, no Soho.

Gibson estava à nossa espera. Ela e eu fomos direto para a sua sala, onde Stuart Millar, seu subeditor, se juntou a nós. Laura ficou esperando do lado de fora: Gibson não a conhecia, e eu queria que falássemos à vontade. Não fazia a menor ideia de como os editores do periódico iriam reagir ao que eu tinha nas mãos, se ficariam com medo ou empolgados. Nunca havia trabalhado com eles antes, e com certeza em nada que sequer se aproximasse daquele nível de gravidade e importância.

Quando abri no laptop os arquivos da fonte, Gibson e Millar se sentaram lado a lado diante de uma mesa para lê-los, murmurando de vez em quando coisas como "Nossa!", "Puta que pariu!" e outras expressões do gênero. Sentado em um sofá e observando-os, vi uma expressão de choque se estampar em seus rostos quando começaram a entender a realidade do que eu tinha nas mãos. Toda vez que terminavam um documento, eu me levantava para abrir o seguinte. Seu espanto só fazia aumentar.

Além dos mais de vinte documentos da NSA, a fonte incluíra também o manifesto que pretendia postar, pedindo assinaturas como demonstração de solidariedade à causa pró-privacidade e antivigilância. O texto era dramático, severo, o que era de esperar, considerando as escolhas dramáticas e severas que ele tinha feito e que iriam influenciar sua vida para sempre. Para mim, fazia sentido alguém que houvesse testemunhado a construção obscura de um sistema generalizado de vigilância estatal, sem qualquer supervisão ou limite, ficar seriamente alarmado com o que vira e com os perigos que isso representava. É claro que o tom dele era exaltado; de tão alarmado, ele tomara a decisão extraordinária de cometer um ato corajoso e extremo. Eu entendia o motivo daquele tom, mas fiquei preocupado com a forma como Gibson e Millar reagiriam à leitura do texto. Não queria que eles pensassem que estávamos lidando com alguém instável, sobretudo porque, depois de passar muitas horas conversando com ele, eu sabia que se tratava de um homem excepcionalmente racional e ponderado.

Meu receio logo se confirmou.

– Tem gente que vai achar isso maluquice – falou Gibson.

– É verdade que algumas pessoas e alguns jornalistas favoráveis à NSA vão dizer que ele tem um quê de Unabomber – concordei. – Mas, em última instância, o que importa são os documentos, não ele nem as motivações que o levaram a nos entregar o material. E qualquer um que faça algo extremo assim tem opiniões extremas. É inevitável.

Além do manifesto, Snowden tinha escrito uma carta aos jornalistas para quem entregara aquele acervo de documentos. O texto tentava explicar sua motivação e seus objetivos, e previa como ele provavelmente seria demonizado:

> Minha única motivação é informar o público sobre o que está sendo feito em seu nome e contra ele. O governo dos Estados Unidos, principal membro dos Cinco Olhos – compostos, ainda, de Reino Unido, Canadá, Austrália e Nova Zelândia –, em conspiração com países clientes, impôs ao mundo um sistema de vigilância secreta e abrangente do qual não há como se esconder. Eles protegem seus sistemas domésticos da supervisão da população por meio da confidencialidade e da mentira, e se resguardam da indignação em caso de vazamento supervalorizando as proteções limitadas que decidem conceder aos governados...
>
> Os documentos anexos são genuínos e originais, e estão sendo oferecidos para permitir a compreensão de como funciona o sistema de vigilância global passivo, a fim de que proteções contra ele possam ser desenvolvidas. No dia em que escrevo este texto, a intenção deles é que todos os novos registros de comunicações passíveis de ser absorvidos e catalogados por esse sistema sejam guardados por anos, e novos "repositórios de dados maciços" (ou, eufemisticamente falando, "repositórios de dados de 'missões') estão sendo construídos e espalhados pelo mundo, sendo o maior deles o novo centro de dados situado em Utah. Embora eu torça para que a conscientização e o debate público conduzam a uma reforma, lembrem que as políticas dos homens mudam com o tempo, e que mesmo a Constituição é subvertida quando o apetite pelo poder exige. Em termos tirados da história: não vamos mais falar na fé nos homens, e sim impedir que eles se comportem mal pelas correntes da criptografia.

No mesmo instante, reconheci a última frase como um trocadilho referente a uma fala de omas

Jefferson de 1798 que com frequência cito em meus textos: "Quando se trata de poder, portanto, não vamos mais falar sobre a confiança nos homens, e sim impedir que eles se comportem mal pelas correntes da Constituição."

Depois de reler todos os documentos, inclusive a carta de Snowden, Gibson e Millar ficaram convencidos.

– Basicamente, você tem que ir a Hong Kong o mais rápido possível, tipo amanhã, certo? – concluiu Gibson menos de duas horas após minha chegada.

O *Guardian* estava dentro. Minha missão em Nova York fora cumprida. Eu agora sabia que Gibson estava comprometida com uma cobertura agressiva daquela reportagem, pelo menos por ora. Nessa tarde, Laura e eu entramos em contato com a agência de viagens do jornal para chegar a Hong Kong o mais depressa possível. A melhor opção era um voo de dezesseis horas da Cathay Pacific que saía do JFK na manhã seguinte. No entanto, assim que começamos a comemorar nosso encontro iminente com a fonte, esbarramos em um obstáculo.

No final do dia, Gibson disse que queria incluir na operação um jornalista veterano do *Guardian* chamado Ewen MacAskill, que trabalhava no jornal havia duas décadas.

– Ele é um ótimo jornalista – afirmou. Considerando a magnitude daquilo em que estava embarcando, eu sabia que precisaria de outros repórteres do *Guardian* para apurar a matéria, e em teoria não tinha objeções. – Eu gostaria que Ewen fosse a Hong Kong com vocês – acrescentou ela.

Eu não conhecia MacAskill. Mais importante ainda: a fonte não o conhecia, e, até onde ele sabia, apenas Laura e eu iríamos a Hong Kong. E era provável que Laura, que sempre planeja tudo com meticulosidade, também fosse ficar furiosa com essa súbita mudança de planos.

Eu tinha razão.

– De jeito nenhum. Não mesmo – exclamou ela. – Não podemos simplesmente incluir outra pessoa na última hora. E eu não conheço o cara. Quem verificou os antecedentes dele?

Tentei explicar qual pensava ser a motivação de Gibson. Eu ainda não conhecia nem confiava no *Guardian*, não em se tratando de uma reportagem daquela magnitude, e imaginava que eles sentissem o mesmo em relação a mim. Levando em conta o risco que o jornal estava assumindo, calculei que sem dúvida eles queriam alguém que conhecessem muito bem – um veterano da empresa – para lhes informar o que estava acontecendo com a fonte e lhes garantir que aquela reportagem era algo que devessem publicar. Além do mais, Gibson precisaria de total apoio e aprovação dos editores do jornal em Londres, que me conheciam ainda menos do que ela. Ela com certeza queria incluir alguém capaz de dar segurança a eles, e Ewen se encaixava à perfeição nesse perfil.

– Não quero nem saber – disse Laura. – Viajar com uma terceira pessoa, um desconhecido, pode atrair vigilância ou afugentar a fonte. – Como um meio-termo, ela sugeriu que mandassem Ewen alguns dias depois, quando já tivéssemos estabelecido contato com a fonte em Hong Kong e criado confiança. – É você quem está dando as cartas. Diga que eles só podem mandá-lo quando dermos o ok.

Voltei a Gibson com o que parecia um meio-termo sensato, mas ela parecia decidida:

– Ewen pode viajar com vocês até Hong Kong, mas não encontrar a fonte até você e Laura darem o ok.

Estava claro que a ida dele a Hong Kong conosco era vital para o *Guardian*. Gibson precisaria de garantias em relação ao que estivesse acontecendo lá, e de uma forma de apaziguar quaisquer

preocupações de seus superiores em Londres. Mas Laura estava igualmente decidida a irmos sozinhos.

– Se a fonte estiver nos vigiando no aeroporto e vir essa terceira pessoa inesperada, que ele não conhece, vai surtar e interromper o contato. De jeito nenhum.

Como um diplomata do Departamento de Estado fazendo a ponte entre dois adversários do Oriente Médio na fútil esperança de conseguir um acordo, voltei a falar com Gibson, que respondeu de maneira evasiva dando a entender que Ewen viajaria alguns dias depois. Ou talvez tenha sido isso que eu quis escutar.

De toda forma, a agência de viagens me avisou, já tarde nessa noite, que a passagem de Ewen estava comprada – para o dia seguinte, no mesmo voo que nós. E que eles iriam mandá-lo nesse avião custasse o que custasse.

Na manhã seguinte, no carro a caminho do aeroporto, Laura e eu tivemos nossa primeira e única briga. Assim que o automóvel se afastou do hotel, dei-lhe a notícia de que no fim das contas Ewen viajaria conosco, e ela reagiu com um acesso de raiva. Insistiu que eu estava pondo em risco a operação toda. Não era sensato incluir um desconhecido naquele estágio avançado. Ela não confiava em alguém que não tinha sido aprovado para trabalhar em algo tão delicado, e me culpou por ter deixado o *Guardian* pôr nosso plano em perigo.

Eu não podia dizer a Laura que as suas preocupações eram infundadas, mas tentei convencê-la de que o jornal havia insistido e não tínhamos escolha. Além disso, Ewen só encontraria a fonte quando nós deixássemos.

Ela não gostou. Para aplacar sua raiva, eu até sugeri não ir, ideia que ela descartou no mesmo instante. Passamos dez minutos calados, frustrados e furiosos, enquanto o carro ficava parado em um engarrafamento a caminho do aeroporto.

Eu sabia que Laura estava certa: as coisas não deveriam ter acontecido daquela forma, e rompi o silêncio lhe dizendo isso. Então propus que ignorássemos Ewen e lhe déssemos um gelo, fazendo de conta que ele não estava conosco.

– Não vamos brigar, nós estamos do mesmo lado – pedi. – Considerando o que está em jogo, esta não vai ser a última vez que as coisas fugirão ao nosso controle.

Tentei convencê-la de que deveríamos focar em trabalhar juntos para superar os obstáculos. Em pouco tempo, nos acalmamos.

Quando chegamos perto do aeroporto, Laura tirou um pen drive da mochila.

– Adivinhe o que tem aqui – falou, com um olhar muito sério.

– O quê?

– Os documentos – respondeu ela. – Todos.

Quando chegamos ao portão de embarque, Ewen já estava lá. Laura e eu fomos cordiais, mas frios, garantindo que ele se sentisse excluído, que soubesse que não teria participação alguma até decidirmos que isso iria acontecer. Ele era o único alvo de nossa irritação no momento, logo nós o tratamos como uma bagagem extra que tínhamos sido obrigados a levar. Foi injusto, mas eu estava ansioso demais pensando nos tesouros do pen drive de Laura e na importância do que estávamos fazendo para me importar com Ewen.

No carro, Laura tinha me dado uma aula rápida sobre o sistema operacional seguro e avisado que pretendia dormir no avião. Entregou-me o pen drive e sugeriu que eu começasse a olhar os

documentos. Quando chegássemos a Hong Kong, falou, a fonte iria garantir que eu tivesse acesso a uma cópia completa.

Assim que a aeronave decolou, peguei meu laptop novo, sem acesso à internet, inseri o pen drive e segui as instruções de Laura para carregar os arquivos.

Ao longo das dezesseis horas seguintes, apesar de exausto, tudo o que consegui fazer foi ler, tecendo comentários febris a cada documento. Muitos dos arquivos eram tão fortes e chocantes quanto aquela primeira apresentação de PowerPoint sobre o PRISM que eu tinha visto no Rio. Vários eram piores ainda.

Um dos primeiros que li foi uma ordem secreta do tribunal da FISA (Lei de Vigilância de Inteligência Estrangeira), criado pelo Congresso dos Estados Unidos em 1978, após o Comitê Church revelar décadas de grampos abusivos do governo. A ideia por trás de sua formação era que o Estado podia seguir praticando a vigilância eletrônica, mas, para evitar abusos como aquele, precisava de autorização prévia do tribunal. Eu nunca tinha visto uma ordem do tribunal da FISA; quase ninguém tinha. Trata-se de uma das instituições mais sigilosas do governo. Todos os seus pareceres são automaticamente classificados como ultrassecretos, e só pouquíssimas pessoas têm acesso às suas decisões.

A decisão que li no avião para Hong Kong era fantástica por vários motivos. Ela ordenava à Verizon Business que entregasse à NSA "todos os registros de detalhes de chamadas" das "comunicações (1) entre os Estados Unidos e países estrangeiros; e (2) feitas inteiramente dentro dos Estados Unidos, inclusive chamadas locais". Isso queria dizer que a NSA estava coletando, de forma secreta e indiscriminada, os registros telefônicos de dezenas de milhares de americanos, no mínimo. Quase ninguém fazia ideia de que o governo Obama estivesse agindo assim. Agora, com aquela decisão, eu não apenas sabia como tinha a ordem secreta do tribunal para provar.

Além disso, a ordem especificava que a coleta em massa de registros telefônicos norte-americanos era autorizada pela Seção 215 da Lei Patriota. Essa interpretação radical era particularmente chocante, quase mais do que a decisão em si.

O que tornou a Lei Patriota tão controversa na época de sua implementação, após os ataques do 11 de Setembro, foi que a Seção 215 reduzia as exigências do que o governo precisava para obter "registros profissionais", de "causa provável" para "relevância". Ou seja, para conseguir documentos altamente delicados e invasivos – históricos médicos, transações bancárias, registros telefônicos –, o FBI só precisava demonstrar que esses documentos eram "relevantes" para uma investigação em curso.

Só que ninguém – nem mesmo os agressivos membros republicanos da Câmara dos Representantes que redigiram a lei em 2001 ou o mais fervoroso defensor das liberdades civis que a houvesse apresentado sob o viés mais ameaçador possível – pensava que a lei fosse autorizar o governo a coletar registros sobre *todo mundo*, de maneira maciça e indiscriminada. Mas era exatamente isso que aquela decisão secreta do tribunal da FISA aberta no meu computador durante o voo para Hong Kong fazia: ordenava à Verizon que entregasse à NSA todos os registros telefônicos de todos os seus clientes norte-americanos.

Durante dois anos, os senadores democratas Ron Wyden, do Oregon, e Mark Udall, do Novo México, haviam percorrido o país alertando que os americanos ficariam "pasmos ao descobrir" as "interpretações secretas da lei" que a administração Obama estava usando para se imbuir de imensos

e desconhecidos poderes de espionagem. No entanto, como essas atividades de espionagem e "interpretações secretas" eram confidenciais, os dois senadores, ambos membros do Comitê de Inteligência do Senado, não chegaram a revelar ao público o que consideravam tão ameaçador, apesar do escudo de imunidade jurídica que a Constituição lhes conferia por fazerem parte do Congresso e que lhes permitia fazer tais revelações caso o desejassem.

Assim que vi a ordem do tribunal da FISA, entendi que aquilo era pelo menos uma parte dos programas de vigilância abusivos e radicais sobre os quais Wyden e Udall haviam tentado alertar o país.

Reconheci na hora o significado daquela decisão. Mal podia esperar para publicá-la, certo de que sua revelação iria provocar um verdadeiro terremoto que levantaria exigências de transparência e prestação de contas. E esse foi apenas um das centenas de documentos ultrassecretos que li a caminho de Hong Kong.

Mais uma vez, senti minha opinião mudar em relação ao significado dos atos da fonte. Isso já tinha acontecido três vezes: quando vi pela primeira vez os e-mails recebidos por Laura, quando comecei a falar com a fonte, e depois de ler os mais de vinte documentos que ele me mandou por e-mail. Só agora eu sentia que estava realmente começando a processar a verdadeira magnitude daquela denúncia.

Durante o voo, em várias ocasiões Laura foi até a fileira na qual eu estava sentado, que ficava de frente para uma das divisórias do avião. Assim que a via, eu me levantava de um pulo e ficava em pé no espaço entre a poltrona e a divisória, mudo, estupefato, atordoado com o que tínhamos nas mãos.

Já fazia anos que Laura trabalhava com o tema da vigilância da NSA, e ela própria fora submetida várias vezes aos seus abusos. Eu escrevia sobre a ameaça representada pela vigilância doméstica irrestrita desde 2006, data de publicação do meu primeiro livro, que chamava a atenção para a ilegalidade e o radicalismo da NSA. Com nosso trabalho, ambos havíamos combatido o grande muro de confidencialidade que protegia a espionagem do governo: como documentar as ações de uma agência completamente envolta em múltiplas camadas de sigilo oficial? Naquele momento, havíamos rompido esse muro. Estávamos de posse, ali, naquele avião, de milhares de documentos que o Estado havia tentado desesperadamente esconder. Tínhamos indícios que provariam de forma incontestável tudo o que o governo fizera para destruir a privacidade dos norte-americanos e de pessoas mundo afora.

Conforme eu avançava na leitura, dois fatos relacionados àquele acervo me chamaram a atenção. O primeiro foi sua organização exemplar: a fonte havia criado incontáveis pastas, subpastas e subsubpastas. Cada documento tinha sido posto no lugar certo. Nunca encontrei sequer um arquivo perdido ou salvo no local errado.

Eu passara muitos anos defendendo o que considero os atos heroicos de Chelsea Manning, soldado do exército e delatora que, horrorizada com o comportamento de seu governo – seus crimes de guerra e suas mentiras sistemáticas –, havia arriscado a própria liberdade ao expor documentos confidenciais para o mundo pelo WikiLeaks. Mas Manning fora criticada (de forma injusta e incorreta, na minha opinião) por supostamente expor documentos que não tinha verificado antes, ao contrário de Daniel Ellsberg. Esse argumento, por menos embasado que fosse (Ellsberg foi um dos defensores mais dedicados de Manning, e ela parecia ter ao menos examinado os documentos), foi

usado com frequência para solapar a ideia de que as ações de Manning tinham sido heroicas.

Estava claro que nada desse tipo poderia ser dito sobre a nossa fonte na NSA. Não restava dúvida de que ele tinha verificado com cuidado todos os documentos que nos passara, compreendido seu significado e em seguida classificado cada um deles dentro de uma estrutura elegantemente organizada.

A outra característica notável do acervo era a extensão das mentiras do governo que estavam sendo reveladas, e cujas provas a fonte assinalara com destaque. Ele havia batizado uma das primeiras pastas com o nome "BOUNDLESS INFORMANT (NSA mentiu para o Congresso)". A pasta continha dezenas de documentos com estatísticas complexas, mantidas pela NSA, relacionadas ao número de ligações e e-mails interceptados pela agência. Continha também provas de que a NSA vinha coletando dados de telefonemas e mensagens eletrônicas de milhões de americanos por dia. BOUNDLESS INFORMANT, ou "informante sem limites", era o nome do programa destinado a quantificar, com exatidão matemática, as atividades diárias de vigilância da agência. Um dos mapas no arquivo mostrava que, durante um período de trinta dias que terminou em fevereiro de 2013, uma unidade da NSA havia coletado mais de *três bilhões* de itens apenas nos sistemas de comunicações dentro dos Estados Unidos.

A fonte havia nos fornecido provas claras de que funcionários da NSA tinham mentido para o Congresso, direta e repetidamente, sobre suas atividades. Durante anos, vários senadores haviam solicitado à agência uma estimativa aproximada do número de americanos que estavam tendo suas ligações e seus e-mails interceptados. Os agentes da NSA insistiam que não podiam responder a essa pergunta porque não mantinham nem poderiam manter dados desse tipo: justamente aqueles que estavam sendo expostos de forma exaustiva nos documentos do BOUNDLESS INFORMANT.

Mais significativo ainda, os arquivos – junto com o documento da Verizon – mostravam que o mais importante funcionário de segurança nacional do governo Obama, James Clapper, diretor de inteligência nacional, mentiu para o Congresso em 12 de março de 2013 ao responder à seguinte pergunta do senador Ron Wyden: "A NSA coleta algum tipo de dado relacionado a milhões ou centenas de milhões de americanos?" Clapper retrucou de forma sucinta e desonesta: "Não."

Em dezesseis horas de leitura quase ininterrupta, consegui dar conta de apenas uma pequena porcentagem dos documentos. Quando o avião pousou em Hong Kong, porém, já tinha certeza de duas coisas. Em primeiro lugar, a fonte era um indivíduo muito sofisticado e politicamente astuto, qualidades evidenciadas pelo fato de ele reconhecer a importância da maioria daqueles documentos. Era também uma pessoa bastante racional: a forma como havia escolhido, analisado e descrito os milhares de documentos que eu agora tinha nas mãos provava isso. Em segundo lugar, seria muito difícil negar seu status de delator clássico. Se revelar provas de que altos funcionários da área de segurança nacional mentiram deslavadamente para o Congresso sobre programas de espionagem domésticos não configura de modo inegável uma delação, o que configura?

Eu sabia que quanto mais dificuldade o governo e seus aliados tivessem para demonizar a fonte, mais potente seria o efeito de suas revelações. As duas linhas de ação preferidas para se desacreditar o responsável por uma denúncia – instabilidade psicológica e ingenuidade – não iriam funcionar naquele caso.

Pouco antes do pouso, li um último arquivo. Embora seu título fosse "LEIA-ME_PRIMEIRO", só

o vi pela primeira vez bem no finalzinho do voo. Tratava-se de outra explicação da fonte sobre o porquê de ter decidido fazer aquilo e o que esperava que fosse acontecer como resultado de seus atos. O tom e o conteúdo eram semelhantes ao manifesto que eu havia mostrado aos editores do *Guardian*.

Mas esse documento continha fatos vitais ausentes dos outros. Incluía o nome da fonte – era a primeira vez que eu o lia – e previsões claras sobre o que provavelmente aconteceria com ele depois que se identificasse. Em relação aos eventos ocorridos desde o escândalo de 2005 da NSA, o texto terminava assim:

> Muitos irão me maldizer por não ter praticado o relativismo nacional, por não ter desviado os olhos dos problemas da [minha] sociedade em direção a males distantes, externos, sobre os quais não temos autoridade e pelos quais não somos responsáveis, mas a cidadania traz consigo um dever de policiar primeiro o próprio governo antes de tentar corrigir outros. Aqui, hoje, em nosso país, estamos sujeitos a um governo que só permite uma supervisão limitada e que se recusa a prestar contas quando crimes são cometidos. Quando jovens marginalizados cometem pequenas infrações, nós, como sociedade, olhamos para o outro lado enquanto eles sofrem consequências atrozes no maior sistema prisional do mundo, mas quando os provedores de telecomunicações mais ricos e poderosos do país cometem, conscientemente, dezenas de milhões de crimes, o Congresso aprova a primeira lei de nossa nação que proporciona a seus amigos da elite uma imunidade retroativa total – cível e penal – para crimes que teriam merecido as mais longas sentenças de prisão da história.
>
> Essas empresas têm os melhores advogados do país em seus quadros, e não enfrentam sequer a menor das consequências. Quando é revelado que funcionários no mais alto nível do poder, incluindo especificamente o vice-presidente, conduziram pessoalmente esses atos criminosos, o que deveria acontecer? Se você acredita que essa investigação deve ser interrompida, que seus resultados devem ser classificados como mais do que ultrassecretos em um compartimento especial de "Informações Excepcionalmente Controladas" chamado STLW (STELLARWIND), que quaisquer investigações futuras sejam impedidas segundo o princípio de que obrigar aqueles que abusam do poder a prestar contas vai contra os interesses nacionais, que nós devemos "olhar para a frente, não para trás", e em vez de acabar com o programa ilegal você o expandiria para incluir ainda mais autoridades, então será bem-vindo nos salões do poder dos Estados Unidos, pois foi nisso que eles se transformaram, e eu estou divulgando os documentos que provam isso.
>
> Entendo que serei obrigado a responder pelos meus atos, e que a revelação dessas informações ao público assinala o meu fim. Ficarei satisfeito se o conluio de leis secretas, perdão desigual e poderes executivos ilimitados que governa o mundo que amo for desmascarado, nem que seja por um único instante. Se você quiser ajudar, faça parte da comunidade *open source* e lute para manter o espírito do jornalismo vivo e a internet gratuita. Eu estive nos cantos mais sombrios do governo, e o que eles mais temem é a luz.
>
> Edward Joseph Snowden, SSN: INFORMAÇÃO OMITIDA
>
> Codinome CIA "INFORMAÇÃO OMITIDA"

Nº de Identificação na Agência: INFORMAÇÃO OMITIDA

Ex-Consultor Sênior | Agência de Segurança Nacional dos Estados Unidos, sob proteção corporativa

Ex-Agente de Campo | Agência Central de Inteligência dos Estados Unidos, sob proteção diplomática

Ex-Palestrante | Agência de Inteligência de Defesa dos Estados Unidos, sob proteção corporativa

2

DEZ DIAS EM HONG KONG

Chegamos a Hong Kong na noite de 2 de junho, um domingo. O plano era encontrar Snowden imediatamente depois de chegarmos ao hotel, situado no bairro chique de Kowloon. Assim que entrei no quarto, liguei o computador para ver se ele estava on-line no programa de chat criptografado que vínhamos usando. Como acontecia quase sempre, lá estava ele, à espera.

Depois de trocar algumas gentilezas relacionadas ao voo, passamos à logística do nosso primeiro encontro.

– Vocês podem vir ao meu hotel – disse ele.

Foi minha primeira surpresa: descobrir que ele estava hospedado em um hotel. Ainda não sabia por que ele se encontrava em Hong Kong, mas àquela altura já imaginava que fosse para se esconder. Imaginara-o entocado em algum minúsculo apartamento barato, onde pudesse ficar fora da vista e que conseguisse custear sem estar recebendo nenhum contracheque regular, e não sentado confortavelmente em um hotel, às claras, acrescentando despesas diárias à conta.

Mudamos nossos planos e resolvemos que o melhor seria esperar até a manhã seguinte para encontrá-lo. Foi Snowden quem tomou essa decisão, estabelecendo a atmosfera hipercautelosa digna de um filme de espionagem que iria prevalecer nos dias seguintes.

– Vocês estarão mais propensos a chamar atenção se deslocando pela cidade à noite – explicou ele. – É estranho dois americanos fazendo check-in no hotel à noite e saindo logo em seguida. Vai ser mais natural vocês virem de manhã.

Snowden estava tão preocupado com a vigilância das autoridades de Hong Kong e da China quanto com a dos americanos. Tinha muito receio de que fôssemos seguidos por agentes da inteligência local. Partindo do princípio de que ele estava profundamente envolvido com agências de espionagem norte-americanas e entendia do assunto, acatei sua decisão, embora tenha ficado decepcionado por não nos encontrarmos naquela noite.

Como Hong Kong tem exatamente doze horas à frente de Nova York, noite e dia estavam agora invertidos para mim, de modo que mal preguei o olho nessa noite ou em qualquer outro momento durante a viagem. A culpa foi do fuso horário apenas em parte: minha empolgação quase incontrolável só me permitia cochilar por uma hora e meia, duas no máximo, e esse se tornou meu padrão de sono durante toda a nossa estadia.

Na manhã seguinte, Laura e eu nos encontramos no lobby e entramos em um táxi que estava à nossa espera para ir até o hotel de Snowden. Tinha sido ela quem combinara com ele todos os detalhes do encontro, e se mostrou muito relutante em conversar durante o trajeto, pois temia que o taxista pudesse ser alguma espécie de agente de inteligência disfarçado. Eu já não descartava mais esses temores como paranoia tão rápido quanto antes. Apesar das restrições, consegui extrair dela informações suficientes para entender o plano.

Tínhamos de ir até o terceiro andar do hotel de Snowden, onde ficavam as salas de reunião. Ele

escolhera uma sala específica que, na sua opinião, tinha um equilíbrio perfeito: era suficientemente afastada para desencorajar qualquer "tráfego humano" substancial, como dizia, mas não tão remota e escondida a ponto de atrairmos atenção ao ficarmos aguardando lá.

Laura me disse que, quando chegássemos ao terceiro andar, deveríamos perguntar ao primeiro funcionário do hotel com quem cruzássemos perto da sala escolhida se havia algum restaurante aberto. A pergunta sinalizaria a Snowden, que estaria em algum lugar por perto, que não tínhamos sido seguidos. Uma vez que encontrássemos a sala certa, deveríamos esperar em um sofá perto de um "jacaré gigante" que, como Laura me confirmou, era alguma espécie de objeto decorativo, não um animal vivo.

Tínhamos dois horários distintos para o encontro: 10h, depois 10h20. Se Snowden não aparecesse até dois minutos depois do primeiro horário, deveríamos sair da sala, ir para outro lugar e voltar no segundo horário, quando ele então iria nos encontrar.

– Como vamos saber que é ele? – perguntei a Laura.

Ainda não tínhamos quase informação nenhuma sobre aquele homem: nem idade, nem raça, nem aparência física; nada.

– Ele vai estar segurando um cubo mágico – respondeu ela.

Isso me fez rir bem alto: a situação toda me pareceu muito bizarra, extrema e improvável. "Isto é um thriller internacional ambientado em Hong Kong", pensei.

Nosso táxi nos deixou na entrada do hotel Mira, que, como pude observar, também fica em Kowloon, bairro altamente comercial cheio de arranha-céus brilhantes e lojas chiques. Ou seja: mais visibilidade, impossível. Ao entrar no lobby, fiquei outra vez bastante impressionado: Snowden não estava hospedado em um hotel qualquer, mas em um estabelecimento enorme e luxuoso, cuja diária eu sabia que devia custar várias centenas de dólares. Por que alguém que pretendia denunciar a NSA e precisava de grande sigilo iria a Hong Kong se esconder em um hotel cinco estrelas em um dos bairros mais visíveis da cidade? Mas naquela hora não havia por que ficar remoendo esse mistério: eu iria encontrá-lo dali a poucos minutos, e com certeza teria todas as respostas.

Como muitos prédios em Hong Kong, o hotel Mira parecia uma pequena cidade. Laura e eu passamos pelo menos quinze minutos vasculhando o labirinto de corredores em busca do local combinado. Tivemos de pegar vários elevadores, atravessar passarelas internas e perguntar o caminho várias vezes. Quando pensamos estar perto da sala, vimos um funcionário do hotel. Com algum constrangimento, fiz a pergunta cifrada, e ele nos respondeu com informações sobre as diversas opções de restaurante.

Ao dobrar uma quina, vimos uma porta aberta e um imenso jacaré de plástico verde no chão. Como combinado, sentamo-nos no sofá perdido no meio daquela sala vazia e esperamos, nervosos e calados. O pequeno recinto não tinha nenhuma função aparente e não parecia haver motivo para alguém entrar ali, uma vez que só havia o sofá e o jacaré. Depois de cinco longos minutos sentados em silêncio, ninguém apareceu, então saímos, encontramos outra sala ali perto e deixamos passar mais quinze minutos.

Às 10h20, voltamos e tornamos a ocupar nosso lugar junto ao jacaré, no sofá, que ficava virado para a parede dos fundos da sala e para um grande espelho. Dali a dois minutos, ouvi alguém entrar na sala.

Em vez de me virar depressa para ver quem era, mantive o olhar fixo no espelho da parede dos

fundos, que mostrou o reflexo de um homem andando na nossa direção. Só quando ele estava a poucos metros do sofá foi que me virei.

A primeira coisa que vi foi o cubo mágico embaralhado, que ele girava na mão esquerda. Edward Snowden disse oi, mas não nos estendeu a mão, já que o objetivo era fazer com que o encontro parecesse ter sido por acaso. Como Laura e ele tinham combinado, ela lhe perguntou sobre a comida do hotel e Snowden respondeu que era ruim. Em meio às inúmeras reviravoltas surpreendentes desta história toda, o momento de nosso primeiro encontro se revelou a maior das surpresas.

Snowden tinha 29 anos na época, mas parecia no mínimo vários anos mais jovem. Usava uma camiseta branca com dizeres desbotados, calça jeans e óculos de nerd chique. Tinha um cavanhaque ralo, mas parecia só ter começado a se barbear recentemente. Era um rapaz distinto e tinha uma postura firme como a de um militar, mas era bastante magro e pálido, e estava, é claro – como todos nós naquele momento –, desconfiado e cauteloso. Parecia um típico cara meio *geek* de 20 e poucos anos, daqueles que trabalham em laboratórios de informática em campi universitários.

Na hora, simplesmente não consegui encaixar as peças do quebra-cabeça. Sem ter pensado no assunto de forma consciente, eu havia suposto, por uma série de motivos, que Snowden fosse mais velho, na casa dos 50 ou mesmo dos 60. Em primeiro lugar, como tivera acesso a muitos documentos ultrassecretos, eu tinha imaginado que ocupasse um cargo importante na área de segurança nacional. Além disso, suas opiniões e estratégias eram sempre sofisticadas e embasadas, o que me levava a crer se tratar de um veterano da cena política. Por fim, eu sabia que ele estava disposto a jogar fora a própria vida e provavelmente a passar o resto dela na prisão para revelar o que achava que o mundo deveria saber, portanto imaginei que estivesse no fim da carreira. Para alguém tomar uma decisão tão extrema e tão sacrificante, pensei, devia ter nas costas muitos anos, ou até mesmo décadas, de profunda desilusão.

Ver que a fonte daquele espantoso acervo de material da NSA era um homem tão jovem foi uma das experiências mais desconcertantes que já tive. Minha mente começou a percorrer depressa todas as possibilidades: seria aquilo uma espécie de fraude? Será que eu tinha perdido meu tempo indo até o outro lado do mundo? Como alguém tão jovem podia ter acesso ao tipo de informação que tínhamos visto? Como aquele rapaz podia ser tão entendido e experiente em matéria de inteligência e espionagem quanto a nossa fonte claramente era? Talvez aquele fosse o filho de Snowden, pensei, ou então seu assistente ou namorado, que agora iria nos conduzir até ele. Todas as possibilidades imagináveis passaram pela minha cabeça, e nenhuma delas fez sentido algum.

– Bom, venham comigo – disse ele, obviamente tenso.

Laura e eu o seguimos. Enquanto caminhávamos, nós três murmuramos algumas expressões incoerentes de boa educação. Eu estava chocado e confuso demais para falar muita coisa, e pude ver que Laura sentia o mesmo. Snowden parecia muito atento, como à procura de alguém que pudesse estar nos observando ou de outro sinal qualquer de problema. Assim, nós o seguimos quase o tempo todo em silêncio.

Sem saber aonde ele estava nos levando, pegamos o elevador, fomos até o décimo andar e nos dirigimos a seu quarto. Snowden tirou da carteira um cartão e abriu a porta.

– Bem-vindos – falou. – Desculpem, está meio bagunçado, mas eu praticamente não saio daqui há algumas semanas.

O quarto estava mesmo uma bagunça: pratos de comida do serviço de quarto consumidos pela

metade empilhados sobre a mesa, roupas sujas por todo lado. Snowden liberou uma cadeira e me disse para sentar. Então se acomodou na cama. Como o quarto era pequeno, ficamos a menos de um metro e meio de distância. Nosso diálogo começou tenso, desajeitado e formal.

Ele foi logo falando em segurança e perguntou se eu tinha um telefone celular. Meu telefone só funcionava no Brasil, mas mesmo assim ele insistiu que eu tirasse a bateria ou pusesse o aparelho dentro do congelador do minibar, o que pelo menos abafaria a conversa e a tornaria mais difícil de interceptar.

Assim como Laura tinha me alertado em abril, Snowden disse que o governo norte-americano tem a capacidade de ativar celulares remotamente e convertê-los em escutas. Eu sabia que essa tecnologia existia, mas mesmo assim atribuí a preocupação deles a uma quase paranoia. Na realidade, quem estava equivocado era eu: há anos o governo dos Estados Unidos vem usando essa tática em investigações criminais. Em 2006, um juiz federal responsável por julgar o caso de supostos mafiosos nova-iorquinos decidira que a utilização pelo FBI dos chamados "grampos móveis" – transformar o próprio celular de uma pessoa em aparelho de escuta por ativação remota – era legal.

Assim que meu telefone foi guardado na segurança do congelador, Snowden tirou os travesseiros da cama e os pôs no pé da porta.

– Para se alguém passar no corredor – explicou. – Pode ser que haja microfones e câmeras no quarto, mas o que vamos falar vai acabar na imprensa de qualquer maneira – completou, meio a sério, meio brincando.

Minha capacidade de avaliar tudo aquilo era muito limitada. Eu ainda sabia bem pouco sobre quem era Snowden, para quem ele trabalhava, o que realmente o motivava ou o que ele tinha feito, portanto não podia ter certeza de quais ameaças nos espreitavam, fossem elas de vigilância ou de qualquer outro tipo. Minha sensação mais palpável era a incerteza.

Sem se dar ao trabalho de sentar ou dizer qualquer coisa, e talvez para aliviar a própria tensão, Laura começou a desembalar e instalar sua câmera e o tripé. Então se aproximou para colocar microfones em mim e em Snowden.

Já tínhamos conversado sobre seu plano de nos filmar enquanto estivéssemos em Hong Kong, afinal de contas, ela era documentarista e estava trabalhando em um filme sobre a NSA. Inevitavelmente, o que estávamos fazendo iria se tornar uma parte imensa do seu projeto. Eu sabia disso, mas não estava preparado para a gravação começar tão cedo. Havia uma enorme discrepância cognitiva entre encontrar em segredo uma fonte que, para o governo dos Estados Unidos, havia cometido crimes sérios, e filmar tudo.

Laura aprontou o equipamento em questão de minutos.

– Vou começar a filmar, então – anunciou, como se fosse a coisa mais natural do mundo.

A consciência de que estávamos prestes a ser filmados intensificou ainda mais a tensão no quarto.

Já havia certo constrangimento na interação inicial entre mim e Snowden, mas, assim que a câmera foi ligada, ficamos ainda mais formais e menos simpáticos; nossa postura se retesou e nossa fala se tornou mais vagarosa. Ao longo dos anos, dei muitas palestras sobre como a vigilância muda o comportamento humano, citando estudos que revelam que, quando observadas, as pessoas se mostram mais reticentes, mais cautelosas em relação ao que dizem, menos livres. Agora eu estava vendo e sentindo na pele uma vívida ilustração dessa dinâmica.

Já que nossas tentativas de trocar gentilezas eram inúteis, não havia nada a fazer senão ir direto ao

que interessava.

– Tenho várias perguntas, então vou fazê-las, uma a uma, e, se estiver tudo bem para você, podemos prosseguir daí – falei.

– Tudo bem – respondeu Snowden, obviamente tão aliviado quanto eu por dar logo início àquilo.

Naquele momento, eu tinha dois objetivos principais. Como todos nós sabíamos que havia o sério risco de que ele fosse preso a qualquer momento, minha principal prioridade era descobrir tudo o que pudesse sobre Snowden: sua vida, seus empregos, o que o levara a tomar aquela decisão extraordinária, como exatamente tinha conseguido obter aqueles documentos e por quê, o que estava fazendo em Hong Kong. Em segundo lugar, queria entender se ele era mesmo honesto e se estava disposto a revelar tudo, ou se estava ocultando fatos importantes sobre quem era e o que tinha feito.

Embora eu já escrevesse sobre política havia quase oito anos, a experiência mais relevante para o que estava prestes a fazer tinha sido minha carreira anterior de advogado litigante, que envolvia, entre outras coisas, tomar o depoimento de testemunhas. Durante um depoimento, o advogado passa horas e horas, às vezes dias, sentado a uma mesa diante da testemunha obrigada por lei a depor, que tem de responder com honestidade a todas as suas perguntas. Um dos objetivos mais importantes desse processo é expor mentiras, detectar discrepâncias no depoimento e destruir qualquer ficção criada pela testemunha, para permitir que a verdade oculta venha à tona. Uma das poucas coisas que de fato me agradava na profissão de advogado era tomar depoimentos, e eu havia desenvolvido táticas de todo tipo para desmontar uma testemunha. Minha estratégia sempre envolvia uma barragem incansável de perguntas, muitas vezes as mesmas, feitas várias vezes, mas em contextos diferentes, de direções e ângulos distintos, para testar a solidez da história.

Ao contrário da minha atitude com Snowden em nossos contatos on-line, quando eu me mostrara disposto a ser passivo e respeitoso, foi essa tática agressiva que usei nesse dia. Sem parar nem para ir ao banheiro ou fazer um lanche, passei cinco horas seguidas interrogando-o. Comecei com sua primeira infância, suas experiências no ensino fundamental, seu histórico de trabalho antes de entrar para o governo. Pedi todos os detalhes que ele conseguisse recordar. Fiquei sabendo que ele havia nascido na Carolina do Norte e sido criado em Maryland, em uma família de classe média baixa de funcionários públicos federais (seu pai trabalhara por trinta anos na Guarda Costeira). Na adolescência, Snowden se sentira muito pouco desafiado no ensino médio, que nunca chegara a concluir; interessava-se muito mais pela internet do que pelas aulas.

Quase na mesma hora, pude ver ao vivo o que tinha observado durante nossas conversas no chat na internet: Snowden era um homem muito inteligente e razoável, e seu raciocínio era metódico. Suas respostas eram sempre concisas, claras e convincentes. Em quase todos os casos, eram atenciosas, ponderadas, e esclareciam exatamente o que eu havia perguntado. Não havia as voltas estranhas nem as histórias do arco da velha típicas das pessoas acometidas por instabilidade emocional ou distúrbios psicológicos. Sua estabilidade e seu foco inspiravam confiança.

Apesar de a interação on-line nos permitir formar rapidamente uma impressão sobre as pessoas, ainda precisamos encontrá-las ao vivo para ter uma noção confiável de quem são. Logo me senti melhor em relação àquela situação toda e me recuperei da dúvida e da desorientação iniciais sobre com quem estava lidando. Mesmo assim, mantive uma atitude muito cética, pois sabia que a credibilidade de tudo o que estávamos prestes a fazer dependia da confiabilidade das afirmações de Snowden em relação a quem era.

Passamos várias horas repassando seu histórico profissional e sua evolução intelectual. A exemplo de muitos americanos, as opiniões políticas de Snowden haviam sofrido uma mudança significativa após os atentados do 11 de Setembro: ele se tornara muito mais "patriota". Em 2004, aos 20 anos, alistou-se no exército com o objetivo de combater na Guerra do Iraque, que na época considerava um esforço nobre para libertar o povo iraquiano da opressão. Após poucas semanas no treinamento básico, porém, viu que se falava muito mais em matar árabes do que em libertar quem quer que fosse. Quando quebrou as duas pernas em um acidente de treinamento e foi forçado a sair do exército, já estava extremamente desiludido em relação ao verdadeiro objetivo daquele conflito.

Mas Snowden continuava acreditando na boa índole fundamental do governo dos Estados Unidos, de modo que decidiu seguir o exemplo de muitos parentes e foi trabalhar em um órgão federal. Mesmo sem diploma do ensino médio, tinha conseguido criar algumas oportunidades profissionais durante os primeiros anos da idade adulta, entre elas a prestação de serviços de tecnologia por 30 dólares a hora antes de completar 18 anos, e desde 2002 era técnico de sistemas certificado pela Microso . Uma carreira no governo federal, porém, lhe parecia ao mesmo tempo nobre e promissora em termos profissionais, e ele começou como segurança no Centro de Estudos Avançados em Linguagem da Universidade de Maryland, edifício secretamente administrado e usado pela NSA. Sua intenção, afirmou, era obter permissão para acessar material ultrassecreto, dando assim o primeiro passo em direção a futuros serviços de tecnologia.

Embora tivesse largado o ensino médio, Snowden tinha uma facilidade inata para a tecnologia, que se evidenciou no início da adolescência. Apesar da pouca idade e da falta de instrução formal, esses atributos, aliados à sua óbvia inteligência, lhe permitiram avançar depressa na vida profissional, e ele logo trocou o cargo de segurança pelo de especialista em tecnologia na CIA, em 2005.

Segundo me explicou, toda a comunidade de inteligência vivia desesperada à procura de funcionários que entendessem de tecnologia, pois havia se transformado em um sistema tão grande e abrangente que era difícil encontrar profissionais suficientes capazes de operá-lo. Portanto, as agências de segurança nacional precisavam recrutar talentos em áreas não tradicionais. Pessoas com habilidade avançada no setor de informática tendiam a ser jovens, às vezes alienadas, e muitas não tinham sido brilhantes no ensino formal; com frequência consideravam a cultura da internet muito mais estimulante do que as instituições convencionais de ensino ou as interações pessoais. Na CIA, Snowden se tornou um membro valorizado de sua equipe de TI, obviamente mais experiente e capaz do que os colegas mais velhos e com ensino superior. Sentiu que havia encontrado o ambiente no qual suas capacidades seriam recompensadas e sua falta de credenciais acadêmicas, ignorada.

Em 2006, deixou de ser prestador de serviços para a CIA e entrou para o quadro de funcionários, o que aumentou ainda mais suas oportunidades. Em 2007, soube de uma vaga na agência que envolvia trabalhar com sistemas de informática no exterior. Com recomendações entusiasmadas de seus gerentes, conseguiu o emprego e acabou indo trabalhar na Suíça. Passou três anos em Genebra, até 2010, operando em segredo, com credenciais diplomáticas.

Segundo a descrição de Snowden de seu cargo em Genebra, ele era muito mais do que um simples "administrador de sistemas". Considerado o maior especialista em tecnologia e cibersegurança da Suíça, ele viajava pela região para solucionar problemas que ninguém mais era capaz de resolver. Foi escolhido a dedo pela CIA para dar suporte ao presidente na reunião de cúpula da OTAN na

Romênia, em 2008. Apesar desse sucesso, foi durante essa temporada que começou a ficar seriamente incomodado com as ações de seu governo.

– Graças ao acesso aos sistemas que os peritos em tecnologia têm, vi muitos materiais secretos, boa parte deles bem ruim – disse-me Snowden. – Comecei a entender que, na verdade, o que o meu governo faz mundo afora é bem diferente daquilo que sempre me ensinaram. Essa consciência, por sua vez, leva você a começar a reavaliar a maneira como vê as coisas, a questionar mais.

Um dos exemplos que ele relatou foi quando agentes da CIA tentavam recrutar um banqueiro suíço para fornecer informações confidenciais. Eles queriam saber sobre as transações financeiras de indivíduos que os Estados Unidos consideravam suspeitos. Snowden me contou que um dos agentes disfarçados fez amizade com o banqueiro, o embebedou certa noite e o incentivou a voltar de carro para casa. Quando o homem foi parado pela polícia e preso por dirigir embriagado, o agente se ofereceu para ajudá-lo de várias maneiras, contanto que ele cooperasse com a agência. No fim das contas, a tentativa de recrutamento acabou fracassando.

– Eles destruíram a vida do sujeito por algo que nem deu certo, e depois simplesmente foram embora – contou Snowden.

Além do estratagema em si, incomodou-o a maneira como o agente se gabou dos métodos usados para conseguir o que queria.

Outro elemento de frustração veio de seus esforços para alertar os superiores quanto a problemas na segurança dos computadores ou nos sistemas que, na sua opinião, ultrapassavam as fronteiras da ética. Segundo ele, essas tentativas foram quase sempre repelidas.

– Eles falavam que não era trabalho meu, ou então que eu não tinha informações suficientes para emitir aquele tipo de juízo. Basicamente, diziam para não me preocupar com o assunto – afirmou.

Snowden começou a ganhar fama entre os colegas como um criador de casos, traço que não lhe valeu o apreço dos superiores.

– Foi nessa época que comecei de fato a perceber como é fácil separar poder de prestação de contas e como quanto mais altas as instâncias de poder, menos supervisão e prestação de contas existem.

Quase no final de 2009, Snowden, desiludido, decidiu que estava na hora de sair da CIA. Foi nessa época, no fim de sua temporada em Genebra, que ele começou a pensar em se tornar delator e em vazar segredos que acreditava revelarem comportamentos questionáveis.

– Por que não agiu naquela época? – indaguei.

Ele respondeu que pensava, ou pelo menos esperava, que a eleição de Barack Obama para a presidência fosse eliminar alguns dos piores abusos que tinha visto. Obama iniciou seu mandato jurando corrigir os abusos da segurança nacional que tinham sido justificados pela guerra ao terror. A expectativa de Snowden era que pelo menos as arestas nas áreas de inteligência e das forças armadas pudessem ser aparadas.

– Mas depois ficou claro que Obama não apenas estava dando continuidade, mas em muitos casos também expandindo esses abusos – disse ele. – Percebi então que não podia esperar que um líder corrigisse a situação. Liderança significa ser proativo e servir de exemplo, não esperar os outros agirem.

Ele também estava preocupado com os danos que ocorreriam caso revelasse o que havia descoberto na CIA.

– Quando você traz à tona segredos da CIA, pode prejudicar pessoas – falou, referindo-se a

agentes e informantes disfarçados. – Isso eu não estava disposto a fazer. Mas, quando você expõe os segredos da NSA, está prejudicando apenas sistemas abusivos. Com isso eu me sentia muito mais confortável.

Assim, Snowden voltou para a NSA, dessa vez como terceirizado da Dell Corporation, que prestava serviços à agência. Em 2010, estava lotado no Japão e tinha um nível muito mais alto de acesso a segredos de vigilância do que antes.

– As coisas que vi começaram a me perturbar de verdade – declarou. – Eu podia assistir em tempo real a imagens, geradas por drones, de pessoas que eles talvez fossem matar. Era possível observar aldeias inteiras e ver o que todo mundo estava fazendo. Vi a NSA monitorar as atividades das pessoas na internet enquanto elas digitavam. Fui percebendo quanto as capacidades de vigilância dos Estados Unidos tinham se tornado invasivas, e me dei conta do verdadeiro escopo desse sistema. E quase ninguém sabia que isso estava acontecendo.

A necessidade – a *obrigação* – que ele sentia de revelar o que estava vendo foi se tornando cada vez mais urgente.

– Quanto mais tempo eu passava na NSA no Japão, mais claro se tornava que eu não poderia ficar calado. Na verdade, sentia que seria errado ajudar a esconder tudo aquilo da população.

Mais tarde, depois que a identidade de Snowden foi revelada, jornalistas tentaram retratá-lo como uma espécie de cara de TI meio bobo e sem importância, que por acaso havia deparado com informações confidenciais. Só que a realidade era bem diferente.

Durante o tempo em que trabalhou para a CIA e a NSA, disse-me Snowden, ele aos poucos foi sendo treinado para se tornar um agente cibernético de alto nível. No Japão, esse treinamento se intensificou. Ele passou a dominar os mais sofisticados métodos para proteger dados eletrônicos da intrusão de outras agências de segurança e recebeu certificação formal como agente cibernético de alto nível, do tipo capaz de hackear sistemas civis e militares de outros países para roubar informações ou preparar ataques sem deixar vestígios. Acabou sendo selecionado pela Academia Conjunta de Treinamento em Contrainteligência da DIA (Agência de Inteligência de Defesa) para dar aulas de contrainteligência cibernética no curso de contrainteligência chinesa.

Os métodos de segurança operacional que ele agora insistia para respeitarmos eram os mesmos que havia aprendido ou mesmo ajudado a criar na CIA, e sobretudo na NSA.

Em julho de 2013, o *New York Times* confirmou o que Snowden tinha me dito ao noticiar que, "enquanto trabalhava para uma empresa terceirizada pela NSA, Edward J. Snowden aprendeu a ser hacker", e que "havia se transformado no tipo de especialista em cibersegurança que a agência vive desesperada para recrutar". O treinamento recebido, afirmou o *NYT*, foi "crucial para sua guinada em direção a uma cibersegurança mais sofisticada". A matéria acrescentava que os arquivos acessados por Snowden mostravam que ele havia "passado para o lado ofensivo da espionagem eletrônica, ou guerra cibernética, na qual a NSA invade os sistemas de computadores de outros países para roubar informações ou preparar ataques".

Embora, no interrogatório, tenha tentado me ater à ordem cronológica, muitas vezes, por conta da minha ansiedade, eu não conseguia resistir a dar um salto no tempo. Queria chegar ao cerne daquilo que, para mim, era o mais incrível mistério desde que eu começara a conversar com aquele homem: o que realmente o levara a jogar no lixo a própria carreira, transformar-se num criminoso em potencial e violar os mandamentos de sigilo e lealdade que haviam sido martelados na sua cabeça

durante anos.

Fiz essa mesma pergunta de muitas formas diferentes, logo Snowden a respondeu de diversas maneiras, mas suas justificativas soavam demasiado superficiais, abstratas ou desprovidas de paixão e convicção. Ele se mostrava muito à vontade para falar sobre os sistemas e a tecnologia da NSA, mas claramente menos quando o assunto era ele próprio, sobretudo em reação às sugestões de que tinha cometido um ato corajoso, que merecia uma explicação psicológica. Como suas respostas pareciam mais abstratas do que íntimas e profundas, considerei-as pouco convincentes. O mundo tinha o direito de saber o que estava sendo feito com sua privacidade, disse ele; afirmou sentir uma obrigação moral de tomar partido contra ações erradas; falou que não poderia, em sã consciência, permanecer calado diante daquela ameaça oculta aos valores que mais prezava.

Eu acreditava que esses valores políticos fossem reais para ele, mas queria saber o que o levara pessoalmente a sacrificar a vida e a liberdade em defesa desses valores, e não sentia que estava escutando a resposta verdadeira. Talvez nem ele mesmo a soubesse, ou talvez, como muitos homens americanos – sobretudo aqueles imersos na cultura da segurança nacional –, relutasse em mergulhar demais na própria psique, mas eu precisava descobrir.

Descartando quaisquer outras considerações, queria ter certeza de que ele havia tomado aquela decisão com uma compreensão genuína e racional das consequências: não estava disposto a ajudá-lo a correr um risco daquela magnitude sem me convencer de que ele agia com total autonomia e por iniciativa própria, com pleno entendimento de seu objetivo.

Finalmente, Snowden me deu uma resposta que soou vibrante e verdadeira:

– A real medida do valor de alguém não é aquilo em que a pessoa diz acreditar, mas o que ela faz para defender essas crenças. Se você não age de acordo com as suas crenças, é provável que elas não sejam sinceras.

E como ele havia desenvolvido essa medida para estimar o próprio valor? De onde tirara a crença de que só poderia estar agindo moralmente caso estivesse disposto a sacrificar os próprios interesses em prol de um bem maior?

– De vários lugares diferentes, várias experiências – retrucou Snowden. Ele havia crescido lendo muita mitologia grega, e fora influenciado pelo livro *O herói de mil faces*, de Joseph Campbell. – Essa obra encontra características comuns nas histórias que todos nós compartilhamos – observou. A principal lição que havia aprendido com o livro era que "somos nós que damos significado à vida, com nossas ações e as histórias que criamos com elas". Uma pessoa é definida apenas por suas ações. – Eu não quero ser alguém que tem medo de agir para defender seus princípios.

Ao longo de seu percurso intelectual, ele havia reencontrado muitas vezes esse mesmo tema, esse construto moral para avaliar a identidade e o valor de cada indivíduo, inclusive, como explicou com certo constrangimento, nos videogames. Segundo ele, a lição aprendida graças à imersão nos games era que uma só pessoa, mesmo a menos poderosa, é capaz de enfrentar uma grande injustiça.

– O protagonista dos videogames muitas vezes é uma pessoa comum, que depara com graves injustiças criadas por forças poderosas, e ele tem a opção de fugir apavorado ou lutar por aquilo em que acredita. A história também mostra que pessoas aparentemente comuns, mas determinadas o suficiente em relação à justiça, podem triunfar na luta contra os mais formidáveis adversários.

Snowden não era o primeiro a me dizer que os jogos de computador tinham sido fundamentais para forjar sua compreensão do mundo. Anos antes, eu poderia ter feito pouco dessa resposta, mas

passara a aceitar que, para a geração dele, os games tinham desempenhado um papel tão sério na formação da consciência política, do raciocínio moral e da compreensão do próprio lugar no mundo quanto a literatura, a televisão e o cinema. Eles também apresentam, muitas vezes, dilemas morais complexos e incentivam a reflexão, sobretudo para quem está começando a questionar o que aprendeu.

O raciocínio moral de Snowden na adolescência, tirado de obras que constituíam, nas suas palavras, "um modelo para quem queremos ser e por quê", evoluiu até virar, na idade adulta, uma séria introspecção em relação às obrigações éticas e aos limites psicológicos. O que faz uma pessoa se manter passiva e dócil, explicou ele, "é o medo das repercussões, mas, quando você se liberta do apego às coisas que no final das contas não têm importância – dinheiro, carreira, segurança física –, consegue superar esse medo".

Igualmente fundamental para a sua visão de mundo era o valor sem precedentes da internet. Como para muitos membros da sua geração, "a internet" não era uma ferramenta isolada usada para tarefas específicas, mas sim o mundo no qual sua mente e personalidade se desenvolveram, um lugar único que proporcionava liberdade, exploração e um grande potencial de crescimento e compreensão intelectual.

Para Snowden, as qualidades singulares da internet tinham um valor incomparável e deviam ser preservadas a qualquer custo. Quando adolescente, ele usava a rede para explorar ideias e conversar com pessoas em lugares distantes e com vidas diferentes da sua em todos os aspectos, indivíduos que de outra forma jamais teria conhecido.

– Basicamente, a internet me permitiu experimentar a liberdade e explorar meu potencial pleno como ser humano. – Obviamente animado, arrebatado até, ao discorrer sobre o valor único da rede, ele prosseguiu: – Para muitos jovens, a internet é uma forma de autorrealização. Ela lhes permite explorar quem eles são e quem querem ser, mas isso só funciona se pudermos ter privacidade e anonimato, se pudermos cometer erros sem que eles nos acompanhem. Fico preocupado ao pensar que a minha geração pode ter sido a última a gozar dessa liberdade.

O peso dessa questão na decisão de Snowden se tornou claro para mim.

– Eu não quero viver em um mundo onde não tenhamos privacidade nem liberdade, onde o valor único da internet seja destruído – disse-me ele.

Sentia-se inclinado a fazer o que pudesse para impedir que isso acontecesse ou, mais exatamente, para permitir que outras pessoas tivessem a chance de decidir agir ou não em defesa desses valores.

Nessa mesma linha de raciocínio, Snowden ressaltou diversas vezes que seu objetivo não era destruir a capacidade da NSA de eliminar a privacidade.

– Tomar essa decisão não é o meu papel – afirmou. O que ele queria mesmo era revelar aos cidadãos norte-americanos e do mundo todo o que estava sendo feito com sua privacidade, informá-los. – Minha intenção não é acabar com esses sistemas, mas permitir que as pessoas decidam se eles devem continuar a existir – insistiu.

Com frequência, delatores como Snowden são demonizados como pessoas solitárias ou perdedores que agem movidos não pela consciência, mas pela alienação e pela frustração de uma vida fracassada. Ele era o oposto disso: tinha uma vida repleta das coisas consideradas mais valiosas. Sua decisão de vazar os documentos significava desistir de uma namorada de longa data que ele amava, de uma vida no paradisíaco Havaí, de uma família que o apoiava, de uma carreira estável, de um

salário alto e de uma vida inteira pela frente cheia de possibilidades de todo tipo.

Ao fim de sua temporada com a NSA no Japão, em 2011, Snowden foi trabalhar em um escritório da CIA no estado de Maryland, outra vez como terceirizado da Dell. Contando os bônus, estava a caminho de embolsar cerca de 200 mil dólares naquele ano, trabalhando com a Microso e outras empresas de tecnologia na construção de sistemas seguros para a CIA e outras agências armazenarem documentos e dados.

– O mundo estava ficando pior – comentou ele em relação a esse período. – Naquele cargo, pude ver em primeira mão que o Estado, principalmente a NSA, estava trabalhando junto com o setor privado de tecnologia para obter acesso integral às comunicações das pessoas.

Durante as cinco horas de interrogatório nesse dia – na verdade, durante todo o tempo que conversamos em Hong Kong –, Snowden falou quase sempre com um tom de voz estoico, calmo e neutro. No entanto, ao relatar a descoberta que enfim o fizera agir, tornou-se arrebatado, até mesmo um pouco nervoso.

– Percebi que eles estavam criando um sistema cujo objetivo era eliminar toda a privacidade, em nível global. Tornar impossível a qualquer ser humano se comunicar eletronicamente com outro sem que a NSA pudesse coletar, armazenar e analisar a comunicação.

Foi essa compreensão que cristalizou sua determinação de se tornar um delator. Em 2012, ele foi transferido pela Dell de Maryland para o Havaí. Passou períodos de 2012 baixando os documentos que, na sua opinião, o mundo precisava ver. Pegou também alguns outros não destinados à publicação, mas que possibilitariam aos jornalistas entender o contexto dos sistemas sobre os quais iriam escrever.

No início de 2013, Snowden percebeu que havia mais um conjunto de documentos de que precisava para completar o retrato que desejava mostrar ao mundo, mas que não poderia acessá-los enquanto estivesse na Dell. Só poderia colocar as mãos neles se conseguisse outro cargo no qual fosse formalmente nomeado analista de infraestrutura, o que lhe daria alcance ilimitado aos repositórios de vigilância gerais da NSA.

Com esse objetivo em mente, Snowden se candidatou a uma vaga no Havaí, na Booz Allen Hamilton, uma das maiores e mais poderosas prestadoras de serviços na área de defesa dos Estados Unidos, em que trabalham muitos ex-altos funcionários do governo. Aceitou um corte de salário para conseguir o emprego, uma vez que este lhe daria o acesso de que precisava para baixar o último conjunto de arquivos que considerava necessário para completar o retrato da espionagem da NSA. Mais importante ainda, esse nível de alcance lhe permitia coletar informações sobre o monitoramento secreto realizado pela NSA de toda a infraestrutura doméstica de telecomunicações dos Estados Unidos.

Em meados de maio de 2013, Snowden solicitou algumas semanas de licença para tratar sua epilepsia, doença da qual descobrira ser portador um ano antes. Fez as malas e incluiu na bagagem quatro laptops vazios com finalidades diversas. Não disse à namorada para onde estava indo; na verdade, viajava com frequência a trabalho sem poder lhe revelar o destino. Não queria que ela conhecesse os seus planos para evitar o assédio do governo depois que sua identidade fosse revelada.

Snowden chegara a Hong Kong depois de partir do Havaí no dia 20 de maio, fizera o check-in no hotel Mira usando seu nome verdadeiro e desde então não saíra mais de lá.

Estava hospedado no hotel às claras, utilizando o próprio cartão de crédito para pagar as

despesas, pois, conforme explicou, sabia que seus movimentos acabariam sendo examinados com minúcia pelo governo, pela mídia e por praticamente todo mundo. Queria evitar qualquer alegação de que ele era algum tipo de agente estrangeiro, o que seria mais fácil caso houvesse passado aquele período escondido. Disse que o objetivo era demonstrar que seus movimentos podiam ser comprovados, que não havia conspiração nenhuma e que ele estava agindo sozinho. Para as autoridades da China e de Hong Kong, ele parecia um executivo como outro qualquer, não alguém se esquivando para não ser notado.

– Não tenho planos de esconder o que sou ou quem sou, logo não tenho motivo algum para me esconder e alimentar teorias de conspiração ou campanhas de demonização.

Então fiz a pergunta que não me saía da cabeça desde que conversáramos na internet pela primeira vez: o que o tinha feito escolher Hong Kong como destino quando chegara a hora de revelar os documentos? Como de hábito, a resposta de Snowden mostrou que a decisão fora baseada em uma análise cuidadosa.

A prioridade número um, contou, era garantir sua integridade física contra qualquer interferência dos Estados Unidos enquanto estivesse trabalhando com Laura e comigo. Caso as autoridades norte-americanas descobrissem seu plano de vazar os documentos, tentariam impedi-lo, prendê-lo ou coisa pior. Embora fosse semi-independente, Hong Kong fazia parte do território chinês, calculou ele, e os agentes americanos teriam mais dificuldade para agir contra ele ali do que em outros lugares nos quais ele cogitara se refugiar em definitivo, como algum país latino-americano menor – Equador ou Bolívia, por exemplo. Hong Kong também estaria mais disposta e em melhores condições de resistir à pressão dos Estados Unidos para entregá-lo do que um país europeu pequeno como a Islândia.

Embora fazer os documentos chegarem ao público fosse o critério mais importante para a escolha do destino de Snowden, não era o único. Ele também queria estar em um lugar onde as pessoas fossem comprometidas com os valores políticos que ele prezava. Como explicou, o povo de Hong Kong, embora em última instância estivesse sujeito às leis repressivas do governo chinês, havia lutado para preservar algumas liberdades políticas básicas e criado um vibrante clima de dissidência. Snowden assinalou que Hong Kong tinha líderes democraticamente eleitos e que lá ocorriam grandes protestos populares, entre eles uma passeata anual contra a repressão na praça Tiananmen.

Ele poderia ter ido para outros lugares, que teriam proporcionado proteção ainda maior contra qualquer ação dos Estados Unidos, incluindo a China continental. E com certeza havia países que gozavam de maior liberdade política, como a Islândia ou outras pequenas nações europeias. No entanto, Snowden sentia que Hong Kong tinha a melhor mistura de segurança física e força política.

Sem dúvida havia aspectos negativos naquela decisão, e ele tinha consciência de todos eles, inclusive do relacionamento da cidade com a China, que proporcionaria aos críticos um jeito fácil de demonizá-lo. No entanto, não havia escolhas perfeitas. "Todas as minhas alternativas são ruins", dizia ele com frequência, e Hong Kong de fato lhe proporcionou certa segurança e uma liberdade de movimento que teriam sido difíceis de conseguir em outro lugar.

Depois de ouvir todos os fatos da história, eu tinha mais um objetivo: certificar-me de que Snowden entendia o que provavelmente iria lhe acontecer quando ele fosse identificado como a fonte por trás daquelas revelações.

O governo Obama vinha travando algo que indivíduos de todas as visões políticas qualificavam como uma guerra sem precedentes contra os delatores. O presidente, que durante a campanha

prometera ter a "administração mais transparente da história" e se comprometera, de forma específica, a proteger os delatores, que qualificava de "nobres" e "corajosos", acabara fazendo exatamente o contrário.

A administração Obama processou mais delatores do governo com base na Lei de Espionagem de 1917, sete no total, do que todos os outros governos da história dos Estados Unidos *juntos*; na verdade, mais do que o dobro desse total. A Lei de Espionagem, adotada durante a Primeira Guerra Mundial para permitir ao presidente Woodrow Wilson criminalizar os detratores do conflito, prevê sanções severas, entre elas a prisão perpétua e até mesmo a pena de morte.

Não havia dúvida de que todo o peso da lei se abateria sobre Snowden. O Departamento de Justiça de Obama o acusaria de crimes que poderiam condená-lo a passar o resto da vida preso, e era provável que ele fosse amplamente denunciado como traidor.

– O que acha que vai lhe acontecer quando se identificar como a fonte desses vazamentos? – perguntei.

O ritmo acelerado da resposta de Snowden deixou claro que ele já refletira muitas vezes sobre o assunto:

– Eles vão dizer que eu violei a Lei de Espionagem. Que cometi crimes graves. Que ajudei os inimigos dos Estados Unidos. Que coloquei em risco a segurança nacional. Tenho certeza de que vão desencavar do meu passado todos os incidentes que conseguirem encontrar, e provavelmente exagerar ou até fabricar alguns outros para me demonizar o máximo possível.

Ele afirmou que não queria ir para a prisão.

– Vou tentar não ser preso. Mas se for esse o desfecho da história, e sei que existe uma chance imensa de ser, já decidi faz algum tempo que posso aguentar qualquer coisa que fizerem comigo. A única coisa que não posso suportar é saber que não fiz nada.

Nesse primeiro dia, e em todos os outros desde então, a determinação de Snowden e sua calma reflexão sobre o que poderia lhe acontecer me surpreenderam e afetaram de forma profunda. Nunca o vi demonstrar qualquer sinal de arrependimento, medo ou ansiedade. Sem pestanejar, ele explicou que havia se decidido, que entendia as possíveis consequências e que estava preparado para aceitá-las.

Parecia derivar certa força do fato de ter tomado essa decisão. Ao falar sobre o que o governo dos Estados Unidos poderia fazer com ele, Snowden irradiava uma tranquilidade extraordinária. Ver aquele rapaz de 29 anos reagindo dessa forma à ameaça de décadas ou de uma vida inteira em uma prisão de segurança máxima – perspectiva que, por definição, deixaria quase qualquer um paralisado de medo – foi profundamente inspirador. E a coragem dele nos contagiou: Laura e eu juramos repetidas vezes um ao outro e a ele que todas as nossas ações e decisões a partir daquele momento iriam honrar a sua escolha. Senti que era meu dever divulgar aquelas notícias respeitando o mesmo espírito que havia inspirado seu ato original: um destemor baseado na convicção de estar tomando uma atitude que se considera correta, e a recusa em ser intimidado ou detido por ameaças sem embasamento de altos funcionários hostis ansiosos por ocultar as próprias ações.

Após cinco horas de interrogatório, eu estava convencido, sem sombra de dúvida, de que todas as alegações de Snowden eram autênticas e suas motivações, ponderadas e genuínas. Antes de irmos embora, ele voltou ao ponto que já mencionara várias vezes: fazia questão de se apresentar como a fonte dos documentos, e de fazê-lo publicamente já na primeira matéria que saísse.

– Qualquer um que faça algo tão significativo assim tem a obrigação de explicar à população seus

motivos e o que espera conseguir com isso – afirmou.

Tampouco queria se esconder, e assim acentuar o clima de medo que o governo dos Estados Unidos vinha fomentando.

Além disso, quando nossas matérias começassem a ser publicadas, Snowden tinha certeza de que a NSA e o FBI identificariam rapidamente a fonte dos vazamentos. Ele não havia tomado todas as providências possíveis para cobrir seu rastro, pois não queria que seus colegas fossem submetidos a investigações ou acusações falsas. Insistiu que, graças às habilidades que adquirira e levando em conta as falhas incríveis do sistema da NSA, poderia ter coberto esse rastro por completo, caso o desejasse, mesmo tendo baixado aquela quantidade de documentos ultrassecretos. No entanto, decidira deixar pelo menos algumas pegadas eletrônicas para serem descobertas, de modo que permanecer escondido não era mais uma alternativa.

Embora eu não quisesse ajudar o governo a saber quem ele era revelando seu nome, Snowden me convenceu de que era inevitável descobrirem sua identidade. Mais importante ainda, ele fazia questão de se definir aos olhos do público, em vez de deixar que o governo o definisse.

Seu único temor em relação a se identificar era que isso pudesse desviar a atenção do conteúdo das revelações.

– Sei que a mídia personaliza tudo, e o governo vai querer me transformar na notícia, vai querer atacar o mensageiro. – Seu plano era dizer quem era logo de cara e então sumir de cena para permitir que o foco fosse na NSA e em suas atividades de espionagem – Depois de me identificar e de me explicar, não vou mais falar com a imprensa. Não quero que seja eu a notícia.

Argumentei que, em vez de expor a identidade de Snowden na primeira matéria, seria melhor aguardar uma semana, para podermos publicar a primeira série de notícias sem essa distração. Nossa ideia era simples: soltar o mais rápido possível várias matérias importantes, uma depois da outra, diariamente, em uma versão jornalística da tática de guerra do "choque e pavor", e culminar com a revelação da fonte. Ao final da reunião nesse primeiro dia, chegamos os três a um acordo; agora tínhamos um plano.

Passei o resto do meu tempo em Hong Kong me encontrando e conversando com Snowden todos os dias, demoradamente. Não dormi mais de duas horas por noite, e mesmo esse pouco tempo de sono só foi possível graças a remédios. Passei o resto do tempo escrevendo matérias baseadas nos documentos por ele revelados e, quando estas começaram a ser publicadas, dando entrevistas a respeito.

Snowden deixou a critério meu e de Laura decidir que fatos deveriam ser divulgados, em que ordem e como eles seriam apresentados. No primeiro dia, porém – como já tinha feito muitas vezes, e como continuou a fazer desde então –, enfatizou a importância de verificarmos cuidadosamente todo o material.

– Escolhi esses documentos com base no que é de interesse público, mas confio na sua avaliação de jornalistas para só publicarem aqueles que as pessoas precisam ver e que podem ser revelados sem prejudicar nenhum inocente.

Entre todas as razões possíveis, a principal era a noção de Snowden de que, para gerar um debate público de verdade, não poderíamos permitir ao governo dos Estados Unidos nenhuma alegação válida de que havíamos posto vidas em perigo ao publicar os documentos.

Ele também enfatizou que era vital publicar o material de maneira jornalística, ou seja, trabalhando com a mídia e escrevendo matérias que lhe proporcionassem contexto, em vez de apenas publicá-lo de uma vez só. Acreditava que essa abordagem fosse proporcionar uma proteção legal maior e, mais importante ainda, permitir ao público processar as revelações de modo muito mais ordenado e racional.

– Se eu quisesse os documentos simplesmente postos na internet todos de uma vez, poderia ter feito isso eu mesmo. Quero que vocês se certifiquem de que essas matérias serão escritas, uma a uma, de forma que as pessoas possam entender o que acontece de fato.

Concordamos que esse princípio iria nortear o nosso trabalho jornalístico.

Em várias ocasiões, Snowden explicou que desde o início desejava o envolvimento de Laura e o meu nas matérias, pois sabia que daríamos as notícias de forma agressiva, sem nos deixar intimidar por ameaças do governo. Citou muitas vezes o *New York Times* e outros veículos importantes que haviam segurado matérias grandes a pedido do governo. No entanto, embora desejasse uma divulgação agressiva, ele queria também jornalistas meticulosos, que levassem todo o tempo necessário para garantir que os fatos ficassem imunes a qualquer ataque e que todas as matérias fossem conferidas de cima a baixo.

– Alguns dos documentos que estou passando para vocês não são para ser publicados, mas para que entendam como o sistema funciona e possam dar a notícia de forma correta – falou.

Depois de meu primeiro dia completo em Hong Kong, saí do quarto de Snowden, voltei ao meu e passei a noite em claro redigindo quatro matérias, na esperança de que o *Guardian* fosse começar a publicá-las imediatamente. Havia certa urgência: nós precisávamos de Snowden para repassar conosco o máximo possível de documentos antes que, de uma forma ou de outra, ele não estivesse mais disponível para falar.

A urgência se devia também a outro fator. No táxi a caminho do aeroporto, em Nova York, Laura me revelara, pela primeira vez, que já havia mencionado os documentos de Snowden para vários jornalistas.

Entre eles estava Barton Gellman, ganhador de dois prêmios Pulitzer, ex-funcionário do *Washington Post*, jornal no qual agora atuava como freelancer. Laura tivera dificuldade para convencer as pessoas a viajarem com ela a Hong Kong, mas Gellman, que já se interessava por questões ligadas à vigilância havia tempos, se mostrou bastante disposto.

Seguindo a recomendação de Laura, Snowden tinha concordado em passar "alguns documentos" a Gellman com a intenção de que ele e o *Post*, junto com ela, noticiassem revelações específicas.

Apesar de respeitar Gellman, eu não tinha a mesma avaliação a respeito do jornal. Para mim, esse periódico é o ventre do monstro midiático da capital americana, e personifica todos os piores atributos da imprensa política dos Estados Unidos: proximidade excessiva do governo, reverência aos órgãos de segurança nacional, exclusão rotineira de qualquer voz dissidente. O próprio crítico de mídia do jornal, Howard Kurtz, relatou em 2004 como o jornal realçou, de forma sistemática, as opiniões a favor da guerra logo antes da invasão ao Iraque ao mesmo tempo que minimizava ou excluía a oposição. A cobertura noticiosa do *Post*, concluiu ele, tinha sido "descaradamente parcial" a favor da invasão. O editorial do jornal continuava a ser um dos mais clamorosos e negligentes defensores do militarismo, do sigilo e da vigilância do governo.

O *Post* tinha ganhado de bandeja um furo dos grandes, que não fizera o menor esforço para

conseguir e sem que a fonte o tivesse escolhido em primeiro lugar (embora houvesse aceitado a recomendação de Laura). De fato, meu primeiro chat criptografado com Snowden aconteceu devido à raiva que ele sentia da atitude medrosa do jornal.

Uma de minhas poucas críticas ao WikiLeaks ao longo dos anos era que, em determinadas ocasiões, o site também havia entregado furos importantes, de bandeja, aos mesmos grandes veículos de imprensa que mais se esforçam para proteger o governo, aumentando assim seu prestígio e sua importância. Notícias exclusivas sobre documentos ultrassecretos são um trampolim incomparável para o status de um veículo e conferem grande poder ao jornalista responsável por elas. Faz muito mais sentido dar esses furos a jornalistas e empresas de mídia independentes, amplificando assim seu alcance, aumentando seu prestígio e maximizando o impacto das informações.

Pior ainda: eu sabia que o *Post* iria obedecer à risca às regras protetoras implícitas que norteiam a forma como a mídia tradicional noticia os segredos do governo. Segundo essas normas, que permitem ao governo controlar revelações e minimizar ou até mesmo neutralizar seu efeito, os editores primeiro procuram as autoridades para lhes informar o que pretendem publicar. Os funcionários de segurança nacional, então, informam aos editores todas as maneiras como a segurança nacional será supostamente prejudicada pelas revelações. Segue-se uma demorada negociação sobre o que será ou não publicado. No melhor dos casos, o resultado é um atraso significativo. Muitas vezes, informações que obviamente constituem notícia são suprimidas. Quando o *Post* divulgou a existência das bases secretas operadas pela CIA, em 2005, foi isso que o levou a não revelar em quais países as prisões estavam situadas, permitindo assim que os locais de tortura ilegais da CIA continuassem a existir.

O mesmo processo levou o *New York Times* a omitir a existência do programa de grampos não autorizado da NSA *por mais de um ano* após os jornalistas James Risen e Eric Lichtblau estarem prontos para dar a notícia, em meados de 2004. O presidente Bush havia convocado o dono do jornal, Arthur Sulzberger, e o editor-chefe, Bill Keller, ao Salão Oval para insistir, absurdamente, que eles estariam ajudando terroristas caso revelassem que a NSA estava espionando cidadãos norte-americanos sem os mandados exigidos por lei. O jornal obedeceu às ordens e segurou a matéria durante *quinze meses*, até o final de 2005, com Bush já reeleito (permitindo-lhe, portanto, se candidatar ao segundo mandato), escondendo da população que o presidente a estava espionando sem autorização. Mesmo depois disso, o *Times* só publicou a matéria porque Risen, frustrado, estava prestes a divulgar as revelações em seu livro, e o jornal não queria ser furado por seu próprio repórter.

Além disso, há o tom usado pelos veículos de mídia tradicionais para discutir o mau comportamento do governo. A cultura jornalística norte-americana exige que os repórteres evitem qualquer afirmação clara ou declaratória, e que incluam citações oficiais em suas matérias, tratando-as com respeito por mais insignificantes que sejam. Eles costumam ter uma atitude que o colunista de mídia do próprio *Post*, Erik Wemple, classifica desdenhosamente como *ficar em cima do muro*: nunca fazer nenhuma afirmação definitiva, mas, em vez disso, dar credibilidade equivalente às defesas do governo e aos fatos em si, estratégia que tem por efeito diluir as revelações e transformá-las em uma confusão turva, incoerente e muitas vezes sem consequências. Acima de tudo, os jornalistas sempre dão um grande destaque às declarações oficiais, mesmo quando elas são obviamente falsas ou enganosas.

Foi esse jornalismo obsequioso, movido pelo medo, que levou o *Times*, o *Post* e muitos outros veículos a se recusarem a usar a palavra "tortura" nas notícias sobre as técnicas de interrogatório de Bush, embora a usassem sem restrição para descrever as mesmas táticas quando utilizadas por outros governos mundo afora. Foi isso também que provocou a enxurrada de veículos de imprensa despejando alegações sem fundamento sobre Saddam e o Iraque de modo a vender ao público norte-americano uma guerra sustentada por falsidades que a mídia do país, em vez de investigar, só fez amplificar.

Outra regra implícita destinada a proteger o governo é o costume dos veículos de imprensa de só publicarem alguns documentos secretos, e depois pararem. Sua forma de noticiar um acervo como o de Snowden teria como objetivo limitar seu impacto: publicar um punhado de matérias, colher os louros de um "grande furo", ganhar prêmios e então se retirar, garantindo que nada tivesse de fato mudado. Snowden, Laura e eu concordamos que revelar os documentos da NSA significava publicar agressivamente, matéria após matéria, e só parar quando todas as questões de interesse público houvessem sido tratadas, por mais raiva que causassem e por mais ameaças que suscitassem.

Desde nossa primeira conversa, Snowden tinha sido claro em relação ao que o levara a não confiar na mídia tradicional para revelar aquelas informações, citando várias vezes o fato de o *New York Times* ter ocultado os grampos da NSA. Ele passara a acreditar que a ocultação dessa informação pelo jornal podia muito bem ter mudado o desfecho da eleição de 2004.

– Esconder essa notícia mudou a história – afirmou.

Ele estava decidido a expor quão extrema era a espionagem revelada pelos documentos, de modo a forçar um debate público longo, com consequências reais, em vez de só um furo de reportagem cuja única consequência fossem elogios ao jornalista. Isso exigia denúncias destemidas, desprezo declarado pelas desculpas esfarrapadas do governo e por suas tentativas de fomentar o medo, uma defesa firme da retidão dos atos de Snowden e uma condenação inequívoca da NSA – justamente o que o *Post* impediria seus repórteres de fazer ao falar sobre o governo. Eu sabia que tudo o que o jornal faria diluiria o impacto das revelações. O fato de eles terem recebido uma pilha dos documentos de Snowden parecia ir totalmente na contramão de tudo o que eu pensava que estávamos tentando alcançar.

Como sempre, Laura tinha motivos coerentes para seu desejo de envolver o *Post*. Para início de conversa, ela achava que seria bom envolver a Washington oficial nas revelações para dificultar que estas fossem atacadas ou mesmo criminalizadas. Se o jornal favorito da cidade divulgasse os vazamentos, seria mais difícil para o governo demonizar os envolvidos.

Além disso, como ela assinalou corretamente, nem ela nem Snowden tinham conseguido se comunicar comigo durante um bom tempo pelo fato de eu não usar criptografia, e portanto, no início, o fardo de ter em seu poder milhares de documentos ultrassecretos da NSA fornecidos por nossa fonte tinha sido só seu. Ela sentira necessidade de encontrar alguém a quem pudesse confiar esse segredo e de trabalhar com uma instituição que lhe proporcionasse alguma proteção. Ela também não queria ir a Hong Kong sozinha. Como a princípio não conseguira falar comigo, e como a fonte achava que outra pessoa deveria ajudar na divulgação da matéria do PRISM, ela concluiu que fazia sentido entrar em contato com Gellman.

Eu entendi, mas nunca concordei com os motivos que levaram Laura a envolver o *Post*. Para mim, a noção de que precisávamos do envolvimento da Washington oficial era o tipo de abordagem

que eu desejava evitar: um comportamento excessivamente avesso ao risco, que respeitava as regras implícitas. Nós éramos tão jornalistas quanto qualquer profissional do *Post*, e entregar os documentos a eles para garantir nossa proteção significava, a meu ver, respaldar as mesmas premissas que estávamos tentando subverter. Embora Gellman tenha acabado por escrever algumas matérias excelentes e importantes com base no material, durante nossas primeiras conversas Snowden começou a lamentar o envolvimento do *Post*, embora tivesse sido ele quem, no fim das contas, decidira aceitar a recomendação de Laura de envolver o jornal.

Snowden ficara incomodado com o que considerava procrastinação por parte do periódico, com a temeridade de reunir tantas pessoas para falar de modo hesitante sobre o que ele tinha feito, e sobretudo com o temor demonstrado pelo fato de este convocar intermináveis reuniões com advogados, que faziam todo tipo de advertência alarmista e impunham exigências incrivelmente opressoras. E irritava-o sobretudo o fato de Gellman, a conselho dos advogados e editores do *Post*, ter se recusado em absoluto a ir a Hong Kong para se encontrar com ele e repassar os documentos.

Segundo Snowden e Laura diziam, os advogados do jornal tinham desaconselhado Gellman a viajar; também sugeriram que Laura não fosse e retiraram a oferta de arcar com as despesas de viagem. Tudo isso com base em uma teoria absurda, inspirada pelo medo: qualquer conversa sobre informações ultrassecretas ocorrida na China, país onde a vigilância era generalizada, poderia ser interceptada pelo governo chinês. Isso, por sua vez, poderia ser interpretado pelo governo dos Estados Unidos como uma transmissão temerária de segredos para os chineses, o que poderia dar margem a acusações criminais contra o jornal e contra Gellman, com base na Lei de Espionagem.

À sua maneira estoica e discreta, Snowden ficou indignado. Ele havia desestruturado a própria vida e arriscado tudo para revelar aquelas informações, sem dispor praticamente de proteção alguma. E aquele veículo de imprensa gigantesco, respaldado por todo tipo de apoio jurídico e institucional, recusava-se a correr o risco irrisório de despachar um repórter até Hong Kong para vê-lo.

– Eu me disponho a lhes dar esta matéria quentíssima, ao custo de um risco pessoal enorme, e eles não são sequer capazes de embarcar em um avião.

Era justamente essa obediência tímida e avessa ao risco demonstrada por nossa "imprensa crítica" em relação ao governo que eu passara anos combatendo.

Mas alguns documentos já tinham sido entregues ao *Post*, e não havia nada que eu pudesse fazer para mudar isso. Nessa segunda noite em Hong Kong, porém, depois de nos encontrarmos, decidi que não seria o *Washington Post*, com seu discurso confuso e pró-governo, com seu medo e sua postura em cima do muro, que iria determinar para sempre a forma como a NSA e Snowden seriam compreendidos. Quem quer que desse aquela notícia pela primeira vez iria desempenhar o papel predominante na forma como ela seria debatida e entendida, e eu estava decidido a garantir que fôssemos eu e o *Guardian*. Para aquilo ter o efeito que deveria ter, as regras implícitas do jornalismo tradicional – criadas para diminuir o impacto das revelações e proteger o governo – precisavam ser quebradas, não obedecidas. O *Post* as obedeceria; eu, não.

Assim, de volta ao meu quarto, terminei de trabalhar em quatro matérias distintas. A primeira era sobre a ordem secreta da FISA que obrigava a Verizon, um dos maiores provedores de telefonia norte-americanos, a ceder à NSA todos os registros de todos os cidadãos dos Estados Unidos. A segunda, baseada em um relatório interno ultrassecreto de 2009 do inspetor-geral da NSA, revelava o

programa de grampos não autorizados da era Bush. A terceira expunha em detalhes o programa BOUNDLESS INFORMANT, sobre o qual eu tinha lido no avião. A quarta e última era sobre o programa PRISM, do qual eu ouvira falar pela primeira vez ainda no Brasil. Era sobretudo essa matéria que eu considerava urgente, pois era esse documento que o *Post* estava se preparando para revelar.

Para agir com rapidez, precisávamos que o *Guardian* estivesse disposto a publicar sem demora. Enquanto a noite caía em Hong Kong – ainda era de manhã cedo em Nova York –, aguardei com impaciência que os editores do jornal acordassem, verificando a cada cinco minutos se Janine Gibson tinha entrado no chat do Google, nosso meio de comunicação habitual. Assim que a vi se logar, enviei a seguinte mensagem: "Precisamos conversar."

Àquela altura, sabíamos que falar por telefone ou pelo chat do Google estava fora de cogitação: ambos eram excessivamente inseguros. Por algum motivo, não conseguimos nos conectar via OTR, o programa de chat criptografado que vínhamos usando, de modo que Janine sugeriu experimentarmos o Cryptocat, programa recente criado para impedir a vigilância do governo que se tornou nosso principal meio de comunicação durante minha estadia em Hong Kong.

Contei a ela sobre meu encontro com Snowden naquele dia e afirmei estar convencido da autenticidade tanto dele quanto do material apresentado. Disse-lhe que já tinha escrito várias matérias. Janine ficou particularmente animada com o texto sobre a Verizon.

"Ótimo", digitei. "A matéria da Verizon está pronta. Se houver pequenas modificações a fazer, tudo bem, façamos." Ressaltei para Janine a urgência de publicar rápido: "Vamos dar logo essa notícia."

Só que havia um problema. Os editores do *Guardian* tinham se reunido com os advogados do periódico e escutado advertências alarmantes. Janine me repetiu o que os advogados tinham dito: mesmo para um jornal, publicar material confidencial pode (ainda que de forma ambígua) ser considerado crime pelo governo dos Estados Unidos, uma violação da Lei de Espionagem. O perigo era particularmente grave quando se tratava de documentos relacionados à inteligência. No passado, o governo evitara processar veículos de imprensa, mas contanto que eles respeitassem as regras implícitas e permitissem a seus funcionários uma leitura prévia do material, dando-lhes assim a oportunidade de argumentar que a publicação daqueles fatos prejudicaria a segurança nacional. Esse processo consultivo com o governo, explicaram os advogados, é o que permite aos jornais demonstrar que não têm a intenção de comprometer a segurança nacional com a publicação de documentos ultrassecretos, e assim, sem intenção criminosa comprovada, eles não podem ser processados.

Nunca houvera nenhum vazamento de documentos da NSA, muito menos daquela magnitude e importância. Os advogados consideravam que existia um potencial risco de acusações criminais, não apenas a Snowden, mas, levando em conta o histórico do governo Obama, também ao jornal. Poucas semanas antes de eu chegar a Hong Kong, fora divulgada a notícia de que o Departamento de Justiça de Obama obtivera um mandado judicial que lhe permitia ler os e-mails e registros telefônicos de repórteres e editores da Associated Press, para descobrir qual tinha sido a fonte de uma notícia.

Quase imediatamente depois disso, uma nova bomba revelou um ataque ainda mais extremo ao processo de apuração jornalística: o Departamento de Justiça registrara uma declaração juramentada no tribunal que acusava o chefe da redação da Fox News em Washington, James Rosen, de "cúmplice

de conspiração" com os supostos crimes de uma fonte, alegando que o jornalista havia "auxiliado e facilitado" a revelação de informações confidenciais pela fonte ao trabalhar junto com ela para receber o material.

Os jornalistas já vinham percebendo havia muitos anos que o governo Obama estava atacando de forma sem precedentes o processo de apuração, mas o caso Rosen foi uma escalada importante. Criminalizar a cooperação com uma fonte taxando-a de "auxílio e facilitação" é criminalizar o jornalismo investigativo em si: nenhum repórter jamais consegue dados secretos sem trabalhar com uma fonte para obtê-los. Esse clima havia tornado todos os advogados da mídia – incluindo os do *Guardian* – cautelosos em excesso, e até mesmo temerosos.

"Estão dizendo que o FBI pode entrar aqui, fechar a redação e confiscar nossos arquivos", disse-me Gibson.

Isso me pareceu ridículo: a simples ideia de que o governo dos Estados Unidos fosse fechar um jornal importante como o *The Guardian US* e fazer uma busca em sua redação era o tipo de conselho excessivamente receoso que, durante minha carreira no direito, me fizera aprender a detestar os alertas exagerados e pouco úteis dos advogados. Eu sabia, porém, que Gibson não iria – e não podia – ignorar aquelas advertências sem discussão.

"O que isso significa para o que estamos fazendo?", perguntei. "Quando vamos poder publicar?"

"Não sei, Glenn, não sei mesmo", respondeu ela. "Primeiro temos de entender tudo direitinho. Amanhã vamos encontrar os advogados de novo, e aí saberemos mais."

Fiquei muito preocupado. Não tinha a menor ideia de como os editores do *Guardian* iriam reagir. Minha independência no jornal e o fato de que eu havia assinado poucas matérias em que precisei consultá-los – e sem dúvida nada daquele calibre – significavam que eu estava lidando com variáveis desconhecidas. De fato, a história toda era *sui generis*: era impossível saber como qualquer pessoa iria reagir, porque nada como aquilo jamais acontecera. Será que os editores iriam se mostrar submissos e intimidados pelas ameaças dos Estados Unidos? Será que optariam por passar semanas negociando com o governo? Ou será que prefeririam deixar o *Post* dar o furo para se sentirem mais seguros?

Eu estava ansioso para publicar logo a matéria da Verizon: nós tínhamos o documento da FISA, e ele obviamente era genuíno. Não havia motivo algum para negar aos americanos, por mais um minuto que fosse, o direito de saber o que o governo estava fazendo com a sua privacidade. Também urgente era a obrigação que eu sentia em relação a Snowden. Sua decisão fora movida por um espírito de destemor, paixão e força. Para fazer justiça ao seu sacrifício, eu estava decidido a imbuir meu trabalho jornalístico do mesmo espírito. Apenas um jornalismo audacioso seria capaz de dar àquela notícia o poder de que ela precisava para suplantar o clima de medo imposto pelo governo aos jornalistas e suas fontes. Alertas paranoicos de advogados e a hesitação do *Guardian* eram a antítese dessa audácia.

Nessa noite, liguei para David e confessei minha preocupação crescente com o *Guardian*. Laura e eu também conversamos sobre minhas apreensões. Concordamos em dar ao jornal até o dia seguinte para publicar a primeira matéria e, caso isso não acontecesse, começaríamos a avaliar outras alternativas.

Algumas horas depois, Ewen MacAskill foi ao meu quarto para atualizar suas informações sobre Snowden, que ele ainda não havia conhecido. Compartilhei com Ewen minha preocupação com o

atraso.

– Não precisa se preocupar – disse ele sobre o jornal. – Eles são muito agressivos.

Ewen me garantiu que Alan Rusbridger, veterano editor-chefe do *Guardian* em Londres, estava "muito envolvido" e "comprometido com a publicação".

Embora eu ainda considerasse Ewen um acompanhante, seu desejo de publicar logo fez com que me sentisse melhor em relação à sua presença. Depois que ele saiu, contei a Snowden sobre como ele viajara conosco, referindo-me a ele como "a babá" do *Guardian*, e disse que gostaria que os dois se conhecessem no dia seguinte. Expliquei que obter o apoio de Ewen era um passo importante para deixar os editores do jornal suficientemente à vontade a ponto de publicar as matérias.

– Sem problemas – retrucou Snowden. – Mas você sabe que está sendo pajeado, foi por isso que eles o mandaram para cá.

Esse encontro foi muito importante. Na manhã seguinte, Ewen foi conosco até o hotel de Snowden e passou cerca de duas horas interrogando-o, fazendo-lhe muitas das mesmas perguntas que eu tinha feito na véspera.

– Como posso saber que você é mesmo quem diz ser? – indagou ele, no final. – Tem alguma prova disso?

Snowden sacou da mala um maço de documentos: seu passaporte diplomático já vencido, um antigo crachá da CIA, sua carteira de motorista e outros documentos de identidade oficiais.

Ewen e eu saímos juntos do quarto de hotel.

– Estou totalmente convencido de que ele está falando sério – afirmou Ewen. – Não tenho nenhuma dúvida. – Em sua opinião, não havia mais motivo algum para esperar. – Vou ligar para Alan assim que voltarmos ao hotel e dizer a ele que devemos começar a publicar agora mesmo.

Daí em diante, Ewen passou a ser parte integrante de nossa equipe. Snowden e Laura ficaram à vontade em sua presença, e tive de confessar que eu me sentia da mesma forma. Percebemos que nossas suspeitas anteriores não tinham qualquer fundamento: debaixo de um exterior afável e bem-educado havia um repórter destemido, ávido por dar continuidade àquela reportagem exatamente da forma que todos julgávamos necessária. Ewen, pelo menos na própria concepção, não estava ali para impor restrições institucionais, mas para praticar o jornalismo e às vezes para ajudar a superar essas restrições. Na realidade, durante nossa estadia em Hong Kong, a voz mais radical muitas vezes foi a dele, defendendo revelações que nem mesmo Laura e eu – ou Snowden, para ser sincero – tínhamos certeza de que deveriam ser feitas na ocasião. Logo percebi que aquela sua defesa de um estilo agressivo dentro do *Guardian* seria vital para garantir o apoio integral de Londres ao que estávamos fazendo, e foi.

Assim que o dia raiou em Londres, Ewen e eu ligamos juntos para Alan. Eu queria transmitir com a maior clareza possível que esperava – exigia, até – que o *Guardian* começasse a publicar naquele mesmo dia, além de querer ter uma noção clara da posição do jornal. Àquela altura – era apenas o segundo dia inteiro que eu passava em Hong Kong –, eu já estava comprometido comigo mesmo a publicar a notícia em outro lugar caso sentisse qualquer hesitação institucional substancial.

Fui direto ao assunto.

– Estou pronto para publicar a matéria sobre a Verizon, e não entendo mesmo por que não fazemos isso imediatamente – falei para Alan. – Que demora é essa?

Ele me garantiu que não havia demora alguma:

– Concordo. Estamos prontos para publicar. Janine só precisa fazer uma última reunião com os advogados hoje à tarde. Tenho certeza de que vamos publicar logo em seguida.

Falei sobre o envolvimento do *Post* na matéria sobre o PRISM, que só fazia aumentar minha sensação de urgência. Alan então me surpreendeu: ele não apenas queria ser o primeiro a publicar as matérias sobre a NSA de modo geral, mas também, obviamente ansioso para furar o *Post*, queria ser o primeiro a publicar especificamente a matéria do PRISM.

– Não temos motivo algum para deixar que eles nos furem – afirmou ele.

– Por mim, ótimo – aprovei.

Como Londres estava quatro horas à frente de Nova York, ainda demoraria um pouco para Janine chegar ao escritório, e mais ainda para ela se reunir com os advogados. Assim, convencido de que Rusbridger estava demonstrando toda a agressividade necessária, passei a noite em Hong Kong com Ewen dando os retoques finais na matéria do PRISM.

Terminamos o texto nesse mesmo dia e o enviamos por e-mail criptografado para Janine e Stuart Millar, em Nova York. Agora tínhamos dois grandes furos quentíssimos, prontos para serem publicados: a matéria da Verizon e a do PRISM. Minha paciência e minha disposição para esperar já estavam se esgotando.

Janine entrou na reunião com os advogados às três da tarde, horário de Nova York – três da manhã em Hong Kong –, e passou duas horas com eles. Fiquei acordado à espera do desfecho. Quando falasse com ela, queria ouvir apenas uma coisa: que iríamos publicar de imediato a matéria da Verizon.

Não foi nem de longe o que aconteceu. Ainda havia questões jurídicas "consideráveis" a serem resolvidas, disse-me ela. Uma vez solucionados esses pontos, o *Guardian* tinha de comunicar nossos planos a funcionários do governo para lhes dar a oportunidade de nos convencer a desistir de publicar – justamente o processo que eu detestava e condenava havia tanto tempo. Aceitei que o *Guardian* deixasse o governo tentar convencê-lo a não publicar, contanto que esse processo não se transformasse em alguma forma prolongada de adiar a matéria por várias semanas ou diluir seu impacto.

"Parece que faltam dias ou até semanas para publicarmos, não horas", escrevi para Janine, tentando concentrar toda a minha irritação e impaciência em um diálogo de chat. "Repito: vou tomar qualquer providência necessária para garantir que essa matéria seja publicada agora." Apesar de implícita, a ameaça era clara: se as matérias não saíssem de imediato no *Guardian*, eu procuraria outro veículo.

"Você já deixou sua posição bem clara quanto a isso", foi a resposta sucinta de Janine.

Já era final do dia em Nova York, e eu sabia que nada iria acontecer no mínimo antes do dia seguinte. Sentia-me frustrado e, àquela altura, muito ansioso. O *Post* estava preparando sua matéria sobre o PRISM, e Laura, que iria coassinar o texto, soubera por Gellman que o plano era publicarem no domingo, ou seja, dali a cinco dias.

Depois de conversar com David e Laura, percebi que não estava mais disposto a esperar pelo *Guardian*. Todos concordamos que eu deveria começar a explorar alternativas, para ter um plano B caso houvesse mais atrasos. Telefonemas para a *Salon* – que publicava meus textos havia muitos anos – e para o semanário *The Nation* logo renderam frutos. Ambos me responderam, em poucas horas, que estariam dispostos a publicar as matérias da NSA sem demora, e ofereceram todo o apoio de que eu pudesse precisar, com advogados a postos para liberar os textos no mesmo instante.

Saber que dois veículos tradicionais estavam dispostos a publicar as matérias da NSA – e ávidos para isso – foi encorajador, mas, quando conversei com David, concluímos que havia uma alternativa ainda mais poderosa: simplesmente criar nosso próprio site, batizado de NSAdisclosures.com (revelaçõesNSA.com), e começar a publicar as matérias ali, sem a necessidade de qualquer veículo de imprensa preexistente. Uma vez que divulgássemos que tínhamos em mãos um imenso tesouro de documentos secretos sobre a espionagem da NSA, seria fácil recrutar editores, advogados, pesquisadores e patrocinadores voluntários: uma equipe inteira motivada apenas pela paixão pela transparência e pelo verdadeiro jornalismo crítico, dedicada a noticiar o que sabíamos ser um dos vazamentos mais importantes da história dos Estados Unidos.

Desde o início, acreditei que aqueles documentos eram uma oportunidade de revelar não apenas a espionagem secreta conduzida pela NSA, mas também a dinâmica corrompida do jornalismo corporativo. Dar um dos furos mais importantes em muitos anos utilizando um modelo de reportagem novo, independente e sem vínculo com uma grande organização de mídia me parecia extremamente atraente. Isso sublinharia de forma enfática o fato de que a garantia da Primeira Emenda Constitucional norte-americana – a liberdade de imprensa – e a possibilidade de fazer um jornalismo importante não dependiam da filiação a um grande veículo de imprensa. A garantia de liberdade de imprensa não protege apenas os jornalistas corporativos, mas qualquer pessoa que pratique o jornalismo, esteja empregada ou não. Além disso, o destemor transmitido por uma atitude assim – *Nós vamos publicar milhares de documentos ultrassecretos da* NSA *sem a proteção de uma grande corporação de mídia* – encorajaria outros e ajudaria a acabar com o clima de medo então reinante.

Nessa noite, mais uma vez quase não dormi. Passei as primeiras horas da manhã em Hong Kong ligando para gente em cuja opinião confio: amigos, advogados, jornalistas, pessoas com quem trabalhei de perto. Todas me deram o mesmo conselho, que na realidade não me espantou: fazer uma coisa dessas sozinho, sem uma estrutura de mídia preexistente, era arriscado demais. Eu queria ouvir argumentos contrários a uma ação independente, e as pessoas com quem falei me deram vários, e bons.

No final da manhã, depois de escutar todas as ressalvas, tornei a ligar para David ao mesmo tempo que conversava on-line com Laura. Ele foi particularmente enfático ao afirmar que procurar a *Salon* ou o *Nation* seria demasiado cauteloso – "um passo para trás", segundo ele – e que, se o *Guardian* continuasse a demorar, apenas a publicação das matérias em um site recém-criado na internet poderia transmitir o espírito intrépido do jornalismo que desejávamos fazer. Assim como eu, ele estava convencido de que isso iria inspirar pessoas mundo afora. Laura também tinha a convicção de que dar um passo corajoso daqueles e criar uma rede global de indivíduos dedicados a garantir a transparência da NSA iria gerar uma gigantesca e poderosa onda de mobilização.

Assim, conforme a tarde em Hong Kong se aproximava, decidimos conjuntamente que, caso o *Guardian* não quisesse publicar antes do final daquele dia – que sequer havia começado na Costa Leste dos Estados Unidos –, eu romperia com eles e postaria imediatamente a matéria da Verizon em nosso novo site. Apesar de entender os riscos que isso acarretava, fiquei muito animado com nossa decisão. Sabia também que ter esse plano alternativo organizado me deixaria em posição bem mais forte nas conversas que teria naquele dia com o jornal. Sentia que não precisava continuar apegado a eles para dar aquelas notícias, e se libertar dos próprios apegos é sempre estimulante.

Nessa mesma tarde, quando falei com Snowden, contei-lhe sobre nosso plano.

"Arriscado. Mas corajoso", digitou ele. "Gostei."

Consegui dormir algumas horas, acordei no meio da tarde de Hong Kong e então me confrontei com o fato de que precisaria esperar muitas horas antes de a manhã de quarta-feira em Nova York começar. Sabia que, de uma forma ou de outra, daria um ultimato ao *Guardian*. Queria andar logo com aquilo.

Assim que vi Janine on-line, perguntei-lhe qual era o plano: "Vamos publicar hoje?"

"Espero que sim", retrucou ela. Sua incerteza me deixou nervoso. O *Guardian* ainda pretendia entrar em contato com a NSA naquela manhã para avisar sobre nossas intenções. Só depois da resposta deles é que saberíamos nosso calendário de publicação, disse ela.

"Não entendo por que vamos esperar", digitei, já sem paciência para os atrasos do jornal. "Para uma notícia limpa e direta como essa, quem se importa com o que eles acham que devemos ou não publicar?"

Tirando meu desprezo pelo processo em si, o governo não deveria colaborar com os jornais como parceiro editorial para determinar suas pautas. Eu sabia que não havia nenhum argumento de segurança nacional plausível contra aquela matéria específica sobre a Verizon, que tratava de uma simples ordem judicial mostrando a coleta sistemática de registros telefônicos da população norte-americana. A ideia de que "terroristas" iriam se beneficiar com a divulgação daquela ordem era risível: quaisquer terroristas com um mínimo de inteligência já sabiam que o governo tentava monitorar suas ligações. As pessoas que descobririam alguma coisa graças à nossa matéria não eram os "terroristas", mas sim a população dos Estados Unidos.

Repetindo o que ouvira dos advogados do jornal, Janine insistiu que eu estava partindo de um pressuposto equivocado se achava que o *Guardian* se deixaria intimidar a ponto de não publicar a matéria. Eles eram obrigados por lei a ouvir o que as autoridades tinham a dizer, afirmou ela. No entanto, garantiu, não se deixaria amedrontar nem fraquejaria diante de alegações vagas e irrisórias sobre segurança nacional.

Eu não estava partindo do princípio de que o jornal se deixaria intimidar; apenas não sabia o que iria acontecer. E temia que, no melhor dos casos, falar com o governo fosse provocar um atraso considerável. De fato, porém, o histórico de jornalismo agressivo e desafiador do *Guardian* fora um dos motivos que me levara a trabalhar para o jornal. Eu sabia que eles tinham o direito de mostrar na prática como iriam agir naquela situação, em vez de me deixar pressupor o pior. A declaração de independência de Janine me reconfortou um pouco.

"Tá bom", concordei, disposto a esperar para ver. "Mas vou dizer de novo: na minha opinião, a matéria tem que sair *hoje*. Não estou disposto a esperar mais."

Por volta de meio-dia, horário de Nova York, Janine me informou que eles tinham ligado para a NSA e para a Casa Branca e dito que pretendiam publicar material ultrassecreto. Só que ninguém havia retornado as ligações. Naquela manhã, a Casa Branca havia nomeado Susan Rice como a nova consultora de segurança nacional. O repórter que começara recentemente a cobrir segurança nacional para o *Guardian*, Spencer Ackerman, tinha bons contatos em Washington, e segundo ele o pessoal do governo estava "ocupado" com Susan Rice.

"Eles ainda não acham que têm de nos ligar de volta", escreveu Janine. "Mas logo vão descobrir que precisam retornar os meus telefonemas."

Às três da manhã – três da tarde em Nova York –, eu ainda não havia tido notícia nenhuma. Janine tampouco.

"Será que eles têm algum tipo de prazo determinado, ou vão ligar quando der na telha?", perguntei, com sarcasmo.

Ela respondeu que o *Guardian* tinha pedido uma resposta da NSA "antes do final do dia".

"E se eles não entrarem em contato até lá?", perguntei.

"Aí nós decidiremos o que fazer", retrucou ela.

Janine, então, acrescentou outro fator complicador: Alan Rusbridger, seu chefe, acabara de pegar um avião de Londres até Nova York para supervisionar a publicação das matérias sobre a NSA. Só que isso queria dizer que ele não estaria disponível durante as próximas sete horas ou algo assim.

"Você consegue publicar sem Alan?" Se a resposta fosse "não", não haveria a menor chance de a matéria sair naquele dia: o avião só chegaria ao JFK tarde da noite.

"Vamos ver", disse Janine.

Tive a sensação de que estávamos deparando exatamente com o tipo de barreira institucional ao jornalismo agressivo que eu entrara no *Guardian* para evitar: preocupações jurídicas. Consultas a funcionários do governo. Hierarquias institucionais. Aversão ao risco. Atrasos.

Pouco depois, mais ou menos às 3h15, Stuart Millar, subeditor de Janine em Nova York, mandou-me uma mensagem instantânea: "O governo retornou. Janine está falando com eles pelo telefone agora."

Esperei um tempo que me pareceu uma eternidade. Cerca de uma hora depois, Janine me ligou para contar o que tinha acontecido. Mais de dez altos funcionários de várias agências do governo haviam participado da ligação, incluindo integrantes da NSA, do Departamento de Justiça e da Casa Branca. No início, haviam se mostrado condescendentes mas simpáticos, dizendo que ela não compreendia nem o significado nem o "contexto" da ordem judicial relativa à Verizon. Queriam agendar uma reunião em "algum momento da semana seguinte" para explicar as coisas.

Quando Janine disse que queria publicar naquele mesmo dia, e que faria isso a menos que ouvisse motivos muito específicos e concretos para agir de outra forma, eles se tornaram mais belicosos, agressivos até. Disseram-lhe que ela não era uma "jornalista séria" e que o *Guardian* não era um "jornal sério", uma vez que se recusava a dar ao governo mais tempo para argumentar em prol da não publicação da matéria.

"Nenhum veículo de imprensa normal publicaria com tanta rapidez sem antes se reunir conosco", argumentaram, claramente tentando ganhar tempo.

É provável que estejam certos, lembro-me de ter pensado. E a questão era justamente essa. As regras hoje em vigor permitem ao governo controlar e neutralizar o processo de apuração jornalística, e eliminam a relação antagonística entre imprensa e poder público. Para mim, era vital que eles soubessem desde o início que aquelas normas corruptas não iriam se aplicar naquele caso. As matérias seriam publicadas com base em um conjunto de regras diferente que definiria uma imprensa independente, não subserviente.

Senti-me encorajado pelo tom de Janine: forte, desafiador. Ela reiterou que, apesar de ter pedido diversas vezes, as autoridades não haviam sido capazes de citar uma única maneira específica como a segurança nacional seria prejudicada pela publicação da matéria. No entanto, mesmo assim não se comprometeu a publicar naquele dia. Ao final da conversa, disse:

– Vou ver se consigo falar com Alan, aí decidimos o que fazer.

Esperei meia hora, então indaguei-lhe sem rodeios: "Vamos publicar hoje ou não? É só isso que eu quero saber."

Ela se esquivou da pergunta; não estava conseguindo entrar em contato com Alan. Estava claro que sua situação era muito difícil: de um lado, agentes do governo dos Estados Unidos acusando-a violentamente de temeridade; do outro, eu, fazendo exigências cada vez mais intransigentes. Para completar, o principal editor da publicação encontrava-se a bordo de um avião, ou seja, as decisões mais difíceis e com maiores consequências nos 190 anos de história do jornal dependiam unicamente dela.

Enquanto continuava on-line com Janine, não parei de falar ao telefone com David.

– Já são quase cinco da tarde – argumentou ele. – Foi esse o prazo que você deu a eles. Está na hora de tomar uma decisão. Eles têm que publicar agora, ou então você precisa dizer que está fora.

Ele tinha razão, mas mesmo assim hesitei. Sair do *Guardian* logo antes de publicar um dos maiores vazamentos de segurança nacional na história dos Estados Unidos iria provocar um enorme escândalo de mídia. Seria péssimo para a imagem do jornal, uma vez que eu teria de dar algum tipo de explicação pública, e isso por sua vez os levaria a se defender, sem dúvida me atacando: um verdadeiro caos, uma enorme distração que prejudicaria todos os envolvidos. E pior: tiraria o foco de onde este deveria estar, ou seja, nas revelações sobre a NSA.

Eu também precisava reconhecer meu medo pessoal: publicar centenas, talvez milhares, de documentos secretos da NSA já seria arriscado o suficiente, mesmo dentro de uma organização grande como o *Guardian*. Fazer isso sozinho, sem proteção institucional, multiplicaria exponencialmente o risco. Todas as advertências sensatas dos amigos e advogados que eu havia consultado não paravam de ecoar na minha cabeça.

Enquanto eu hesitava, David disse:

– Você não tem escolha. Se eles estiverem com medo de publicar, esse jornal não é o seu lugar. Você não pode agir por medo; se fizer isso, não vai conseguir nada. Foi essa a lição que Snowden acabou de lhe ensinar.

Juntos, redigimos o que eu diria a Janine na caixa de diálogo do chat: "Já são cinco da tarde, o prazo que dei a vocês. Se não publicarmos de imediato – na próxima meia hora –, meu contrato com o *Guardian* está encerrado." Quase cliquei em "enviar", mas então reconsiderei. O texto era uma ameaça explícita demais, praticamente um pedido de resgate. Se eu saísse do jornal naquelas circunstâncias, a história toda viria a público, inclusive aquela frase. Portanto, suavizei o tom: "Entendo que vocês tenham as suas preocupações e precisem fazer o que julgam certo. Eu também vou seguir em frente e cumprir o que acho que deve ser feito. Sinto muito que não tenha dado certo." Em seguida, cliquei em "Enviar".

Quinze segundos depois, o telefone do meu quarto de hotel tocou. Era Janine.

– Acho que você está sendo extremamente injusto – disse ela, claramente abalada.

Se eu saísse da jogada, o *Guardian*, que não tinha documento nenhum, perderia a reportagem toda.

– Acho que quem está sendo injusta é você – retruquei. – Já perguntei várias vezes quando o jornal pretende publicar, mas você se recusa a me dar uma resposta e fica só se esquivando de maneira dissimulada.

– Nós *vamos* publicar hoje. No máximo daqui a meia hora. Só estamos fazendo alguns ajustes finais, pondo títulos e formatando. A matéria vai sair no máximo às cinco e meia.

– Ok. Se o plano for esse, sem problemas – falei. – É claro que estou disposto a esperar mais meia hora.

Às 17h40, Janine me mandou uma mensagem instantânea com um link, aquele que eu passara dias esperando para ver. "Está no ar", escreveu ela.

"NSA faz coleta diária dos registros telefônicos de milhões de clientes da Verizon", dizia o título, seguido pelo subtítulo "Exclusivo: ordem judicial ultrassecreta obriga Verizon a ceder todos os dados telefônicos e revela a escala da vigilância doméstica do governo Obama".

Em seguida vinha um link para o texto integral da ordem judicial da FISA. Os primeiros três parágrafos de nossa matéria já contavam a história toda:

> A Agência de Segurança Nacional coleta atualmente os registros telefônicos de milhões de clientes norte-americanos da Verizon, uma das maiores operadoras de serviços de telecomunicações dos Estados Unidos, em cumprimento a uma ordem judicial ultrassecreta emitida em abril.
>
> Essa ordem, da qual o *Guardian* obteve uma cópia, exige que a empresa entregue à NSA, de forma "contínua e diária", informações sobre todas as chamadas realizadas em seu sistema, tanto dentro dos Estados Unidos quanto entre os Estados Unidos e outros países.
>
> O documento mostra, pela primeira vez, que no governo Obama os registros das comunicações de milhões de cidadãos estão sendo coletados de forma indiscriminada e generalizada, independentemente de eles serem suspeitos de alguma contravenção.

O impacto da matéria foi instantâneo, gigantesco, maior do que qualquer coisa que eu pudesse ter imaginado. Na mesma noite, a bomba encabeçou os noticiários televisivos dos Estados Unidos e dominou os debates políticos e jornalísticos. Fui soterrado com pedidos de entrevistas de quase todos os canais nacionais: CNN, MSNBC, NBC, os programas *Today Show* e *Good Morning America*, além de muitos outros. Passei horas em Hong Kong conversando com vários entrevistadores de TV que se mostraram solidários – experiência incomum durante minha carreira de jornalista político, na qual eu muitas vezes antagonizava a imprensa tradicional – e trataram a reportagem como um acontecimento importante e um verdadeiro escândalo.

Em resposta à publicação da matéria, o porta-voz da Casa Branca justificou de forma previsível o programa de coleta generalizada, qualificando-o de "ferramenta crítica para proteger o país de ameaças terroristas". A presidente democrata do Comitê de Inteligência do Senado, Dianne Feinstein, uma das maiores defensoras no Congresso do Estado de segurança nacional de forma geral e da vigilância norte-americana em particular, recorreu aos habituais argumentos que fomentam o medo típicos do pós-11 de Setembro e afirmou aos repórteres que o programa era necessário porque "a população quer que o seu país esteja seguro".

Mas quase ninguém levou a sério essas alegações. O *New York Times* publicou em seu editorial pró-Obama uma ácida denúncia ao governo. Em um texto intitulado "O arrastão do presidente Obama", o jornal afirmou: "O presidente Obama está provando o clichê de que o Executivo irá utilizar qualquer poder que lhe for conferido, e muito provavelmente abusar dele." Zombando da evocação automática de "terrorismo" usada pelo governo para justificar o programa, o editorial

afirmava que "a administração agora perdeu qualquer credibilidade". (Gerou alguma controvérsia o fato de o periódico, sem qualquer comentário, ter suavizado a denúncia horas depois da primeira publicação com o acréscimo da expressão "no que diz respeito a essa questão".)

O senador democrata Mark Udall divulgou um pronunciamento afirmando: "Esse tipo de vigilância generalizada deveria preocupar a todos nós e é o tipo de abuso do governo que eu disse que os americanos iriam considerar chocante." Segundo a ACLU (União Americana pelas Liberdades Civis), "do ponto de vista das liberdades civis, o programa não poderia ser mais alarmante... Mais do que orwelliano, é outra prova de quanto os direitos democráticos básicos estão sendo violados em segredo para suprir as demandas de agências de inteligência não submetidas a qualquer prestação de contas." O ex-vice-presidente Al Gore tuitou um link para a nossa matéria e a frase: "Sou só eu que acho ou a vigilância generalizada é mesmo um acinte obsceno?"

Logo depois que a matéria foi ao ar, a Associated Press confirmou, com base na declaração de um senador não identificado, aquilo de que nós já desconfiávamos: o programa de coleta em massa de registros telefônicos já durava anos e incluía não só a Verizon, mas todas as operadoras de telefonia norte-americanas.

Nos sete anos que passara escrevendo e falando sobre a NSA, eu nunca tinha visto nenhuma revelação produzir nada parecido com aquele nível de interesse e mobilização. Mas não havia tempo para analisar por que a notícia tivera tamanho impacto e provocara aquele maremoto de interesse e indignação; por ora, eu pretendia apenas surfar aquela onda, não tentar entendê-la.

Quando enfim acabei de dar as entrevistas para a televisão, por volta do meio-dia em Hong Kong, fui direto para o quarto de hotel de Snowden. Quando entrei, ele estava com a TV ligada na CNN. Convidados falavam sobre a NSA e se mostravam chocados com o alcance do programa de espionagem. Apresentadores se diziam indignados por tudo aquilo estar sendo feito em segredo. Quase todos aqueles convidados a se pronunciar condenavam a espionagem doméstica em massa.

– Está em todo lugar – disse Snowden, obviamente empolgado. – Assisti a todas as suas entrevistas. Todo mundo pareceu entender.

Nesse momento, tive uma genuína sensação de dever cumprido. O maior temor de Snowden – jogar a vida fora em troca de revelações que ninguém julgaria importantes – havia se mostrado infundado já no primeiro dia: não tínhamos visto qualquer sinal de indiferença ou apatia. Laura e eu o ajudáramos a iniciar justamente o debate que todos acreditávamos ser necessário e urgente, e eu agora podia vê-lo presenciar o desenrolar dos acontecimentos.

Como o plano dele era se identificar depois da primeira semana de matérias, ambos sabíamos que sua liberdade provavelmente iria terminar dali a bem pouco tempo. Para mim, a deprimente certeza de que ele logo começaria a ser atacado – caçado como um animal, se não enjaulado – era uma nuvem que pairava acima de tudo o que tínhamos feito. Isso não parecia incomodá-lo nem um pouco, mas me deixou determinado a fazer jus à sua escolha, a maximizar o valor das revelações que ele arriscara tudo para expor ao mundo. Tínhamos tido um bom começo, e aquilo era apenas o início.

– Todo mundo acha que essa é uma reportagem isolada, um furo avulso – observou Snowden. – Ninguém sabe que é só a ponta do iceberg e que tem muito mais coisa vindo por aí. – Ele se virou para mim. – O que vem agora, e quando vai sair?

– A matéria sobre o PRISM – respondi. – Amanhã.

Voltei ao meu quarto de hotel e, apesar de estar me aproximando da sexta noite sem dormir, simplesmente não consegui me desconectar. A adrenalina era potente demais. Às quatro e meia da tarde, como último recurso para descansar um pouco, tomei um sonífero e programei o despertador para as sete e meia da noite, horário no qual sabia que os editores do *Guardian* em Nova York começariam a ficar on-line.

Nesse dia, Janine se logou cedo. Parabenizamos um ao outro e trocamos impressões maravilhadas sobre a repercussão da matéria. Na mesma hora, ficou evidente que o tom do nosso diálogo havia mudado de forma radical. Nós tínhamos acabado de atravessar juntos um desafio jornalístico de grande porte. Janine estava orgulhosa da matéria, e eu estava orgulhoso por ela ter resistido às intimidações do governo e decidido publicá-la. O *Guardian* tinha feito a sua parte de forma destemida e admirável.

Embora na ocasião eu tenha achado que houve atrasos consideráveis, em retrospecto ficou claro que o jornal tinha agido com rapidez e ousadia notáveis, muito mais, tenho certeza, do que qualquer veículo de imprensa de tamanho e importância comparáveis teria feito. E Janine, nesse dia, foi clara ao afirmar que o *Guardian* não tinha qualquer intenção de descansar sobre os louros conquistados. "Alan está insistindo para publicarmos hoje mesmo a matéria sobre o PRISM", escreveu ela. Nada poderia ter me deixado mais feliz, claro.

O que tornava as revelações a respeito do PRISM tão importantes era que o programa permitia à NSA obter praticamente o que quisesse das empresas de internet que centenas de milhões de pessoas no mundo agora usavam como principal meio de comunicação. Isso fora possibilitado pelas leis implementadas pelo governo dos Estados Unidos após o 11 de Setembro, que conferiam à NSA poderes abrangentes para vigiar os cidadãos americanos e uma autorização quase ilimitada para conduzir uma vigilância indiscriminada de populações estrangeiras inteiras.

A Lei de Emendas FISA, de 2008, é hoje a legislação que rege a vigilância da NSA. Possibilitada por um Congresso bipartidário na esteira do escândalo dos grampos não autorizados da NSA na era Bush, um de seus principais resultados foi legalizar efetivamente os pontos cruciais do programa ilegal do ex-presidente. Como o escândalo revelou, Bush havia concedido uma autorização secreta à NSA para grampear cidadãos americanos e estrangeiros dentro dos Estados Unidos, justificada pela necessidade de identificar atividades terroristas. A ordem eliminou a necessidade de obter os mandados aprovados judicialmente em geral necessários para a espionagem doméstica, e resultou na vigilância secreta de no mínimo milhares de pessoas dentro do país.

Apesar de protestos alegando que o programa era ilegal, a lei de 2008 buscou institucionalizar o esquema, não encerrá-lo. Ela tem por base uma distinção entre "indivíduos dos Estados Unidos" (cidadãos norte-americanos e pessoas que estejam legalmente em território norte-americano) e todos os outros. Para ter como alvo as ligações ou os e-mails de um indivíduo dos Estados Unidos, a NSA precisa de um mandado específico do tribunal da FISA.

Para todas as outras pessoas, porém, onde quer que estejam, não é necessário nenhum mandado específico, mesmo que elas estejam se comunicando com indivíduos dos Estados Unidos. Pela seção 702 da lei de 2008, a NSA só precisa submeter uma vez por ano ao tribunal da FISA suas diretrizes gerais relativas aos alvos daquele ano – o critério exige apenas que a vigilância "auxilie a coleta legítima de inteligência estrangeira" – de modo a receber autorização geral para prosseguir. Depois que essas diretrizes recebem o carimbo de "aprovadas" do tribunal da FISA, a NSA pode eleger como

alvo de vigilância qualquer cidadão estrangeiro que quiser, e também obrigar empresas de telefonia e de internet a lhe dar acesso a todas as comunicações de qualquer pessoa não americana: chats do Facebook, e-mails do Yahoo!, buscas do Google. Não é preciso convencer o tribunal de que a pessoa é culpada de alguma coisa, nem mesmo de que existe motivo para desconfiar do alvo, e tampouco filtrar os indivíduos dos Estados Unidos que acabarem sendo vigiados pelo meio do caminho.

A primeira coisa que os editores do *Guardian* precisavam fazer era avisar o governo sobre nossa intenção de publicar a matéria do PRISM. Mais uma vez, nós lhes ofereceríamos um prazo até o final do dia, horário de Nova York. Isso lhes daria um dia inteiro para nos comunicar qualquer objeção, invalidando assim as inevitáveis reclamações de que não tinham tido tempo suficiente para replicar. No entanto, era igualmente crucial obter declarações das empresas que, segundo os documentos da NSA, haviam proporcionado à agência acesso a seus servidores dentro do programa PRISM: Facebook, Google, Apple, YouTube e Skype, entre outras.

Como precisava mais uma vez esperar muitas horas, voltei ao quarto de Snowden, onde Laura estava trabalhando com ele em várias frentes. Àquela altura, depois de ter cruzado uma fronteira significativa com a publicação da primeira revelação importante, ele já estava ficando visivelmente mais atento à própria segurança. Depois que entrei no aposento, pôs mais travesseiros para vedar a porta. Em vários momentos, quando queria me mostrar algo em seu computador, colocou um cobertor em cima da cabeça para impedir que câmeras no teto filmassem suas senhas. Quando o telefone tocou, nós três gelamos: quem poderia ser? Depois de vários toques, Snowden atendeu com bastante hesitação: era o setor de arrumação do hotel, que, ao ver o aviso de "não perturbe" pendurado na porta, estava entrando em contato para confirmar se ele não queria mesmo que fossem limpar o quarto.

– Não, obrigado – respondeu ele, sucinto.

O clima era sempre tenso quando nos reuníamos no quarto de Snowden, e isso se exacerbou depois que começamos a publicar. Não tínhamos a menor ideia se a NSA havia identificado a origem do vazamento. Caso houvesse, será que sabia onde Snowden estava? Será que agentes de Hong Kong ou da China sabiam? A qualquer momento, uma batida na porta daquele quarto poderia pôr um fim imediato e desagradável ao nosso trabalho conjunto.

Na televisão ligada ao fundo, alguém sempre parecia estar falando sobre a NSA. Após a publicação da matéria da Verizon, os noticiários praticamente só falavam em "coleta em massa e indiscriminada", "registros de ligações locais" e "abusos de vigilância". Enquanto discutíamos nossas próximas matérias, Laura e eu víamos Snowden assistir ao frenesi desencadeado por ele.

Então, às duas da manhã, horário de Hong Kong, quando a matéria do PRISM estava prestes a ir ao ar, Janine entrou em contato.

"Aconteceu uma coisa muito esquisita", disse ela. "As empresas de tecnologia estão negando com veemência as informações contidas nos documentos da NSA. Insistem que nunca ouviram falar no programa PRISM."

Pensamos nas possíveis explicações para esse desmentido. Talvez os documentos da NSA superestimassem as capacidades da agência. Talvez as empresas de tecnologia estivessem simplesmente mentindo, ou as pessoas entrevistadas não tivessem conhecimento do acordo de suas empregadoras com a NSA. Podia ser também que PRISM fosse apenas um codinome interno à NSA, jamais comunicado às companhias.

Qualquer que fosse a explicação, tínhamos que reescrever nossa matéria, não apenas para incluir os desmentidos, mas para mudar o foco e enfatizar a estranha disparidade entre os documentos da NSA e a postura das empresas de internet.

"Não vamos tomar partido em relação a quem está certo, vamos apenas expor o desacordo e deixar a questão se resolver em público", sugeri. Nossa intenção era que a matéria forçasse um debate aberto sobre o que o setor da internet havia concordado em fazer com as comunicações de seus usuários; caso a sua versão fosse conflitante com os documentos da NSA, os envolvidos teriam de resolver a situação com o mundo inteiro observando, como deve ser.

Janine concordou, e duas horas depois me mandou a nova versão preliminar da matéria sobre o PRISM. O título era:

Programa PRISM da NSA coleta dados de usuários da Apple, Google e outras empresas

- Programa ultrassecreto afirma ter acesso direto aos servidores de empresas como Google, Apple e Facebook
- Empresas negam qualquer conhecimento do programa, em curso desde 2007

Após citar os documentos da NSA que descreviam o PRISM, a matéria observava: "Embora o texto afirme que o programa funciona com o auxílio das empresas, todos os que responderam ao pedido de comentários feito pelo *Guardian* na quinta-feira negaram saber da existência de qualquer programa desse tipo." A matéria me pareceu ótima, e Janine garantiu que estaria no ar dali a meia hora.

Enquanto eu aguardava, impaciente, os minutos passarem, ouvi o som que indicava o recebimento de uma mensagem no chat. Torci para que fosse uma confirmação de Janine de que a matéria tinha saído. A mensagem de fato era dela, mas não a que eu esperava.

"O *Post* acabou de soltar a matéria deles sobre o PRISM", digitou.

O quê? Perguntei-me por que o *Post* havia mudado de repente seu cronograma e adiantado a matéria em três dias.

Laura logo soube por Barton Gellman que o jornal descobrira nossa intenção depois que funcionários do governo dos Estados Unidos foram procurados pelo *Guardian* naquela manhã para falar sobre o PRISM. Ciente de que o *Post* estava preparando uma reportagem parecida, uma dessas pessoas passara adiante a informação de que pretendíamos publicar uma notícia sobre o mesmo assunto. O *Post*, então, acelerara seus planos para não ser furado.

Eu agora detestava ainda mais aquele processo deliberativo: um funcionário do governo dos Estados Unidos havia explorado esse procedimento prévio à publicação, supostamente destinado a proteger a segurança nacional, para garantir que seu jornal preferido publicasse a matéria antes.

Uma vez absorvida a informação, reparei em uma explosão no Twitter sobre a matéria do PRISM publicada pelo *Post*. Quando fui ler os tuítes, porém, vi que faltava uma coisa: a discrepância entre a versão da NSA e as declarações das empresas de internet.

Intitulada "Inteligência dos Estados Unidos e da Grã-Bretanha coleta dados de nove empresas norte-americanas de internet em amplo programa secreto", a matéria afirmava que "a Agência de Segurança Nacional e o FBI estão acessando diretamente os servidores centrais de nove das maiores

empresas de internet dos Estados Unidos para obter chats de áudio e vídeo, fotos, e-mails, arquivos e logs de conexão que permitam aos analistas rastrear alvos estrangeiros". Mais significativamente, contudo, o texto afirmava que as nove empresas "participam de forma consciente das operações do PRISM".

Nossa matéria sobre o mesmo assunto foi ao ar dez minutos depois, com um foco bem diferente e um tom mais cauteloso, enfatizando os veementes desmentidos das empresas de internet.

A reação, mais uma vez, foi explosiva. E, além disso, internacional. Ao contrário das operadoras de telefonia como a Verizon, em geral baseadas em um só país, os gigantes da internet são globais. Bilhões de pessoas no mundo inteiro – em nações de todos os continentes – usam o Facebook, o Gmail, o Skype e o Yahoo! como principal meio de comunicação. Saber que essas empresas tinham feito acordos secretos com a NSA para dar acesso às comunicações de seus clientes foi um choque de dimensão mundial.

E agora as pessoas já estavam começando a desconfiar que a primeira matéria sobre a Verizon não era um evento isolado: juntas, as duas reportagens sugeriam um vazamento sério da NSA.

A publicação da matéria sobre o PRISM marcou o último dia em muitos meses no qual consegui ler, que dirá responder, todos os e-mails que recebi. Ao percorrer minha caixa de entrada, vi o nome de quase todos os maiores veículos de imprensa do mundo solicitando entrevistas: o debate mundial que Snowden queria provocar havia realmente começado, e isso depois de apenas dois dias de matérias. Pensei na imensa e valiosa coleção de documentos que ainda estavam por vir, no que isso iria significar para minha vida, no impacto que teria no mundo e em como o governo dos Estados Unidos reagiria quando entendesse o que estava enfrentando.

Em um replay da véspera, passei as primeiras horas da manhã em Hong Kong participando de programas televisivos do horário nobre nos Estados Unidos. Assim criou-se o padrão que adotei durante toda a estadia em Hong Kong: preparar matérias com o *Guardian* durante a noite, dar entrevistas à imprensa durante o dia, depois ir encontrar Laura e Snowden no quarto de hotel dele.

Várias vezes percorri Hong Kong de táxi às três ou quatro da manhã rumo a estúdios de televisão, sem jamais esquecer as instruções de "segurança operacional" de Snowden: nunca me separar do laptop nem dos pen drives cheios de documentos, para impedir manipulações ou furtos. Percorria as ruas desertas da cidade com minha mochila pesada sempre grudada nas costas, fosse qual fosse o local ou o horário. Combati a paranoia a cada passo do caminho, mas em muitos momentos me peguei olhando por cima do ombro e apertando um pouco mais a mochila junto ao corpo quando alguém se aproximava.

Terminada a bateria de entrevistas, eu voltava ao quarto de Snowden, onde ele, Laura e eu – agora às vezes acompanhados por McCaskill – continuávamos a trabalhar, parando apenas para dar uma olhada na TV. Ficamos assombrados com a reação positiva, com a aparente solidez do compromisso da imprensa com as revelações, e com a raiva exibida pela maioria dos comentaristas não com aqueles que haviam possibilitado a transparência, mas com o extraordinário nível de vigilância estatal que tínhamos denunciado.

Eu agora me sentia capaz de implementar uma das estratégias que pretendíamos usar: reagir de forma desafiadora, ou mesmo com desdém, à tática manipuladora do governo de evocar o 11 de Setembro como justificativa para sua espionagem. Comecei a denunciar as acusações batidas e previsíveis de que tínhamos posto em risco a segurança nacional, de que estávamos ajudando o

terrorismo, de que havíamos cometido um crime ao revelar segredos nacionais.

Senti-me corajoso o bastante para argumentar que essas eram estratégias óbvias e manipuladoras de autoridades que haviam sido flagradas cometendo atos que as constrangiam e prejudicavam sua reputação. Esses ataques não iriam frear nosso trabalho, e continuaríamos a publicar muitas outras matérias baseadas naqueles documentos, indiferentes a ameaças e atitudes que fomentassem o medo, cumprindo nosso dever de jornalistas. Queria que aquilo ficasse bem claro: a intimidação e a demonização de sempre não iriam funcionar. Nada nos impediria de seguir noticiando. Apesar dessa postura desafiadora, a maior parte da mídia demonstrou apoio ao nosso trabalho nesses primeiros dias.

Fiquei surpreso com isso porque, sobretudo desde o 11 de Setembro (embora antes também), a imprensa norte-americana em geral havia demonstrado um ultranacionalismo agressivo e uma lealdade extrema ao governo, sendo, portanto, hostil – às vezes, cruelmente hostil – com qualquer um que revelasse os seus segredos.

Quando o WikiLeaks começou a publicar documentos confidenciais relacionados às guerras no Iraque e no Afeganistão, em especial despachos diplomáticos, os próprios jornalistas norte-americanos lideraram o movimento que pedia a condenação do site, o que por si só já é um comportamento espantoso. A própria instituição pretensamente dedicada a tornar transparentes os atos dos poderosos não apenas denunciava como tentava criminalizar um dos mais importantes atos de transparência em muitos anos. O que o WikiLeaks fez – receber informações confidenciais de uma fonte oficial para depois revelá-las ao mundo – é, em essência, o mesmo que as organizações de mídia vivem fazendo.

Eu imaginava que a imprensa norte-americana fosse direcionar sua hostilidade para mim, sobretudo quando continuamos a publicar as matérias e o escopo inédito do vazamento começou a se evidenciar. Na condição de crítico feroz do jornalismo tradicional e de muitos de seus membros mais importantes, eu seria, calculei, um ímã natural para esse tipo de agressividade. Tinha poucos aliados na mídia tradicional, e esta era composta sobretudo por pessoas que eu havia atacado publicamente, de maneira frequente e implacável. Portanto, supunha que eles fossem se virar contra mim na primeira oportunidade, mas aquela primeira semana de participações na mídia foi um verdadeiro festival de amor, e não só enquanto eu estava no ar.

Na quinta-feira, meu quinto dia em Hong Kong, quando cheguei ao quarto de Snowden, ele me disse na hora que tinha uma notícia "um pouco alarmante". Um equipamento de segurança conectado à internet da casa em que ele morava com a namorada de longa data no Havaí havia detectado que duas pessoas da NSA – um funcionário de recursos humanos e um "agente de polícia" da agência – tinham ido até lá à sua procura.

Snowden tinha quase certeza de que isso significava que a NSA o identificara como a fonte provável dos vazamentos, mas eu me mostrei cético.

– Se eles achassem que você fez isso, mandariam hordas de agentes do FBI com mandados de busca, e provavelmente equipes da SWAT, não um único funcionário da NSA e alguém de recursos humanos.

Calculei que aquilo fosse apenas uma investigação de rotina, pro forma, acionada quando um empregado da NSA falta algumas semanas ao trabalho sem dar explicação. Snowden, contudo, sugeriu que eles talvez estivessem sendo discretos de propósito, para evitar atrair a atenção da mídia

ou acarretar alguma tentativa de destruir indícios.

O que quer que aquela notícia significasse, ela ressaltava a necessidade de preparar rapidamente nossa matéria e o vídeo que identificaria Snowden como a fonte do vazamento. Fazíamos questão de que o mundo ouvisse falar pela primeira vez nele, em suas ações e em seus motivos de sua própria boca, e não por meio de uma campanha de demonização propalada pelo governo dos Estados Unidos enquanto ele estivesse escondido ou preso, sem poder falar por si.

Nosso plano era publicar mais duas matérias, uma no dia seguinte, sexta, e outra no sábado. No domingo, então, soltaríamos um longo artigo sobre Snowden acompanhado de uma entrevista em vídeo e um bate-bola impresso com ele a ser conduzido por Ewen.

Laura havia passado as 48 horas anteriores editando as imagens de minha primeira entrevista com Snowden, mas disse que o material era detalhado, longo e fragmentado demais para poder ser usado. Queria filmar logo outra entrevista, mais concisa e focada, e elaborou uma lista com cerca de vinte perguntas específicas para que eu lhe fizesse. Enquanto ela montava a câmera e nos indicava onde sentar, acrescentei várias outras.

O vídeo agora famoso começa assim: "Ahn... meu nome é Ed Snowden. Tenho 29 anos. Trabalho para a Booz Allen Hamilton como analista de infraestrutura terceirizado para a NSA no Havaí."

Snowden prosseguiu com respostas sucintas, estoicas e racionais a cada pergunta: por que decidira vazar aqueles documentos? Por que aquilo era tão importante para ele a ponto de levá-lo a sacrificar a própria liberdade? Quais eram as revelações mais importantes? Os documentos denunciavam algo criminoso ou ilegal? O que ele imaginava que iria lhe acontecer?

Conforme ia dando exemplos de vigilância ilegal e invasiva, Snowden começou a se mostrar mais animado e arrebatado. Foi só quando lhe perguntei se ele esperava alguma repercussão que demonstrou preocupação, pois temia que o governo, como retaliação, começasse a visar sua família e sua namorada. Para reduzir esse risco, falou, evitaria entrar em contato com eles, mas sabia que não poderia protegê-los totalmente. "Esta é a única coisa que me tira o sono: pensar no que vai acontecer com eles", afirmou, com os olhos marejados; foi a primeira e única vez que vi isso acontecer.

Enquanto Laura editava o vídeo, Ewen e eu terminamos nossas duas matérias seguintes. A terceira denunciava uma diretriz presidencial ultrassecreta, assinada pelo presidente Obama em novembro de 2012, ordenando ao Pentágono e a outras agências correlatas que se preparassem para uma série de operações cibernéticas ofensivas e agressivas mundo afora. "Altos funcionários de segurança nacional e inteligência", explicava o primeiro parágrafo do texto, foram solicitados a "elaborar uma lista de alvos estrangeiros potenciais para ciberataques norte-americanos, como revela uma diretriz presidencial ultrassecreta obtida pelo *Guardian*".

A quarta matéria, publicada no sábado conforme o planejado, era sobre o BOUNDLESS INFORMANT, programa de rastreamento de dados da NSA, e descrevia os relatórios que mostravam como a agência vinha coletando, analisando e armazenando *bilhões* de chamadas telefônicas e e-mails obtidos da estrutura norte-americana de telecomunicações. O texto também questionava se funcionários da NSA tinham mentido para o Congresso ao se recusarem a revelar a senadores o número de comunicações domésticas interceptadas, alegando que não mantinham esse tipo de registro nem tinham capacidade para reunir esses dados.

Depois de publicada a matéria sobre o BOUNDLESS INFORMANT, Laura e eu tínhamos combinado nos encontrar no quarto de hotel de Snowden. Antes de sair do meu quarto, porém, do

nada, enquanto estava sentado na cama, lembrei-me de Cincinnatus, meu correspondente eletrônico anônimo de seis meses antes, que havia me bombardeado com e-mails pedindo que eu instalasse o programa de criptografia PGP para poder me passar informações importantes. Em meio ao entusiasmo por todos aqueles acontecimentos, pensei que talvez ele também tivesse algo importante a me revelar. Sem conseguir me lembrar de seu endereço de e-mail, finalmente localizei uma de suas mensagens fazendo uma busca por palavras-chave.

"Oi. Boas notícias", escrevi. "Sei que demorou, mas enfim estou usando um e-mail PGP. Então estou pronto para conversar quando você quiser, se ainda estiver interessado." Cliquei em "Enviar".

Pouco depois que cheguei ao seu quarto, Snowden falou, com um quê de gozação na voz:

– Aliás, aquele tal de Cincinnatus para quem você acabou de escrever sou eu.

Levei alguns instantes para processar a informação e recuperar a compostura. Aquela pessoa que muitos meses antes havia tentado desesperadamente me fazer começar a usar a criptografia em meus e-mails... era Snowden. Meu primeiro contato com ele não acontecera em maio, um mês antes, mas fora muito anterior a isso. Antes de procurar Laura para falar sobre os vazamentos, antes de procurar qualquer pessoa, ele havia tentado entrar em contato comigo.

Dia após dia, as muitas horas que nós três passávamos juntos iam criando um vínculo cada vez mais forte. O constrangimento e a tensão de nosso primeiro encontro logo se transformaram em uma relação de colaboração, confiança e objetivo comum. Sabíamos que tínhamos embarcado juntos em um dos acontecimentos mais importantes de nossa vida.

No entanto, depois de publicada a matéria do BOUNDLESS INFORMANT, o astral relativamente descontraído que conseguíramos manter ao longo dos dias anteriores deu lugar outra vez a uma ansiedade palpável: faltavam menos de 24 horas para revelarmos a identidade de Snowden, e sabíamos que isso mudaria tudo – especialmente para ele. Nós três tínhamos compartilhado uma experiência curta, mas muito intensa e gratificante. E um de nós seria, em breve, retirado do grupo e sem dúvida despachado para a prisão por muito tempo, um fato que pairava no ar de modo deprimente desde o início, tornando o clima pesado, ao menos para mim. Apenas Snowden parecera imune a esse fato. Agora, um humor negro nervoso começava a se insinuar em nossa interação.

"Eu fico com a cama de baixo do beliche em Guantanamo", brincava ele ao imaginar o que iria nos acontecer. Enquanto conversávamos sobre matérias futuras, Snowden dizia coisas do tipo "Isso aí vai entrar na acusação. Só resta saber se na sua ou na minha". Na maior parte do tempo, ele manteve uma calma inimaginável. Mesmo então, com seu tempo de liberdade cada vez mais perto de se esgotar, continuava indo para a cama às dez e meia, como tinha feito todas as noites desde que eu chegara a Hong Kong. Enquanto eu mal conseguia dormir duas horas seguidas, e tinha sempre um sono agitado, ele mantinha uma rotina regular. "Bom, vou deitar", dizia de forma casual todas as noites antes de se retirar para sete horas e meia de sono profundo e reaparecer no dia seguinte, totalmente descansado.

Quando lhe perguntamos sobre sua capacidade de dormir tão bem naquelas circunstâncias, ele respondeu que sentia uma paz profunda em relação ao que tinha feito, e que portanto era fácil dormir à noite.

– Imagino que me restem muito poucos dias com um travesseiro confortável, então é melhor aproveitar – brincou.

No domingo à tarde, horário de Hong Kong, Ewen e eu demos os retoques finais na matéria que apresentaria Snowden ao mundo enquanto Laura terminava de editar o vídeo. Falei com Janine, que entrou no chat de manhã cedo em Nova York, sobre a importância fundamental de tratar aquela notícia com cuidado e sobre meu sentimento de obrigação pessoal com Snowden para fazer jus às suas escolhas. Eu passara a confiar cada vez mais nos meus colegas do *Guardian*, tanto do ponto de vista editorial quanto por sua coragem. Nesse caso, porém, quis verificar cada modificação, por menor que fosse, no texto que revelaria Snowden ao mundo.

Algum tempo depois naquela tarde em Hong Kong, Laura foi ao meu quarto para mostrar o vídeo a Ewen e a mim. Nós três assistimos a ele em silêncio. O trabalho estava excelente – o vídeo era sóbrio e a edição, brilhante –, mas sua força vinha sobretudo de ouvir Snowden falar por si. Ele transmitia de forma muito coerente a convicção, a paixão e o poder do comprometimento que o tinham levado a agir. Sua coragem de aparecer e reivindicar o que tinha feito, de assumir a responsabilidade por seus atos, sua recusa em se esconder e ser caçado, tudo isso, eu sabia, iria inspirar milhões de pessoas.

Mais do que tudo, eu queria que o mundo visse o destemor de Snowden. Ao longo da última década, o governo dos Estados Unidos se esforçara muito para demostrar um poder sem limites. Havia começado guerras, torturado e prendido pessoas sem acusação, usado drones para bombardear alvos em atentados não autorizados pela justiça. E os mensageiros não haviam ficado imunes: delatores tinham sido molestados e processados, e jornalistas, ameaçados de prisão. Por meio de uma demonstração de intimidação cuidadosamente sustentada a qualquer um que cogitasse uma contestação expressiva, o governo se esforçara para mostrar à população mundial que seu poder não era limitado pelas leis, pela ética, pela moralidade ou pela Constituição: *vejam o que podemos e vamos fazer com quem atrapalhar nossos propósitos.*

Snowden havia desafiado essa intimidação da maneira mais direta possível. A coragem é algo contagioso. Eu sabia que ele poderia inspirar muitas outras pessoas a agirem da mesma forma.

No dia 9 de junho, um domingo, às duas da tarde no horário da Costa Leste dos Estados Unidos, o *Guardian* publicou a matéria que apresentava Snowden ao mundo: "Edward Snowden: o delator responsável pelas revelações sobre a vigilância da NSA". No alto da reportagem estava o vídeo de doze minutos feito por Laura, e o texto começava assim: "O responsável por um dos vazamentos mais importantes da história política dos Estados Unidos chama-se Edward Snowden, tem 29 anos, é ex-assistente de tecnologia da CIA e atual funcionário da Booz Allen Hamilton, prestadora de serviços na área de defesa." A matéria trazia sua biografia, enumerava suas motivações e afirmava: "Snowden vai entrar para a história como um dos delatores mais importantes dos Estados Unidos, ao lado de Daniel Ellsberg e Bradley Manning." Citava também o texto que ele mostrara logo no início a Laura e a mim: "Entendo que serei obrigado a responder pelos meus atos, [mas] ficarei satisfeito se o conluio de leis secretas, perdão desigual e poderes executivos ilimitados que governa o mundo que amo for desmascarado, nem que seja por um único instante."

A reação provocada pela matéria e pelo vídeo foi mais explosiva do que qualquer outra coisa que eu já vivenciara como jornalista. O próprio Ellsberg, em um texto publicado pelo *Guardian* no dia seguinte, afirmou que "jamais houve, em toda a história dos Estados Unidos, vazamento mais importante do que a revelação do material da NSA por Edward Snowden – nem mesmo, seguramente, os Documentos do Pentágono, quarenta anos atrás".

Só nos primeiros dias, centenas de milhares de pessoas postaram o link para a matéria em seus perfis no Facebook. Quase 3 milhões de pessoas assistiram à entrevista no YouTube, e muitas outras no site do *Guardian*. A reação predominante era de assombro e inspiração com a coragem de Snowden.

Ele, Laura e eu acompanhamos juntos a repercussão da revelação de sua identidade, enquanto eu também avaliava, junto com dois estrategistas de mídia do *Guardian*, quais entrevistas televisivas deveria aceitar fazer na manhã de segunda-feira. Optamos pelo programa *Morning Joe*, da MSNBC, seguido pelo *Today Show*, da NBC – os dois primeiros a irem ao ar, que dariam o tom da cobertura do caso ao longo do dia.

Antes que eu pudesse dar as entrevistas, porém, fomos distraídos por um telefonema: às cinco da manhã – poucas horas depois de publicada a matéria sobre Snowden –, um leitor meu muito antigo que mora em Hong Kong e com quem eu havia me comunicado periodicamente ao longo da semana me ligou. Afirmou que o mundo inteiro logo estaria à procura de Snowden em Hong Kong e insistiu que ele precisava, com urgência, arrumar advogados influentes na cidade. Estava com dois dos melhores advogados de direitos humanos de prontidão, dispostos a representá-lo. Será que os três podiam ir ao meu hotel naquele mesmo instante?

Combinamos nos encontrar pouco tempo depois, por volta das oito. Dormi por algumas horas até que ele ligou, uma hora antes, às sete.

– Já estamos aqui no lobby do seu hotel – falou. – Estou com os dois advogados. Aqui está lotado de câmeras e jornalistas. A imprensa está procurando o hotel de Snowden e não vai demorar a encontrar, e os advogados estão dizendo que é fundamental falarem com ele antes dos jornalistas.

Ainda meio dormindo, vesti as primeiras roupas que consegui encontrar e fui cambaleando até a porta. Assim que a abri, os flashes de várias câmeras dispararam na minha cara. A horda de repórteres com certeza devia ter pago algum funcionário do hotel para conseguir o número do meu quarto. Duas mulheres se identificaram como repórteres do *Wall Street Journal* baseadas em Hong Kong; outros, inclusive um cinegrafista com uma câmera bem grande, eram da Associated Press.

Eles formaram um semicírculo à minha volta, sabatinando-me enquanto eu caminhava até o elevador. Entraram na cabine junto comigo, metralhando perguntas; respondi à maioria delas com monossílabos sucintos, secos e pouco informativos.

No lobby, um novo enxame de câmeras e jornalistas se juntou ao grupo. Tentei procurar meu leitor e os advogados, mas não conseguia avançar meio metro sem que algum repórter entrasse na minha frente.

Fiquei particularmente preocupado que aquela multidão tentasse me seguir e impedisse o acesso dos advogados a Snowden. Por fim, decidi dar uma coletiva improvisada ali mesmo, no lobby, e responder às perguntas para que os jornalistas fossem embora. Depois de uns quinze minutos, a maioria de fato se dispersou.

Senti, então um grande alívio ao esbarrar com Gill Phillips, principal advogada do *Guardian*, que tinha feito escala em Hong Kong em uma viagem da Austrália para Londres a fim de prestar assessoria jurídica a Ewen e a mim. Ela disse que queria explorar todos os modos possíveis de o *Guardian* proteger Snowden. "Alan faz questão de que o jornal dê a ele todo o apoio que puder legalmente", falou. Tentamos conversar mais, porém não conseguimos ter privacidade, pois alguns dos repórteres continuavam rondando.

Enfim consegui localizar meu leitor e os dois advogados de Hong Kong que o acompanhavam. Tentamos arrumar um jeito de nos falar sem sermos seguidos e acabamos todos no quarto de Gill. Batemos a porta na cara do punhado de jornalistas que ainda nos seguia.

Fomos direto ao assunto. Os advogados queriam falar com Snowden com urgência e obter sua permissão formal para que o representassem, quando então poderiam começar a agir em seu nome.

Gill fazia pesquisas frenéticas pelo celular para investigar aqueles advogados que acabáramos de conhecer antes de lhes entregar Snowden. Ela conseguiu descobrir que eles eram mesmo bastante conhecidos e experientes na área de direitos humanos e asilo a refugiados, e pareciam muito bem relacionados politicamente em Hong Kong. Enquanto Gill realizava sua pesquisa improvisada, entrei no programa de chat. Tanto Snowden quanto Laura estavam on-line.

Laura, agora hospedada no mesmo hotel que Snowden, tinha certeza de que era só uma questão de tempo até que os repórteres descobrissem a localização deles também. É claro que ele estava ansioso para sair de lá. Contei-lhe sobre os advogados dispostos a ir até seu quarto e Snowden disse que eles deveriam ir buscá-lo e levá-lo para um lugar seguro. Estava "na hora de começar a parte do plano em que eu peço ao mundo proteção e justiça", falou.

"Só que eu preciso sair do hotel sem ser reconhecido pelos jornalistas", prosseguiu. "Caso contrário, eles simplesmente vão me seguir para onde eu for."

Transmiti essa preocupação aos advogados.

– Ele tem alguma ideia para evitar isso? – indagou um deles.

Fiz a pergunta a Snowden.

"Estou tomando providências para mudar de aparência", respondeu ele. Ficou claro que já tinha pensado naquilo. "Posso me tornar irreconhecível."

Àquela altura, pensei que os advogados e Snowden deveriam se falar diretamente. Antes disso, ele precisava recitar uma frase formal sobre aceitar ser representado por eles a partir dali. Mandei a frase para ele, que a digitou de volta para mim. Os advogados então assumiram meu lugar no computador e começaram a falar com ele.

Dali a dez minutos, anunciaram que estavam a caminho do hotel de Snowden para encontrá-lo quando ele tentasse sair sem ser visto.

– O que vocês pretendem fazer com ele depois? – perguntei.

Eles provavelmente o levariam à missão da ONU em Hong Kong e pediriam a proteção formal da organização contra o governo dos Estados Unidos, alegando que Snowden era um refugiado pedindo asilo. Senão, disseram, tentariam arrumar um "esconderijo".

Mas como conseguir tirar os advogados do hotel sem que ninguém os seguisse? Bolamos um plano: eu sairia do quarto com Gill e desceria até o lobby para convencer os jornalistas ainda acampados em frente à nossa porta a me seguirem. Os advogados, então, aguardariam alguns minutos e iriam embora do hotel, com sorte sem atrair atenção.

O estratagema deu certo. Depois de conversar por meia hora com Gill em um shopping anexo ao hotel, tornei a subir para meu quarto e, ansioso, liguei para o celular de um dos advogados.

– Conseguimos tirá-lo pouco antes de os jornalistas começarem a invadir o lobby – contou ele. – Nós o encontramos em seu quarto, aí atravessamos uma passarela até um shopping anexo ao hotel. – Em frente à sala com o jacaré onde Snowden tinha nos encontrado pela primeira vez, como descobri depois. – Então entramos no nosso carro, que já estava lá. Ele está conosco agora.

Para onde eles iriam levá-lo?

– É melhor não falarmos sobre isso pelo telefone – respondeu o advogado. – Ele vai estar seguro, por enquanto.

Fiquei profundamente aliviado ao saber que Snowden estava em boas mãos, mas nós sabíamos que havia uma grande chance de nunca mais o vermos nem falarmos com ele, pelo menos não enquanto ele fosse um homem livre. O mais provável, pensei, era que o víssemos da próxima vez na TV, em um tribunal dos Estados Unidos, usando o macacão laranja de um presidiário americano e com os pés e mãos acorrentados, sendo indiciado por acusações de espionagem.

Enquanto eu digeria a notícia, alguém bateu na minha porta. Era o gerente geral do hotel, avisando que não paravam de receber ligações para o meu quarto (eu deixara instruções na recepção para que todas as chamadas fossem bloqueadas). Havia também uma multidão de jornalistas, fotógrafos e cinegrafistas no lobby esperando que eu aparecesse.

– Se o senhor quiser, pode deixar o hotel usando um elevador dos fundos e uma saída que ninguém vai ver – sugeriu ele. – E a advogada do *Guardian* fez uma reserva em outro hotel com um nome diferente, se for de sua preferência.

Na língua dos gerentes de hotel, aquilo obviamente significava: *nós queremos que o senhor saia daqui por causa do caos que está gerando*. Eu sabia que aquilo era mesmo uma boa ideia: eu gostaria de continuar a trabalhar com alguma privacidade, e ainda tinha esperanças de manter contato com Snowden. Assim, fiz as malas, segui o gerente pela saída dos fundos, encontrei Ewen me esperando dentro de um carro e me registrei em outro hotel usando o nome da advogada do *Guardian.*

A primeira coisa que fiz foi me conectar à internet, torcendo para ter notícias de Snowden. Vários minutos depois, ele entrou on-line.

"Está tudo bem", escreveu. "Estou em um lugar seguro, por enquanto. Só não sei quão seguro, nem quanto tempo vou passar aqui. Vou ter que ficar mudando de lugar e meu acesso à internet é precário, então não sei quando nem com que frequência vou estar logado."

Ele estava claramente relutante em dar qualquer detalhe sobre sua localização, e eu tampouco perguntei. Tinha consciência de que a minha capacidade de me envolver no processo de escondê-lo era muito limitada. Snowden era agora o homem mais procurado pelo governo mais poderoso do mundo. Os Estados Unidos já haviam solicitado às autoridades de Hong Kong que o prendessem e entregassem aos americanos.

Assim, nossa conversa foi curta e vaga, e ambos expressamos o desejo de manter contato. Eu lhe disse para se cuidar.

Quando enfim cheguei ao estúdio para as entrevistas do *Morning Joe* e do *Today Show*, reparei no mesmo instante que o teor das perguntas tinha sofrido uma mudança dramática. Em vez de me tratarem como jornalista, as apresentadoras preferiram atacar um novo alvo: o próprio Snowden, agora foragido em Hong Kong. Muitos jornalistas norte-americanos tornaram a assumir seus papéis habituais de vassalos do governo. A notícia não era mais como jornalistas tinham exposto sérios abusos da NSA, mas como um americano que trabalhava para o governo tinha "traído" suas obrigações, cometido crimes e depois "fugido" para a China.

Minhas entrevistas para ambas as apresentadoras – Mika Brzezinski e Savannah Guthrie – foram pungentes, amargas. Sem dormir havia mais de uma semana, não tive paciência para as críticas

veladas a Snowden contidas em suas perguntas; na minha opinião, os jornalistas deveriam estar comemorando, não crucificando alguém que dera mais transparência ao Estado de segurança nacional do que qualquer outra pessoa em muitos anos.

Depois de mais alguns dias de entrevistas, decidi que estava na hora de ir embora de Hong Kong. Era óbvio que agora seria impossível encontrar ou mesmo ajudar Snowden na cidade, e àquela altura eu já estava totalmente exausto física, emocional e psicologicamente. Estava louco para voltar ao Rio.

Pensei em retornar por Nova York e ficar lá por um ou dois dias dando entrevistas, só para deixar bem claro que podia fazê-lo e que o faria. No entanto, um advogado me demoveu da ideia, argumentando que não fazia sentido correr riscos legais desse tipo antes de sabermos como o governo dos Estados Unidos planejava reagir.

– Você acabou de facilitar o maior vazamento de segurança nacional da história dos Estados Unidos, e apareceu na televisão com a mensagem mais desafiadora possível – disse ele. – Só faz sentido planejar uma ida ao país quando tivermos ideia de qual vai ser a resposta do Departamento de Justiça.

Eu discordava: achava muito improvável que o governo Obama fosse prender um jornalista no meio de uma reportagem tão em evidência. Mas estava exausto demais para discutir ou correr o risco. Assim, pedi ao *Guardian* que me pusesse em um voo para o Rio passando por Dubai, bem longe dos Estados Unidos. Por ora, pensei, o que eu tinha feito bastava.

3

COLETAR TUDO

O acervo de documentos reunido por Edward Snowden era espantoso tanto pelo tamanho quanto pela abrangência. Mesmo depois de anos escrevendo sobre os perigos da vigilância secreta norte-americana, fiquei muito chocado com a vastidão do sistema de espionagem, e mais ainda por ele ter sido claramente implementado quase sem qualquer prestação de contas, transparência ou limite.

Os milhares de programas de vigilância distintos descritos por aquele acervo não tinham sido previstos para ir a público por quem os implementara. Muitos tinham por alvo a população dos Estados Unidos, mas dezenas de países mundo afora – inclusive democracias em geral vistas como aliadas dos Estados Unidos, como França, Brasil, Índia e Alemanha – também eram alvo de uma vigilância em massa indiscriminada.

Apesar da organização elegante, o tamanho e a complexidade do acervo de Snowden tornavam-no muito difícil de explorar. As dezenas de milhares de documentos da NSA que continha haviam sido produzidas por quase todos os setores e subdivisões dessa vasta agência, e também faziam parte dele arquivos de agências de inteligência de países estrangeiros aliados próximos dos Estados Unidos. Os documentos surpreendiam pelas datas recentes: 2011 e 2012 na maioria, 2013 em muitos casos. Alguns chegavam a ter datas de março e abril de 2013, poucos meses antes de conhecermos Snowden em Hong Kong.

Grande parte dos documentos do acervo tinha a classificação *top secret*, "ultrassecreto". Destes, a maioria estava assinalada pelo acrônimo "FVEY", ou seja, só tinha aprovação para circular entre os quatro aliados de vigilância mais próximos da NSA, a aliança dos Cinco Olhos (*Five Eyes*), formada com os países de língua inglesa Grã-Bretanha, Canadá, Austrália e Nova Zelândia. Outros, ainda, só podiam ser lidos por norte-americanos (marcados como "NOFORN", acrônimo de *no foreign distribution*, "sem distribuição no exterior"). Alguns documentos, como a ordem judicial da FISA que permitia a coleta de registros telefônicos e a diretriz da administração Obama que ordenava a preparação de operações cibernéticas ofensivas, estavam entre os segredos mais bem guardados do governo dos Estados Unidos.

Decifrar esse acervo e o idioma da NSA pressupunha uma curva de aprendizagem acentuada. Tanto nas comunicações internas quanto com parceiros, a agência usa uma linguagem própria, idiossincrática, um jargão burocrático e rígido, embora ocasionalmente fanfarrão ou até mesmo irritadiço. A maioria dos documentos era também bastante técnica, recheada de acrônimos e codinomes medonhos, e às vezes, para entendê-los, era necessária a leitura prévia de outros documentos.

Snowden tinha previsto esse problema e providenciado glossários de acrônimos e nomes de programas, além de dicionários internos da agência que esclareciam termos específicos ao ofício. Mesmo assim, alguns documentos eram incompreensíveis à primeira, segunda ou mesmo terceira leitura. Seu significado só se revelava depois que eu relacionava partes diferentes de outros documentos

e consultava alguns dos maiores especialistas mundiais em vigilância, criptografia, hacking, história da NSA e na estrutura jurídica que rege a espionagem norte-americana.

Para dificultar ainda mais, a montanha de documentos muitas vezes estava organizada não por tema, mas segundo o departamento da agência no qual haviam se originado, e revelações importantíssimas estavam misturadas a grandes quantidades de material banal ou altamente técnico. Embora o *Guardian* tenha criado um programa que permitia efetuar buscas por palavra-chave no interior dos arquivos, que foi bastante útil, a ferramenta estava longe de ser perfeita. O processo de assimilação do acervo foi lento e árduo, e, muitos meses após recebermos os documentos, alguns termos e programas ainda exigiam uma apuração mais ampla antes de poderem ser revelados de forma segura e coerente.

Apesar desses problemas, porém, os arquivos de Snowden expunham de maneira inquestionável uma complexa teia de vigilância de cidadãos tanto americanos (explicitamente fora do escopo da missão da NSA) quanto não americanos. O acervo revelava os recursos técnicos usados para interceptar comunicações: o monitoramento, pela agência, de servidores de internet, satélites, cabos de fibra óptica submarinos, sistemas de telefonia nacionais e estrangeiros e computadores pessoais. Identificava indivíduos escolhidos para serem alvo de formas de espionagem invasivas ao extremo, lista que ia de supostos terroristas e suspeitos de crimes a líderes democraticamente eleitos de aliados dos Estados Unidos e até mesmo cidadãos norte-americanos comuns. E mostrava quais eram as estratégias e os objetivos gerais da NSA.

Snowden tinha posto no início do acervo os documentos mais cruciais e abrangentes, assinalando sua importância especial. Esses arquivos revelavam o extraordinário alcance da agência, bem como sua ação dissimulada e até mesmo criminosa. Uma das primeiras revelações desse tipo foi o programa BOUNDLESS INFORMANT, que mostra como a NSA contabiliza com exatidão matemática todas as chamadas e todos os e-mails coletados todos os dias no mundo inteiro. Snowden tinha colocado esses documentos em uma posição tão proeminente não só porque eles quantificavam o volume de ligações e e-mails coletados e armazenados – bilhões por dia, literalmente –, mas também porque provavam que o diretor da NSA, Keith Alexander, e outros funcionários da agência tinham mentido para o Congresso nacional. Em mais de uma ocasião, autoridades da NSA tinham afirmado serem incapazes de fornecer números específicos – justo os dados que o BOUNDLESS INFORMANT fora concebido para coletar.

No período de um mês a partir de 8 de março de 2013, por exemplo, um slide do BOUNDLESS INFORMANT mostrava que uma única unidade da NSA, chamada Global Access Operations (Operações de Acesso Global, GAO na sigla em inglês), tinha coletado dados sobre mais de 3 bilhões de chamadas telefônicas e e-mails que haviam transitado pelo sistema de telecomunicações norte-americano. ("DNR", ou "Dialed Number Recognition", "reconhecimento de número discado", refere-se a chamadas telefônicas; "DNI", ou "Digital Network Intelligence", "inteligência de rede digital", refere-se a comunicações feitas via internet, como e-mails.) Esse número excedia coletas nos sistemas da Rússia, do México e de quase todos os países da Europa, e equivalia mais ou menos ao total de dados coletado na China.

No geral, em apenas trinta dias, a unidade coletara dados sobre mais de 97 bilhões de e-mails e 124 bilhões de chamadas do mundo inteiro. Outro documento do BOUNDLESS INFORMANT oferecia detalhes dos dados coletados em um único período de trinta dias na Alemanha (500

milhões), Brasil (2,3 bilhões) e Índia (13,5 bilhões). Outros arquivos mostravam, ainda, a coleta de metadados em parceria com os governos francês (70 milhões), espanhol (60 milhões), italiano (47 milhões), holandês (1,8 milhão), norueguês (33 milhões) e dinamarquês (23 milhões).

BOUNDLESS INFORMANT

De cima para baixo, da esquerda para a direita: Visão geral (últimos 30 dias) / Total de DNI / Total de DNR / SIGADs (Designador de Atividade de Inteligência de Sinais) / Notações de caso / Sistemas de processamento / Cinco principais países (últimos 30 dias) / TOTAL / VISÃO DE PAÍSES / Estados Unidos

Apesar de o foco definido pelos estatutos da NSA ser "inteligência estrangeira", os documentos confirmavam que o público norte-americano era um alvo igualmente importante da vigilância secreta. Nada deixava isso mais claro do que a ordem ultrassecreta de 25 de abril de 2013 do tribunal da FISA exigindo que a Verizon entregasse à NSA todas as informações sobre as ligações de seus clientes norte-americanos, os "metadados de telefonia". A linguagem usada na ordem judicial (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 1), marcada como "NOFORN", era ao mesmo tempo clara e definitiva:

POR ESTA SE ORDENA que o Responsável pelos Registros apresente à Agência de Segurança Nacional (NSA), ao receber esta Ordem, e continue a apresentar em um regime constante e diário a partir de então, enquanto vigorar esta Ordem, a menos que o Tribunal emita Contraordem, uma cópia eletrônica dos seguintes objetos tangíveis: todos os registros de detalhes de ligações, ou "metadados de telefonia", gerados pela Verizon para comunicações (i) entre os Estados Unidos e o exterior, e (ii) internas às fronteiras dos Estados Unidos, incluindo as ligações locais.

Os metadados de telefonia incluem informações exaustivas sobre roteamento

de comunicações, que incluem, mas não se limitam a, informações de identificação da sessão (por exemplo, número de telefone de origem e destino da chamada, identidade internacional de usuário de telefone celular [IMSI], identidade internacional de equipamento de estação móvel [IMEI], etc.), identificador de tronco, números de cartões telefônicos e horário e duração da chamada.

Esse programa de coleta em massa de dados de telefonia foi uma das descobertas mais significativas em um acervo recheado com todo tipo de programa secreto de vigilância – desde a larga escala do PRISM (que envolvia a obtenção de dados diretamente dos servidores das maiores empresas de internet do mundo) e do PROJECT BULLRUN ("projeto corrida de touros", esforço conjunto da NSA e de sua contraparte no Reino Unido, a Central de Comunicações do Governo, para burlar as formas mais corriqueiras de criptografia usadas para garantir a segurança das transações na internet) até empreitadas de menor escala, com nomes que refletem o espírito desdenhoso e fanfarrão da supremacia responsável por sua implementação: EGOTISTICAL GIRAFFE ("girafa egomaníaca"), cujo alvo é o navegador Tor, destinado a permitir a navegação anônima na internet; MUSCULAR ("musculoso"), que torna possível invadir as redes pessoais do Google e do Yahoo!; e OLYMPIA, o programa canadense destinado a vigiar o Ministério das Minas e Energia brasileiro.

Parte da vigilância era dedicada, de maneira ostensiva, a suspeitos de terrorismo. No entanto, é claro que uma porcentagem importante dos programas nada tinha a ver com segurança nacional. Os documentos não deixavam dúvidas de que a NSA praticava também espionagem econômica e diplomática, além da vigilância de populações inteiras sem qualquer base para suspeita.

Considerado em sua totalidade, o acervo de Snowden levava, em última instância, a uma conclusão bem simples: o governo dos Estados Unidos construíra um sistema cujo objetivo é a completa eliminação da privacidade eletrônica no mundo inteiro. Longe de ser uma hipérbole, esse é o objetivo literal e explicitamente declarado do Estado de vigilância: coletar, armazenar, monitorar e analisar todas as comunicações eletrônicas de todas as pessoas ao redor do mundo. A agência se dedica a uma única missão maior: evitar que qualquer comunicação eletrônica, por mais ínfima que seja, fuja ao seu alcance sistemático.

Essa missão autoimposta exige uma expansão contínua do alcance da NSA. Todos os dias, a agência trabalha para identificar comunicações eletrônicas que não estejam sendo coletadas e armazenadas, e então desenvolve novas tecnologias e métodos para retificar essa falha. Em sua visão, ela não precisa de nenhuma justificativa específica para colher comunicações eletrônicas pessoais, nem de qualquer motivo para considerar determinado alvo suspeito. O objetivo da NSA é o que a agência chama de SIGINT: *all signals intelligence*, "inteligência de todos os sinais". E o simples fato de que ela, sozinha, tenha capacidade para coletar essas comunicações tornou-se a explicação racional para fazê-lo.

Braço do Pentágono, a NSA é a maior agência de inteligência do mundo, e grande parte de seu trabalho de vigilância é conduzida pela aliança dos Cinco Olhos. Até a primavera de 2014, quando a

controvérsia provocada pelas revelações de Snowden se intensificou, a agência era dirigida pelo general Keith B. Alexander, que durante seu mandato de nove anos ampliou de forma agressiva seu tamanho e sua influência. Ao fazer isso, Alexander se transformou no que o jornalista James Bamford descreveu como "o mais poderoso chefe de inteligência da história dos Estados Unidos".

A NSA "já era um gigante dos dados quando Alexander assumiu o comando", observou o jornalista da revista *Foreign Policy* Shane Harris, "mas sob a sua batuta o escopo, a escala e a ambição de sua missão se expandiu além de qualquer coisa sequer imaginada por seus predecessores". Nunca antes "uma agência governamental norte-americana tivera capacidade ou autorização judicial para coletar e armazenar tantas informações eletrônicas". Um ex-funcionário administrativo que trabalhou com o diretor da NSA disse a Harris que a "estratégia de Alexander" era clara: "Preciso obter todos os dados." Além disso, acrescentou Harris, "ele quer conservar esses dados pelo máximo de tempo possível".

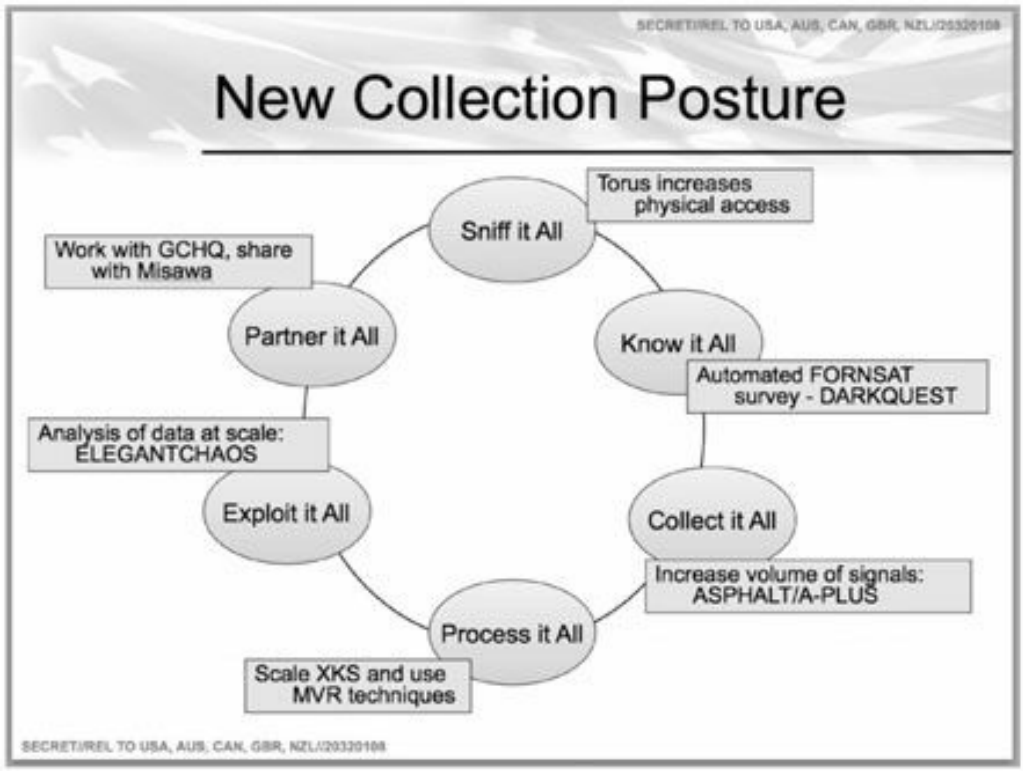
A máxima pessoal de Alexander, "Coletem tudo", transmite com perfeição o objetivo principal da NSA. Ele começou a pôr em prática essa filosofia em 2005, durante a coleta de dados de inteligência relacionados à ocupação do Iraque. Conforme o *Washington Post* noticiou em 2013, Alexander ficou insatisfeito com o foco limitado da inteligência militar norte-americana, direcionada apenas a suspeitos de insurgência e outras ameaças às forças armadas dos Estados Unidos, abordagem que o recém-nomeado diretor da NSA considerava demasiado restritiva. "Ele queria tudo: todas as mensagens de texto, todos os telefonemas e e-mails iraquianos que pudessem ser sugados pelos potentes computadores da agência." Assim, o governo lançou mão, de forma indiscriminada, de métodos de tecnologia para coletar todos os dados de comunicação da população iraquiana inteira.

Alexander, então, teve a ideia de aplicar esse sistema de vigilância onipresente – originalmente concebido para uma população estrangeira em uma zona de conflito ativo – aos cidadãos norte-americanos. "Assim como no Iraque, ele fez muita pressão para obter tudo o que fosse possível: ferramentas, recursos e autorização legal para coletar e armazenar enormes quantidades de informações brutas sobre comunicações norte-americanas e estrangeiras", afirmou o *Post*. Desse modo, "nos oito anos que passou no comando da agência de vigilância eletrônica nacional, Alexander, 61 anos, encabeçou de forma discreta uma revolução na capacidade do governo de coletar informações em nome da segurança nacional".

A reputação de Alexander como fanático por vigilância é amplamente documentada. Ao descrever sua "faina descontrolada e quase ilegal de construir a máquina de espionagem mais potente do mundo", a *Foreign Policy* o chamou de "caubói da NSA". Segundo a revista, até mesmo o chefe da CIA e da NSA na era Bush, general Michael Hayden – que supervisionou pessoalmente a implementação do programa ilegal de grampos não autorizados do ex-presidente e é conhecido por seu militarismo agressivo –, muitas vezes tinha "engulhos" diante da abordagem sem limites de Alexander. Um ex-alto funcionário de inteligência caracterizou assim suas opiniões: "Não vamos nos preocupar com a lei. Vamos nos preocupar em como fazer o trabalho." No mesmo viés, o *Post* observou que "até mesmo os defensores de Alexander consideram que sua agressividade às vezes o levou a ultrapassar os limites de sua autoridade legal".

Embora algumas das declarações mais extremadas de Alexander – como a pergunta incisiva "Por que não podemos coletar todos os sinais o tempo todo?", supostamente feita por ele durante uma visita em 2008 à Central de Comunicações do Governo, organização britânica – tenham sido

descartadas por porta-vozes da agência como simples piadas sem importância tiradas de contexto, documentos da própria NSA demonstram que Alexander não estava brincando. Uma apresentação ultrassecreta feita na conferência anual dos Cinco Olhos em 2011, por exemplo, mostra que a NSA abraçou de forma explícita a máxima de Alexander de ter a onisciência como seu principal objetivo:

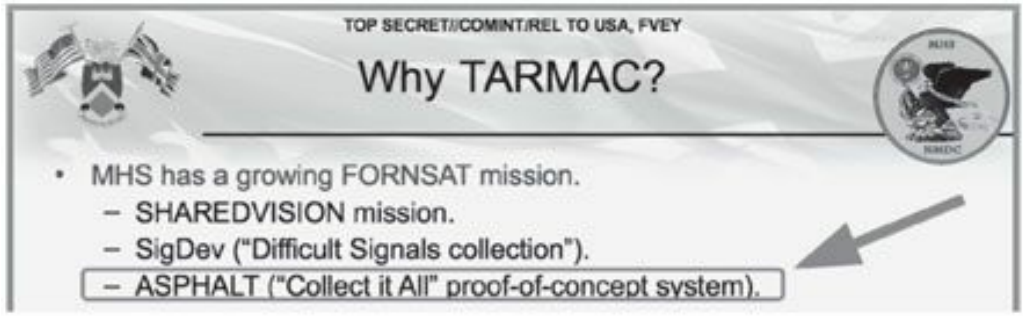


NOVA POSTURA DE COLETA

Ovais no sentido horário desde cima: Farejar tudo / Saber tudo / Coletar tudo / Processar tudo / Explorar tudo / Dividir tudo com parceiros

Retângulos no sentido horário: Torus aumenta o acesso físico / Levantamento automatizado FORNSAT – DARKQUEST / Aumentar volume de sinais: ASPHALT/A-PLUS / Ajustar escala do XKS e usar técnicas MVR / Análise dos dados na escala: ELEGANTCHAOS / Trabalhar com a Central de Comunicações do Governo (GCHQ), compartilhar com Misawa

Um documento de 2010 apresentado pela Central de Comunicações do Governo na conferência dos Cinco Olhos – referente ao seu programa ativo de interceptação de comunicações por satélite, cujo codinome é TARMAC, "asfalto" – deixa claro que a agência de espionagem britânica também usa a mesma expressão para descrever sua missão:



POR QUE O TARMAC?

A missão de FORNSAT da MHS está cada vez maior / Missão SHAREDVISION / SigDev ("coleta de sinais difíceis") / ASPHALT (sistema-modelo "coletar tudo").

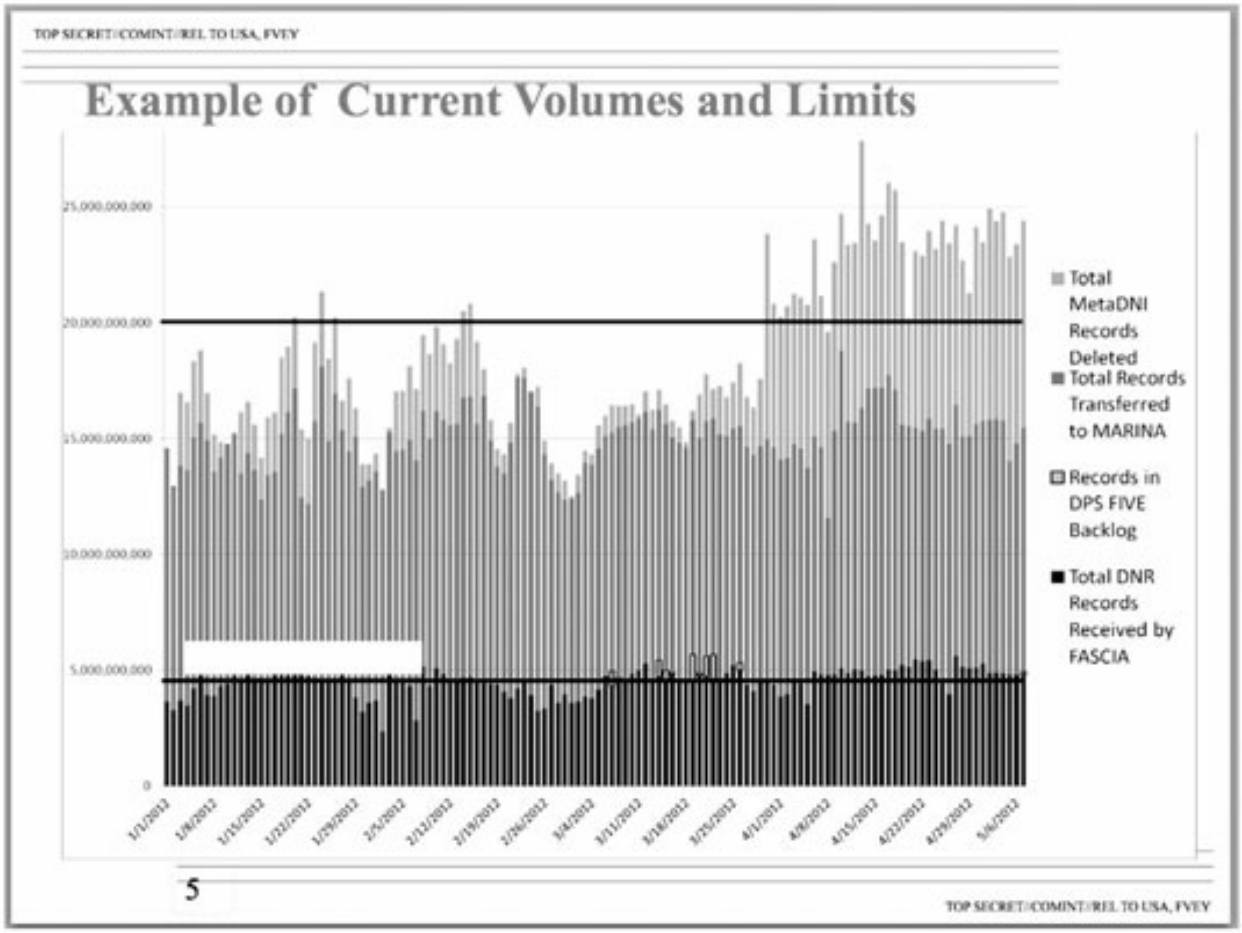
Até mesmo memorandos internos de rotina da NSA evocam esse bordão para justificar a expansão das capacidades da agência. Um memorando de 2009 do diretor de tecnologia da divisão Operações de Missão da NSA, por exemplo, tece elogios a melhorias recentes no posto de coleta da agência em Misawa (MSOC), no Japão (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 2):

Planos para o futuro (U)

(TS//SI//REL) No futuro, a MSOC espera expandir o número de plataformas WORDGOPHER para permitir a desmodulação de milhares de outros provedores de rede menores.

Esses alvos são ideais para a desmodulação de software. Além disso, a MSOC desenvolveu a habilidade de escanear e desmodular automaticamente os sinais à medida que eles são ativados nos satélites. Há inúmeras possibilidades, o que deixa nossa missão um passo mais perto de "coletar tudo".

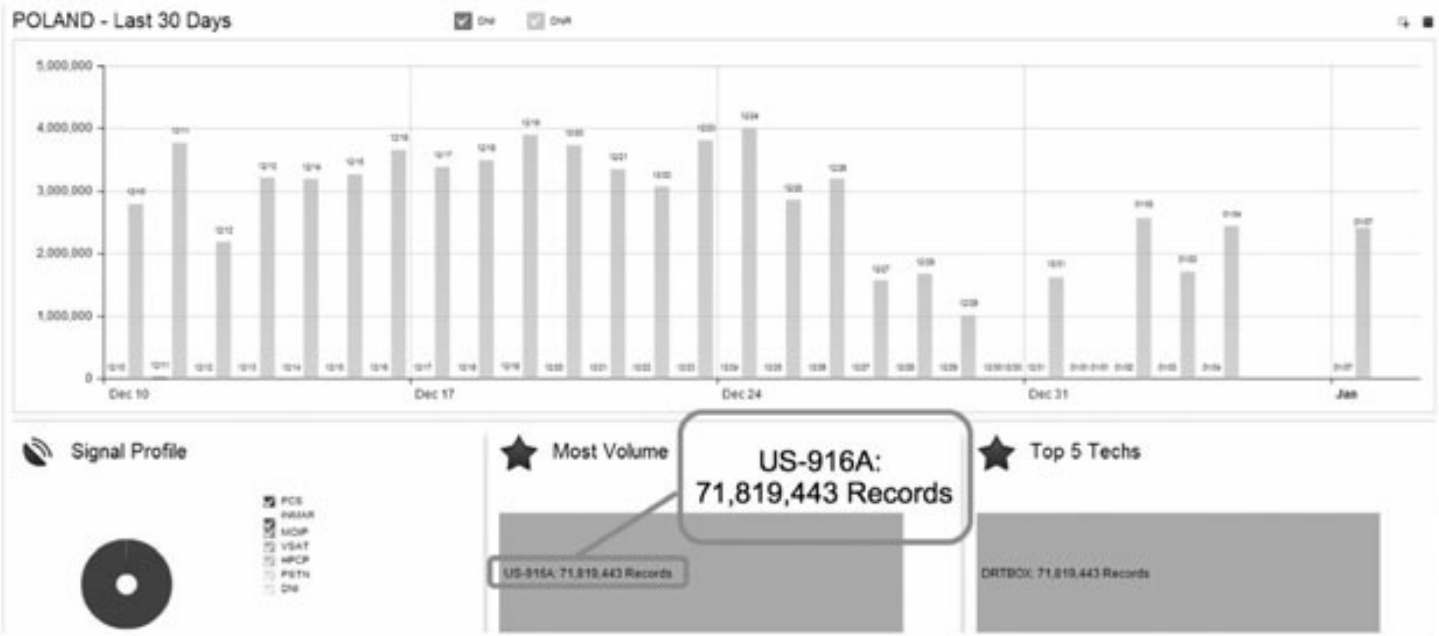
Longe de ser uma brincadeira sem importância, "coletar tudo" define a aspiração da NSA, e é um objetivo que ela está cada vez mais próxima de alcançar. O total de telefonemas, e-mails, chats, atividades de navegação e metadados de telefonia coletados pela agência é espantoso. De fato, como afirma um documento de 2012, com frequência "a quantidade de conteúdo coletada é muito superior àquela em geral útil para os analistas". Em meados de 2012, a agência estava processando mais de 20 bilhões de ocorrências de comunicação (tanto de internet quanto de telefonia) no mundo inteiro *a cada dia*:



EXEMPLO DE VOLUMES E LIMITES ATUAIS

Legenda, de cima para baixo: Total de registros MetaDNI deletados / Total de registros transferidos para MARINA / Registros armazenados no backlog do DPS FIVE / Total de registros DNR recebidos por FASCIA

Para cada país, a NSA também gera um total parcial diário que quantifica o número de ligações e e-mails coletados; o gráfico abaixo, referente à Polônia, mostra mais de 3 milhões de ligações em determinados dias, e um total de 71 milhões no período de trinta dias:



POLÔNIA – ÚLTIMOS 30 DIAS

Da esquerda para a direita: Perfil de sinais / Maior volume / US-916A: 71.819.443 registros / Cinco maiores tecnologias / DRTBOX 71.819.443 registros

O total coletado pela NSA nos próprios Estados Unidos é igualmente assustador. Mesmo antes das revelações de Snowden, o *Washington Post* noticiou, em 2010, que "todos os dias, sistemas de coleta da Agência Nacional de Segurança interceptam e armazenam 1,7 bilhão de e-mails, telefonemas e outros tipos de comunicação" de cidadãos norte-americanos. William Binney, um matemático que trabalhou para a NSA por três décadas e se demitiu na esteira do 11 de Setembro em protesto contra o foco cada vez mais doméstico da agência, também fez inúmeras declarações sobre a quantidade de dados coletada nos Estados Unidos. Em uma entrevista concedida em 2012 ao programa de TV *Democracy Now!*, Binney declarou que "eles reuniram algo em torno de 20 trilhões de interações de cidadãos norte-americanos com outros cidadãos norte-americanos".

Depois das revelações de Snowden, o *Wall Street Journal* noticiou que o sistema de interceptação global da NSA "tem capacidade para alcançar aproximadamente 75% de todo o tráfego interno dos Estados Unidos na busca por inteligência estrangeira, o que inclui uma grande quantidade de comunicações entre estrangeiros e americanos". Em declarações anônimas, funcionários atuais e antigos da agência disseram ao *Journal* que, em alguns casos, a NSA "guarda o conteúdo escrito de e-mails trocados por cidadãos dentro do país, além de filtrar ligações domésticas feitas por meio de tecnologia da internet".

De modo semelhante, a Central de Comunicações do Governo da Grã-Bretanha também coleta uma quantidade tão grande de dados relativos a comunicações que mal consegue armazenar o que já tem. Como diz um documento preparado pelos britânicos em 2011:

SABER O QUE TEMOS – UM GUIA

A Central de Comunicações do Governo tem amplo acesso a comunicações de internet internacionais / Recebemos mais de 50 *bilhões* de ocorrências *por dia* (e esse número está aumentando)

A fixação da NSA por coletar tudo é tamanha que o acervo de Snowden é permeado por memorandos comemorativos internos celebrando determinado marco de coleta. Esta mensagem de intranet de dezembro de 2012, por exemplo, observa orgulhosamente que o programa SHELLTRUMPET processou seu trilionésimo registro (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 3):

(S//SI//REL PARA EUA, FVEY) SHELLTRUMPET processa o trilionésimo registro de metadados

Por INFORMAÇÃO OMITIDA em 31/12/2012 0738

(S//SI//REL PARA EUA, FVEY) Em 21 de dezembro de 2012, o SHELLTRUMPET processou seu trilionésimo registro de metadados. O SHELLTRUMPET começou, em 8 de dezembro de 2007, como um analisador de metadados quase em tempo real para um sistema de coleta CLASSIC. Em seus cinco anos de existência, vários outros sistemas em toda a Agência passaram a usar as capacidades de processamento do SHELLTRUMPET para monitoramento de desempenho, alerta direto de e-mail, alerta de TRAFFICTHIEF e filtragem e captura de Portal Regional em Tempo Real (RTRG). Embora tenha levado cinco anos para chegar à marca de um trilhão, quase metade desse volume foi processada neste ano-calendário, e metade do volume provém do programa DANCINGOASIS da SSO. O SHELLTRUMPET processa,

atualmente, 2 bilhões de ocorrências de ligação por dia em sistemas selecionados da SSO (Ram-M, OAKSTAR, MYSTIC e sistemas habilitados pelo NCSC), MUSKETEER e sistemas parceiros. Ao longo de 2013, expandiremos seu alcance para outros sistemas da SSO. O trilhão de registros processados resultou em mais de 35 milhões de alertas para o TRAFFICTHIEF.

Para coletar uma quantidade tão avassaladora de comunicações, a NSA depende de inúmeros métodos. Entre eles estão a interceptação direta dos cabos de fibra óptica (inclusive os marítimos) usados para transmitir comunicações internacionais, o redirecionamento das mensagens para repositórios da NSA quando estas atravessam o sistema dos Estados Unidos (como é o caso da maioria das comunicações no mundo) e a cooperação com serviços de inteligência de outros países. Com frequência cada vez maior, a agência também conta com as empresas de internet e de telefonia, que repassam as informações coletadas de seus próprios clientes.

Embora a NSA seja oficialmente um órgão público, mantém incontáveis parcerias com empresas do setor privado, e muitas de suas principais funções foram terceirizadas. A agência em si tem em torno de 30 mil funcionários, mas também mantém sob contrato cerca de 60 mil funcionários de companhias particulares, que muitas vezes prestam serviços essenciais. O próprio Snowden não era funcionário da NSA, mas sim da Dell Corporation e da grande prestadora de serviços da área de defesa Booz Allen Hamilton. No entanto, assim como outros prestadores de serviços de empresas privadas, trabalhava dentro das instalações da NSA, executando uma de suas principais funções e com acesso a seus segredos.

Segundo Tim Shorrock, que há muito tempo estuda a relação da NSA com o setor privado, "70% do nosso orçamento de inteligência nacional estão sendo gastos no setor privado". Quando Michael Hayden afirmou que "a maior concentração de poder cibernético do planeta está no cruzamento da Avenida Baltimore com a Rodovia 32, em Maryland", Shorrock comentou que "ele não estava se referindo à NSA em si, mas sim ao parque empresarial situado a cerca de 1,5 quilômetro do gigantesco edifício preto que abriga a sede da NSA em Fort Meade, Maryland. É ali que todas as grandes prestadoras de serviços da NSA, da Booz à SAIC, passando pela Northrop Grumman, executam o trabalho de vigilância e inteligência para a agência".

Além das prestadoras de serviços de inteligência e defesa, essas parcerias corporativas incluem também algumas das maiores e mais importantes empresas de internet e telecomunicações, justamente aquelas que processam a maior parte das comunicações do mundo e podem facilitar o acesso a dados pessoais. Após descrever as missões da agência – "Defensiva" (proteger os sistemas de telecomunicações e computadores dos Estados Unidos de qualquer exploração) e "Ofensiva" (interceptar e explorar sinais estrangeiros) –, um documento ultrassecreto da NSA enumera alguns dos serviços fornecidos por essas empresas:

PARCERIAS ESTRATÉGICAS DA NSA

Alianças com mais de 80 grandes corporações globais para possibilitar as duas missões

Provedores de serviços de telecomunicações e redes / Infraestrutura de rede / Plataformas de hardware para desktops/servidores / Sistemas operacionais / Software de aplicativos / Hardware & software de segurança / Integradores de sistemas

Essas parcerias corporativas, que fornecem os sistemas e o acesso dos quais a NSA depende, são gerenciadas pela unidade altamente secreta chamada Operações de Fontes Especiais (SSO), divisão que supervisiona as parcerias corporativas. Snowden descrevia a SSO como a "joia da coroa" da agência.

BLARNEY, FAIRVIEW, OAKSTAR e STORMBREW são alguns dos programas supervisionados pela SSO dentro de seu portfólio Acesso de Parceiros Corporativos (CPA).

OPERAÇÕES DE FONTES ESPECIAIS

Acesso de Parceiros Corporativos

Responsável pelo briefing: INFORMAÇÃO OMITIDA

Nesses programas, a NSA explora o acesso de determinadas empresas de telecomunicações a sistemas internacionais depois de elas terem firmado contratos com companhias semelhantes no exterior para criação, suporte e melhoria de suas redes. Em seguida, as empresas norte-americanas redirecionam os dados de comunicação do país-alvo para repositórios da NSA.

O principal objetivo do programa BLARNEY é descrito em um documento informativo da NSA:

RELACIONAMENTOS & AUTORIDADES

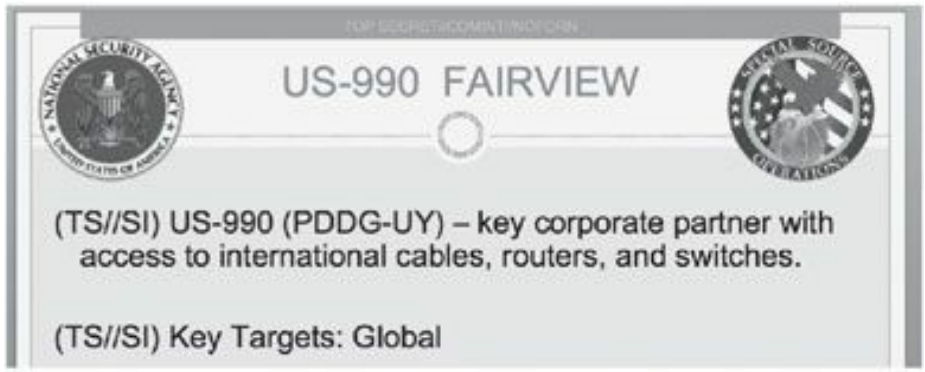
Obter parcerias-chave exclusivas com empresas que permitam o acesso a cabos de fibra óptica, comutadores e/ou roteadores internacionais de alta capacidade localizados em diversas partes do mundo

O BLARNEY dependia de uma relação em especial: uma parceria de longa data com a AT&T Inc., segundo o *Wall Street Journal* em uma reportagem sobre o programa. Segundo os arquivos da NSA, a lista de países-alvo do BLARNEY em 2010 incluía Brasil, França, Alemanha, Grécia, Israel, Itália, Japão, México, Coreia do Sul e Venezuela, além da União Europeia e da ONU.

O FAIRVIEW, outro programa da SSO, também coleta o que a NSA enaltece como "uma

imensa quantidade de dados" do mundo inteiro. Ele também depende, em grande medida, de um único "parceiro corporativo", e em especial do acesso desse parceiro aos sistemas de telecomunicações de outras nações. O resumo interno do FAIRVIEW feito pela NSA é simples e claro:

ASPECTOS SINGULARES
Acesso a imensas quantidades de dados
Controlado por diversas autoridades oficiais
A maioria dos acessos é controlada pelo parceiro

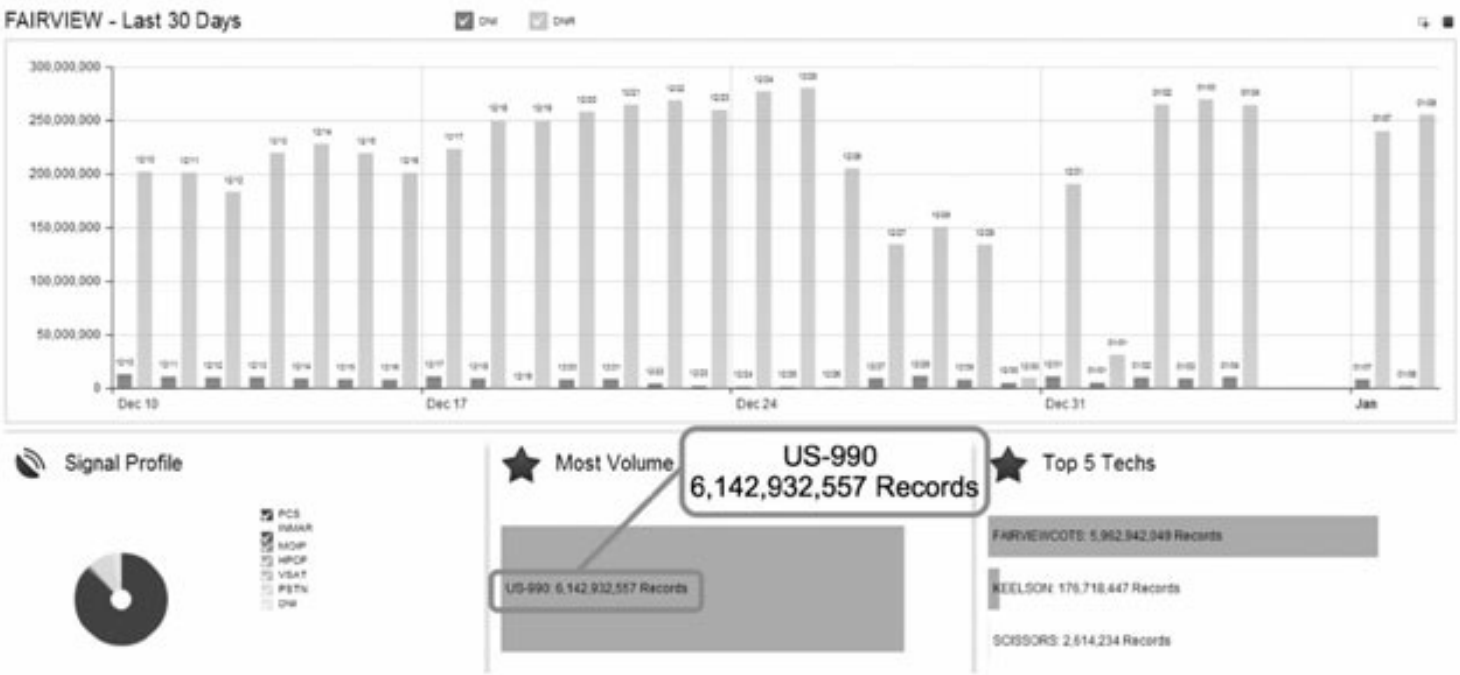


US-990 FAIRVIEW
Parceiro corporativo chave com acesso a cabos, roteadores e comutadores internacionais.
Alvos-chave: Global

De acordo com documentos da NSA, o FAIRVIEW "está tipicamente entre os cinco maiores programas da NSA em matéria de coleta de dados para produção em série" – ou seja, vigilância constante – "e é um dos maiores fornecedores de metadados". Sua dependência avassaladora de apenas uma empresa de telecomunicações é demonstrada pela afirmação de que "cerca de 75% da transmissão provém de uma única fonte, o que reflete o acesso privilegiado do programa a uma grande variedade de comunicações-alvo". Embora a empresa não seja identificada, uma descrição do parceiro do FAIRVIEW deixa clara sua disposição para cooperar (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 4):

FAIRVIEW – Parceiro corp. desde 1985 com acesso a cabos, roteadores, switches internac. Parceiro opera dentro dos Estados Unidos, mas tem acesso a informações que transitam pelo país e, graças às suas relações corporativas, proporciona acesso privilegiado a outras telecoms e ISPs. Realiza modelagem de tráfego agressiva para fazer os sinais passíveis de interesse transitarem por nossos monitores.

Graças a essa cooperação, o FAIRVIEW coleta imensas quantidades de informações sobre chamadas telefônicas. Um gráfico relativo a um período de trinta dias iniciado em 10 de dezembro de 2012 mostra que o programa, por si só, foi responsável pela coleta de cerca de 200 milhões de registros em cada dia desse mês, um total de mais de 6 bilhões de registros no período. As colunas claras se referem a coletas de "DNR" (chamadas telefônicas), enquanto as escuras representam "DNI" (atividade na internet).



FAIRVIEW – ÚLTIMOS 30 DIAS

Da esquerda para a direita: Perfil dos sinais / Maior volume / US-990 6.142.932.557 registros / Cinco maiores tecnologias / FAIRVIEWCOTS 5.962.942.049 registros / KEELSON 176.718.447 registros / SCISSORS 2.614.234 registros

Para coletar esses bilhões de registros telefônicos, a SSO colabora tanto com os parceiros corporativos da NSA quanto com agências de governos estrangeiros – como, por exemplo, o serviço de inteligência polonês (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 5):

(TS//SI//NF) O ORANGECRUSH, parte do programa OAKSTAR dentro do portfólio corporativo da SSO, começou a encaminhar metadados de um local sob responsabilidade de terceiros (Polônia) para os repositórios da NSA em 3 de marco, e conteúdos em 25 de marco. Esse programa é um esforco colaborativo entre SSO. NCSC. ETC. FAD. um Parceiro Corporativo da NSA e um órgão do governo polonês. O ORANGECRUSH só é conhecido pelos poloneses como BUFFALOGREEN. Essa parceria entre vários grupos começou em maio de 2009 e irá incorporar o projeto da OAKSTAR chamado ORANGEBLOSSOM, assim como suas capacidades de DNR. O novo acesso fornecerá SIGINT de links comerciais administrados pelo Parceiro Corporativo da NSA, e antecipa-se que incluirá comunicações do Exército Nacional Afegão, do Oriente Médio, de parte do continente africano e da Europa. Uma notificação foi postada em SPRINGRAY e o material desta coleta está disponível para parceiros via TICKETWINDOW.

O programa OAKSTAR explora de maneira semelhante o acesso de um dos "parceiros" corporativos da NSA (cujo codinome é STEELKNIGHT) a sistemas de telecomunicações estrangeiros, e usa esse acesso para redirecionar dados para os repositórios da agência. Outro parceiro corporativo, de codinome SILVERZEPHYR, é citado em um documento de 11 de novembro de 2009 (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 6) que descreve o trabalho feito com a empresa para obter "comunicações internas" tanto do Brasil quanto da Colômbia:

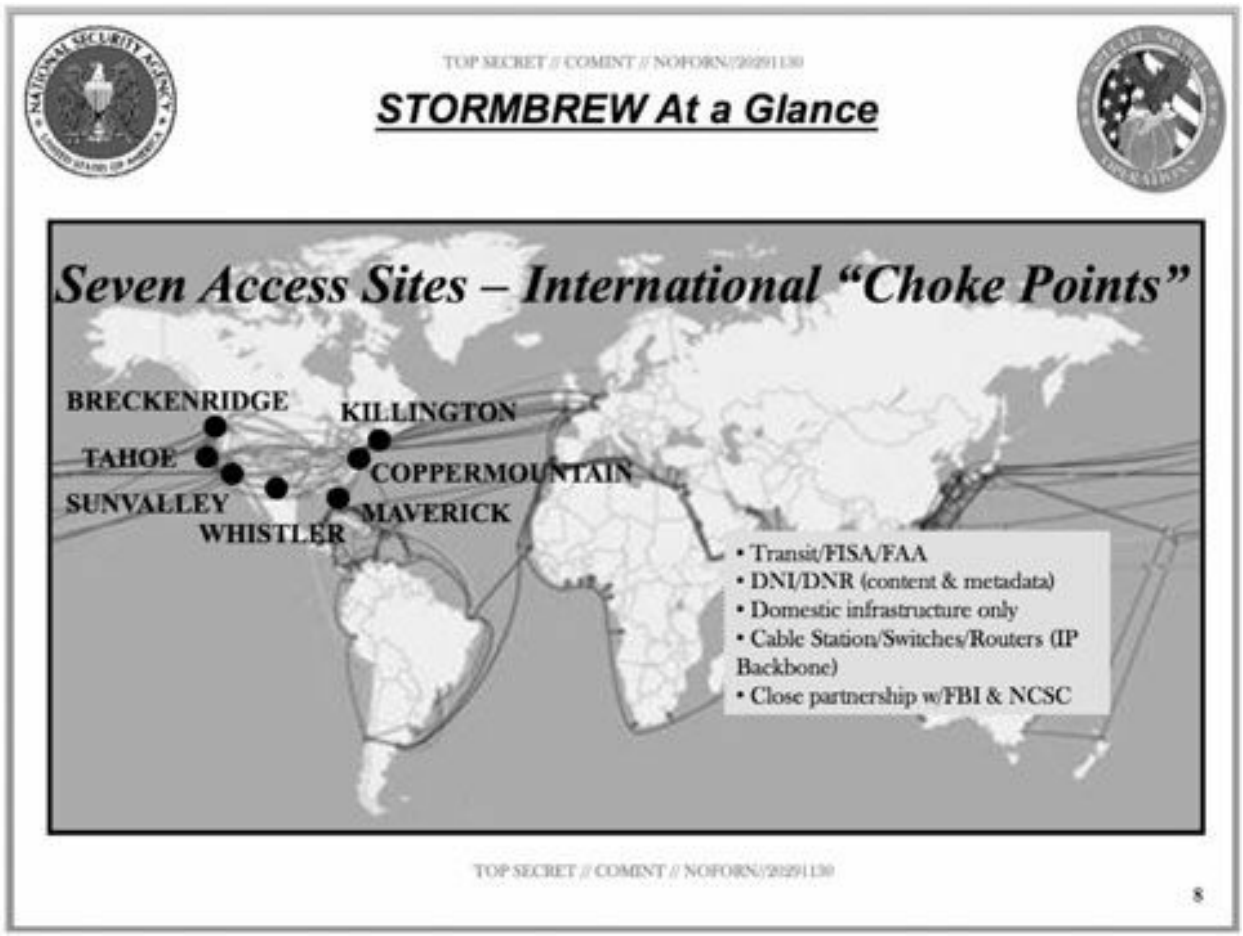
Acesso de DNI para FAA via SILVERZEPHYR iniciado em NSAW

Por INFORMAÇÃO OMITIDA em 6/11/2009 0918

(TS//SI//NF) Na quinta-feira, 5/11/2009, o acesso SSO-OAKSTAR SILVERZEPHYR (SZ) começou a encaminhar, para a NSAW, registros de DNI para FAA (Lei de Emendas da FISA) através do sistema WealthyCluster2/Tellurian da FAA instalado na sede do parceiro. A SSO coordenou o processo junto com o Escritório de Fluxo de Dados e encaminhou vários arquivos de amostragem para uma partição de teste com fins de validação, o que ocorreu com sucesso total. A SSO continuará monitorando o fluxo e a coleta para garantir que quaisquer anomalias sejam identificadas e corrigidas conforme necessário. SILVERZEPHYR

continuará a fornecer aos clientes uma coleta autorizada de DNR em trânsito. A SSO está trabalhando com o parceiro para obter acesso a mais 80Gbs de dados DNI em sua rede pareada, divididos em incrementos de 10Gbs. A equipe do OAKSTAR, com apoio da NSAT e do GNDA, acaba de concluir um levantamento de SIGINT de 12 dias no local, que identificou mais de 200 novos links. Durante o levantamento, o GNDA trabalhou com o parceiro para testar a saída de seu sistema de ACS. O OAKSTAR também está atuando junto à NSAT para examinar amostras coletadas pelo parceiro no Brasil e na Colômbia, ambas podendo conter comunicações internas desses países.

Enquanto isso, o programa STORMBREW, conduzido em "estreita parceria com o FBI", proporciona à NSA acesso ao tráfego de internet e telefonia que entra nos Estados Unidos por vários "gargalos" situados em território norte-americano. O programa explora o fato de que a grande maioria do tráfego de internet do mundo passa em algum momento pela infraestrutura de comunicação dos Estados Unidos, subproduto residual do papel central desempenhado pelo país no desenvolvimento da rede. Alguns desses pontos de gargalo escolhidos são designados por codinomes:



STORMBREW VISÃO RÁPIDA

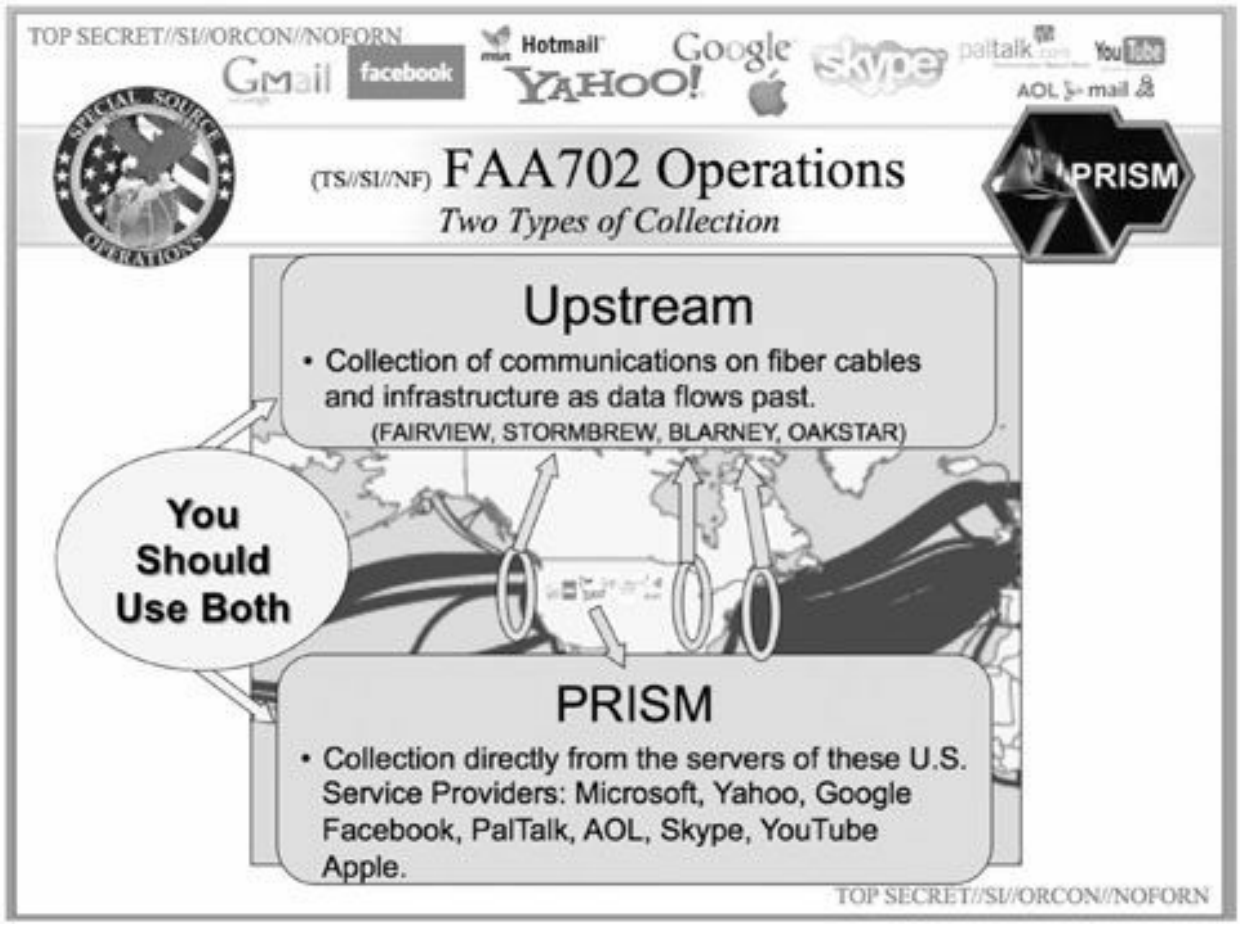
Sete locais de acesso – "Gargalos" internacionais

No quadro: Trânsito/FISA/FAA / DNI/DNR (conteúdo & metadados) / Somente infraestrutura doméstica / Estação de cabo/Comutadores/Roteadores (Suporte principal de IP) / Parceria estreita com FBI & NCSC

Segundo a NSA, o STORMBREW "é, atualmente, constituído por relações muito delicadas com dois provedores de telecomunicações norte-americanos (designados pelos codinomes ARTIFICE e WOLFPOINT)". Além do acesso a gargalos situados dentro dos Estados Unidos, "o programa STORMBREW também administra dois pontos de entrada de cabos submarinos, um na Costa Oeste do país (codinome BRECKENRIDGE) e outro na Costa Leste (codinome QUAILCREEK).

Como demonstrado pela profusão de codinomes, a identidade dos parceiros corporativos da NSA é um de seus segredos mais bem guardados. Os documentos que contêm a chave desses codinomes são protegidos com grande cuidado pela agência, e Snowden não conseguiu obter muitos deles. Apesar disso, suas revelações desmascararam algumas das empresas que cooperam com a NSA. Em particular, seu acervo incluía os documentos relacionados ao PRISM, que detalhavam acordos secretos entre a NSA e as maiores empresas de internet do mundo – Facebook, Yahoo!, Apple, Google –, bem como importantes esforços da Microso para proporcionar à agência acesso a suas plataformas de comunicação, como o Outlook.

Ao contrário dos programas BLARNEY, FAIRVIEW, OAKSTAR e STORMBREW, que envolvem a interceptação de cabos de fibra óptica e outros tipos de infraestrutura (vigilância *upstream*, ou "correnteza acima", no jargão da NSA), o PRISM permite à agência coletar dados diretamente dos servidores de nove das maiores empresas da internet:



OPERAÇÕES DA FAA702

Dois tipos de coleta / *Upstream* / Coleta de comunicações em cabos de fibra e infraestruturas à medida que o fluxo de dados ocorre / (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR) / Você deve usar ambos / PRISM / Coleta direta dos servidores dos seguintes provedores de serviços dos Estados Unidos: Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple

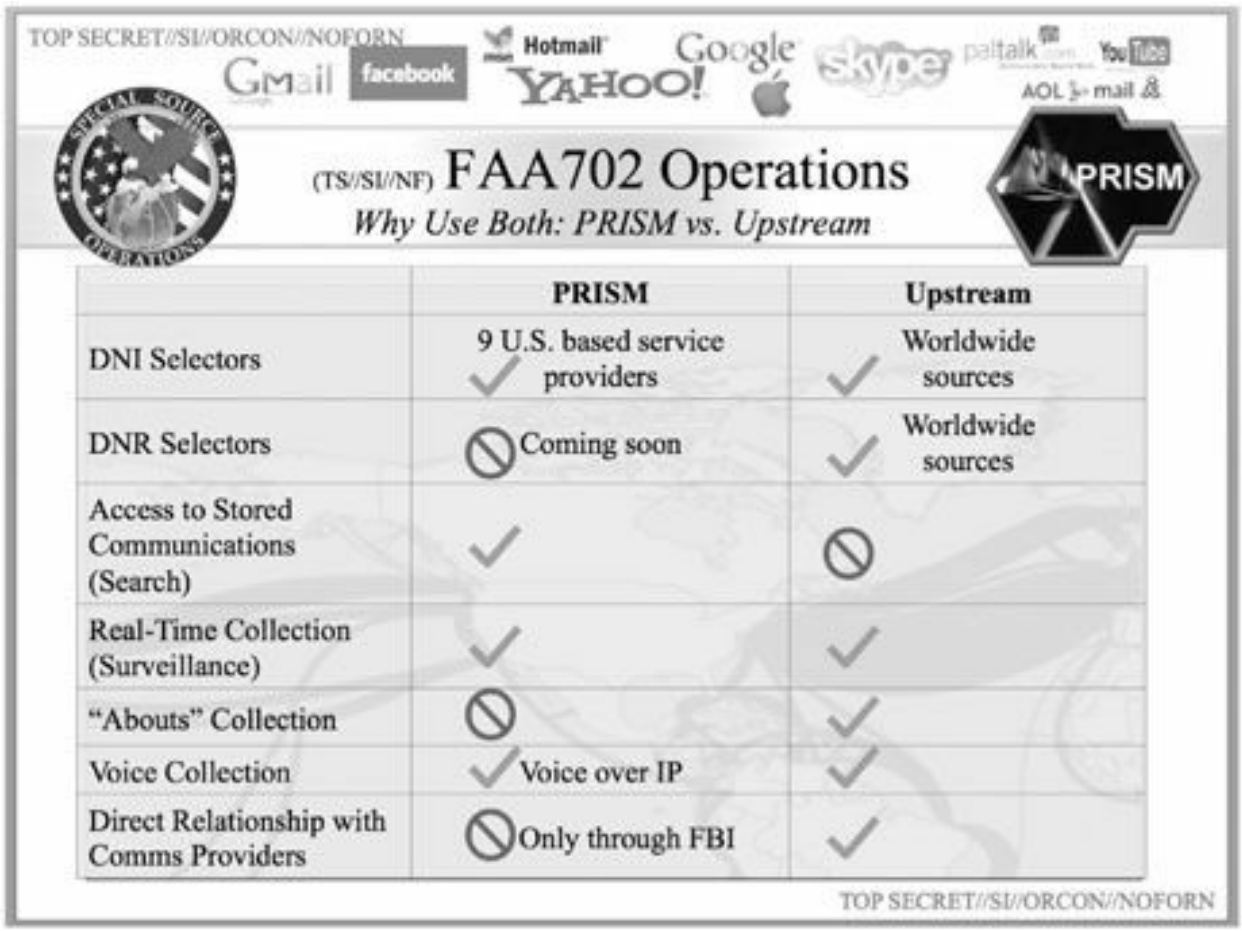
As empresas listadas no slide do PRISM negaram proporcionar à NSA acesso ilimitado a seus servidores. Facebook e Google alegaram que só fornecem à NSA informações para as quais a agência tem um mandado, e tentaram descrever o PRISM como pouco mais do que um detalhe técnico banal: um sistema de entrega ligeiramente aprimorado pelo qual a NSA recebe, dentro de um "cofre", dados que as empresas são obrigadas por lei a fornecer.

Só que esse raciocínio é desmentido por diversos fatores. Em primeiro lugar, sabemos que o Yahoo! travou uma briga ferrenha na justiça contra os esforços da NSA para obrigá-lo a entrar para o PRISM, tentativa improvável caso o programa fosse apenas uma modificação banal em um sistema de entrega. (Os argumentos do Yahoo! foram negados pelo tribunal da FISA, e a empresa recebeu ordem de participar do PRISM.) Em segundo lugar, após ser duramente criticado por "superestimar" o impacto do PRISM, Bart Gellman, do *Washington Post*, tornou a investigar o programa e declarou que confirmava a principal afirmação do jornal: "De suas estações de trabalho em qualquer lugar do mundo, funcionários do governo credenciados com acesso ao PRISM podem solicitar uma 'tarefa' ao sistema" – ou seja, fazer uma busca – "e receber resultados de uma empresa

de internet sem qualquer outra interação com seus funcionários."

Em terceiro lugar, os desmentidos das empresas foram formulados de modo evasivo, em "juridiquês", e muitas vezes confundiram mais do que esclareceram. Por exemplo, o Facebook alegou não fornecer "acesso direto", enquanto o Google negou ter criado uma "porta dos fundos" para a NSA. No entanto, como declarou à *Foreign Policy* Chris Soghoian, especialista em tecnologia da ACLU, esses são termos extremamente técnicos, que denotam maneiras muito específicas de se obter informações. Em última instância, as empresas não negaram ter trabalhado com a NSA para montar um sistema por meio do qual a agência pudesse ter acesso direto aos dados de seus clientes.

Por fim, a própria NSA alardeou repetidas vezes os méritos do PRISM por suas capacidades de coleta ímpares, observando que o programa foi vital para o aumento da vigilância. Um slide da agência detalha os poderes de vigilância especiais do PRISM:



OPERAÇÕES DA FAA702

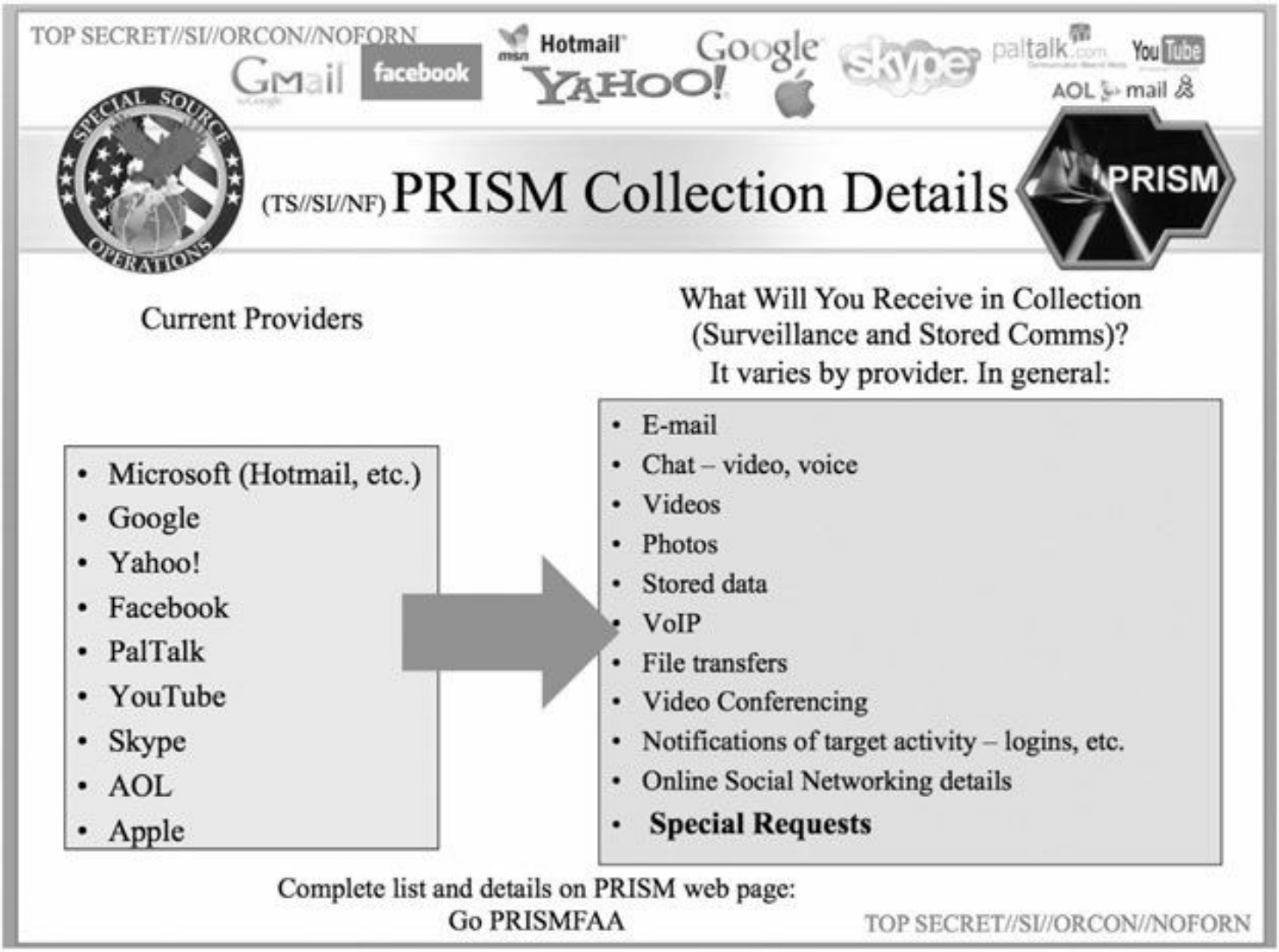
Por que usar ambos: PRISM *versus Upstream*

Coluna da esquerda: Seletores de DNI / Seletores de DNR / Acesso a comunicações armazenadas (Busca) / Coleta em tempo real (Vigilância) / Coleta de "Sobres" / Coleta de voz / Relação direta com provedores de comunicação

Coluna do meio: PRISM / 9 provedores de serviço baseados nos EUA / Em breve / Voz por IP / Somente via FBI

Coluna da direita: Upstream / Fontes mundiais / Fontes mundiais

Outro slide detalha a ampla gama de comunicações que a NSA pode acessar graças ao PRISM:



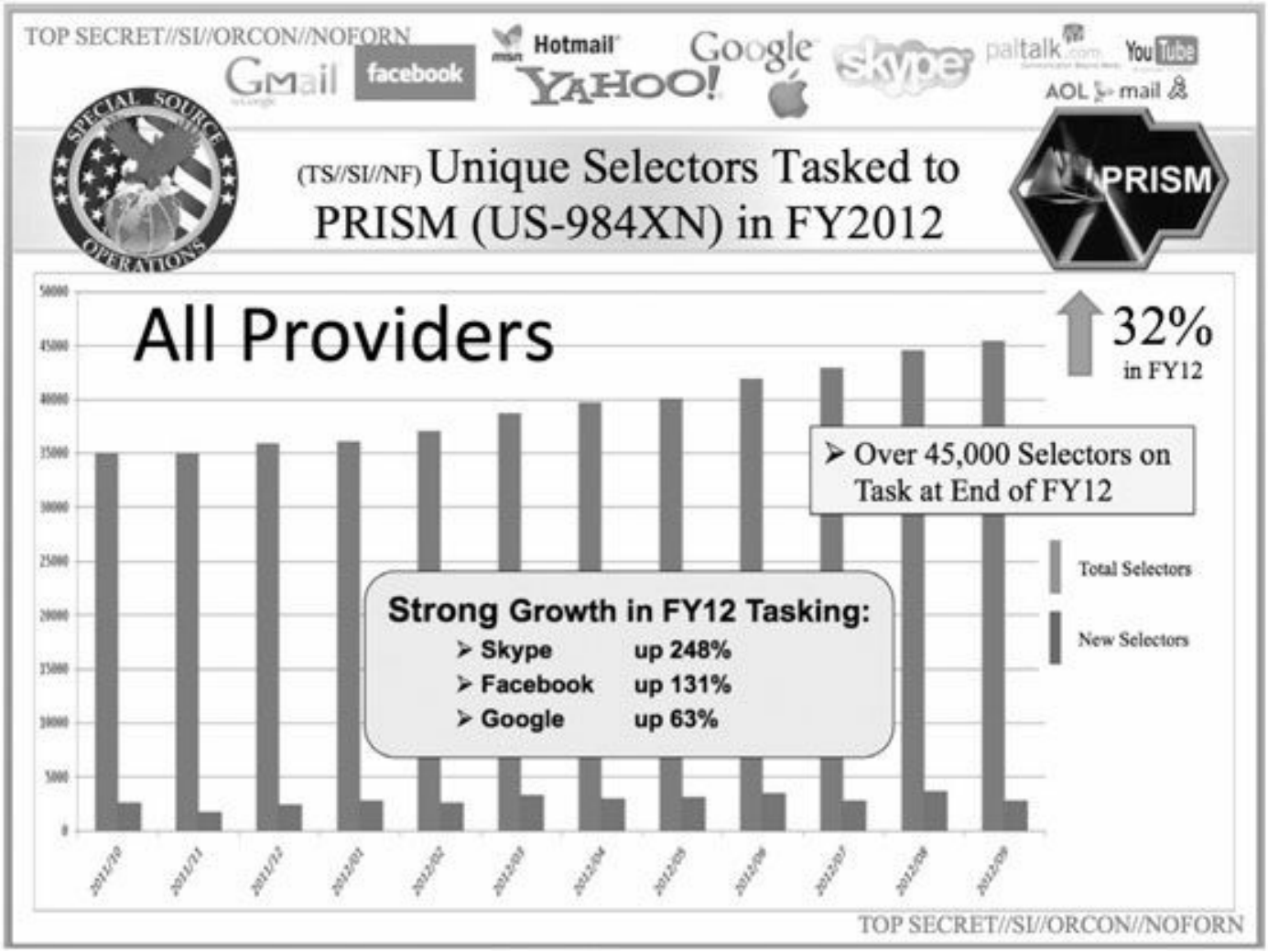
PRISM DETALHES DE COLETA

Coluna da esquerda: Provedores atuais

Coluna da direita: O que você obterá na coleta (vigilância e comunicações armazenadas)? Varia conforme o provedor. De modo geral: / E-mail / Chat – vídeo, voz / Vídeos / Fotos / Dados armazenados / VoIP / Transferências de arquivos / Videoconferências / Notificações de atividade do alvo – logins, etc. / Detalhes de redes sociais na internet / Solicitações especiais

Abaixo: Lista completa e detalhes na página do PRISM na web: Acesse PRISMFAA

Outro slide revela detalhes de como o PRISM aumentou de forma regular e significativa o volume de coleta da agência:



SELETORES INDIVIDUAIS EM TAREFAS SOLICITADAS NO PRISM (US-984XN) NO ANO FISCAL DE 2012

Da esquerda para a direita, de cima para baixo: Todos os provedores / 32% no ano fiscal de 2012 / Mais de 45.000 seletores de tarefa ativos no fim do ano fiscal de 2012 / Forte crescimento das tarefas no ano fiscal de 2012: Skype aumento de 248% / Facebook aumento de 131% / Google aumento de 63% / Seletores totais / Seletores novos

Em sua intranet, a divisão SSO com frequência alardeia o imenso incremento na coleta proporcionado pelo PRISM. Uma mensagem de 19 de novembro de 2012 (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 7) tem o título "PRISM expande impacto: Números para o ano fiscal de 2012":

(TS//SI//NF) O programa PRISM (US-984XN) expandiu, no ano fiscal de 2012, seu impacto na missão de informação da NSA por meio de um aumento de tarefas, coleta e melhorias operacionais. Eis alguns destaques do programa PRISM no ano fiscal de 2012:

O PRISM é a fonte de coleta mais citada nos relatórios finais de informação internos da NSA. Mais relatórios de informação da NSA tiveram por base o PRISM do que qualquer outro SIGAD individual, considerando-se todos os relatórios internos da NSA durante o ano fiscal de 2012: o programa foi citado em 15,1% de todos os relatórios (contra 14% no ano fiscal de 2011). O PRISM foi citado em 13,4% de todos os relatórios internos, de parceiros e de terceiros da NSA (contra 11,9% no ano fiscal de 2011), e é também o SIGAD mais citado de forma geral.

Número de relatórios finais de informação baseados no PRISM emitidos no ano fiscal de 2012: 24.096, aumento de 27% em relação ao ano fiscal de 2011.

Porcentagem de informações de fonte única nos anos fiscais de 2011 e 2012: 74%.

Número de relatórios finais derivados de coleta via PRISM e citados como fontes em artigos no Briefing Diário ao Presidente no ano fiscal de 2012: 1.477 (18% de todos os relatórios de SIGINT citados como fontes em artigos no BDP – mais alto SIGAD individual para a NSA). No ano fiscal de 2011: 1.152 (15% de todos os relatórios de SIGINT citados como fontes em artigos no BDP – mais alto SIGAD individual para a NSA).

Número de elementos essenciais de informação com contribuição do PRISM no ano fiscal de 2012: 4.186 (32% de todos os EEIs para todas as Necessidades de Informação); 220 EEIs atendidos somente pelo PRISM.

Solicitações de tarefa: o número de seletores aumentou em 32% no ano fiscal de 2012, para 45.406 em set./2012.

Grande sucesso em coleta e processamento no Skype: alvos valiosos e privilegiados adquiridos.

Expansão dos domínios de e-mail buscáveis via PRISM de apenas 40 para 22.000.

Essas declarações congratulatórias não sustentam a tese de que o PRISM seja apenas uma tecnicalidade sem importância, e negam os desmentidos das empresas do Vale do Silício quanto à sua cooperação. De fato, em uma reportagem sobre o programa PRISM após as revelações de Snowden, o *New York Times* descreveu uma miríade de negociações secretas entre a NSA e o Vale do Silício sobre o fornecimento de acesso irrestrito aos sistemas dessas empresas para a agência. "Quando autoridades do governo foram ao Vale do Silício solicitar maneiras mais fáceis de as maiores empresas de internet do mundo entregarem dados de usuários como parte de um programa secreto de

vigilância, as empresas reclamaram", escreveu o *Times*. "No final, porém, muitas cooperaram pelo menos um pouco." Em especial:

> O Twitter se negou a facilitar as coisas para o governo. Outras companhias, no entanto, se mostraram mais cooperativas, segundo pessoas com acesso às negociações. Em resposta a solicitações juridicamente respaldadas do governo, elas entabularam conversas com funcionários de segurança nacional sobre o desenvolvimento de métodos de tecnologia que permitissem compartilhar de maneira mais eficiente e segura os dados pessoais de usuários estrangeiros. Em alguns casos, modificaram seus sistemas com essa finalidade.

Segundo o jornal, essas negociações "ilustram como o trabalho do governo e das empresas de tecnologia está relacionado de forma intrincada, bem como a profundidade das transações conduzidas nos bastidores". A matéria também contesta as alegações das empresas de que só fornecem à NSA os acessos juridicamente solicitados, observando que, "embora a entrega de dados em resposta a uma solicitação legítima da FISA seja uma obrigação legal, facilitar o acesso do governo às informações não é, motivo pelo qual o Twitter pôde se negar a fazê-lo".

A alegação das empresas de internet de que só entregam à NSA informações solicitadas por meio de mandado também não significa muita coisa. Isso porque a NSA só é obrigada a obter um mandado individual quando tem como alvo específico um indivíduo dos Estados Unidos. Nenhuma permissão especial desse tipo é necessária para obter os dados relativos às comunicações de qualquer cidadão que não seja norte-americano em território estrangeiro, *mesmo quando essa pessoa estiver se comunicando com americanos*. Da mesma forma, não há restrições nem limites para a coleta em massa de metadados efetuada pela NSA devido à interpretação feita pelo governo da Lei Patriota, interpretação tão ampla que até os autores originais da lei ficaram chocados ao descobrir como ela vinha sendo usada.

A estreita colaboração entre a NSA e corporações privadas talvez fique mais explícita nos documentos relacionados à Microso , que revelam os esforços vigorosos da empresa para fornecer acesso à NSA a vários de seus serviços on-line mais usados, entre eles SkyDrive, Skype e Outlook.com.

O SkyDrive, que permite às pessoas armazenarem arquivos on-line e acessá-los de vários equipamentos, tem mais de 250 milhões de usuários no mundo. "Nós acreditamos que é importante você ter controle sobre quem pode e quem não pode acessar seus dados pessoais na nuvem", afirma o site do SkyDrive. No entanto, como mostra um documento da NSA (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 8), a Microso gastou "muitos meses" de trabalho para facilitar o acesso do governo a esses dados:

(TS//SI//NF) Destaque da SSO – Coleta do Skydrive da Microsoft agora faz parte da Coleta-padrão de Comunicações Armazenadas do PRISM

Por INFORMAÇÃO OMITIDA em 8/3/2013 1500

(TS//SI//NF) A partir de 7 de março de 2013, o PRISM passa a coletar dados do Skydrive da Microsoft como parte de seu pacote-padrão de coleta de Comunicações Armazenadas para um seletor solicitado em uma tarefa com base na seção 702 da Lei de Emendas da FISA (FAA702). Isso significa que os analistas não precisarão mais apresentar uma solicitação especial à SSO para tal fim, um passo no procedimento do qual muitos analistas talvez não estivessem cientes. Essa nova capacidade terá como resultado uma resposta de coleta da SSO muito mais completa e oportuna para nossos clientes Enterprise. Tal sucesso é resultado de um trabalho de muitos meses do FBI junto à Microsoft para implantar essa solução de solicitações de tarefa e coleta. "O Skydrive é um serviço que permite aos usuários armazenar e acessar seus arquivos na nuvem usando diversos aparelhos. O serviço inclui também suporte gratuito na web para os programas do Office da Microsoft, possibilitando ao usuário criar, editar e visualizar documentos de Word, PowerPoint e Excel sem precisar ter o MS Office instalado em seu equipamento." (fonte: S314 wiki)

No fim de 2011, a Microso comprou o Skype, serviço de telefonia e chat baseado na internet com mais de 663 milhões de usuários registrados. Na época da compra, a Microsoft garantiu aos usuários que "o Skype está comprometido com o respeito à sua privacidade e à confidencialidade dos seus dados pessoais, do seu tráfego e do conteúdo das suas comunicações". Na realidade, porém, como a Microso devia saber, esses dados também estavam facilmente disponíveis para o governo. No início de 2013, várias mensagens internas da NSA comemoraram o acesso cada vez maior da agência às comunicações dos usuários do Skype (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 9 e 10):

(TS//SI//NF) Nova capacidade no PRISM para comunicações armazenadas no Skype

Por INFORMAÇÃO OMITIDA em 3/4/2013 0631

(TS//SI//NF) O PRISM ganhou uma nova capacidade de coleta: as comunicações armazenadas no Skype. Essas comunicações contêm dados específicos que não são recolhidos pela coleta de vigilância normal em tempo real. A SSO espera receber listas de contatos, informações de cartão de crédito, registros de dados de ligações, informações de conta de usuários e outros

materiais. Em 29 de março de 2013, a SSO encaminhou aproximadamente 2.000 seletores relativos a comunicações armazenadas no Skype para serem avaliados pelo SV41 e pela Unidade de Vigilância de Comunicações Eletrônicas (ECSU) do FBI. O SV41 já vinha trabalhando com antecedência na avaliação dos seletores com prioridade mais alta e tinha cerca de 100 deles prontos para a avaliação da ECSU. Talvez sejam necessárias várias semanas para o SV41 tratar e aprovar todos os 2.000 seletores, e é provável que a ECSU leve mais tempo ainda para dar a sua aprovação. Em 2 de abril, a ECSU tinha aprovado mais de 30 seletores a serem enviados ao Skype para coleta. A coleta do PRISM no Skype criou, em menos de dois anos, um nicho vital de informações para a NSA cujos tópicos mais importantes foram terrorismo, oposição e regime na Síria, além de informações executivas/séries especiais. Mais de 2.800 relatórios de informação baseados na coleta do PRISM no Skype foram emitidos desde abril de 2011, dos quais 76% eram provenientes de uma única fonte.

(TS//SI//NF) SSO expande capacidade de tarefas do PRISM no Skype

Por INFORMAÇÃO OMITIDA em 3/4/2013 0629

(TS//SI//NF) Em 15 de março de 2013, o programa PRISM da SSO começou a usar todos os seletores da Microsoft no PRISM em solicitações de tarefas no Skype, uma vez que o Skype permite aos usuários fazer login usando identificadores de conta, além dos nomes de usuário do próprio Skype. Até agora, o PRISM não coletava nenhum dado do Skype quando o usuário se logava usando qualquer outra coisa que não o nome de usuário do Skype, produzindo uma coleta com falhas; esta ação irá resolver isso. Na verdade, um usuário pode criar uma conta no Skype usando qualquer endereço de e-mail com qualquer domínio no mundo. No momento, a UTT não permite que os analistas solicitem tarefas pelo PRISM nesses endereços de e-mail externos à Microsoft, mas a SSO pretende corrigir isso no verão deste ano. Enquanto isso, a NSA, o FBI e o Dpto. de Justiça coordenaram esforços ao longo dos últimos seis meses

para obter a aprovação do PRINTAURA de modo a enviar todos os atuais e futuros seletores do PRISM na Microsoft para o Skype. Isso resultou no envio de cerca de 9.800 seletores para o Skype em uma coleta bem-sucedida que de outra forma teria sido perdida.

Essa colaboração toda não apenas foi conduzida sem transparência como contradizia as declarações públicas feitas pelo Skype. Segundo o especialista em tecnologia da ACLU Chris Soghoian, as revelações iriam surpreender muitos usuários do Skype. "No passado, o Skype fez promessas afirmativas aos usuários sobre sua incapacidade de grampear chamadas", afirmou ele. "É difícil equacionar a colaboração secreta da Microso com a NSA e seus alardeados esforços para competir com o Google em termos de privacidade."

Em 2012, a Microso iniciou um upgrade em seu portal de e-mail, o Outlook.com, no sentido de unificar todos os seus serviços de comunicação – incluindo o amplamente utilizado Hotmail – em um programa central. A empresa exaltou as qualidades do novo Outlook, prometendo altos níveis de criptografia para proteger a privacidade. A NSA logo começou a se preocupar com a possibilidade de a criptografia oferecida pela Microso aos clientes do Outlook impedir a agência de espionar suas comunicações. Um memorando da SSO com data de 22 de agosto de 2012 expressa o receio de que "usar esse portal signifique que qualquer e-mail nele originado esteja criptografado com os ajustes-padrão" e de que "as sessões de chat realizadas dentro do portal também estejam criptografadas quando ambos os interlocutores estiverem usando um chat criptografado da Microsoft".

Mas esse problema teve vida curta. Em poucos meses, as duas organizações se uniram para bolar métodos que permitissem à NSA contornar a mesma proteção por criptografia que a Microso vinha anunciando ao público como vital para proteger a privacidade (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 11):

(TS//SI//NF) Microsoft lança novo serviço que afeta coleta para FAA702

Por INFORMAÇÃO OMITIDA em 26/12/2012 0811

(TS//SI//NF) Em 31 de julho, a Microsoft (MS) começou a criptografar chats baseados na internet com a introdução do novo sistema Outlook.com. Essa nova criptografia por Secure Socket Layer (SSL) impede de forma eficaz a coleta do novo serviço para a seção 702 e possivelmente seção 12.333 (em algum grau) da FAA para a Comunidade de Inteligência (IC). Em parceria com o FBI, a MS desenvolveu um procedimento de vigilância para lidar com o novo SSL. Essas soluções foram testadas com sucesso e começaram a ser usadas em 12 de dezembro de 2012. A solução SSL foi aplicada a todas as

exigências atuais da FISA e da seção 702/PRISM; não foi necessária nenhuma mudança nos procedimentos de solicitação de tarefas por UTT. A solução SSL não coleta voz/vídeo baseados no servidor nem transferências de arquivos. O sistema de coleta original da MS permanecerá ativo para coletar voz/vídeo e transferências de arquivo. Em consequência, haverá alguma duplicação na coleta de chats com base em texto pelos sistemas novo e antigo, que será solucionada em uma data futura. Um aumento do volume coletado como resultado dessa solução já foi assinalado por CES.

Outro documento descreve mais colaborações entre a Microso e o FBI, uma vez que esta agência também procurou garantir que as novas funcionalidades do Outlook.com não interferissem em seus hábitos de vigilância: "A equipe da DITU (Unidade de Tecnologia de Interceptação de Dados) do FBI está trabalhando com a Microso para entender uma funcionalidade adicional do Outlook.com que permite aos usuários criar pseudônimos de e-mail, o que pode afetar nosso processo de solicitação de tarefas (...) Atividades compartimentadas e outras estão em curso para mitigar esses problemas."

Essa referência à vigilância do FBI no acervo de documentos da NSA compilado por Snowden não foi uma ocorrência isolada. Toda a comunidade de inteligência pode acessar a informação coletada pela NSA: a agência compartilha de forma rotineira sua imensa coleção de dados com outros órgãos, entre as quais o FBI e a CIA. Um dos principais objetivos da grande farra de coleta da NSA era justamente intensificar o compartilhamento de informações com outras agências. De fato, quase todos os documentos relacionados aos diversos programas de coleta mencionam a inclusão de outras unidades de inteligência. A mensagem de 2012 da unidade SSO da NSA reproduzida abaixo (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 12), sobre o compartilhamento de dados do PRISM, comemora que "o PRISM é um esporte de equipe!".

(TS//SI//NF) Expansão do compartilhamento do PRISM com FBI e CIA

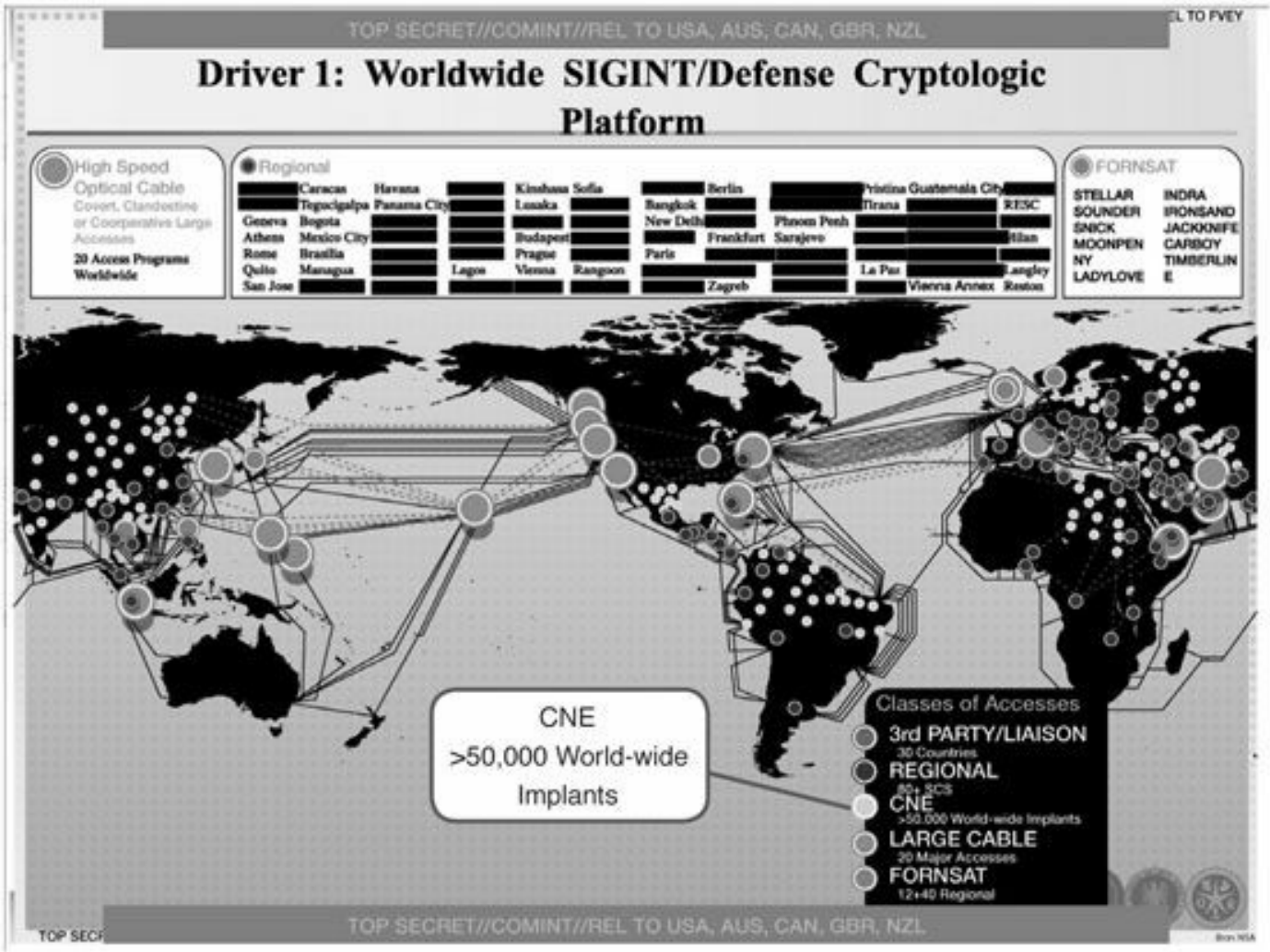
Por INFORMAÇÃO OMITIDA em 31/8/2012 0947

(TS//SI//NF) A SSO expandiu recentemente o compartilhamento das operações do PRISM com o FBI e a CIA por meio de dois projetos. Com esses esforços, a SSO criou um ambiente de compartilhamento e colaboração relacionado às operações do PRISM que abrange toda a Comunidade de Inteligência. Primeiro, a equipe PRINTAURA da SSO solucionou um problema para o SID (Diretório de Inteligência de Sinais) programando softwares que reunissem de forma automática, a cada quinze dias, uma lista de seletores solicitados em tarefas no PRISM

para transmitir ao FBI e à CIA. Isso permite que nossos parceiros vejam que seletores a NSA usou para solicitar tarefas no PRISM. FBI e CIA podem então solicitar uma cópia da coleta do PRISM relacionada a qualquer seletor, conforme permitido pela Lei de Emendas FISA de 2008. Antes do trabalho de PRINTAURA, o SID vinha fornecendo ao FBI e à CIA listas incompletas e imprecisas, impedindo nossos parceiros de fazer pleno uso do programa PRISM. PRINTAURA se ofereceu para reunir em múltiplos locais os dados detalhados relacionados a cada seletor e unificá-los em um formato utilizável. No segundo projeto, o MPM (Gerente de Missão de Programa) do PRISM começou, há pouco tempo, a enviar notícias e dicas operacionais sobre o PRISM ao FBI e à CIA, de modo que seus analistas pudessem solicitar tarefas de forma adequada no sistema do PRISM, estar cientes de quedas e mudanças e otimizar seu uso do PRISM. O MPM coordenou um acordo com a equipe de FAA do SID para compartilhar essas informações semanalmente, esforço que foi bem recebido e apreciado. Ambas as atividades ressaltam o fato de que o PRISM é um esporte de equipe!

A coleta *upstream* (a partir de cabos de fibra óptica) e a coleta direta nos servidores das empresas de internet (programa PRISM) fornecem a maioria dos registros obtidos pela NSA. Além dessa ampla vigilância, porém, a agência também realiza o que chama de Exploração de Rede Computacional (CNE), inserindo *malwares* em computadores específicos para vigiar seus usuários. Quando consegue inserir *malwares* desse tipo, a NSA torna-se, no jargão da agência, "dona" do computador: passa a ver cada tecla digitada e cada tela visualizada. A divisão responsável por esse tipo de manobra, Operações de Acesso Customizado (TAO), é, na realidade, a unidade de hacking interna da agência.

A prática de hacking é, por si só, bastante generalizada: um documento da NSA indica que a agência conseguiu infectar pelo menos 50 mil computadores individuais com um tipo de *malware* chamado "inserção quântica". Um mapa mostra os lugares em que essas operações foram realizadas e o número de inserções bem-sucedidas:



DRIVER 1: PLATAFORMA CRIPTOLÓGICA MUNDIAL DE SIGINT/DEFESA

Da esquerda para a direita: Cabo óptico de alta velocidade / Grandes acessos secretos, clandestinos ou cooperativos / 20 programas de acesso no mundo / Regionais / Genebra / Atenas / Roma / Quito / San José / Caracas / Tegucigalpa / Bogotá / Cidade do México / Brasília / Manágua / Havana / Cidade do Panamá / Lagos / Kinshasa / Lusaka / Budapeste / Praga / Viena / Sófia / Rangoon / Bancoc / Nova Délhi / Paris / Berlim / Frankfurt / Zagreb / Phnom Penh / Sarajevo / Pristina / Tirana / La Paz / Cidade da Guatemala / Anexo Viena / RESC / Milão / Langley / Reston

Abaixo, da esquerda para a direita: CNE: > 50.000 implantações no mundo / Classes de acesso / Terceiros/Intermediários / 30 países / Regionais / 80 + SCs / CNE / > 50.000 implantações no mundo / Cabos grandes / 20 acessos importantes / FORNSAT / 12 + 40 regionais

Com base nos documentos de Snowden, o *New York Times* noticiou que a NSA na verdade implantou esse so ware específico "em quase 100.000 computadores espalhados pelo mundo". Embora o *malware* em geral seja instalado por meio da "obtenção de acesso a redes de computador, a NSA cada vez mais vem lançando mão de uma tecnologia secreta que lhe permite acessar e alterar dados em computadores mesmo quando não conectados à internet".

Além do trabalho com empresas de telecomunicações e de internet dispostas a cooperar, a NSA também se uniu a governos estrangeiros para ampliar o alcance de seu sistema de vigilância. De modo geral, a agência tem três categorias diferentes de relações com países estrangeiros. A primeira delas é com o grupo dos Cinco Olhos: os Estados Unidos espionam junto com esses países, mas raramente os espionam, a menos que solicitados pelas autoridades dos próprios países parceiros. O segundo grupo é formado por países com os quais a NSA trabalha em projetos de vigilância específicos ao mesmo tempo que os espiona de forma ampla. O terceiro é formado por países que os Estados Unidos espionam de forma rotineira, mas com os quais quase nunca coopera.

Dentro do grupo dos Cinco Olhos, o aliado mais próximo da NSA é a Central de Comunicações do Governo (GCHQ) britânica. Conforme noticiado pelo *Guardian* com base em documentos fornecidos por Snowden, "nos últimos três anos, o governo dos Estados Unidos pagou no mínimo 100 milhões de libras à agência de espionagem do Reino Unido, a GCHQ, para garantir acesso e influência nos programas de coleta de inteligência britânicos". Esses pagamentos eram um incentivo para que a GCHQ apoiasse as ações de vigilância da NSA. "A GCHQ precisa exercer sua influência, e deve fazer isso de modo visível", afirmava um briefing estratégico secreto da agência britânica.

Os países-membros dos Cinco Olhos compartilham a maioria de suas atividades de vigilância e se reúnem todo ano em uma conferência de Desenvolvimento de Sinais durante a qual se gabam de sua expansão e dos sucessos do ano anterior. Sobre a aliança dos Cinco Olhos, o vice-diretor da NSA John Inglis afirmou que esses países, "sob muitos aspectos, praticam a inteligência de modo combinado – basicamente certificando-se de alavancar as capacidades um do outro, visando ao benefício mútuo".

Muitos dos programas de vigilância mais invasivos são implementados pelos parceiros dos Cinco Olhos, e um número significativo deles envolve a GCHQ. Especialmente dignos de nota são os esforços conjuntos da agência britânica e da NSA para decifrar as técnicas de criptografia comuns usadas para proteger transações pessoais na internet, como as operações de *on-line banking* ou o acesso a históricos médicos. O sucesso das duas agências em implementar acessos do tipo "porta dos fundos" nesses sistemas de criptografia não apenas lhes permitiu espiar transações privadas das pessoas, mas também enfraqueceu os sistemas para todo mundo, tornando-os mais vulneráveis a hackers mal-intencionados e a outras agência de inteligência estrangeiras.

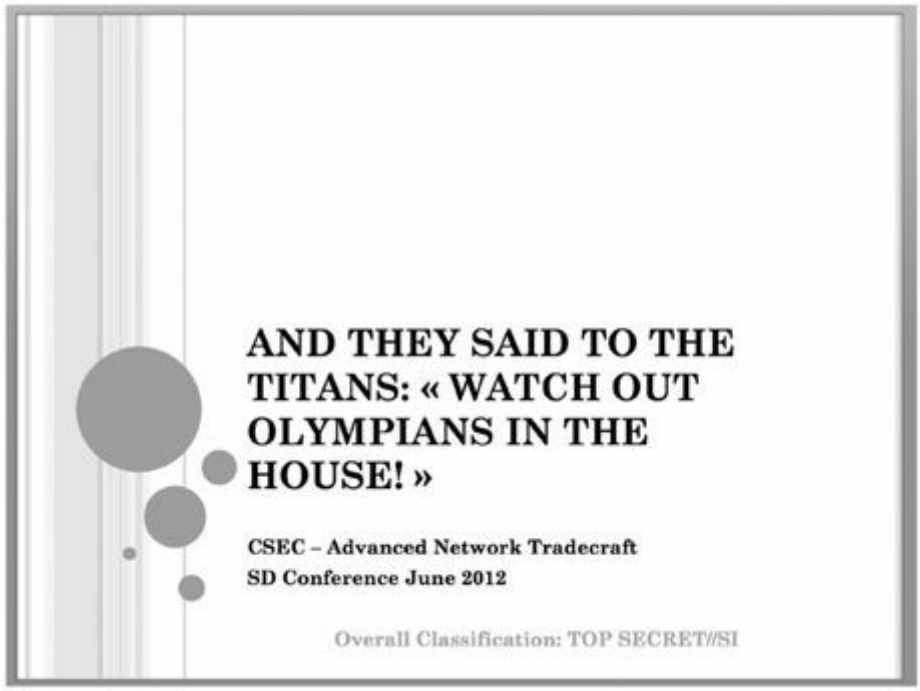
A GCHQ também realizou uma interceptação em massa de dados de comunicação nos cabos submarinos de fibra óptica do mundo. Em um programa chamado Tempora, a GCHQ desenvolveu "a capacidade de acessar e armazenar um grande volume de dados extraídos de cabos de fibra óptica por até trinta dias, de modo que possam ser peneirados e analisados", noticiou o *Guardian*, e "a GCHQ e a NSA podem, portanto, acessar e processar grandes quantidades de comunicações entre pessoas totalmente inocentes". Os dados interceptados incluem todo tipo de atividade on-line, entre "registros de chamadas telefônicas, conteúdo de e-mails, posts no Facebook e o histórico de navegação de qualquer usuário da internet".

As atividades de vigilância da GCHQ são tão abrangentes – e tão isentas de prestação de contas – quanto as da NSA. Como observado pelo *Guardian*:

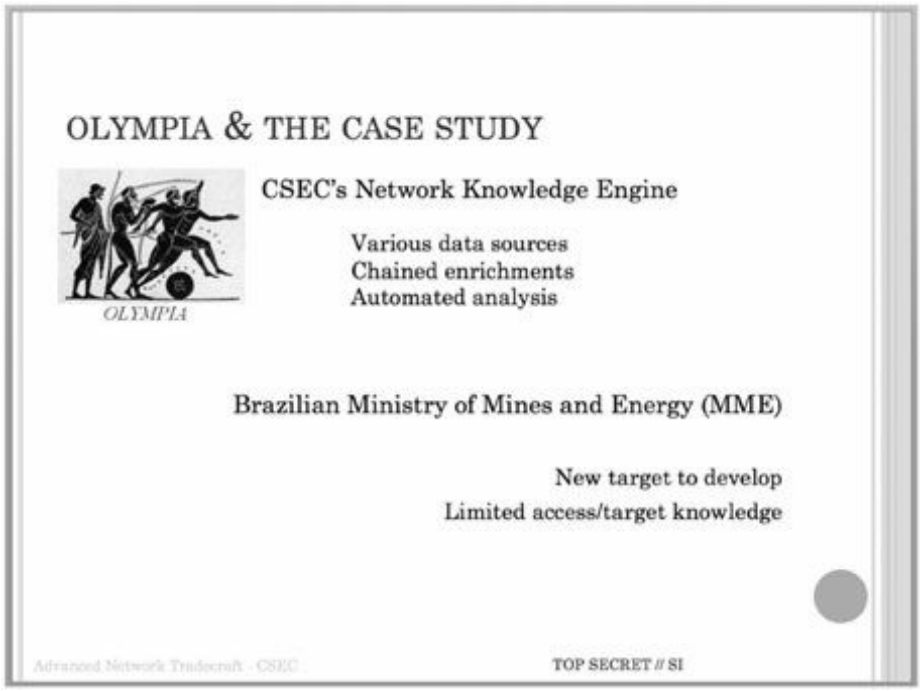
> A magnitude da ambição da agência se reflete nos títulos de seus dois principais componentes: Dominação da Internet e Exploração Global de Telecoms, cujo objetivo é recolher o máximo

possível de tráfego on-line e telefônico. Isso tudo está sendo feito sem qualquer tipo de conhecimento ou debate público.

O Canadá também é um parceiro muito ativo da NSA e, por si só, uma enérgica força de vigilância. Na conferência de Desenvolvimento de Sinais de 2012, a CSEC (Organização de Serviços de Comunicações do Canadá) gabou-se de ter tido como alvo o Ministério das Minas e Energia do Brasil, agência responsável por regulamentar o setor de maior interesse para as empresas canadenses:



E eles disseram aos Titãs: "Cuidado, olímpios no recinto!"
CSEC – Conferência de Operações Avançadas de Rede, Junho 2012



OLYMPIA & O ESTUDO DE CASO

Motor de Conhecimento de Rede da CSEC / Várias fontes de dados / Acréscimos encadeados / Análise automatizada / Ministério das Minas e Energia do Brasil (MME) / Novo alvo a desenvolver / Acesso limitado/conhecimento do alvo

Como mostra o documento a seguir (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 13), há indícios de uma cooperação generalizada entre a CSEC e a NSA, que inclui esforços do Canadá para criar postos de espionagem destinados a vigiar comunicações mundo afora a pedido da NSA e para o seu benefício, e a espionar parceiros comerciais de interesse para a agência norte-americana.

TOP SECRET//SI//REL USA, FVEY

Agência Nacional de Segurança/
Serviço Central de Segurança

Documento Informativo

Assunto: (U//FOUO) Relação de inteligência entre a NSA e a CSEC canadense

3 de abril de 2013

(U) O que a NSA fornece ao parceiro:

(S//SI//REL. A EUA, CAN) SIGINT: NSA e CSEC cooperam para identificar alvos em aproximadamente vinte países de alta prioridade. INFORMAÇÃO OMITIDA A NSA compartilha avanços tecnológicos, habilidades criptográficas, softwares e recursos para esforços de coleta, processamento e análise de última geração, e capacidades de análise da informação. O compartilhamento de inteligência com a CSEC abrange alvos nacionais e transnacionais no mundo todo. Nenhum recurso do CCP (Programa Consolidado de Criptografia) é alocado para a CSEC, mas a NSA às vezes cobre os custos de P&D (pesquisa e desenvolvimento) e tecnologia nos projetos em parceria com a CSEC.

(U) O que o parceiro fornece à NSA:

(TS//SI//REL. A EUA, CAN) A CSEC oferece recursos para coleta, processamento e análise avançados, e estabeleceu locais secretos a pedido da NSA. A CSEC compartilha com a NSA seu acesso geográfico privilegiado a áreas não disponíveis aos Estados Unidos INFORMAÇÃO OMITIDA e fornece produtos de criptografia, análise criptográfica, tecnologia e software. A CSEC aumentou seu investimento em projetos de pesquisa e desenvolvimento de interesse mútuo.

O relacionamento entre os Cinco Olhos é tão estreito que os governos dos países-membros colocam os desejos da NSA acima da privacidade de seus próprios cidadãos. O *Guardian* publicou uma notícia sobre um memorando de 2007, por exemplo, que descrevia um acordo "permitindo à agência 'desocultar' e conservar dados pessoais sobre britânicos anteriormente fora dos limites". Além

disso, as regras foram modificadas em 2007 "para permitir à NSA analisar e armazenar os números de celular e fax, e-mails e endereços de IP de qualquer cidadão britânico recolhidos por esse arrastão".

Em 2011, o governo australiano deu um passo além e pediu à NSA, de forma explícita, que "estendesse sua parceria", ou aumentasse a vigilância sobre os próprios cidadãos. Em uma carta de 21 de fevereiro, o vice-presidente interino do Diretório de Inteligência de Sinais de Defesa da Austrália escreveu para o Diretório de Inteligência de Sinais da NSA dizendo que seu país estava "enfrentando agora uma ameaça sinistra e determinada de extremistas 'caseiros' ativos tanto no exterior quanto dentro da Austrália". Ele solicitou um aumento da vigilância sobre as comunicações de cidadãos australianos considerados suspeitos por seu próprio governo (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 14):

Embora nós mesmos tenhamos feito um esforço significativo de análise e coleta para encontrar e explorar essas comunicações, as dificuldades que enfrentamos para obter acesso regular e confiável a tais comunicações prejudica nossa capacidade de detectar e impedir ataques terroristas e diminui nossa capacidade de proteger a vida e a segurança tanto dos cidadãos australianos como as de nossos amigos e aliados próximos.

Temos tido uma longa e produtiva parceria com a NSA para obter um acesso minimizado à coleta judicialmente aprovada dos Estados Unidos relacionada a nossos mais valiosos alvos terroristas na Indonésia. Esse acesso tem sido fundamental para os esforços do Diretório de Sinais de Defesa no sentido de desorganizar e conter as capacidades operacionais dos terroristas na nossa região, como mostra a prisão recente do foragido Umar Patek, responsável pelos atentados a bomba em Bali.

A oportunidade de ampliar essa parceria com a NSA para cobrir o número cada vez maior de australianos envolvidos em atividades extremistas internacionais – em especial os australianos envolvidos com a AQAP – seria muito bem-vinda.

Para além da parceria dos Cinco Olhos, o nível seguinte de cooperação da NSA é com os aliados do "grupo B": países que têm uma cooperação limitada com a agência e que também são alvo de uma vigilância agressiva e não solicitada. A NSA definiu claramente esses dois níveis de aliança:

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

GRUPO A / Cooperação abrangente / Austrália / Canadá / Nova Zelândia / Reino Unido

GRUPO B / Cooperação focada / Alemanha / Áustria / Bélgica / Coreia do Sul / Dinamarca / Espanha / Grécia / Hungria / Islândia / Itália / Japão / Luxemburgo / Noruega / Países Baixos / Polônia / Portugal / República Tcheca / Suécia / Suíça / Turquia

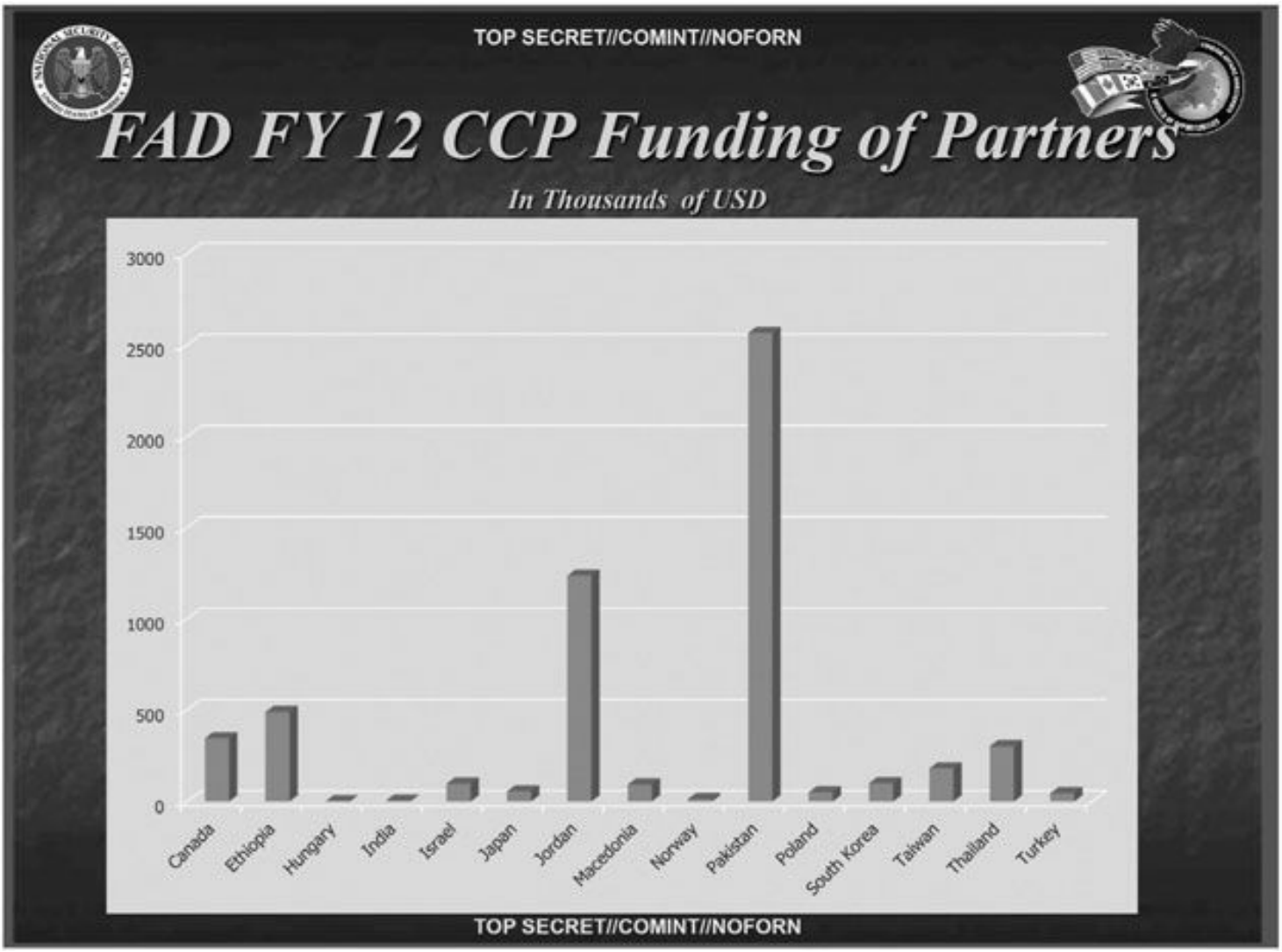
Usando designações distintas (e referindo-se ao Grupo B como "terceiros"), um documento mais recente da NSA – da "Retrospectiva de Parceiros Estrangeiros" do ano fiscal de 2013 – mostra uma lista ainda mais extensa de parceiros da NSA, que inclui organizações internacionais como a OTAN:

PARCEIROS DE SIGINT APROVADOS

Coluna da esquerda: Parceiros / Austrália / Canadá / Nova Zelândia / Reino Unido / Coalizões/Multilaterais / AFSC / OTAN / SSEUR / SSPAC

Colunas da direita: Terceiros / Alemanha / Arábia Saudita / Argélia / Áustria / Bélgica / Cingapura / Coreia / Croácia / Dinamarca / Emirados Árabes Unidos / Espanha / Etiópia / Finlândia / França / Grécia / Hungria / Índia / Israel / Itália / Japão / Jordânia / Macedônia / Noruega / Países Baixos / Paquistão / Polônia / República Tcheca / Romênia / Suécia / Tailândia / Taiwan / Tunísia / Turquia

Assim como no caso da GCHQ, a NSA muitas vezes mantém essas alianças pagando ao parceiro para que desenvolva tecnologias e pratique vigilância, podendo assim direcionar a forma como a espionagem é feita. A "Retrospectiva de Parceiros Estrangeiros" do ano fiscal de 2012 revela vários países que receberam pagamentos desse tipo, entre os quais Canadá, Israel, Japão, Jordânia, Paquistão, Taiwan e Tailândia.



FINANCIAMENTO DE PARCEIROS DO CCP PELA FAD NO ANO FISCAL DE 2012

Em milhares de US$

Canadá / Etiópia / Hungria / Índia / Israel / Japão / Jordânia / Macedônia / Noruega / Paquistão / Polônia / Coreia do Sul / Taiwan / Tailândia / Turquia

Em especial, a NSA tem uma relação de vigilância com Israel que muitas vezes acarreta uma cooperação tão estreita quanto a parceria dos Cinco Olhos, quando não mais estreita ainda. Um Memorando de Acordo entre a NSA e o serviço de inteligência israelense expõe em detalhes como os Estados Unidos dão o passo pouco usual de compartilhar com Israel, de forma rotineira, dados brutos de inteligência contendo comunicações de cidadãos norte-americanos. As informações fornecidas a Israel incluem "transcrições, *gists*, fac-símiles, telex, voz, além de metadados e conteúdo de DNI".

O que torna esse compartilhamento particularmente detestável é que o material é encaminhado para Israel sem ter passado pelo processo de "minimização" previsto em lei. Os procedimentos de minimização visam supostamente a garantir que, quando a vigilância em massa da NSA recolher alguns dados de comunicação que mesmo suas amplas diretrizes não lhe permitam coletar, essa informação seja destruída o mais rápido possível e não seja passada adiante. Da forma como a lei

está redigida hoje, as exigências de minimização já têm várias brechas, entre elas isenções para "informações importantes de inteligência estrangeira" ou "qualquer indício de crime". No entanto, quando se trata de compartilhar dados com a inteligência de Israel, a NSA parece ter deixado de lado qualquer preocupação com essa lei.

O memorando é claro: "A NSA envia rotineiramente para a ISNU (Unidade Nacional de Inteligência de Sinais Israelense) material bruto de coleta, tanto minimizado quanto não minimizado."

Ao ressaltar como um país pode, ao mesmo tempo, cooperar com a vigilância e ser alvo desta, um documento da NSA (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 15) que retraça a história da cooperação com Israel menciona "questões de confiança relacionadas a operações prévias israelenses" e identifica o país como um dos serviços de vigilância mais agressivos nas ações contra os Estados Unidos:

(TS//SI//REL) Há também algumas surpresas... A França coleta informações técnicas do Departamento de Defesa dos Estados Unidos, e Israel também nos tem como alvo. Por um lado, os israelenses são parceiros de SIGINT extraordinários para nós, mas por outro nos têm como alvo para saber nosso posicionamento sobre questões relacionadas ao Oriente Médio. Uma NIE (Estimativa de Inteligência Nacional) classificou Israel como o terceiro serviço de inteligência mais agressivo contra os Estados Unidos.

O mesmo documento (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 15) observou que, apesar do relacionamento estreito entre as agências de inteligência norte-americanas e israelenses, a grande quantidade de informações fornecida pelos Estados Unidos a Israel gerou pouco retorno. O serviço de inteligência israelense só estava interessado em coletar dados que pudessem ajudá-lo. A NSA se queixa de que a parceria estava "quase totalmente" direcionada às necessidades de Israel.

Equilibrar o compartilhamento de SIGINT de forma igualitária entre as necessidades dos Estados Unidos e as de Israel tem sido um desafio constante. Na última década, esse equilíbrio pendeu de forma pronunciada a favor das preocupações de segurança israelenses. O 11 de Setembro aconteceu e passou, e o único verdadeiro relacionamento de CT [contraterrorismo] com Terceiros da NSA foi quase inteiramente pautado pelas necessidades do parceiro.

Um nível abaixo, depois dos parceiros dos Cinco Olhos e dos países do "segundo grupo" como Israel, o terceiro grupo é composto por países que com frequência são alvo, mas nunca parceiros, dos programas de espionagem dos Estados Unidos. De forma previsível, entre eles estão governos considerados adversários, como China, Rússia, Irã, Venezuela e Síria, mas também países que vão de geralmente amigáveis a neutros, como Brasil, México, Argentina, Indonésia, Quênia e África do Sul.

Quando as revelações sobre a NSA vieram à tona, o governo dos Estados Unidos tentou defender suas ações argumentando que, ao contrário dos cidadãos estrangeiros, os norte-americanos estão

protegidos da vigilância sem autorização da agência. Em 18 de junho de 2013, o presidente Obama disse ao entrevistador e jornalista Charlie Rose: "Uma coisa eu posso afirmar de modo inequívoco: se você é cidadão norte-americano, a NSA não pode escutar suas ligações (...) É a lei, o regulamento, a menos que a agência (...) vá ao tribunal, consiga um mandado e busque uma causa provável, como sempre foi." Da mesma forma, o presidente republicano do Comitê de Inteligência da Câmara, Mike Rogers, declarou à CNN que a NSA "não está escutando as ligações dos norte-americanos. Se estiver, é ilegal. A agência está agindo contra a lei".

Foi uma linha de defesa um tanto estranha: para todos os efeitos, o que se fez foi dizer ao resto do mundo que a NSA viola, sim, a privacidade dos não americanos. Ao que parece, proteções de privacidade só valem para os cidadãos norte-americanos. Essa declaração gerou tamanha indignação internacional que até o CEO do Facebook, Mark Zuckerberg, que não se destaca exatamente por uma defesa veemente da privacidade, reclamou que o governo de seu país tinha "estragado tudo" em sua reação ao escândalo da NSA, pondo em risco os interesses das empresas internacionais de internet: "O governo disse que não se preocupem, não estamos espionando nenhum americano. Maravilha, isso é muito útil mesmo para empresas que estão tentando trabalhar com pessoas do mundo todo. Obrigado por ter sido bem claro. Eu acho que foi péssimo."

Além de ser uma estratégia estranha, a declaração também é escancaradamente falsa. Na realidade, apesar dos repetidos desmentidos do presidente Obama e das mais altas autoridades de seu governo, a NSA intercepta de forma contínua o conteúdo das comunicações de cidadãos norte-americanos, sem qualquer mandado individual de "causa provável" para justificar tal vigilância. Isso porque, conforme já observado, a lei FISA de 2008 permite à NSA, sem mandado individual, monitorar o conteúdo das comunicações dos americanos, contanto que sejam feitas entre eles e um cidadão estrangeiro alvo de monitoramento. A NSA rotula isso de coleta "incidental", como se o fato de a agência espionar americanos fosse alguma espécie de acidente sem importância. Só que essa sugestão é enganosa. Como explicou Jameel Jaffer, vice-diretor jurídico da ACLU:

> O governo muitas vezes afirma que a vigilância das comunicações dos cidadãos americanos é "incidental," o que dá a impressão de que a espionagem das ligações e dos e-mails desses cidadãos pela NSA é involuntária, ou até mesmo algo que o governo lamenta.
>
> No entanto, quando as autoridades do governo Bush solicitaram ao Congresso esse novo poder de vigilância, afirmaram de maneira bem explícita que as comunicações de maior interesse para elas eram as dos próprios americanos. Basta ver, por exemplo, FISA para o século XXI, Audiência do Comitê do Senado sobre o Judiciário, 109º Congresso (depoimento de Michael Hayden), afirmando que determinadas comunicações "com uma das pontas nos Estados Unidos" são "as mais importantes para nós".
>
> O principal objetivo da lei de 2008 era possibilitar ao governo coletar as comunicações internacionais justamente dos americanos, e fazer isso sem referência à possibilidade de qualquer participante dessas comunicações estar cometendo um ato ilegal. Grande parte da defesa do governo tem por objetivo ocultar esse fato, mas ele é crucial: o governo não precisa ter americanos como "alvo" para coletar um grande volume das suas comunicações.

Jack Balkin, professor da Faculdade de Direito de Yale, concorda que a lei FISA de 2008 dava ao

presidente, de forma efetiva, autoridade para conduzir um programa "de efeito semelhante ao programa de vigilância sem autorização" antes implementado em segredo por George Bush. "Tais programas podem incluir, inevitavelmente, muitas chamadas telefônicas envolvendo americanos que podem não ter qualquer ligação com terrorismo ou com a Al-Qaeda."

Outro fato que desmente as garantias de Obama é a postura subserviente do tribunal da FISA, que autoriza quase todas as solicitações de vigilância apresentadas pela NSA. Defensores da agência com frequência citam os procedimentos judiciais da FISA como uma prova de supervisão efetiva de suas atividades. No entanto, o tribunal da FISA foi criado não para manter um controle genuíno sobre o poder do governo, mas como uma medida ornamental, para proporcionar apenas uma aparência de reforma que aplacasse a ira da população quanto aos abusos de vigilância denunciados nos anos 1970.

A inutilidade desse órgão como verdadeiro controle dos abusos de vigilância é evidente, pois o tribunal da FISA não possui nenhum dos atributos que nossa sociedade em geral considera os elementos mínimos necessários a um sistema de justiça. Reúne-se em total sigilo; apenas uma das partes – o governo – tem permissão para assistir às audiências e defender seu ponto de vista; suas decisões são automaticamente classificadas como "ultrassecretas". De modo revelador, o tribunal da FISA funcionou, durante anos, dentro do Departamento de Justiça, deixando claro seu papel como parte do Executivo, e não um órgão judiciário independente que exerça uma supervisão real.

Os resultados foram exatamente o que era de esperar: o tribunal quase nunca rejeita solicitações específicas da NSA para vigiar alvos americanos. Desde sua criação, a FISA sempre teve a última palavra. Em seus primeiros 24 anos, de 1978 a 2002, o tribunal rejeitou um total de *zero* solicitações do governo e aprovou muitos milhares. Na década subsequente, até 2012, rejeitou apenas onze solicitações oficiais e aprovou, no total, mais de 20 mil pedidos.

Uma das exigências da lei FISA de 2008 é que o Executivo apresente todos os anos, ao Congresso, o número de solicitações de grampo recebidas e em seguida aprovadas, modificadas ou rejeitadas pelo tribunal. A prestação de contas de 2012 (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 16) mostrou que o tribunal havia aprovado cada uma das 1.788 solicitações de vigilância eletrônica avaliadas e feito "modificações" – ou seja, restringido o escopo da ordem – em apenas quarenta delas, ou seja, menos de 3%.

Solicitações feitas ao tribunal da FISA durante o ano-calendário de 2012 (seção 107 da Lei, título 50 do Código Legal dos EUA, §1.807)

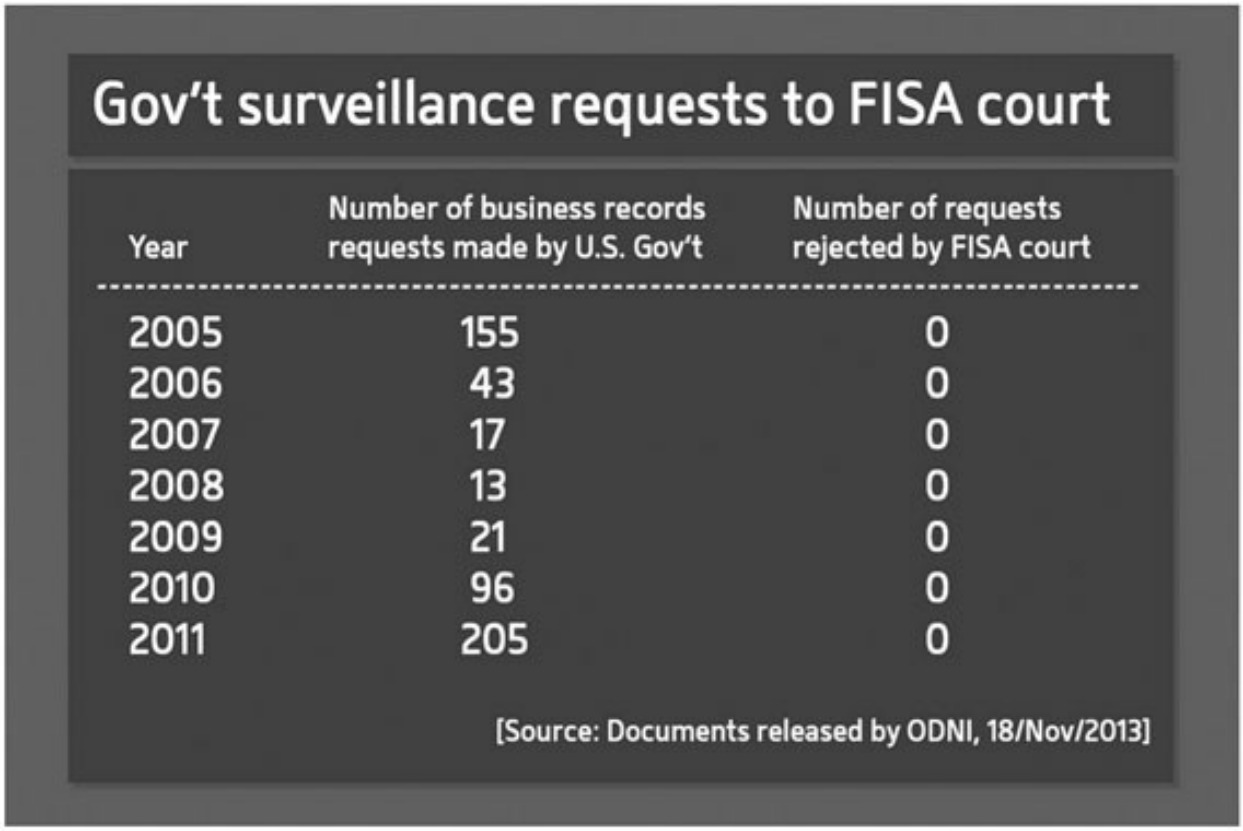
Durante o ano-calendário de 2012, o governo apresentou 1.856 solicitações de autorização ao FISC (Tribunal de Vigilância de Inteligência Internacional) para efetuar vigilância eletrônica e/ou buscas físicas com fins de inteligência estrangeira. Os 1.856 pedidos incluem os feitos apenas para vigilância eletrônica, os efetuados apenas para buscas físicas e solicitações combinadas pedindo autorização para vigilância eletrônica e busca física. Destas, 1.789 solicitações incluíam solicitações de autorização para efetuar vigilância eletrônica.

Dessas 1.789 solicitações, uma foi retirada pelo governo. O FISC não negou nenhuma delas, seja no todo ou em parte.

Quase o mesmo aconteceu em 2011, quando a NSA declarou 1.676 solicitações e o tribunal da

FISA, embora tenha modificado trinta delas, "não negou nenhuma, seja no todo ou em parte".

A subserviência desse tribunal à NSA também é demonstrada por outra estatística. Eis a seguir, por exemplo, a reação do tribunal da FISA, ao longo dos últimos seis anos, a diversos pedidos da NSA com base na Lei Patriota para obter os históricos profissionais – telefônicos, financeiros ou médicos – de indivíduos dos Estados Unidos:



Gov't surveillance requests to FISA court

Year	Number of business records requests made by U.S. Gov't	Number of requests rejected by FISA court
2005	155	0
2006	43	0
2007	17	0
2008	13	0
2009	21	0
2010	96	0
2011	205	0

[Source: Documents released by ODNI, 18/Nov/2013]

SOLICITAÇÕES DE VIGILÂNCIA DO GOVERNO AO TRIBUNAL DA FISA

Da esquerda para a direita: Ano / Número de solicitações de históricos profissionais feitas pelo governo dos Estados Unidos / Número de solicitações rejeitadas pelo tribunal da FISA

(Fonte: Documentos liberados pelo ODNI, 18/nov./2013)

Portanto, mesmo nos casos limitados em que a aprovação do tribunal da FISA é necessária para monitorar as comunicações de alguém, o procedimento é mais uma pantomima vazia do que um verdadeiro controle da NSA.

Outra camada de supervisão à agência seria supostamente representada pelos comitês de inteligência do Congresso, também criados na esteira dos escândalos de vigilância dos anos 1970, mas estes são ainda mais subservientes do que o tribunal da FISA. Embora devessem efetuar uma "atenta vigilância legislativa" da comunidade de inteligência, esses comitês na realidade são hoje presididos pelos mais esmerados defensores da NSA em Washington: a democrata Dianne Feinstein, no Senado, e o republicano Mike Rogers, na Câmara. Em vez de proporcionar qualquer tipo de controle antagônico às atividades da agência, os comitês de Feinstein e Rogers existem sobretudo para defender e justificar qualquer coisa que esta faça.

Como afirmou o jornalista da revista *e New Yorker* Ryan Lizza em uma reportagem de dezembro de 2013, "em vez de supervisionar, o comitê do Senado na maioria das vezes trata os altos funcionários de inteligência como ídolos de matinê". Pessoas que assistiram a audiências do comitê sobre as atividades da NSA ficaram chocadas ao ver como os senadores interrogavam os funcionários da NSA que compareciam diante deles. As "perguntas" em geral nada mais eram do que longos monólogos dos senadores sobre suas lembranças do atentado de 11 de setembro e como era vital impedir futuros ataques. Os integrantes do comitê dispensavam a oportunidade de interrogar esses funcionários e exercer suas responsabilidades de supervisão em prol de uma propaganda em defesa da NSA. A cena traduz com perfeição a verdadeira função dos comitês de inteligência na última década.

Na verdade, os membros dos comitês do Congresso algumas vezes defenderam a NSA com vigor ainda maior do que os funcionários da própria agência. Em determinada ocasião, em agosto de 2013, dois membros do Congresso – o democrata Alan Grayson, da Flórida, e o republicano Morgan Griffith, da Virgínia – me procuraram separadamente para reclamar que o Comitê Especial Permanente de Inteligência da Câmara estava impedindo que eles e outros representantes acessassem as informações mais básicas sobre a NSA. Ambos me entregaram cartas que haviam escrito para os assessores do diretor Rogers solicitando dados sobre os programas da NSA descritos pela imprensa; os pedidos tinham sido rechaçados repetidas vezes.

Na esteira de nossas reportagens sobre Snowden, um grupo de senadores de ambos os partidos, preocupado com os abusos de vigilância havia tempos, iniciou esforços para propor leis que impusessem limites verdadeiros aos poderes da NSA. Contudo, esses reformadores, liderados pelo senador democrata Ron Wyden, do Oregon, esbarraram imediatamente em uma barreira: os defensores da NSA no Senado revidaram propondo leis que tinham apenas a aparência de uma reforma, quando na verdade mantinham ou até mesmo aumentavam os poderes da NSA. Conforme escreveu Dave Wiegel na *Slate*, em novembro:

> Críticos da coleta de dados em massa e dos programas de vigilância da NSA nunca se preocuparam com a *inação* do Congresso. Já esperavam que este fosse propor algo parecido com uma reforma, mas que na realidade codificava e relevava as práticas que estavam sendo reveladas e criticadas. É isso que sempre aconteceu: todas as emendas ou reautorizações da Lei Patriota de 2001 criaram mais portas dos fundos do que paredes.
>
> "Teremos de enfrentar um 'esquadrão da normalidade' formado por membros influentes da liderança de inteligência no governo, seus aliados em *think tanks* e na academia, altos funcionários públicos aposentados e legisladores simpatizantes", alertou no mês passado Ron Wyden, senador pelo Oregon. "Em última instância, eles querem garantir que qualquer reforma da vigilância seja apenas superficial... Proteções da privacidade que na verdade não protegem a privacidade e não valem sequer o papel em que estão escritas."

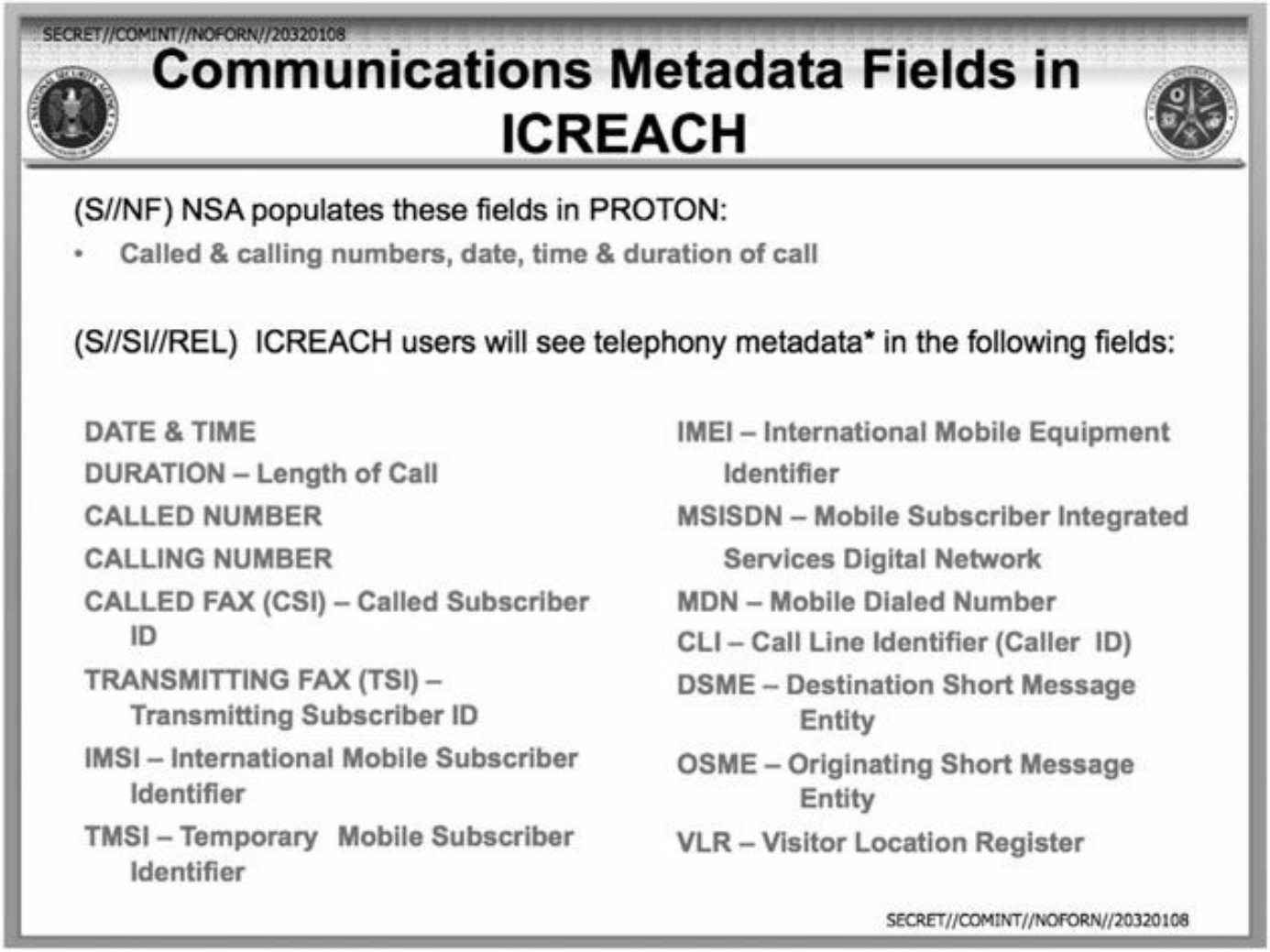
A facção da "falsa reforma" era liderada por Dianne Feinstein, justamente a senadora encarregada de realizar a principal supervisão da NSA. Feinstein tem se mostrado há tempos uma dedicada partidária do setor de segurança nacional dos Estados Unidos, de seu apoio veemente à guerra no Iraque à sua firme defesa dos programas da NSA da era Bush. (Enquanto isso, seu marido tem

participação importante em diversos contratos militares.) Feinstein, ao que tudo indica, era uma escolha natural para chefiar um comitê que alega supervisionar a comunidade de inteligência, mas que na verdade vem, há muitos anos, cumprindo a função oposta.

Assim, apesar de todos os desmentidos do governo, a NSA não tem nenhuma restrição significativa em relação a quem pode vigiar e como. Mesmo quando essas restrições existem nominalmente – nos casos em que os alvos da vigilância são cidadãos americanos –, o processo se tornou em grande parte vazio. A NSA é o exemplo perfeito de agência descontrolada: com poderes para fazer o que quiser, sem quase nenhuma supervisão, transparência ou prestação de contas.

Em termos bastante genéricos, a NSA coleta dois tipos de informação: conteúdo e metadados. "Conteúdo", nesta acepção, significa escutar de fato as chamadas telefônicas das pessoas, ler seus e-mails e chats, bem como ter acesso às suas ações na internet, como históricos de navegação e atividades de busca. A coleta de "metadados", por sua vez, envolve colher dados *sobre* essas comunicações. A NSA define isso como "informações sobre conteúdo (mas não o conteúdo em si)".

Metadados sobre um e-mail, por exemplo, incluem quem mandou mensagens para quem, quando a mensagem foi enviada e a localização de quem a enviou. Em relação às chamadas telefônicas, os metadados são, entre outras coisas, os números de quem liga e de quem recebe a ligação, o tempo de duração da chamada e muitas vezes a localização e o tipo de aparelho usado pelos interlocutores. Em um documento sobre chamadas telefônicas, a NSA especificou quais metadados acessa e armazena:



CAMPOS DE METADADOS DE COMUNICAÇÕES NO ICREACH

A NSA preenche estes campos no PROTON:
Números de destino & origem, data, horário & duração da chamada
Usuários do ICREACH verão metadados* de telefonia nos seguintes campos:
DATA & HORA / DURAÇÃO – Tempo da Chamada / NÚMERO CHAMADO / NÚMERO DE ORIGEM / FAX CHAMADO (CSI) – ID do Assinante Chamado / FAX DE ORIGEM (TSI) – ID do Assinante Transmissor / IMSI – Identificador Internacional de Assinante de Celular / TMSI – Identificador Temporário de Assinante de Celular / IMEI – Identificador Internacional de Equipamento Móvel / MSISDN – Rede Digital de Serviços Integrados do Assinante de Celular / MDN – Número de Celular Chamado / CLI – Identificador de Linha de Origem (Identidade de quem liga) / DSME – Entidade de Destino de Mensagem de Texto / OSME – Entidade de Origem de Mensagem de Texto / VLR – Registro de Localização do Visitante

O governo dos Estados Unidos insistiu que boa parte da vigilância revelada pelo acervo de Snowden diz respeito à coleta de "metadados, não de conteúdo", tentando dar a entender que esse tipo de espionagem não é intrusivo, ou pelo menos não no mesmo grau que a interceptação de conteúdo.

Dianne Feinstein argumentou explicitamente no *USA Today* que a coleta de metadados sobre todos os registros de chamadas dos norte-americanos "não é vigilância" de forma alguma, uma vez que "não coleta o conteúdo de nenhuma comunicação".

Esses argumentos insinceros ocultam o fato de que a vigilância de metadados pode ser, no mínimo, tão intrusiva quanto a interceptação de conteúdo, e muitas vezes ainda mais. Quando o governo sabe para quem você liga e quem liga para você, além da duração exata de todas essas ligações; quando é capaz de listar todos os seus correspondentes de e-mail e todos os locais de onde seus e-mails foram enviados, pode traçar um retrato surpreendentemente completo da sua vida, dos seus contatos e atividades, inclusive algumas de suas informações mais íntimas e pessoais.

Em uma declaração juramentada apresentada pela ACLU questionando a legalidade do programa de coleta de metadados da NSA, o professor de ciências da computação e de assuntos públicos de Princeton Edward Felten explicou por que a vigilância de metadados pode ser especialmente reveladora:

> Considerem o seguinte exemplo hipotético: uma jovem liga para o seu ginecologista; logo em seguida, para a mãe; depois, para um homem com quem, nos últimos meses, falou ao telefone várias vezes após as onze da noite; por fim, para um centro de planejamento familiar que também pratica abortos. Surge assim uma narrativa provável que não ficaria tão evidente caso houvéssemos examinado o registro de um único telefonema.

Mesmo para uma única ligação, os metadados podem ser mais informativos do que o conteúdo da chamada. Escutar a ligação de uma mulher para uma clínica de abortos talvez não revele nada além de uma pessoa marcando ou confirmando uma consulta em um estabelecimento de nome genérico ("Clínica East Side" ou "consultório do Dr. Jones"). Os metadados, contudo, revelariam muito mais do que isso: a identidade de quem recebeu a ligação. O mesmo se aplica às ligações para um serviço de acompanhantes, para um centro de gays e lésbicas, uma clínica especializada em dependentes químicos, um especialista em HIV ou um S.O.S suicídio. Os metadados também exporiam uma conversa entre um ativista defensor dos direitos humanos e um informante em um regime repressor, ou ainda uma fonte sigilosa que estivesse contatando um jornalista para revelar irregularidades em altos escalões da sociedade. Se você faz ligações frequentes tarde da noite para alguém com quem não é casado, isso também vai aparecer nos metadados. Além de registrar todas as pessoas com quem você se comunica e com que regularidade, os metadados também vão registrar todas as pessoas com quem os seus amigos e conhecidos se comunicam, criando assim um panorama completo da sua rede de contatos.

De fato, como observa o professor Felten, escutar ligações pode ser bastante complicado devido a diferenças de idioma, conversas cifradas, uso de gírias ou códigos deliberados e outros atributos que, seja de propósito ou por acidente, confundem o significado. "Como o conteúdo das chamadas tem uma natureza desestruturada, é muito mais difícil analisá-lo de modo automatizado", afirma ele. Os metadados, por sua vez, são matemáticos: limpos, precisos e, portanto, fáceis de analisar. Além disso, como diz Felten, eles são muitas vezes "um substituto do conteúdo".

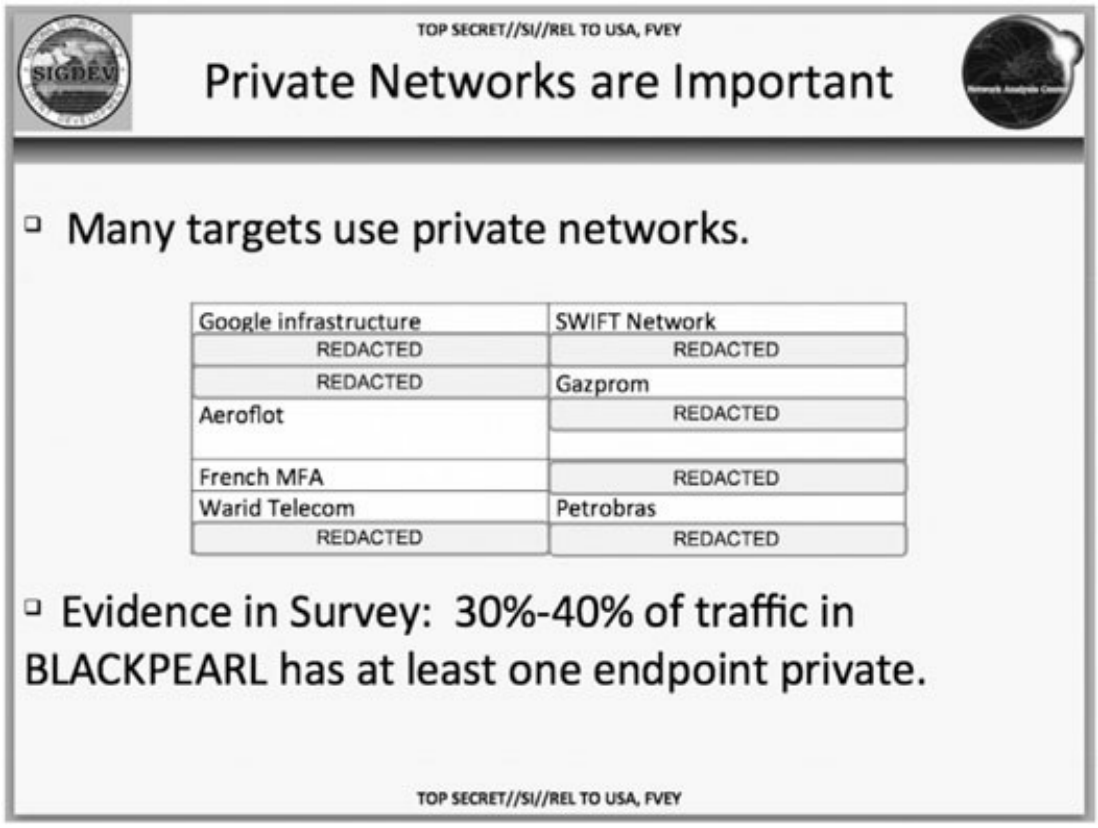
> Os metadados de telefonia podem (...) revelar uma quantidade extraordinária de informações

sobre nossos hábitos e conexões. Padrões de chamadas podem revelar quando estamos acordados e dormindo; nossa religião, caso alguém não costume usar o telefone no dia do sabá ou faça um grande número de ligações no dia de Natal; nossos hábitos profissionais e nossas aptidões sociais; quantos amigos nós temos, e até mesmo nossas afiliações civis e políticas.

Em suma, escreve Felten, "a coleta em massa não apenas possibilita ao governo obter informações sobre mais pessoas como também lhe permite conhecer fatos novos e anteriormente privados que a simples coleta de informações sobre alguns indivíduos específicos não teria permitido".

A preocupação com os muitos usos que o governo poderia encontrar para esse tipo de informação delicada se justifica sobretudo porque, contrariando repetidas alegações do presidente Obama e da NSA, já está claro que um número substancial das atividades da agência nada tem a ver com esforços para combater o terrorismo ou mesmo com a segurança nacional. Boa parte do acervo de Snowden revelou o que só pode ser qualificado de espionagem econômica: escuta e interceptação de e-mails da gigante brasileira de petróleo Petrobras, de conferências econômicas na América Latina, de empresas de energia da Venezuela e do México, e uma vigilância conduzida por aliados da NSA (entre os quais Canadá, Noruega e Suécia) sobre o Ministério das Minas e Energia do Brasil e empresas do setor de energia em vários outros países.

Um documento notável apresentado pela NSA e pela GCHQ enumera vários alvos de espionagem de caráter claramente econômico: a Petrobras, o sistema bancário SWIFT, a petrolífera russa Gazprom e a empresa aérea também russa Aeroflot.



REDES PRIVADAS SÃO IMPORTANTES

Muitos alvos usam redes privadas

Coluna da esquerda: Infraestrutura do Google / INFORMAÇÃO OMITIDA /

INFORMAÇÃO OMITIDA / Aeroflot / MFA da França / Warid Telecom / INFORMAÇÃO OMITIDA

Coluna da direita: Rede SWIFT / INFORMAÇÃO OMITIDA / Gazprom / INFORMAÇÃO OMITIDA / INFORMAÇÃO OMITIDA / Petrobras / INFORMAÇÃO OMITIDA

Indícios do levantamento: 30%-40% do tráfego do BLACKPEARL tem pelo menos um *endpoint* privado

O presidente Obama e as mais altas autoridades de seu governo passaram anos denunciando com veemência a China, por usar suas capacidades de vigilância para obter vantagens econômicas, ao mesmo tempo que insistiam que os Estados Unidos e seus aliados jamais fariam nada parecido. O *Washington Post* citou um porta-voz da NSA segundo o qual o Departamento de Defesa, órgão de que a agência faz parte, "'de fato explora' redes de computadores", mas que "***não*** conduz espionagem econômica em qualquer âmbito que seja, inclusive 'ciberespionagem'" (os asteriscos são do original).

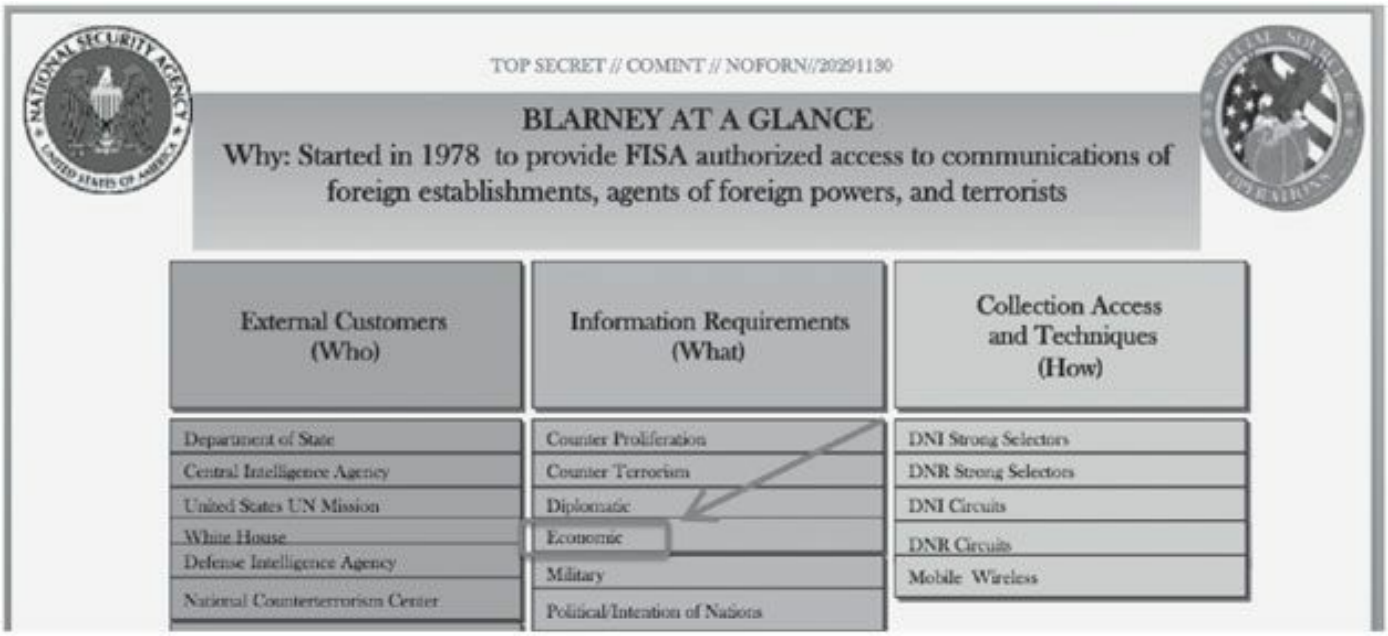
O fato de que a NSA espiona justamente pelos motivos econômicos que nega é provado por seus próprios documentos. A agência age em benefício do que chama de seus "clientes", que incluem não apenas a Casa Branca, o Departamento de Estado e a CIA, mas também agências primordialmente econômicas, como o Representante de Comércio e os departamentos de Agricultura, Tesouro e Comércio dos Estados Unidos:

ATENDIMENTO AOS NOSSOS CLIENTES

Coluna da esquerda: Principais geradores de inteligência final: / CIA / DIA / Estado/INR (Escritório de Inteligência e Pesquisa) / NGA (Associação Nacional de Governadores) / Conselho Nacional de Inteligência

Coluna do meio: Legisladores/Segurança pública: / Casa Branca / Autoridades do Conselho Consultivo do presidente / Diretor da CIA / Embaixadores dos EUA / Representante de Comércio dos EUA / Congresso / Departamentos de: / Agricultura / Justiça / Tesouro / Comércio / Energia / Estado / Segurança Doméstica *Coluna da direita:* Militares/Táticos: / JCS (Estado-Maior Conjunto das forças armadas) / CINCs (comandantes-supremos das forças armadas) / Forças-tarefa / Comandos táticos / Todos os serviços militares / Departamento de Defesa / Alianças / Forças da ONU / OTAN

Na descrição do programa BLARNEY, a NSA discrimina as informações que deve supostamente fornecer aos seus "clientes" como "antiterrorismo", "diplomáticas" e "econômicas".



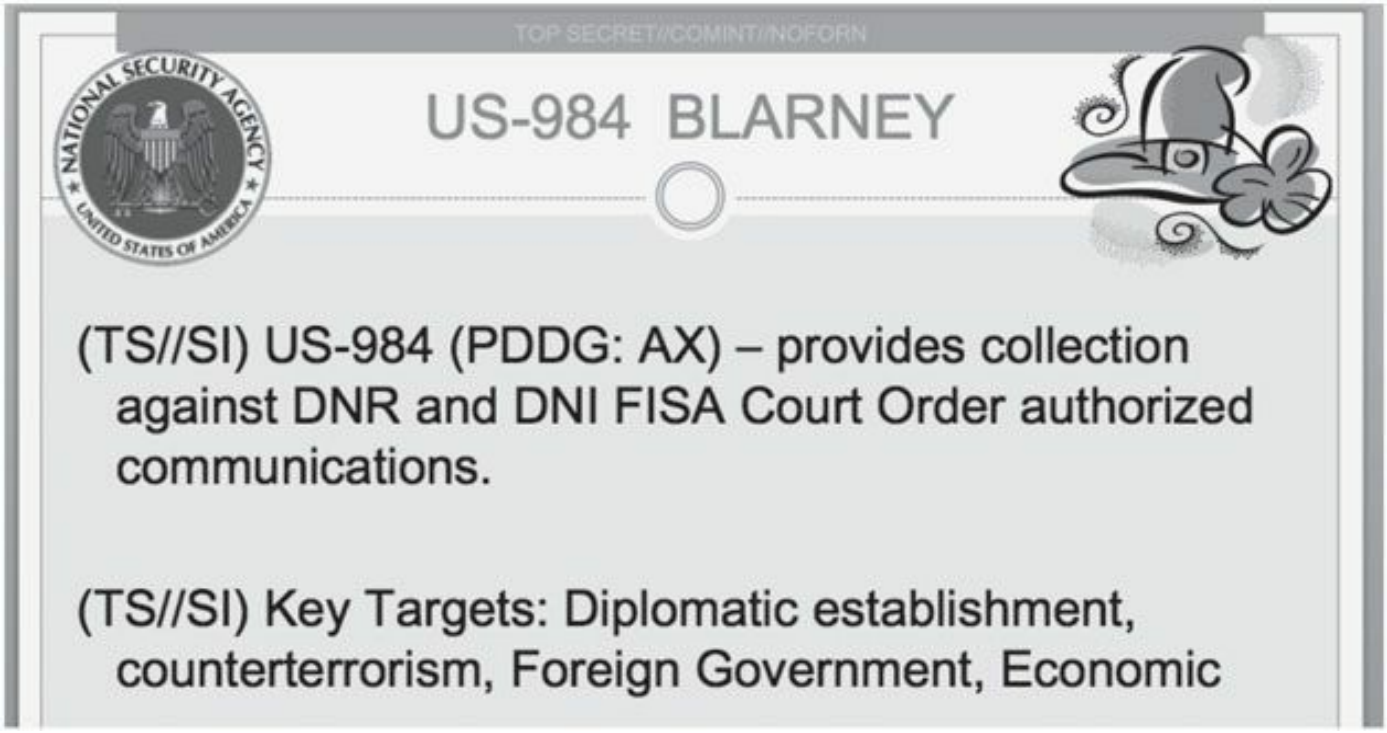
BLARNEY VISÃO GERAL

Por quê: iniciado em 1978 para fornecer acesso autorizado pela FISA a comunicações de estabelecimentos estrangeiros, agentes de potências estrangeiras e terroristas

Coluna da esquerda: Clientes externos (Quem) / Departamento de Estado / CIA / Missão dos Estados Unidos junto à ONU / Casa Branca / Agência de Inteligência de Defesa / Centro Nacional Antiterrorismo

Coluna do meio: Exigências de informação (O quê) / Combate à proliferação / Combate ao terrorismo / Diplomáticas / Econômicas / Militares / Políticas/Intenção de nações

Coluna da direita: Acesso e técnicas de coleta (Como) / Fortes seletores de DNI / Fortes seletores de DNR / Circuitos de DNI / Circuitos de DNR / Rede móvel sem fio



US-984 BLARNEY

US-984 (PDDG: AX) – proporciona coleta de comunicações de DNR e DNI autorizada por ordens judiciais da FISA / Alvos-chave: meio diplomático, antiterrorismo, governos estrangeiros, econômicos

Outros indícios do interesse econômico da NSA ficam patentes em um documento do PRISM que traz uma "amostragem" dos "Tópicos de Relatório" relativos à semana de 2 a 8 de fevereiro de 2013. A lista dos tipos de informação recolhidos em diversos países inclui claramente categorias econômicas e financeiras, entre as quais "energia", "comércio" e "petróleo".

UMA SEMANA NA VIDA DOS RELATÓRIOS DO PRISM

Amostra de Tópicos de Relatório de 2-8 de fev. de 2013

México / Narcóticos / Energia / Segurança interna / Questões políticas / Japão / Comércio / Israel / Venezuela / Fornecimento militar / Petróleo

Um memorando de 2006 (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 17) do diretor de capacidades globais da missão ISI (Questões de Segurança Internacionais) da agência descreve em termos claros a espionagem econômica e comercial da NSA contra países tão diversos quanto Bélgica, Japão, Brasil e Alemanha:

(U) **Missão da NSA em Washington**

(U) **Regional**

(TS//SI) A ISI é responsável por treze estados-nações individuais em três continentes. Um vínculo significativo que une todos esses países é sua importância para as preocupações econômicas, comerciais e defensivas dos Estados Unidos. A divisão da Europa Ocidental e Parcerias Estratégicas tem como foco principal a política externa e atividades comerciais de Bélgica, França, Alemanha, Itália e Espanha, bem como de Brasil, Japão e México.

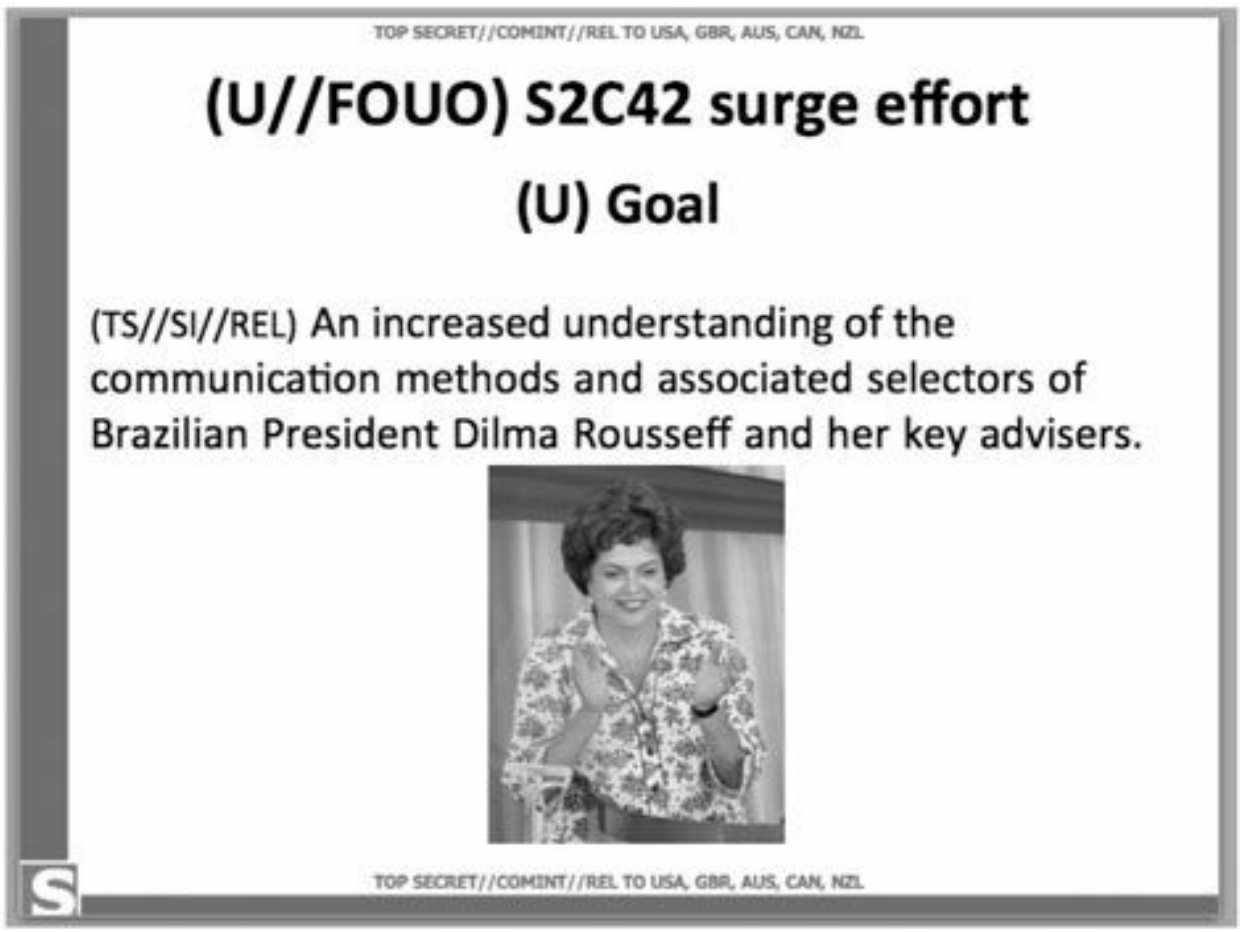
(TS//SI) A divisão Energia e Recursos fornece inteligência privilegiada sobre a produção de energia mundial e o desenvolvimento de países-chave que afetam a economia global. Os alvos atualmente mais importantes são INFORMAÇÃO OMITIDA. Os relatórios incluíram o monitoramento de investimentos internacionais no setor de energia dos países-alvo, melhorias elétricas e de SCADA (Sistemas de Supervisão e Aquisição de Dados), e modelos gerados por computador de projetos de energia previstos.

Em uma notícia sobre um grupo de documentos da GCHQ vazados por Snowden, o *New York Times* observou que os alvos de vigilância da agência britânica muitas vezes incluíam instituições financeiras e "líderes de organizações de auxílio internacional, empresas de energia estrangeiras e um funcionário da União Europeia envolvido em disputas antitruste com companhias de tecnologia norte-americanas". A reportagem acrescentava ainda que as agências norte-americana e britânica "monitoravam as comunicações de funcionários graduados da União Europeia, líderes estrangeiros, entre os quais chefes de Estado africanos e ocasionalmente seus familiares, diretores da ONU e outros programas de auxílio [como, por exemplo, o UNICEF], além de autoridades responsáveis pela supervisão de ministérios de petróleo e finanças".

Os motivos para a espionagem econômica são bem claros. Quando os Estados Unidos usam a NSA para espionar as estratégias de planejamento de outros países durante discussões sobre comércio e economia, podem obter enorme vantagem para a indústria norte-americana. Em 2009, por exemplo, o secretário de Estado assistente omas Shannon escreveu a Keith Alexander para expressar sua "gratidão e [seus] parabéns pelo extraordinário apoio de inteligência de sinais" recebido pelo Departamento de Estado durante a Quinta Cúpula das Américas, conferência destinada à negociação de acordos econômicos. Na carta (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 18), Shannon observou especificamente que a vigilância da NSA havia proporcionado aos Estados Unidos vantagens de negociação em relação aos outros participantes:

Os mais de cem relatórios recebidos da NSA nos proporcionaram uma profunda compreensão dos planos e intenções dos outros participantes da Cúpula e garantiram que nossos diplomatas estivessem bem preparados para aconselhar o presidente Obama e a secretária Clinton na condução de questões controversas, como, por exemplo, Cuba, e na interação com interlocutores difíceis como o presidente venezuelano Chávez.

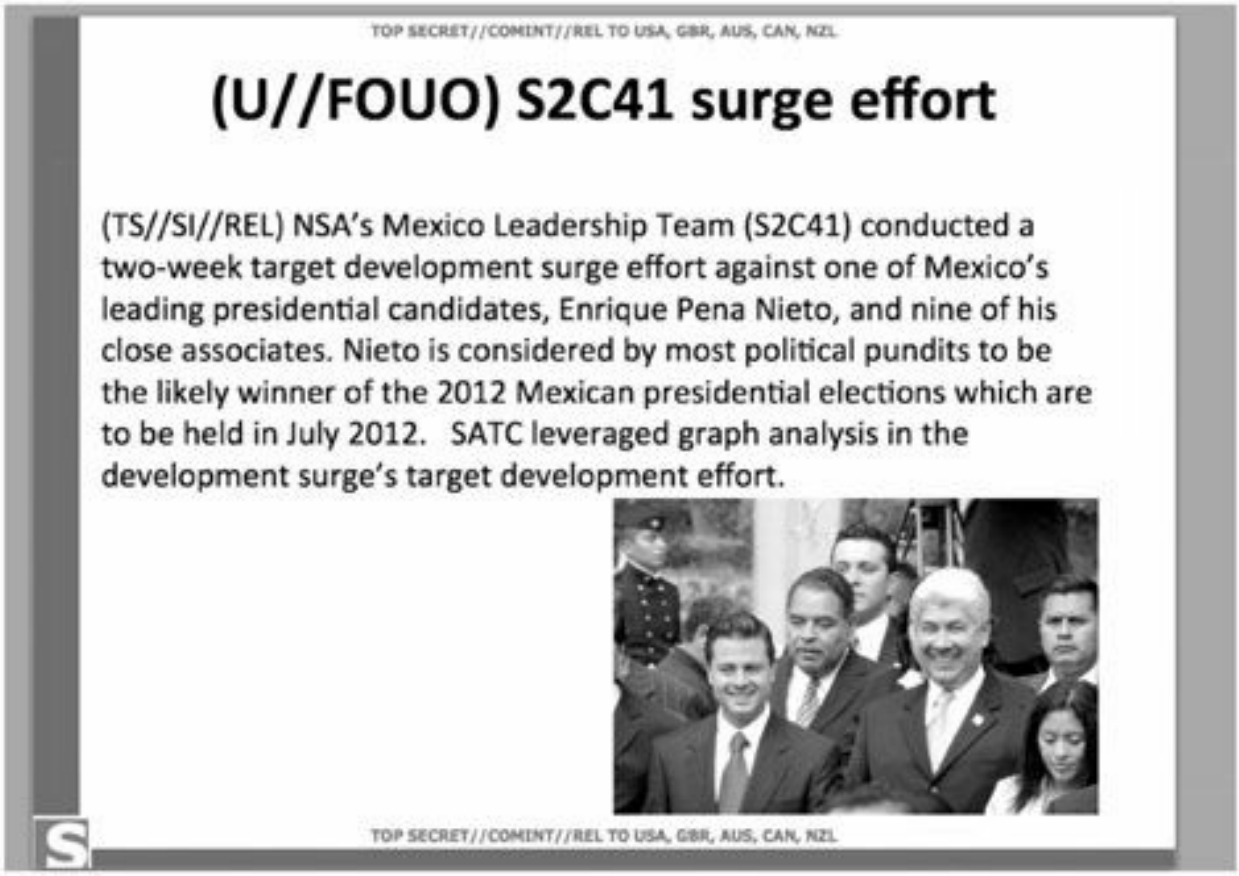
A NSA também se dedica à espionagem diplomática, como demonstram os documentos referentes a "questões políticas". Um exemplo particularmente chocante, de 2011, mostra que a agência teve como alvo dois líderes latino-americanos – a atual presidente do Brasil, Dilma Rousseff, assim como seus "principais consultores", e o então líder da disputa presidencial (e hoje presidente) do México Enrique Peña Nieto, junto com "nove de seus colaboradores mais próximos" – para um "esforço especial" de vigilância especialmente invasiva. O documento chega a incluir algumas das mensagens de texto interceptadas entre Nieto e um "colaborador próximo":



ESFORÇO ESPECIAL DE S2C42

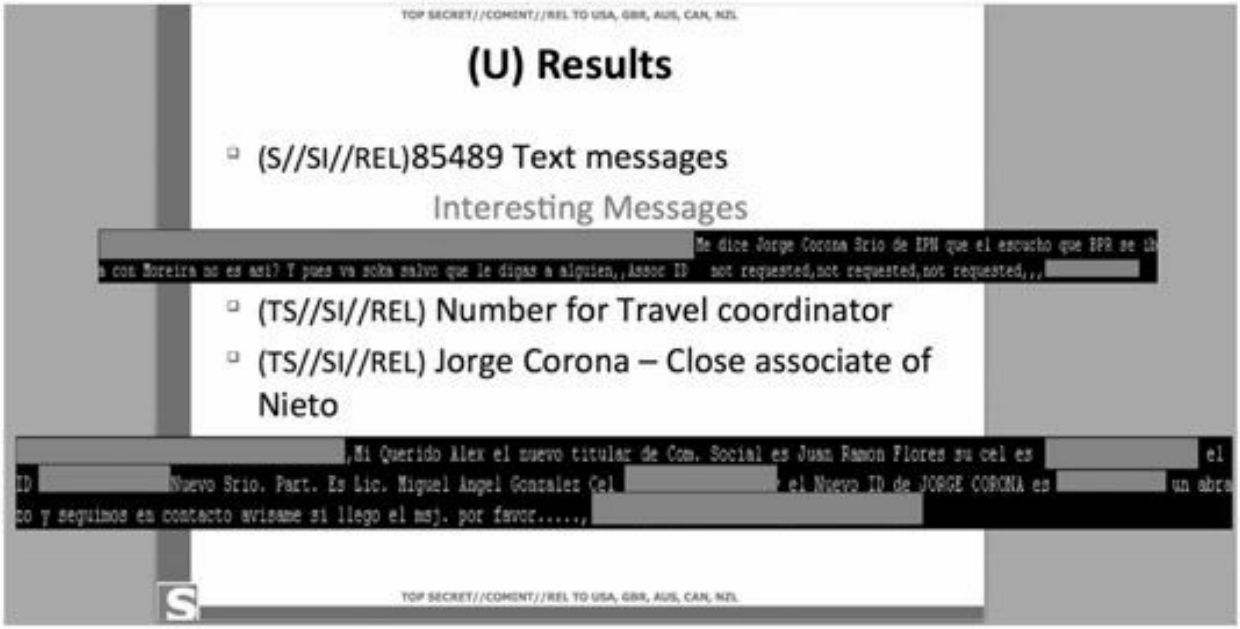
Objetivo

Melhorar a compreensão dos métodos de comunicação e seletores associados relativos à presidente brasileira Dilma Rousseff e seus principais consultores.



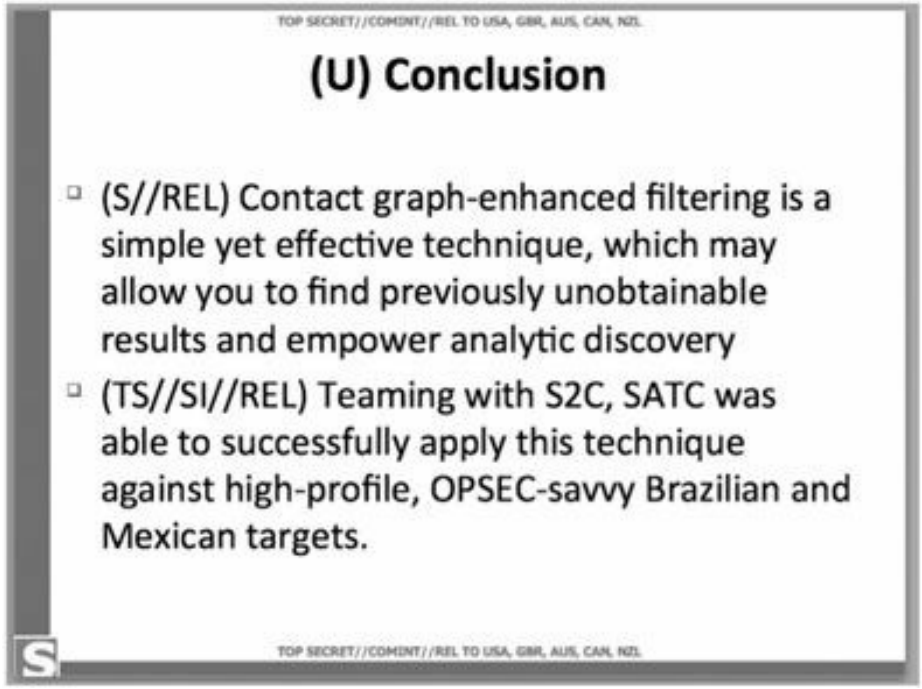
ESFORÇO ESPECIAL DE S2C41

A equipe de Liderança da NSA no México (S2C41) conduziu durante duas semanas um esforço especial para desenvolvimento de alvo visando um dos principais candidatos mexicanos à Presidência, Enrique Peña Nieto, e nove de seus colaboradores mais próximos. Nieto é considerado pela maioria dos especialistas em política o provável vencedor das eleições presidenciais mexicanas de 2012, que ocorrerão em julho deste ano. A SATC contribuiu para o esforço de desenvolvimento com análise de gráficos.



RESULTADOS

85.489 Mensagens de texto / Mensagens interessantes / Coordenador de número de viagem / Jorge Corona – Colaborador próximo de Nieto



CONCLUSÃO

Filtragem auxiliada por gráficos de contatos é uma técnica simples, mas eficaz, que pode conduzir a resultados anteriormente impossíveis de obter e possibilitar conclusões analíticas em parceria com S2C, a SATC conseguiu aplicar com sucesso essa técnica a alvos brasileiros e mexicanos de grande importância e proficientes em segurança de operações.

Pode-se especular sobre o motivo que levou líderes políticos do Brasil e do México a serem alvos da NSA. Ambos os países são ricos em recursos petrolíferos e têm uma presença forte e influente em suas regiões. Além disso, embora estejam longe de ser adversários, também não são os aliados mais próximos e confiáveis dos Estados Unidos. De fato, um documento de planejamento da NSA – intitulado "Identificação de desafios: Tendências geopolíticas para 2014-2019" – lista os dois países abaixo do subtítulo "Amigos, inimigos ou problemas?" Na mesma lista estão Arábia Saudita, Egito, Iêmen, Índia, Irã, Somália, Sudão e Turquia.

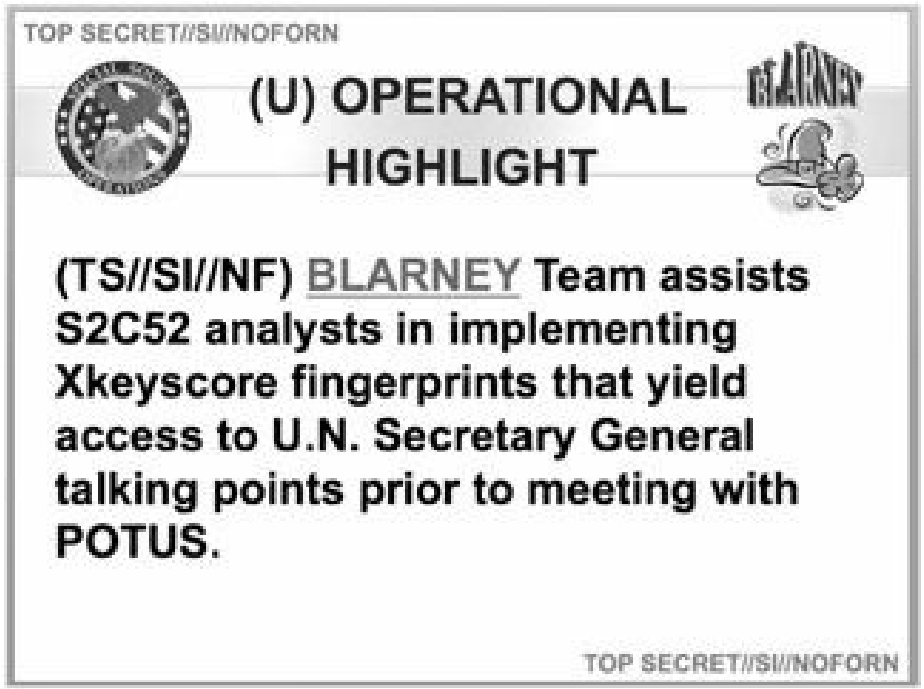
Em última instância, porém, tanto nesse caso quanto na maioria dos outros, especulações sobre qualquer alvo individual baseiam-se em uma falsa premissa. A NSA não precisa de nenhum motivo ou explicação específica para invadir as comunicações privadas das pessoas. Sua missão institucional é coletar tudo.

Na verdade, as revelações sobre a espionagem de líderes estrangeiros pela NSA são *menos* significativas do que sua vigilância em massa e sem autorização de populações inteiras. Países vêm espionando chefes de Estado há séculos, inclusive aliados. Não chega a ser motivo para espanto, apesar da indignação provocada, por exemplo, a revelação de que durante muitos anos a NSA teve

como alvo o celular pessoal da chanceler alemã Angela Merkel.

Mais notável é o fato de, em vários países, revelações de que a NSA estava espionando centenas de milhões de seus cidadãos terem produzido pouco mais do que discretas objeções de seus líderes políticos. A verdadeira indignação só surgiu quando esses chefes de Estado entenderam que eles também tinham sido alvo, não só os cidadãos.

Mesmo assim, a escala da vigilância diplomática praticada pela NSA é incomum e digna de nota. Além de líderes estrangeiros, os Estados Unidos também espionaram de forma extensiva, por exemplo, organizações internacionais como a ONU, de modo a obter vantagens diplomáticas. Um briefing típico da SSO com data de abril de 2013 observa que a agência usou seus programas para obter os principais tópicos a serem abordados pelo secretário-geral da ONU antes de seu encontro com o presidente Obama:



DESTAQUE OPERACIONAL

Equipe do BLARNEY auxilia os analistas de S2C52 na implementação de impressões digitais Xkeyscore que geram acesso aos tópicos de discussão do secretário-geral da ONU antes do encontro com POTUS [o presidente dos Estados Unidos].

Vários outros documentos expõem em detalhes como Susan Rice, então embaixadora dos Estados Unidos na ONU e hoje consultora de segurança nacional de Obama, solicitou diversas vezes à NSA que espionasse as discussões internas de Estados-membros especialmente relevantes para saber quais seriam suas estratégias de negociação. Um relatório da SSO de maio de 2010 (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 19) descreve esse processo em relação a uma resolução que estava sendo debatida pela ONU para impor novas sanções ao Irã:

(S//SI) Apoio notável da equipe do BLARNEY possibilita coleta no Conselho de Segurança da ONU

Por INFORMAÇÃO OMITIDA em 28/5/2010 1430

(TS//SI//NF) Com a aproximação da votação na ONU sobre as sanções contra o Irã e vários países indecisos quanto a uma decisão, a embaixadora Rice recorreu à NSA e solicitou SIGINT relacionada a esses países, de modo a poder desenvolver uma estratégia. Com a exigência de que isso fosse feito rápido e dentro dos limites de nossa autorização judicial, a equipe do BLARNEY pôs mãos à obra junto com organizações e parceiros tanto internos quanto externos à NSA.

(TS//SI//NF) Enquanto OGC [Escritório de Vigilância da Diretoria de Inteligência de Sinais], SV [Conselho Geral da NSA] e analistas técnicos destrinchavam agressivamente os documentos jurídicos para expedir quatro novas ordens do tribunal da FISA à NSA relativas a Gabão, Uganda, Nigéria e Bósnia, o pessoal da Divisão de Operações do BLARNEY trabalhava nos bastidores, reunindo dados para determinar quais informações de levantamento estavam disponíveis ou podiam ser obtidas por meio de seus contatos de longa data com o FBI. Enquanto eles trabalhavam para obter informações tanto sobre as missões da ONU em Nova York quanto sobre as embaixadas em Washington, a equipe de desenvolvimento de alvos acelerou o processo com a equipe de fluxo de dados adequada, e todos os preparativos foram feitos para garantir que os dados pudessem chegar aos analistas técnicos o mais rápido possível. Vários colaboradores, entre eles um da equipe jurídica e outro da equipe de desenvolvimento de alvos, foram convocados no sábado 22 de maio para dar apoio ao exercício de 24 horas de treinamento em documentação jurídica, fazendo a sua parte para garantir que as ordens estivessem prontas para a assinatura do diretor da NSA no início da manhã de 24 de maio.

(S//SI) Com OGC e SV dando duro para emitir as quatro ordens, estas partiram em tempo recorde para a assinatura do diretor da NSA, para o Departamento de Defesa para a assinatura do secretário, e em seguida para o Departamento de Justiça para a assinatura do juiz do FISC. Todas as quatro ordens foram assinadas pelo juiz na quarta-feira, 26 de maio! Uma vez

recebidas pela equipe jurídica do BLARNEY, esta começou a agir, esmiuçando essas quatro ordens mais uma renovação "normal" em apenas um dia. Cinco ordens judiciais analisadas em um só dia: um recorde para o BLARNEY! Enquanto a equipe jurídica do BLARNEY estava ocupada analisando as ordens, a equipe de gerenciamento de acesso do programa trabalhava com o FBI para transmitir informações de solicitação de tarefas e coordenar o contato com parceiros de telecomunicações.

Um documento de vigilância semelhante, de agosto de 2010 (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 20), revela que os Estados Unidos espionaram oito membros do Conselho de Segurança da ONU em relação a uma subsequente resolução referente a sanções ao Irã. A lista incluía França, Brasil, Japão e México – todos países considerados amigos. A espionagem proporcionou ao governo norte-americano informações valiosas sobre as intenções de voto desses países, dando vantagem a Washington nas conversas com outros membros do Conselho de Segurança.

TOP SECRET//COMINT//NOFORN

Agosto de 2010

(U//FOUO) Sucesso silencioso: sinergia de SIGINT ajuda a moldar política externa dos Estados Unidos

(TS//SI//NF) No início dessas demoradas negociações, a NSA aumentou a coleta no Japão, México, Brasil, França

(TS//SI//REL) No final da primavera de 2010, onze ramificações de cinco Linhas de Produção uniram esforços com facilitadores da NSA para fornecer as informações mais atuais e mais exatas à embaixadora dos Estados Unidos na ONU e a outros clientes sobre como os membros do CS da ONU iriam votar na Resolução sobre Sanções ao Irã. Observando que o Irã continuava a não acatar resoluções anteriores do CS relacionadas a seu programa nuclear, a ONU impôs novas sanções em 9 de junho de 2010. A SIGINT teve um papel fundamental em manter a embaixadora dos Estados Unidos na ONU informada sobre como os outros membros do CS iriam votar.

(TS//SI//REL) A resolução foi aprovada por doze votos a favor, dois contra (Brasil e Turquia) e uma abstenção do Líbano. Segundo a embaixadora dos Estados Unidos na ONU, a SIGINT "me ajudou a saber quando os outros Permreps [Representantes Permanentes] estavam dizendo a verdade (...) revelou seu verdadeiro posicionamento em relação às sanções (...) nos beneficiou nas negociações (...) e forneceu informações sobre os 'limites de negociação' de diversos países".

Para facilitar a espionagem diplomática, a NSA obteve várias formas de acesso às embaixadas e consulados de muitos de seus aliados mais próximos. Um documento de 2010 – reproduzido aqui com alguns países específicos removidos – lista os países cuja estrutura diplomática nos Estados Unidos foi invadida pela agência. Um glossário no final explica os vários tipos de de vigilância utilizados.

10 de setembro de 2010

SIGADS ACESSO RESTRITO

SIGADS ACESSO RESTRITO
Toda a coleta doméstica de acesso restrito usa o SIGAD US-3136 com um sufixo específico de duas letras para a localização e missão de cada alvo. A coleta de acesso restrito GENIE no exterior recebeu o SIGAD US-3137 com um sufixo de duas letras.

(Observação: alvos marcados com * foram abandonados ou têm previsão de serem abandonados em um futuro próximo. Favor verificar o status das autorizações com TAO/RTD/ROS [961-1578s])

SIGAD US-3136

SUFIXO	ALVO/PAÍS	LOCAL
BE	Brasil/Emb.	Washir D.C.
SI	Brasil/Emb.	Washir D.C.
VQ	Brasil/ONU	Nova Y

HN	Brasil/ONU	Nova Y
LJ	Brasil/ONU	Nova Y
YL*	Bulgária/Emb.	Washir D.C.
QX*	Colômbia/Escritório de Comércio	Nova Y
DJ	UE/ONU	Nova Y
SS	UE/ONU	Nova Y
KD	UE/Emb.	Washir D.C.
IO	UE/Emb.	Washir D.C.
		Washir

XJ	UE/Emb.	D.C.
OF	França/ONU	Nova Y
VC	França/ONU	Nova Y
UC	França/Emb.	Washir D.C.
LO	França/Emb.	Washir D.C.
NK*	Geórgia/Emb.	Washir D.C.
BY*	Geórgia/Emb.	Washir D.C.
RX	Grécia/ONU	Nova Y
HB	Grécia/ONU	Nova Y

CD	Grécia/Emb.	Washir D.C.
PJ	Grécia/Emb.	Washir D.C.
JN	Grécia/Emb.	Washir D.C.
MO*	Índia/ONU	Nova Y
QL*	Índia/ONU	Nova Y
ON*	Índia/ONU	Nova Y
IS*	Índia/ONU	Nova Y
OX*	Índia/Emb.	Washir D.C.

CQ*	Índia/Emb.	Washir D.C.
TQ*	Índia/Emb.	Washir D.C.
CU*	Índia/AnexoEmb.	Washir D.C.
DS*	Índia/AnexoEmb.	Washir D.C.
SU*	Itália/Emb.	Washir D.C.
MV*	Itália/Emb.	Washir D.C.
IP*	Japão/ONU	Nova Y

HF*	Japão/ONU	Nova Y
BT*	Japão/ONU	Nova Y
RU*	Japão/ONU	Nova Y
LM*	México/ONU	Nova Y
UX*	Eslováquia/Emb.	Washir D.C.
SA*	Eslováquia/Emb.	Washir D.C.
XR*	África do Sul/ONU e Consulado	Nova Y
RJ*	África do Sul/ONU e Consulado	Nova Y
YR*	Coreia do Sul/ONU	Nova Y

TZ*	Taiwan/TECO	Nova Y
VN*	Venezuela/Emb.	Washir D.C.
UR*	Venezuela/ONU	Nova Y
NO*	Vietnã/ONU	Nova Y
OU*	Vietnã/ONU	Nova Y
GV*	Vietnã/Emb.	Washir D.C.

SIGAD US-3137

Descrição geral dos termos

HIGHLANDS: Coleta a partir de escutas

VAGRANT: Coleta de telas de computador

MAGNETIC: Coleta de emanações magnéticas por sensores

MINERALIZE: Coleta de implantes LAN

OCEAN: Sistema de coleta óptica para telas de computador baseadas em *raster*

LIFESAVER: Cópia por imagem do disco rígido

GENIE: Operação de estágios múltiplos; salto de *air gap*, etc.

BLACKHEART: Coleta a partir de escutas do FBI

PBX: Switch de PBX

CRYPTO ENABLED: Coleta derivada de esforços da AO para possibilitar criptografia

DROPMIRE: Coleta passiva de emanações usando uma antena

CUSTOMS: Oportunidades customizadas (que não sejam LIFESAVER)

DROPMIRE: Coleta de impressões a laser, apenas por acesso de proximidade (**SEM** escuta)

DEWSWEEPER: Grampo de USB no hardware do host que proporciona um link COVERT via link USB para entrar na rede de um alvo. Opera com subsistema de relé por frequência de rádio para proporcionar uma ponte wireless até a rede do alvo.

RADON: Grampo bidirecional no host capaz de introduzir pacotes de Ethernet no mesmo alvo. Permite exploração bidirecional de redes negadas usando ferramentas comuns conectadas à Internet.

Alguns dos métodos da NSA servem a todos os propósitos – econômicos, diplomáticos, de segurança, e obtenção de vantagens globais com múltiplos objetivos – e estão entre os mais invasivos e hipócritas do repertório da agência. Durante anos, o governo dos Estados Unidos alardeou para o mundo que os roteadores e outros equipamentos de internet chineses representavam uma "ameaça" por serem fabricados com recursos de vigilância do tipo "porta dos fundos" que tornam o governo chinês capaz de espionar quem quer que os utilize. Entretanto, o que os documentos da NSA revelam é que os americanos vêm realizando justamente a atividade da qual acusavam os chineses.

O ritmo das acusações americanas contra os fabricantes chineses de equipamentos de internet era inflexível. Em 2012, por exemplo, um relatório do Comitê de Inteligência da Câmara, liderado por Mike Rogers, alegou que as duas principais empresas chinesas de equipamentos de telecomunicações, Huawei e ZTE, "poderiam estar violando leis norte-americanas" e "não respeitaram obrigações legais dos Estados Unidos nem padrões internacionais de conduta empresarial". O comitê recomendou que "os Estados Unidos vissem com desconfiança a crescente penetração do mercado norte-americano de telecomunicações por empresas de telecomunicações chinesas".

O Comitê Rogers expunha temores de que as duas empresas estivessem possibilitando uma vigilância estatal da China, embora reconhecesse não ter conseguido nenhum indício concreto de que houvessem implantado funções de vigilância em seus roteadores e outros equipamentos. Apesar disso, citava a não cooperação dessas companhias e instava as empresas norte-americanas a evitar a compra de seus produtos:

> Entidades do setor privado nos Estados Unidos são fortemente aconselhadas a considerar os riscos de segurança a longo prazo associados a transações com a ZTE ou com a Huawei para equipamentos ou serviços. Provedores de rede e desenvolvedores de sistemas norte-americanos são

enfaticamente encorajados a procurar outros fornecedores para seus projetos. Com base em informações sigilosas e não sigilosas disponíveis, não é possível confiar que a ZTE e a Huawei estejam livres de influência estatal estrangeira, e que portanto não representem uma ameaça de segurança para os Estados Unidos e nossos sistemas.

As constantes acusações começaram a pesar tanto que, em novembro de 2013, Ren Zhengfei, 69 anos, fundador e CEO da Huawei, anunciou que a empresa iria sair do mercado norte-americano. Conforme noticiado pela *Foreign Policy*, Zhengfei declarou a um jornal francês: "'Se a Huawei for se intrometer nas relações Estados Unidos-China' e causar problemas, 'não vale a pena.'"

Mas, enquanto as empresas norte-americanas eram alertadas a manter distância de roteadores chineses supostamente não confiáveis, organizações estrangeiras teriam sido mais sensatas se houvessem desconfiado daqueles fabricados nos Estados Unidos. Um relatório de junho de 2010 do chefe do Departamento de Desenvolvimento de Acesso e Alvos da NSA é de uma clareza chocante. A agência recebe ou intercepta, de forma rotineira, roteadores, servidores e outros equipamentos de rede que serão exportados pelos Estados Unidos antes que sejam despachados para os clientes internacionais. Ela então implanta ferramentas de vigilância do tipo porta dos fundos, reembala os produtos com um selo de fábrica e os despacha. Assim, a NSA consegue acesso a redes inteiras e aos seus usuários. O documento (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 21 e 22) observa de forma bem-humorada que para realizar "atividades de SIGINT (...) às vezes é preciso meter a mão na massa (literalmente!)":

TOP SECRET//COMINT//NOFORN

Junho de 2010

Técnicas sub-reptícias podem penetrar os alvos mais difíceis de SIGINT

Por: (U//FOUO) INFORMAÇÃO OMITIDA, Chefe, Desenvolvimento de Acesso e Alvos (S3261)

IMAGEM EXCLUÍDA

(TS//SI//NF) Nem todas as atividades de SIGINT consistem em acessar sinais e redes a milhares de quilômetros de distância (...). Na realidade, às vezes é preciso meter a mão na massa (literalmente!). Funciona assim: carregamentos com equipamentos de rede (servidores, roteadores, etc.) destinados a serem entregues a nossos alvos espalhados pelo mundo são ***interceptados***. Os equipamentos são, então, ***redirecionados a um local secreto*** onde funcionários de Operações de Acesso Customizado/Operações de Acesso (AO-S326), com o apoio do Centro de Operações Remotas (S321), possibilitam a ***instalação de implantes sinalizadores*** direto nos equipamentos eletrônicos de nossos alvos. Esses equipamentos são em seguida reembalados e ***recolocados em trânsito*** rumo

ao destino original. Tudo isso acontece com o apoio de parceiros da Comunidade de Inteligência e dos mágicos da tecnologia do TAO.

(TS//SI//NF) Tais operações envolvendo **interrupção da cadeia de suprimento** estão entre as mais produtivas do TAO, uma vez que pré-posicionam pontos de acesso em redes de alvos difíceis mundo afora.

(TS//SI//NF) À esquerda: pacotes interceptados são abertos cuidadosamente; à direita: uma "estação de carregamento" implanta um sinalizador

Em algum momento após a operação, o sinalizador implantado torna a se conectar à infraestrutura da NSA (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 23):

(TS//SI//NF) Em um caso recente, após vários meses, um sinalizador implantado por interrupção da cadeia de suprimento se reconectou à infraestrutura secreta da NSA. Essa reconexão nos proporcionou acesso para explorar mais a fundo o equipamento e vasculhar a rede.

Entre outros equipamentos, a agência intercepta e interfere em roteadores e servidores fabricados pela Cisco para direcionar uma grande quantidade de tráfego da internet de volta para os repositórios da NSA. Não há indícios nos documentos de que a Cisco esteja ciente ou aprove essas interceptações. Em abril de 2013, a agência enfrentou dificuldades técnicas com os *switches* de rede da Cisco interceptados, que derrubaram os programas BLARNEY, FAIRVIEW, OAKSTAR e STORMBREW (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 24):

TOP SECRET//COMINT//REL PARA EUA, FVEY

(Relatório gerado em 11/4/2013 15:31:05)

Novo Programa Cruzado	
Programa Cruzado-1-13	Novo
Título da mudança:	Atualização Cisco
Responsável:	INFORMITID
Locais:	APPLE1 : CLEVERDEV : HOMEMAK DOGHUT : QUARTERF QUEENSLAN SCALLION

	: SPORTCO/ SUBSTRATU POINTE : SU : BIRCHWOO : EAGLE : EDI
Sistemas:	Comms/Netv Comms/Netv Comms/Netv Comms/Netv
Descrição da mudança:	Atualização ópticos de re
Motivo da mudança:	Todos os no Cisco estão que os faz c

Impacto na missão: O impacto n
falha existen
aplicação da
fazê-lo. Infel
podemos sir
portanto é in
vai acontece
software. No
dos nós em
atualização

Há pouco te
gerenciamer
Quando isso
forma manua
não imaginá
entanto, qua
inteira caiu e

Foi preciso r
queda.

O pior que p
desconfigura
iniciar a atua
assim, se tiv
zero, podere
configuraçã
ficaremos fo
para cada n

Informações adicionais:

26/3/2013 8:

OMITID

Testamos a
está funcion
replicar a fal
sabemos se
um nó que e

Último registro CCB: 10/4/13 16:0

OMITID

aprovado pe

ECP em 9 d

líder ECP:

OMITID

Programas afetados: Blarney Fairv

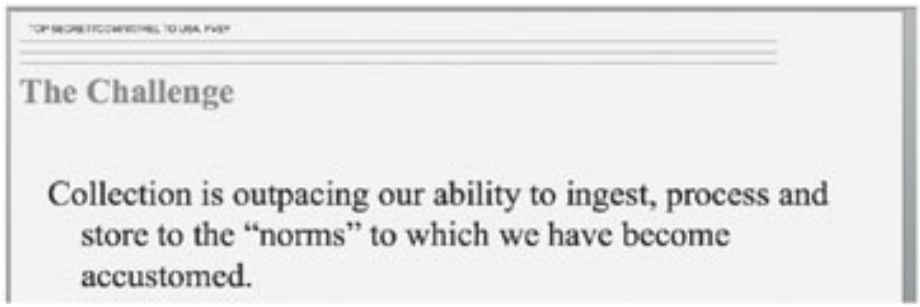
Nenhuma

É bem possível que as empresas chinesas estejam implantando mecanismos de vigilância em seus equipamentos de rede. Mas os Estados Unidos sem dúvida estão fazendo a mesma coisa.

Alertar o mundo sobre a espionagem chinesa podia ser um dos motivos por trás das alegações do governo dos Estados Unidos de que os equipamentos chineses não merecem confiança. No entanto, uma razão igualmente importante parece ter sido impedir que os aparelhos chineses suplantassem os norte-americanos, o que limitaria o alcance da NSA. Em outras palavras, roteadores e servidores chineses representam competição não apenas econômica, mas também de vigilância: quando alguém compra um equipamento chinês e não um americano, a NSA perde uma forma crucial de espionar uma grande quantidade de atividades de comunicação.

Se o volume de coleta revelado já era estarrecedor, a missão da NSA de coletar todos os sinais o tempo todo só levou a agência a expandir e conquistar cada vez mais terreno. De fato, a quantidade de dados captados é tão grande que o principal desafio do qual a agência reclama é conseguir armazenar toda a informação acumulada de todas as partes do mundo. Um documento da NSA

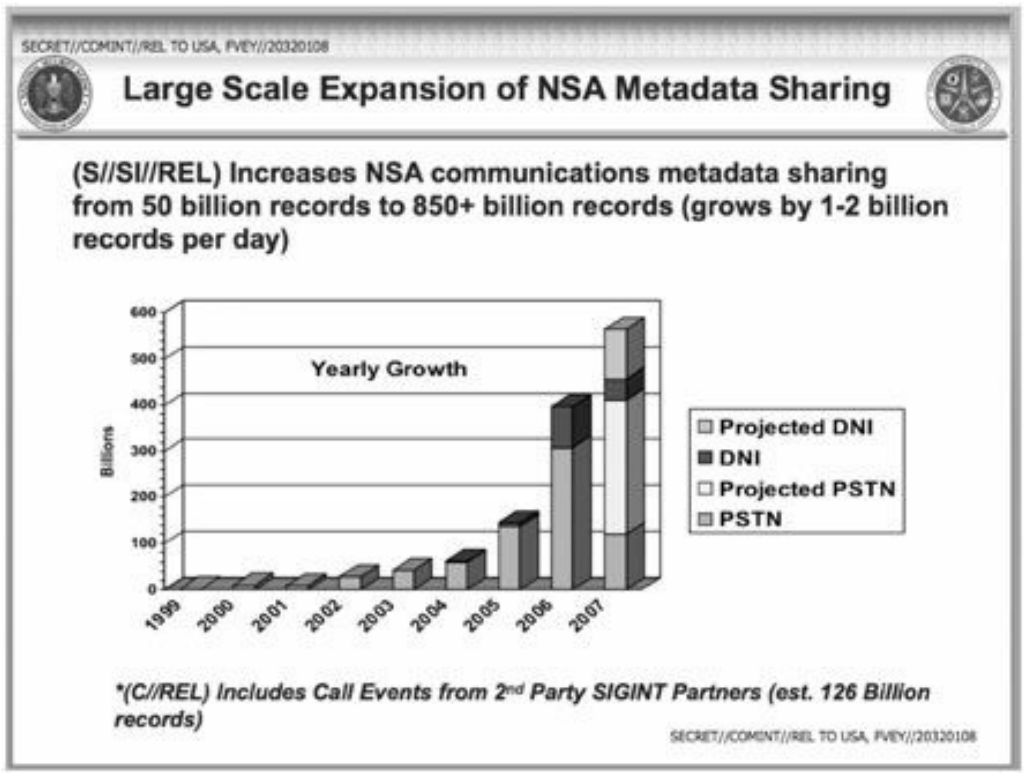
preparado para a conferência de Desenvolvimento de Sinais dos Cinco Olhos apresentava esse problema central:



O DESAFIO

A coleta está superando nossa capacidade de ingerir, processar e armazenar de acordo com as "normas" com as quais nos acostumamos.

A história remonta a 2006, quando a agência embarcou no que chamou de "Expansão em Larga Escala do Compartilhamento de Metadados da NSA". Na época, previa-se que sua coleção de metadados iria aumentar em 600 bilhões de registros *por ano*, crescimento que incluiria um ou dois bilhões de novas ocorrências de chamadas telefônicas coletadas por dia:



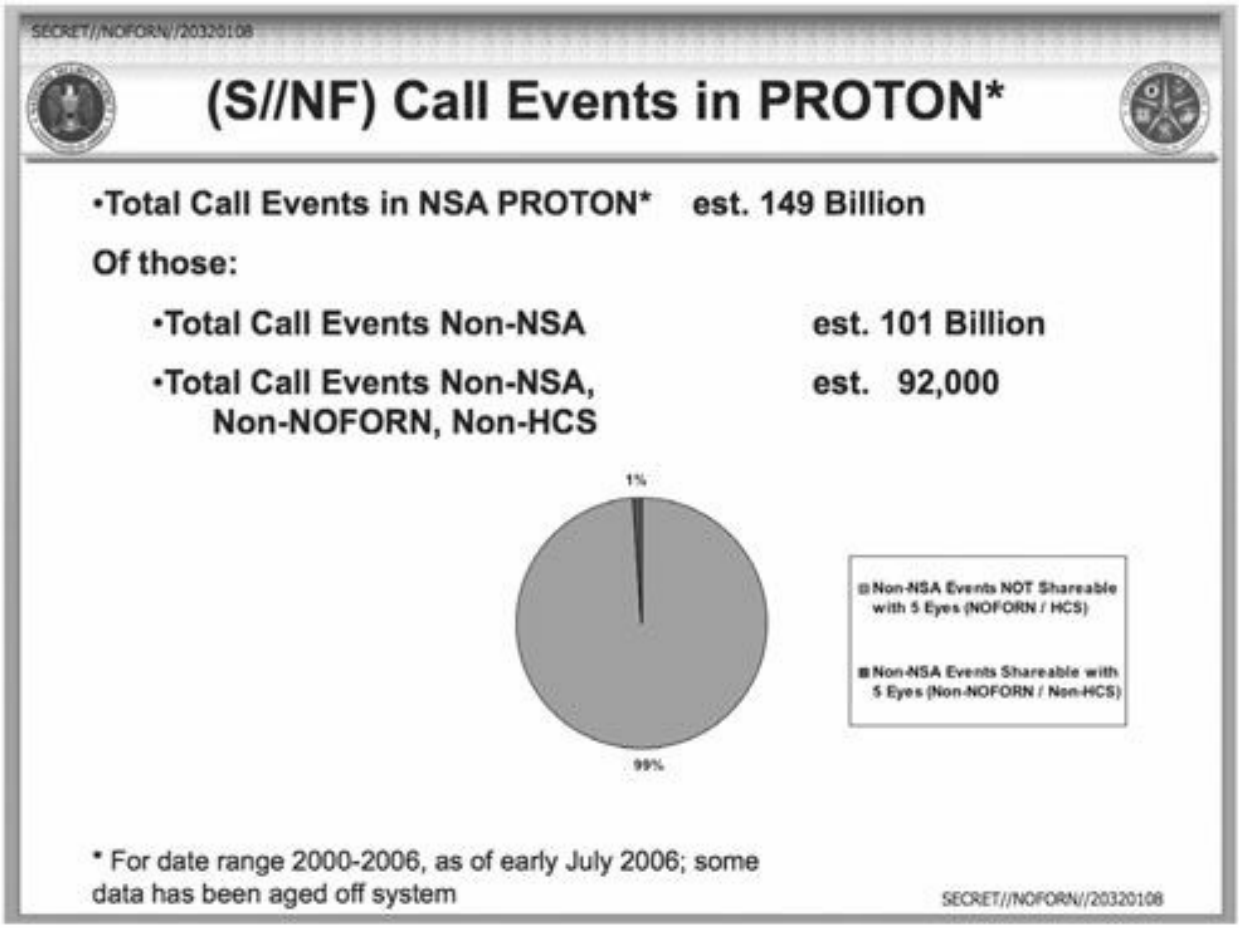
EXPANSÃO EM LARGA ESCALA DO COMPARTILHAMENTO DE METADADOS PELA NSA

Aumenta o compartilhamento de metadados de comunicações da NSA de 50 bilhões de registros para >850 bilhões de registros (aumento de 1-2 bilhões de registros por dia)

Da esquerda para a direita, de cima para baixo: Bilhões / Crescimento anual / Projeção de DNI / DNI / Projeção de PSTN / PSTN / *Inclui ocorrências de chamadas de parceiros

de SIGINT (estimadas em 126 bilhões de registros)

Em maio de 2007, a expansão obviamente já dera frutos: a quantidade de metadados telefônicos armazenada pela agência – sem contar e-mails e outras informações de internet, e desconsiderando os dados que a NSA havia apagado devido à falta de espaço de armazenamento – tinha aumentado para 150 bilhões de registros:



OCORRÊNCIAS DE CHAMADAS NO PROTON*

Total de ocorrências de chamadas no PROTON* da NSA / 149 bilhões estimados Dos quais: / Total de ocorrências de chamadas não NSA / 101 bilhões estimados / Total de ocorrências de chamadas não NSA, não NOFORN, não HCS / 92.000 estimados / Ocorrências não NSA não compartilháveis com Cinco Olhos (NOFORN/HCS) / Ocorrências não NSA compartilháveis com Cinco Olhos (Não NOFORN/Não HCS) / Para o período 2000-2006 em início de julho de 2006; alguns dados saíram do sistema por caducidade

Uma vez acrescentadas as comunicações com base na internet, o número total de ocorrências de comunicação armazenados beirava um trilhão (e essas informações, deve-se frisar, eram então compartilhadas pela NSA com outras agências).

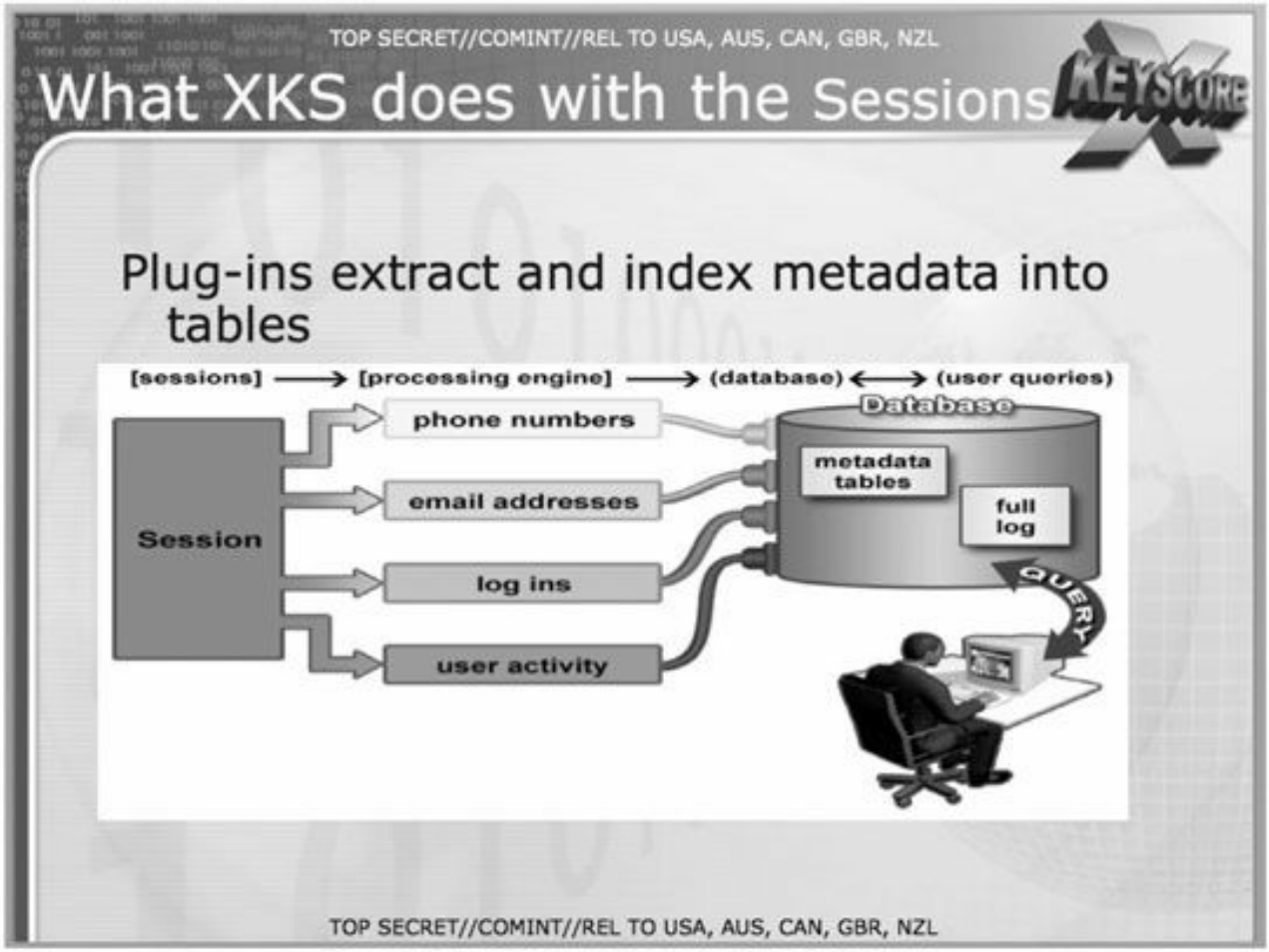
Para tratar desse problema de armazenamento, a NSA começou a construir uma imensa instalação nova em Bluffdale, Utah, que tem entre suas principais finalidades a retenção de todas essas informações. Conforme comentou o jornalista James Bamford em 2012, o prédio de Bluffdale

ampliará a capacidade de armazenamento da agência com o acréscimo de "quatro salões de 2.300 m^2 cheios de servidores, com espaço para cabos e armazenamento sob o piso elevado. Além disso, haverá quase 84 mil metros quadrados para suporte técnico e administração". Levando em conta o tamanho do prédio e o fato de, como diz Bamford, "um terabyte de dados agora poder ser armazenado em um pen drive do tamanho de um dedo mindinho", as implicações para a coleta de dados são profundas.

A necessidade de instalações cada vez maiores é particularmente urgente, considerando-se as invasões atuais da atividade de internet mundial realizadas pela agência, que vão muito além da coleta de metadados e incluem o conteúdo de e-mails, históricos de navegação, históricos de busca e chats. O principal programa usado pela NSA para coletar, classificar e pesquisar essas informações, que começou a ser usado em 2007, é o X-KEYSCORE, que permite um salto radical no escopo dos poderes de vigilância da agência. A NSA qualifica o X-KEYSCORE de seu sistema "de maior alcance" para a coleta de dados eletrônicos, e não é para menos.

Um documento preparado para o treinamento de analistas alega que o programa capta "praticamente tudo o que um usuário típico faz na internet", incluindo texto contido em e-mails, buscas no Google e o nome dos sites visitados. O X-KEYSCORE proporciona até o monitoramento "em tempo real" das atividades de um indivíduo na internet, permitindo à NSA observar e-mails e atividades de navegação na hora em que acontecem.

Além da coleta exaustiva de dados sobre as atividades on-line de centenas de milhões de pessoas, o X-KEYSCORE permite a qualquer analista da NSA pesquisar as bases de dados do sistema por endereço de e-mail, número de telefone ou outros atributos específicos (como, por exemplo, um endereço de IP). O escopo da informação disponível e as formas básicas que um analista usa para pesquisá-la estão ilustrados no slide a seguir:



O QUE O XKS FAZ COM AS SESSÕES

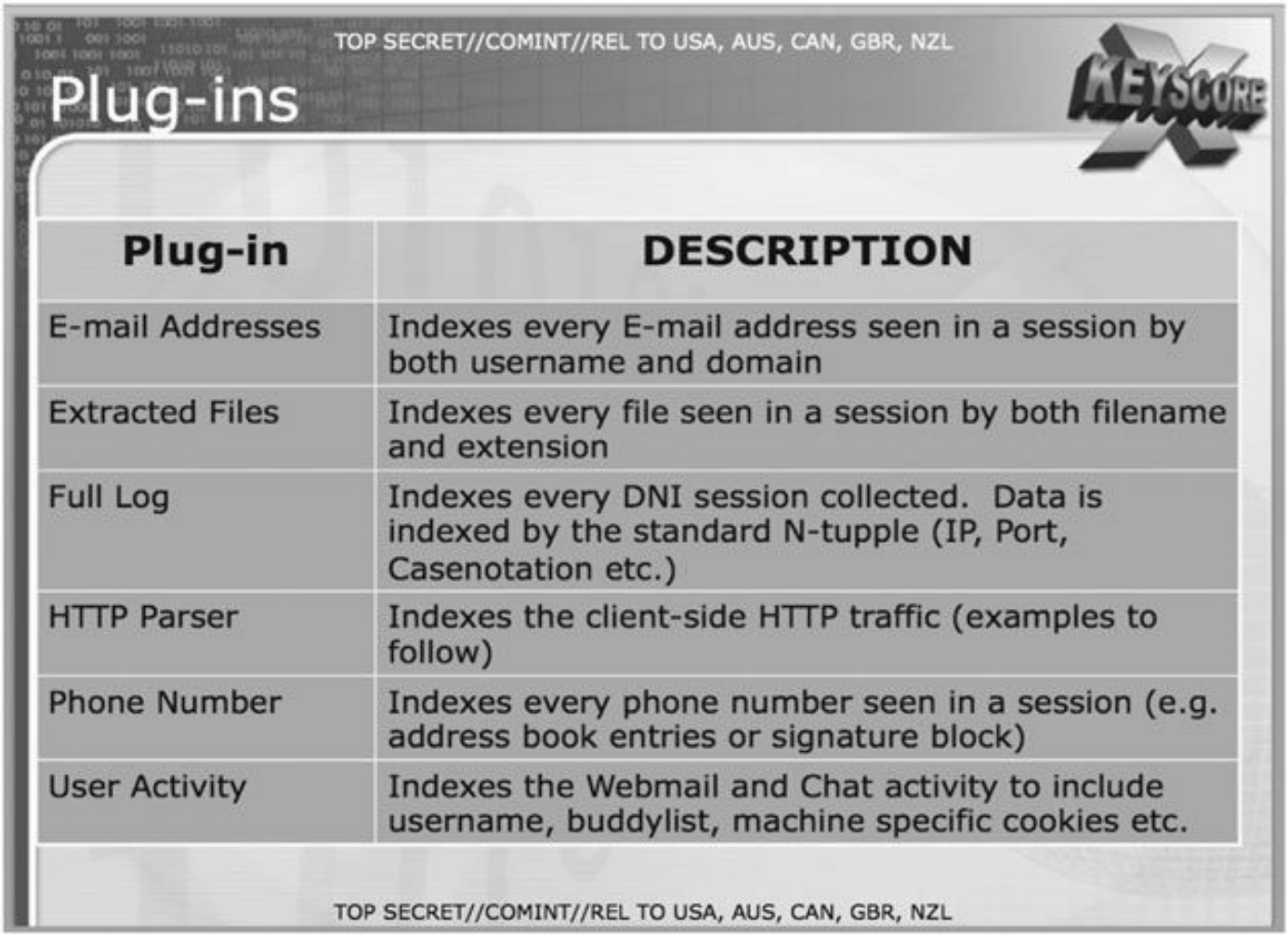
Extração de plug-ins e indexação de metadados em tabelas

(sessões) / (mecanismo de processamento) / (base de dados) / (solicitações de usuários)

Sessão / números de telefone / endereços de e-mail / logins / atividade do usuário

Base de dados / tabelas de metadados / log completo / solicitação

Outro slide do X-KEYSCORE lista os vários campos de informação que podem ser pesquisados usando os plug-ins do programa. Entre eles estão "todos os endereços de e-mail vistos em uma sessão", "todos os números de telefone vistos em uma sessão" (incluindo "contatos de agenda de endereços") e "atividade de correio eletrônico e chat".

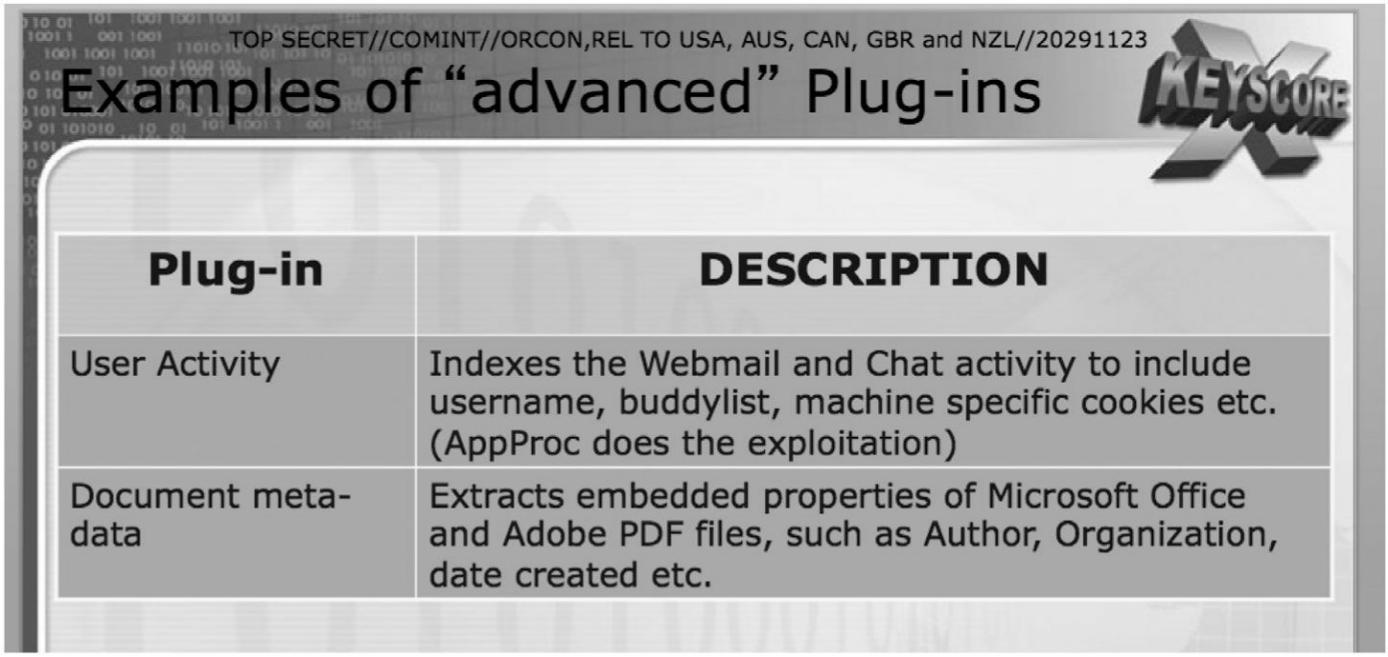


PLUG-INS

Coluna da esquerda: Plug-in / Endereços de e-mail / Arquivos extraídos / Log completo / Análise sintática de HTTP / Número de telefone / Atividade do usuário

Coluna da direita: Descrição / Indexa todos os endereços de e-mail vistos em uma sessão, tanto por nome de usuário quanto por domínio / Indexa todos os arquivos vistos em uma sessão, tanto por nome de arquivo quanto por extensão / Indexa todas as sessões de DNI coletadas. Os dados são indexados pelo padrão N-tupple (IP, porta, notação de caso, etc.) / Indexa o tráfego de HTTP do lado do cliente (exemplos a seguir) / Indexa todos os números de telefone vistos em uma sessão (por exemplo, registros de caderno de endereços ou bloco de assinatura) / Indexa a atividade de webmail e chat, incluindo nome de usuário, lista de contatos, cookies específicos da máquina, etc.

O programa também possibilita pesquisar e recuperar documentos e imagens embutidas que foram criados, enviados ou recebidos:



Plug-in	DESCRIPTION
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc. (AppProc does the exploitation)
Document meta-data	Extracts embedded properties of Microsoft Office and Adobe PDF files, such as Author, Organization, date created etc.

EXEMPLOS DE PLUG-INS “AVANÇADOS”

Coluna da esquerda: Plug-in / Atividade do usuário / Metadados de documento

Coluna da direita: Descrição / Indexa atividade de webmail e chat, incluindo nome de usuário, lista de contatos, cookies específicos à máquina, etc. (AppProc explora os dados) / Extrai propriedades embutidas de arquivos do Microsoft Office e do Adobe PDF, tais como autor, organização, data de criação, etc.

Outros slides da NSA declaram abertamente a ambição global de escopo irrestrito do X-KEYSCORE.

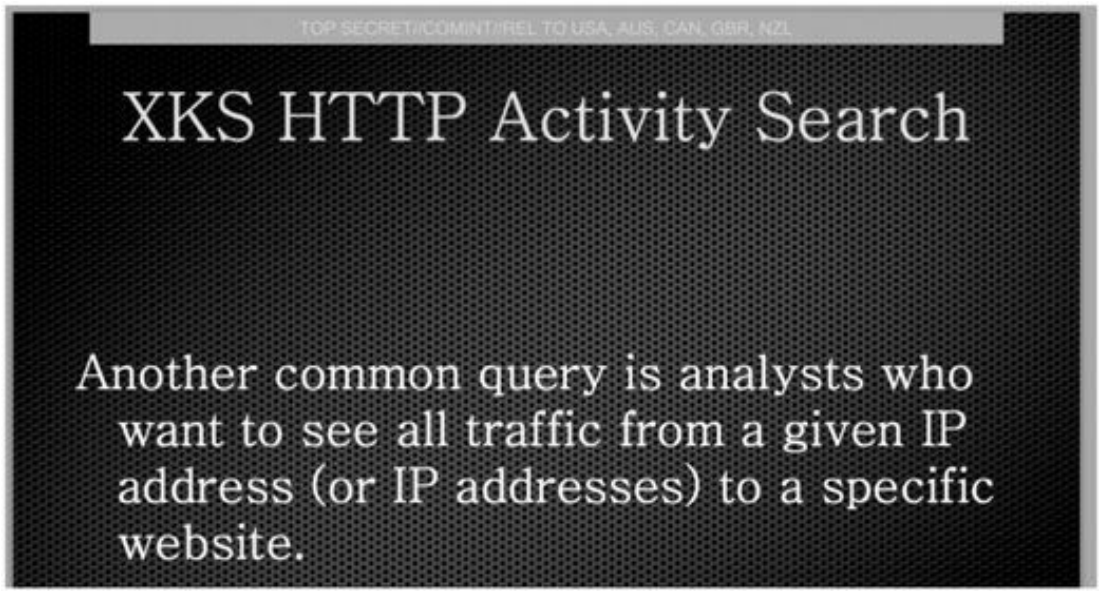
POR QUE O HTTP NOS INTERESSA?

Porque quase tudo o que um usuário típico faz na internet usa HTTP

POR QUE O HTTP NOS INTERESSA?

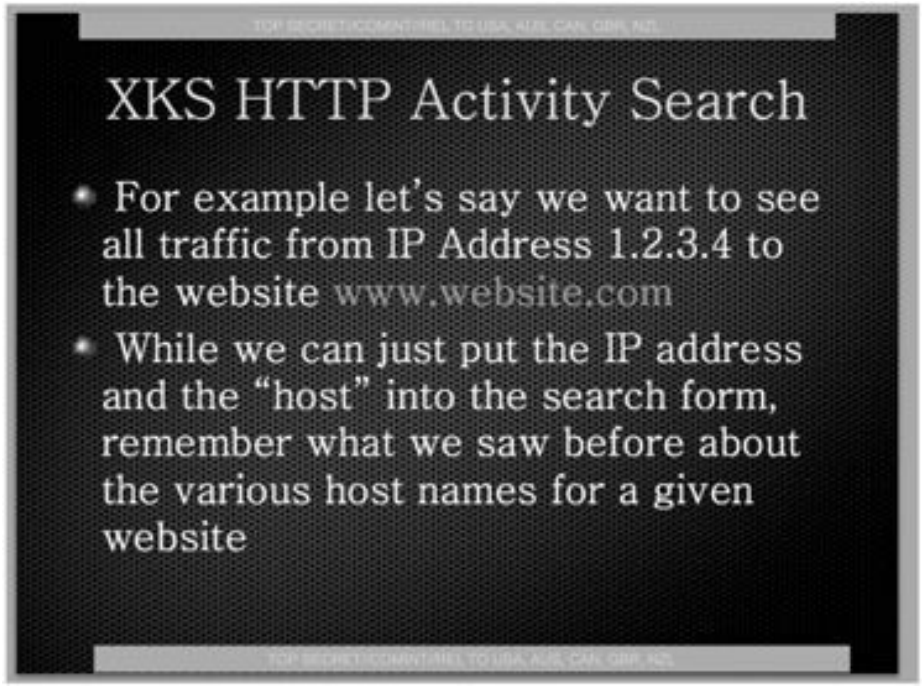
Quase toda a navegação na internet usa HTTP: / Navegar na internet / Webmail (Yahoo!/Hotmail/GMail/etc.) / Redes sociais (Facebook/MySpace/etc.) / Busca (Google/Bing/etc.) / Mapas (Google Maps/Mapquest/etc.)

As buscas possibilitadas pelo programa são tão específicas que qualquer analista da NSA pode não apenas descobrir que sites alguém visitou, mas também criar uma lista completa de todas as visitas a um site específico feitas a partir de determinados computadores:



BUSCA POR ATIVIDADE DE HTTP DO XKS

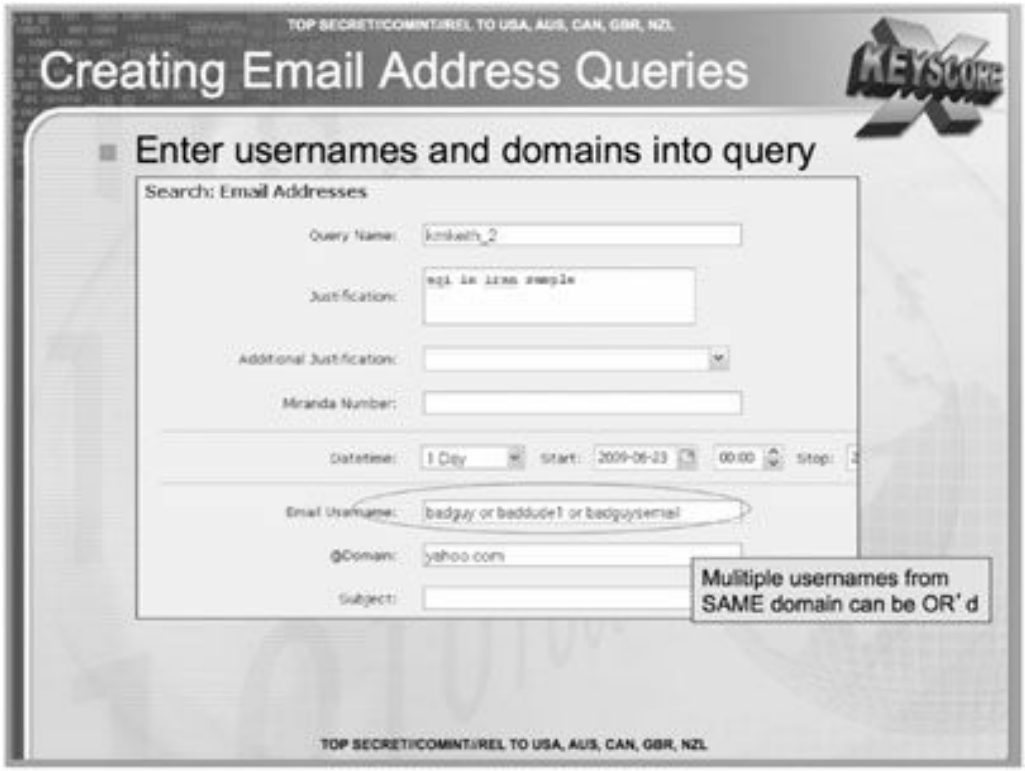
Outra solicitação comum é quando os analistas querem ver todo o tráfego de determinado endereço (ou endereços) de IP para um site específico.



BUSCA POR ATIVIDADE DE HTTP DO XKS

Por exemplo, digamos que queremos ver todo o tráfego do endereço de IP 1.2.3.4 para o site www.site.com / Embora baste colocar o endereço de IP e o "host" no formulário de busca, lembrem-se do que vimos antes sobre os vários nomes de host para um mesmo site

O mais notável é a desenvoltura com a qual os analistas podem pesquisar tudo o que quiserem sem qualquer supervisão. Um analista com acesso ao X-KEYSCORE não precisa submeter nenhum pedido a um supervisor ou qualquer outra autoridade. Basta preencher um formulário básico para "justificar" a vigilância e o sistema devolve a informação solicitada.



COMO CRIAR SOLICITAÇÕES DE ENDEREÇO DE E-MAIL

Inserir nomes de usuário e domínios no pedido / Busca: endereços de e-mail / Nome da busca: kmkeith_2 / Justificativa: / Justificativa adicional: / Número de Miranda: / Data/hora: / Início: / Fim: / Nome de usuário do e-mail: caramau ou bandido1 ou emaildocaramau / @Domínio: yahoo.com / Assunto: / Múltiplos nomes de usuário de um MESMO domínio podem ser solicitados

Na primeira entrevista em vídeo que deu, em Hong Kong, Edward Snowden fez uma afirmação audaciosa: "Sentado à minha mesa, eu podia grampear qualquer pessoa, de você ou seu contador até um juiz federal ou mesmo o presidente; bastava ter um endereço de e-mail pessoal." Funcionários do governo negaram com veemência que isso fosse verdade. Mike Rogers acusou Snowden, de maneira explícita, de estar "mentindo" e acrescentou: "É impossível fazer o que disse que era capaz." Mas o X-KEYSCORE permite a um analista fazer exatamente o que Snowden falou: escolher qualquer usuário como alvo de um monitoramento extenso, que inclui a leitura do conteúdo de seus e-mails. Na verdade, o programa permite até que um analista busque todos os e-mails que incluírem um usuário-alvo na linha de "cc" ou que o mencionarem no corpo do texto.

As instruções da própria NSA sobre como pesquisar em e-mails demonstra quão simples e fácil é para os analistas monitorar qualquer pessoa cujo endereço de e-mail seja conhecido (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 25):

Solicitação de endereços de e-mail:

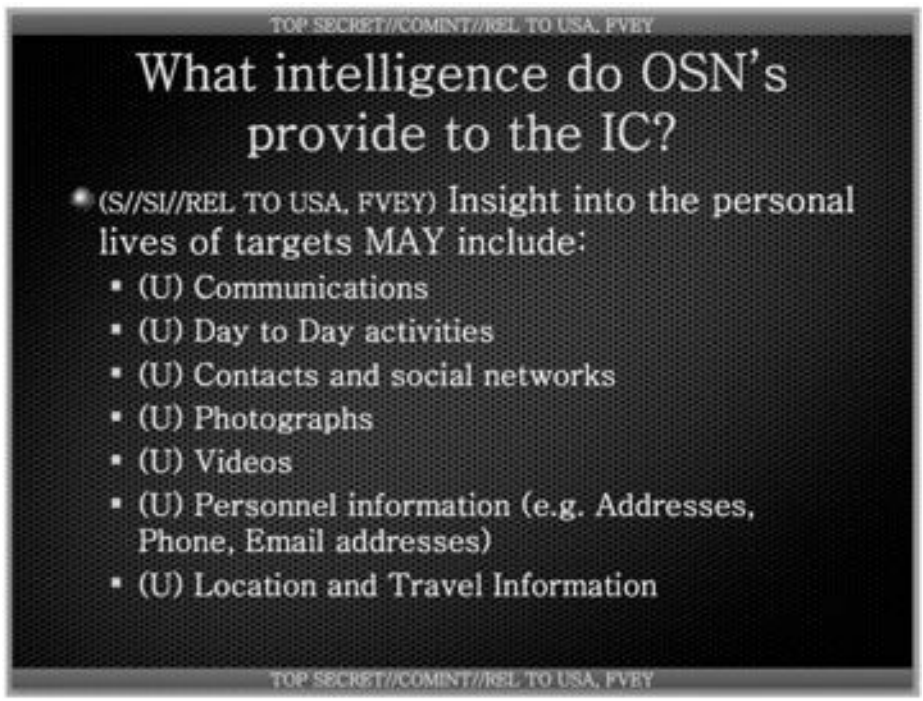
Uma das solicitações mais comuns é (você adivinhou) uma **Solicitação de Endereço de E-mail** para fazer buscas em um endereço de e-mail. Para criar uma solicitação para um endereço de e-mail específico, é preciso preencher o nome da solicitação, justificá-la e estabelecer um limite

de datas, em seguida basta preencher com o(s) endereço(s) de e-mail no(s) qual(is) se deseja fazer a busca e enviar o formulário.

Ficaria parecido com isto aqui...

De cima para baixo, da esquerda para a direita: Campos / Características avançadas / Mostrar campos de busca ocultos / Limpar termos de busca anteriores / Recarregar termos de busca anteriores / Busca: endereço de e-mail / Nome da solicitação: abujihad / Justificativa: alvo de contraterrorismo na África / Justificativa adicional: / Número Miranda: / Data/hora: / Início: / Nome do usuário de e-mail: abujihad / @Domínio: yahoo.com

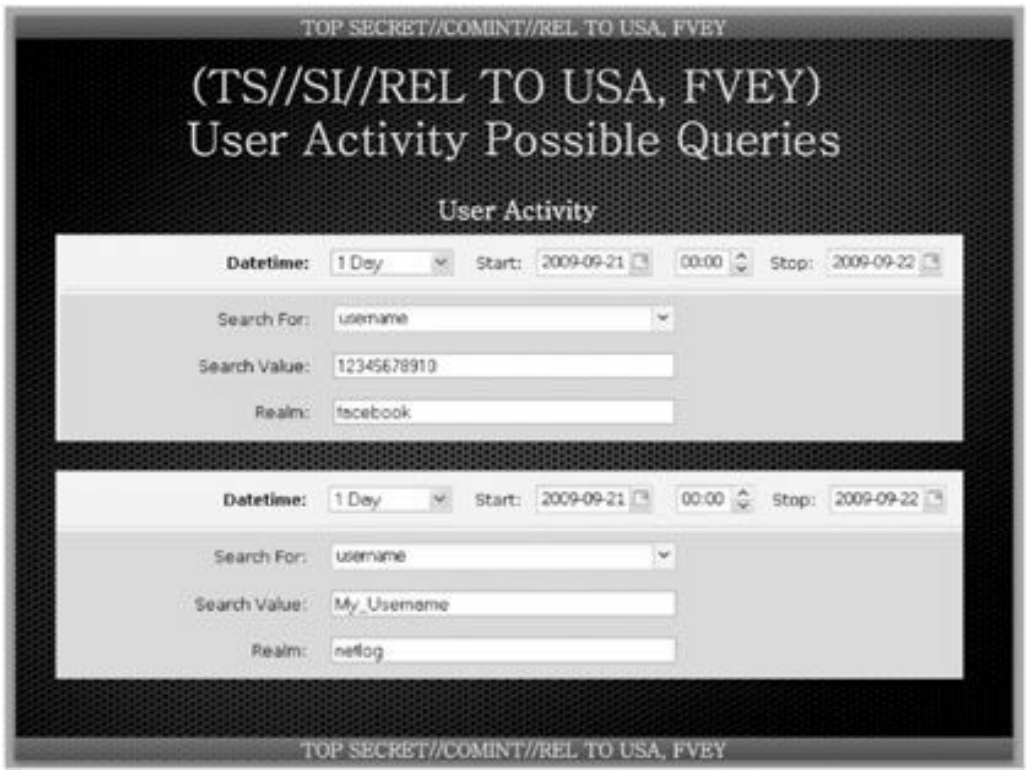
Uma das funcionalidades mais valiosas do X-KEYSCORE para a NSA é a capacidade de vigiar as atividades nas redes sociais da internet como Facebook e Twitter, que a agência acredita representarem um tesouro de informações e "de compreensão sobre a vida pessoal dos alvos".



QUE INTELIGÊNCIA AS REDES SOCIAIS FORNECEM À COMUNIDADE DE INTELIGÊNCIA?

Detalhes sobre a vida pessoal dos alvos PODEM incluir:
Comunicações / Atividades diárias / Contatos e redes sociais / Fotografias / Vídeos / Informações pessoais (como, por exemplo, endereços, telefone, endereços de e-mail) / Localização e informações sobre viagens

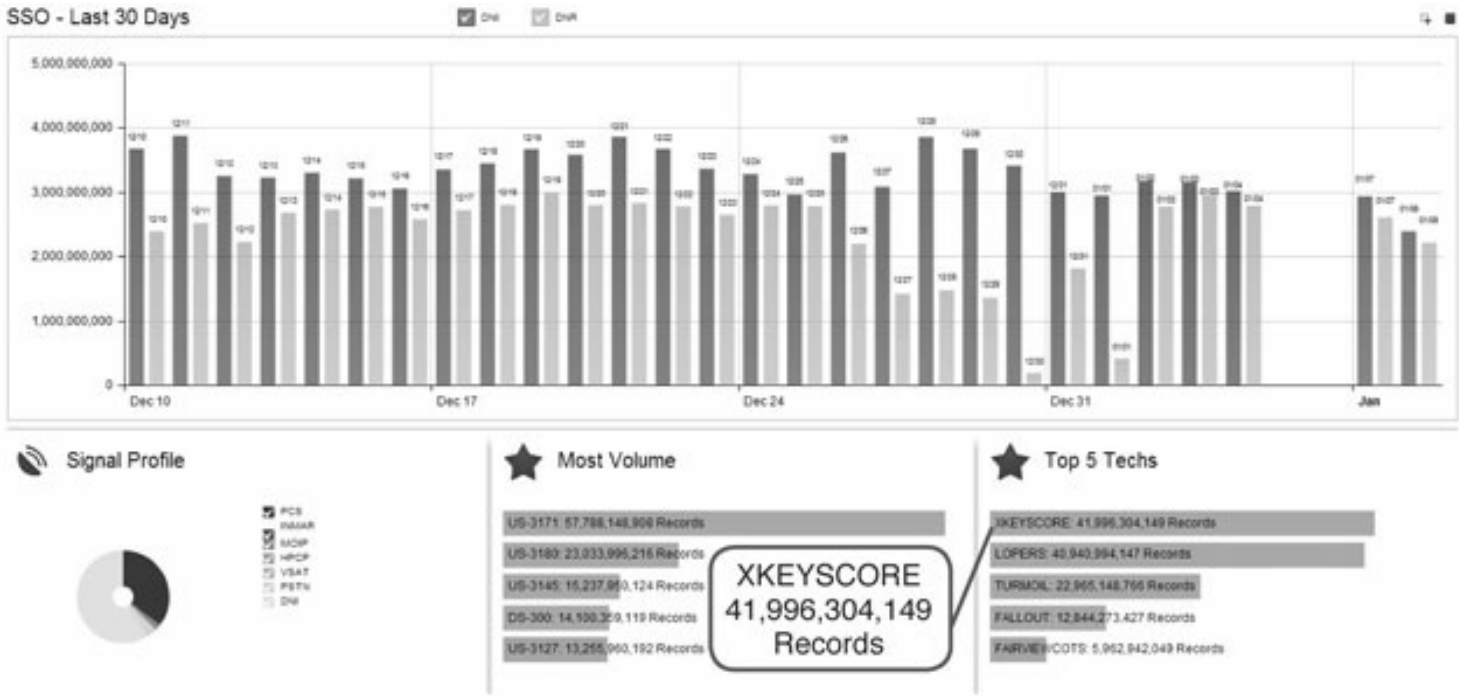
Os métodos para pesquisar a atividade nas mídias sociais são tão simples quanto a pesquisa de e-mail. O analista preenche o nome do usuário desejado, digamos, no Facebook, junto com um limite de datas para a atividade, e o X-KEYSCORE então fornece todas as informações desse usuário, incluindo mensagens, chats e outros posts privados.



POSSÍVEIS BUSCAS DE ATIVIDADE DE USUÁRIO

Atividade de usuário / Data/hora: / Início: / Fim: / Buscar por: nome de usuário / Termo buscado: 12345678910 / Onde: facebook / Data/hora: / Início: / Fim: / Buscar por: nome de usuário / Termo buscado: Meu_nomedeusuario / Onde: netlog

Talvez o aspecto mais notável do X-KEYSCORE seja a espantosa quantidade de informações catalogadas e armazenadas pelo programa em múltiplos locais de coleta espalhados pelo mundo. "Em alguns lugares", afirma um relatório, "com base nos recursos disponíveis, a quantidade de informações que recebemos por dia (superior a 20 terabytes) só pode ser armazenada por um período de 24 horas." Para um período de trinta dias iniciado em dezembro de 2012, a quantidade de registros coletada pelo X-KEYSCORE – apenas para uma unidade, a SSO – ultrapassou 41 bilhões:

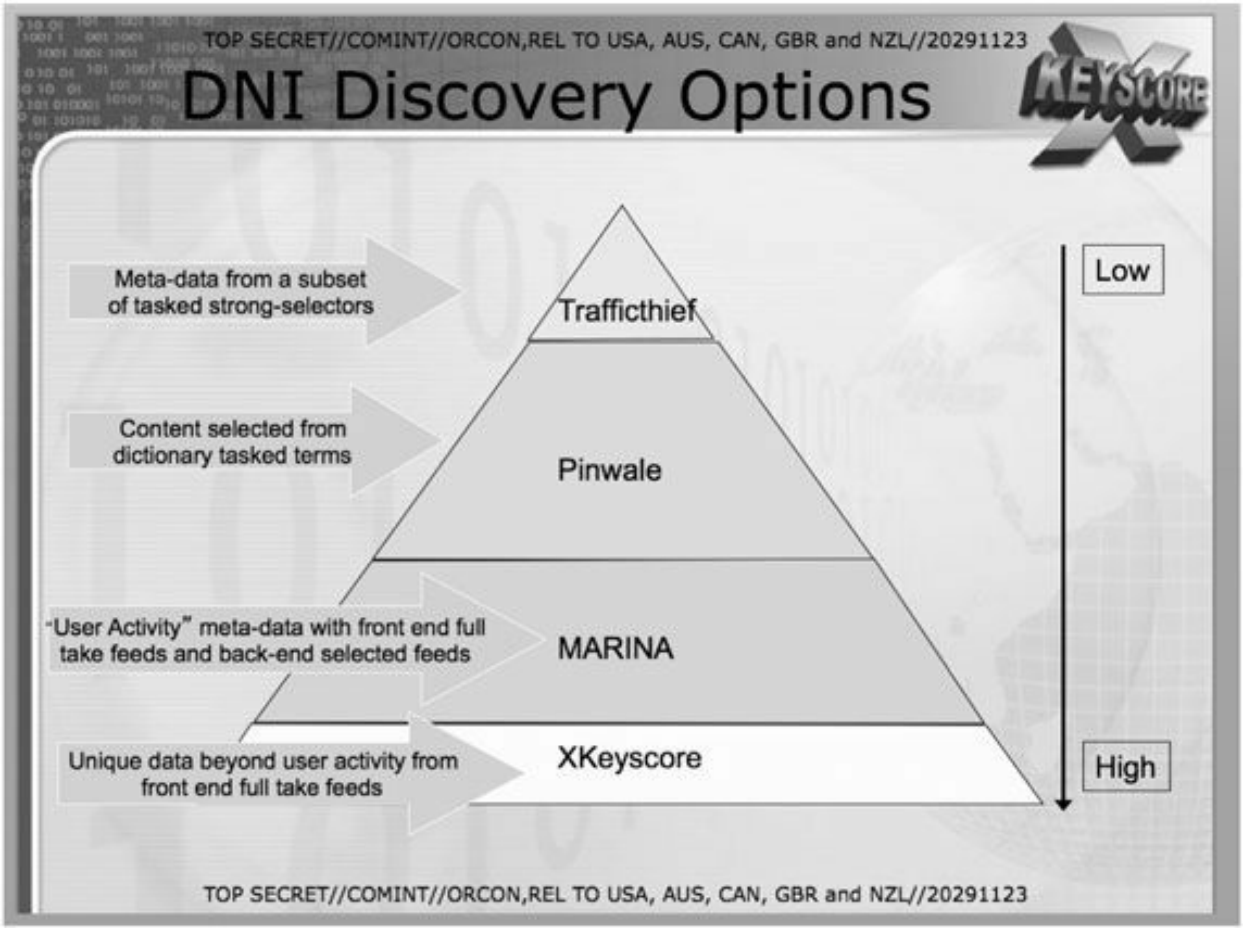


SSO – ÚLTIMOS 30 DIAS

Da esquerda para a direita: Perfil de sinais / Maior volume / 57.788.148.908 registros / 23.033.996.216 registros / 15.237.950.124 registros / 14.100.359.119 registros / 13.255.960.192 registros / Cinco maiores tecnologias / 41.996.304.149 registros / 40.940.994.147 registros / 22.965.148.766 registros / 12.844.273.427 registros / 5.962.942.049 registros

Destaque: X-KEYSCORE: 41.996.304.149 registros

O X-KEYSCORE "armazena o conteúdo total por 3-5 dias, efetivamente 'tornando a internet mais lenta'" – ou seja, os "analistas podem voltar e recuperar as sessões". Então o "conteúdo que for 'interessante' pode ser retirado do X-KEYSCORE e inserido no Agility ou no PINWALE", bases de dados de armazenagem nas quais podem ficar por mais tempo.



OPÇÕES DE DESCOBERTA DE DNI

Setas: Metadados de um subconjunto de seletores fortes solicitados em tarefas / Conteúdo selecionado em termos de dicionário solicitados em tarefas / Metadados de "atividade do usuário" com feeds completos no lado cliente e feeds selecionados no lado servidor / Dados privilegiados além da atividade do usuário obtidos por feeds completos no lado cliente

Legenda: Baixa / Alta

A capacidade do X-KEYSCORE de acessar o Facebook e outras mídias sociais é turbinada por outros programas, entre os quais o BLARNEY, que permitem à NSA monitorar "um amplo leque de dados do Facebook por meio de atividades de vigilância e busca" (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 26).

(TS//SI//NF) BLARNEY explora rede social via coleta expandida no Facebook

Por INFORMAÇÃO OMITIDA em 14/3/2011 0737

(TS//SI//NF) Destaque da SSO – BLARNEY explora rede social

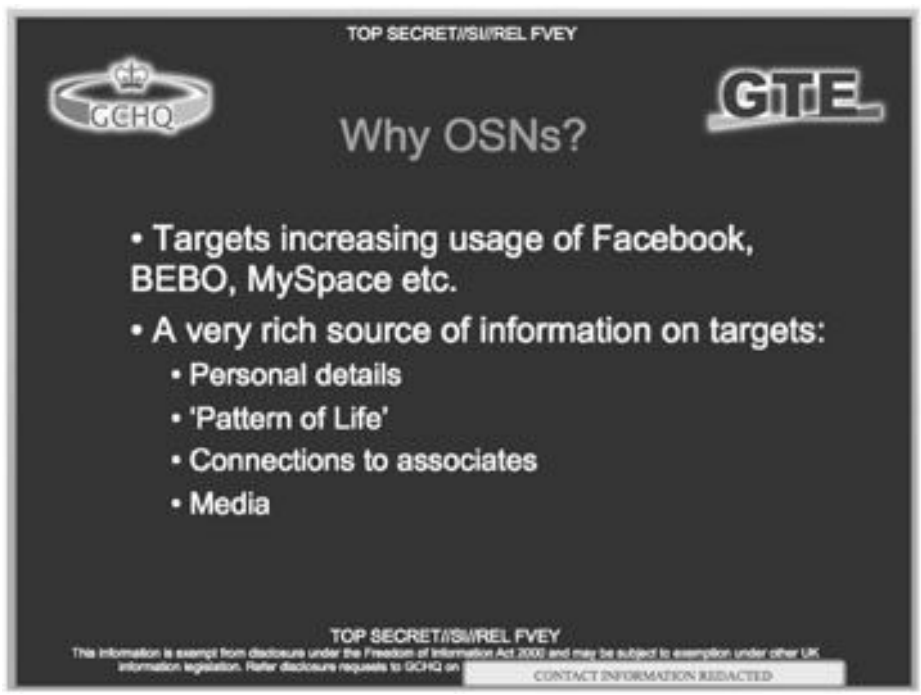
via coleta expandida no Facebook

(TS//SI//NF) Em 11 de março de 2011, BLARNEY iniciou uma entrega significativamente melhorada e mais completa de conteúdo do Facebook. Trata-se de um salto importante na capacidade da NSA de explorar o Facebook usando as autorizações da FISA e da FAA. Esse esforço foi iniciado seis meses atrás, em parceria com o FBI, para solucionar um sistema de coleta não confiável e incompleto no Facebook. A NSA agora consegue acessar uma ampla gama de dados do Facebook por meio de atividades de busca e vigilância. Analistas estão animados por receber muitos campos de conteúdo, como chats, com uma constância antes só disponível de forma ocasional. Parte do conteúdo será completamente nova, como os vídeos dos usuários. De modo geral, a nova coleta no Facebook proporcionará uma excelente oportunidade de SIGINT contra nossos alvos – da geolocalização com base em seus endereços de IP e softwares utilizados à coleta de todas as suas mensagens particulares e informações de perfil. Múltiplos elementos dentro da NSA fizeram uma parceria para garantir a entrega bem-sucedida desses dados. Um representante da NSA no FBI coordenou o rápido desenvolvimento do sistema de coleta; a equipe do PRINTAURA da SSO programou novos softwares e realizou mudanças de configuração; a CES [Serviços de Análise Criptográfica e Exploração] modificou seus sistemas de exploração de protocolo e o Diretório de Tecnologia acelerou as atualizações de suas ferramentas de apresentação de dados para que os analistas pudessem visualizar os dados de forma correta.

Enquanto isso, no Reino Unido, a divisão GTE (Exploração Global de Telecomunicações) da GCHQ também empregou recursos significativos na tarefa, o que foi detalhado em uma apresentação na conferência dos Cinco Olhos em 2011.

EXPLORAÇÃO DE TRÁFEGO DO FACEBOOK
NO AMBIENTE PASSIVO PARA OBTER INFORMAÇÕES ESPECÍFICAS

INFORMAÇÃO OMITIDA Desenvolvedor de Capacidades / Exploração Global de Telecomunicações (GTE) / GCHQ / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA



POR QUE AS REDES SOCIAIS?

Aumento de uso do Facebook, BEBO, MySpace, etc. pelos alvos / Fonte muito rica de

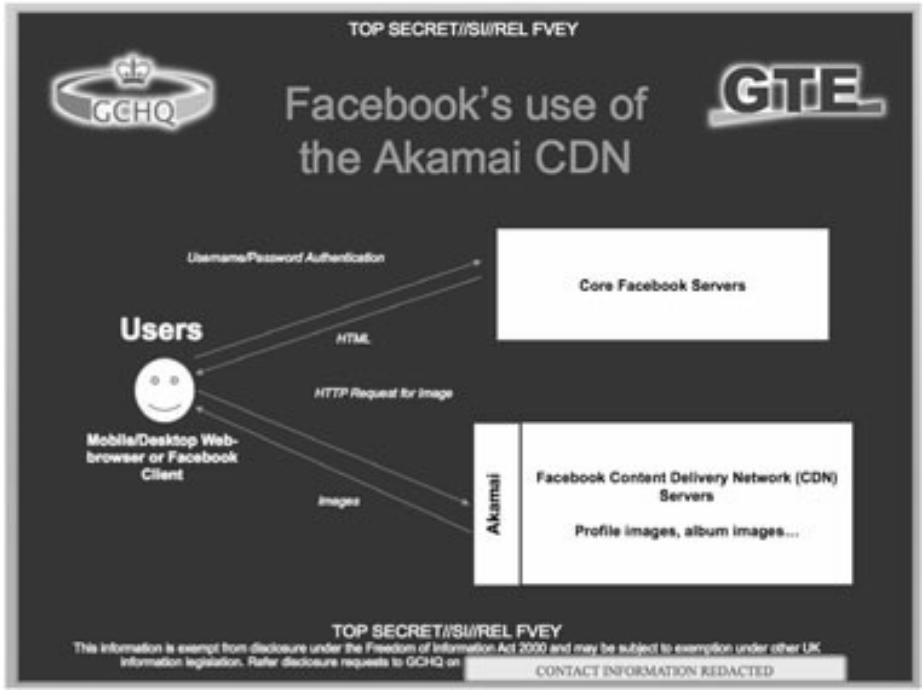
informações sobre alvos: / Detalhes pessoais / “Padrão de vida” / Conexões com colaboradores / Mídia / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

A GCHQ prestou especial atenção às fraquezas do sistema de segurança do Facebook e à obtenção do tipo de informação que seus usuários tentam proteger:

ATENÇÃO AO AMBIENTE PASSIVO

Muitos alvos no Facebook protegem seus perfis, tornando impossível visualizar todas as suas informações... / Mas o ambiente passivo proporciona a oportunidade de coletar essas informações graças à exploração de fraquezas inerentes ao modelo de segurança do Facebook. / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

Em especial, a GCHQ encontrou vulnerabilidades no sistema usado pela rede social para armazenar fotos, que pode ser usado para obter acesso às identidades do Facebook e a imagens de álbuns:



USO DA REDE DE CDN AKAMAI PELO FACEBOOK

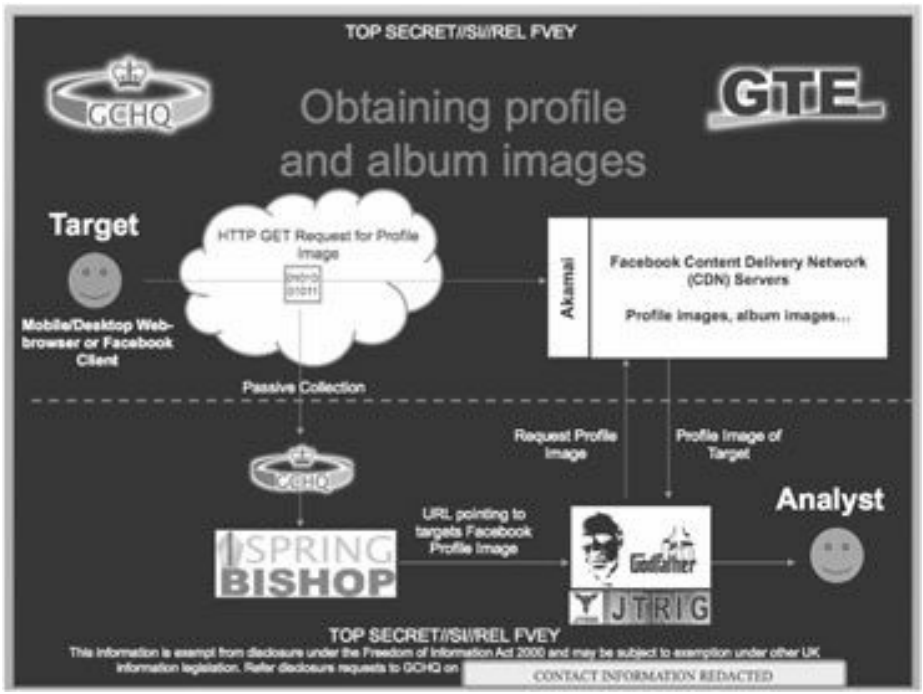
Colunas esquerda e do meio, de cima para baixo: Nome de usuário/Autenticação de senha / Usuários / Navegador do celular/computador ou cliente do Facebook / HTML / Solicitação de HTTP para imagem / Imagens

Coluna da direita, de cima para baixo: Servidores centrais do Facebook / Akamai / Servidores de CDN do Facebook / Imagens de perfil, imagens de álbuns... / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no

INFORMAÇÃO OMITIDA

EXPLORAÇÃO DO CDN DO FB

Fraquezas / Autenticação pressuposta / Segurança pela obscuridade / É possível dissecar a URL do CDN gerada pelo Facebook de modo a extrair a ID do usuário a cujas fotos o arquivo esteja relacionado. Por exemplo, eis abaixo uma típica URL de imagem de perfil: http://**perfil.ak.fbcdn.net**/hprofile-ak-s12p/hs621.snc3/27353_ INFORMAÇÃO OMITIDA _2215_q.jpg / O texto realçado em verde está exclusivamente relacionado ao servidor específico dentro dos CDNs do Facebook. E o texto realçado em amarelo é a ID do usuário do Facebook. / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA



OBTENÇÃO DE IMAGENS DE PERFIL E DE ÁLBUNS

Da esquerda para a direita, de cima para baixo: Alvo / Navegador do celular/computador ou cliente do Facebook / HTTP recebe solicitação para imagem de perfil / Coleta passiva / Akamai / Servidores de CDN do Facebook / Imagens de perfil, imagens de álbuns... / Solicitação de imagem de perfil / URL aponta para imagem de perfil dos alvos no Facebook / Imagem de perfil do alvo / Analista / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

Além das redes de mídias sociais, a NSA e a GCHQ continuam a buscar quaisquer brechas em

sua rede de vigilância, quaisquer comunicações que ainda estejam fora do seu alcance, para então desenvolver formas de submetê-las ao olhar atento das agências. Um programa aparentemente obscuro ilustra esse ponto.

Tanto a NSA quanto a GCHQ vêm tentando obstinadamente monitorar as comunicações de internet e telefone das pessoas durante voos comerciais. Como estas são redirecionadas por sistemas de satélite independentes, são muito difíceis de detalhar. A ideia de que haja um momento em que alguém possa usar a internet no celular sem ser detectado – ainda que por apenas algumas horas, a bordo de um avião – é intolerável para as agências de vigilância. Por esse motivo, elas dedicaram recursos significativos ao desenvolvimento de sistemas capazes de interceptar comunicações durante os voos.

Na conferência dos Cinco Olhos de 2012, a GCHQ apresentou um programa de interceptação chamado ieving Magpie ("pega-ladrão"), que tem por alvo o cada vez mais frequente uso de celulares durante voos de avião:

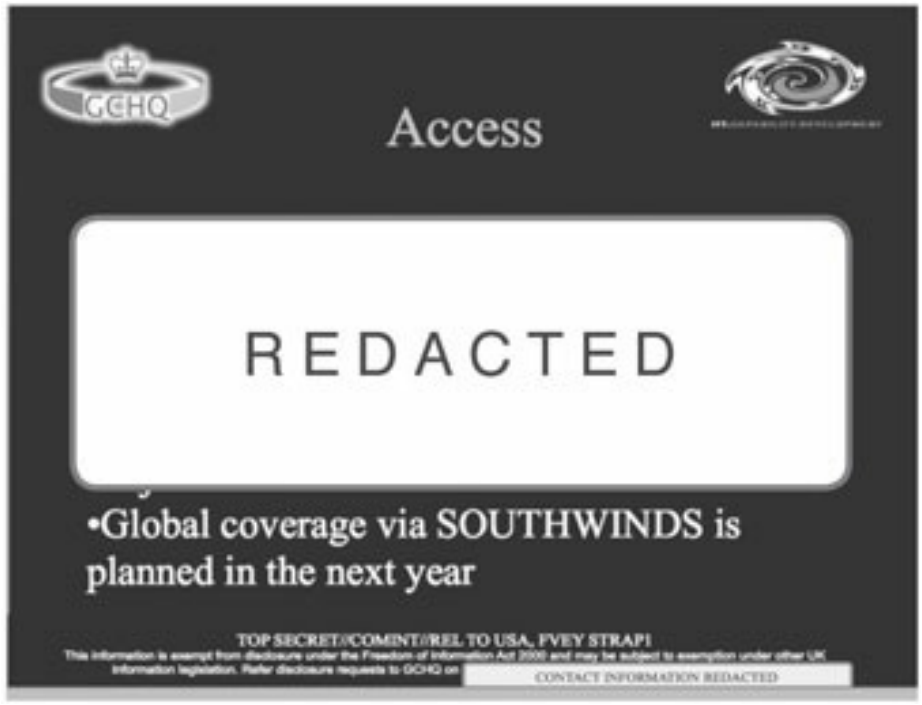
THIEVING MAGPIE

Uso de serviços de GSM/GPRS a bordo para rastrear alvos / INFORMAÇÃO OMITIDA / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

SERVIÇOS DE GSM A BORDO

Muitas empresas aéreas agora oferecem serviços de telefonia móvel a bordo, sobretudo para voos de longa distância e na classe executiva (a lista vem aumentando) / Pelo menos a British Airways restringe o serviço a dados e SMS apenas – o uso de voz não é permitido / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

A solução proposta imaginava um sistema que garantisse uma "cobertura global" completa:



ACESSO

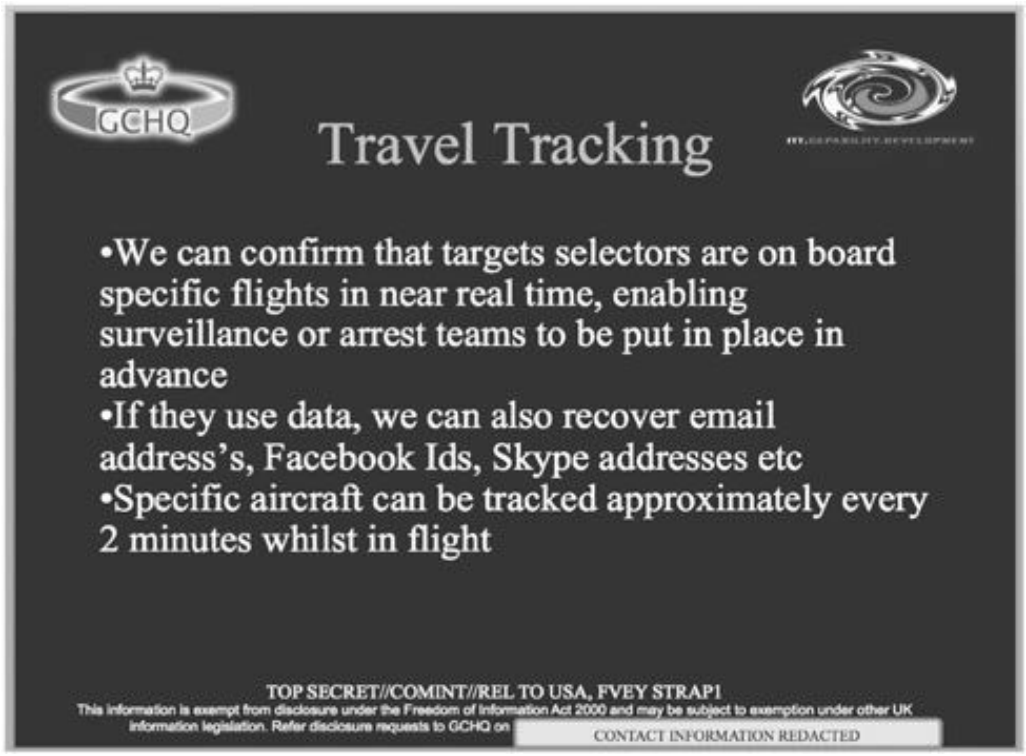
INFORMAÇÃO OMITIDA / Uma cobertura global via SOUTHWIND está prevista para o ano que vem / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

Avanços significativos foram feitos para garantir que determinados equipamentos sejam suscetíveis a vigilância nas aeronaves de passageiros:

OCORRÊNCIAS GPRS

Atualmente capaz de gerar ocorrências pelo menos para os aparelhos Blackberry durante

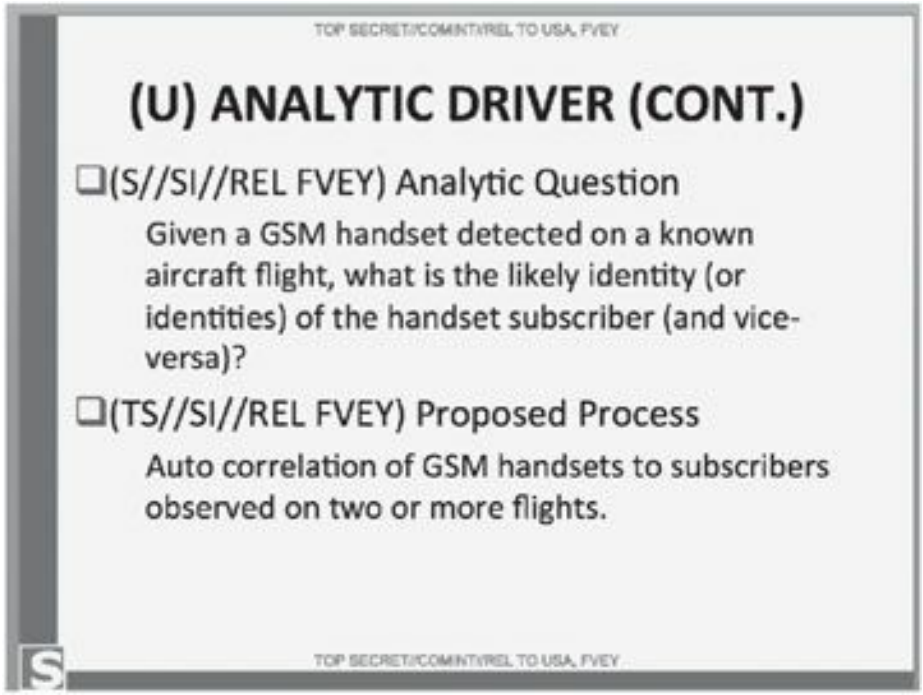
os voos / Capaz de identificar o PIN do Blackberry e os endereços de e-mail associados / Conteúdo solicitado em tarefas encaminhado para armazenagem de dados, conteúdo não selecionado para o Xkeyscore, mais detalhes sobre uso disponíveis / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA



RASTREAMENTO EM VIAGEM

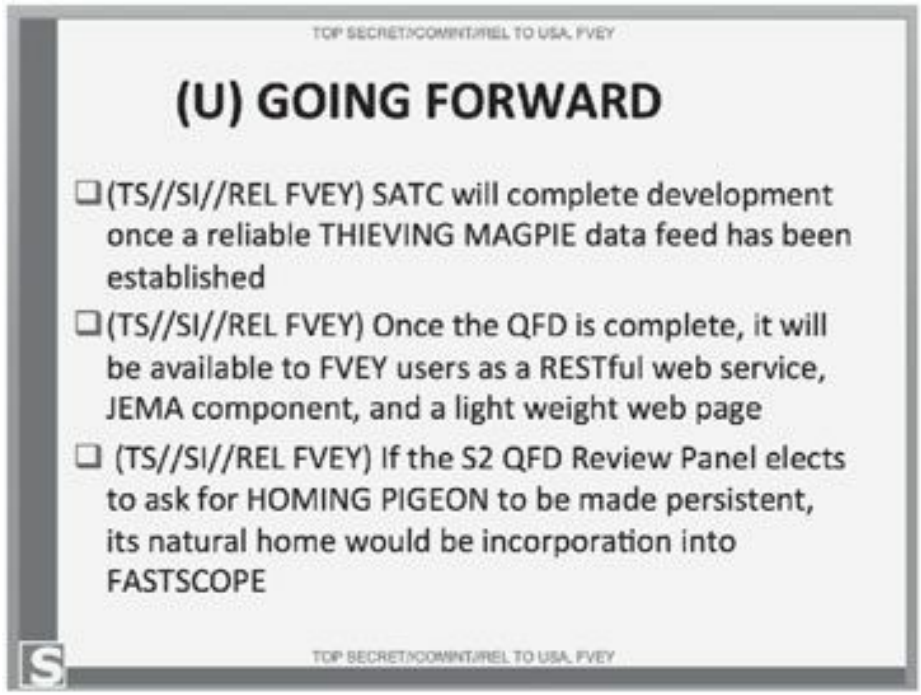
Podemos confirmar que seletores de alvos estão a bordo de determinados voos quase em tempo real, o que permite o posicionamento antecipado de equipes de vigilância ou prisão / Se os alvos usarem dados, podemos também obter endereços de e-mail, IDs do Facebook, endereços de Skype, etc. / Aeronaves específicas podem ser rastreadas aproximadamente a cada 2 minutos durante o voo / Esta informação está isenta de revelação de acordo com a Lei de Liberdade de Informação de 2000 e pode estar sujeita a isenções de acordo com outras leis do Reino Unido relativas à informação. Solicitações de revelação devem ser submetidas à GCHQ no INFORMAÇÃO OMITIDA

Um documento de teor semelhante apresentado pela NSA na mesma conferência, sobre um programa chamado HOMING PIGEON ("pombo-correio"), também descreve esforços para monitorar comunicações a bordo. O programa deveria ser coordenado com a GCHQ, e o sistema todo, disponibilizado para o grupo dos Cinco Olhos:



CONTROLADOR ANALÍTICO (CONT.)

Pergunta analítica / Quando um aparelho portátil GSM for detectado em um voo conhecido, qual é a provável identidade (ou identidades) do assinante do aparelho (e vice-versa)? / Processo sugerido / Autocorrelação de aparelhos GSM com assinantes observados em dois ou mais voos.



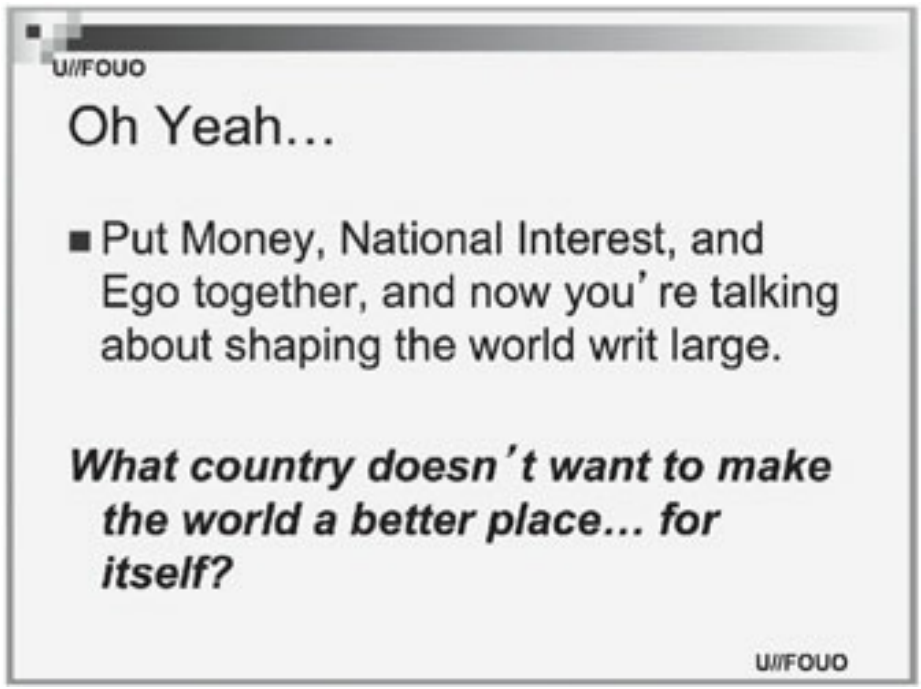
INDO MAIS ADIANTE

A SATC completará desenvolvimento quando uma transmissão confiável de dados do THIEVING MAGPIE houver sido estabelecida / Uma vez concluída, a QFD estará disponível para usuários FVEY como serviço de internet RESTful, componente JEMA e

uma página leve na internet / Se o Grupo de Revisão S2 QFD decidir pedir a continuação de HOMING PIGEON, seu destino natural será a incorporação ao FASTSCOPE

Em determinadas áreas da NSA, existe uma sinceridade notável em relação ao verdadeiro objetivo de se construir um sistema de vigilância secreta tão abrangente. Uma apresentação de PowerPoint elaborada para um grupo de altos funcionários da agência encarregado de discutir a perspectiva de padrões internacionais de internet proporciona uma visão crua. O autor da apresentação é um "Alto Funcionário de Inteligência Nacional da NSA/SIGINT (SINIO) para Ciência e Tecnologia", que descreve a si mesmo como "um cientista e hacker experiente".

O título bem claro de sua apresentação é "O papel dos interesses nacionais, do dinheiro e dos egos". Segundo ele, esses três fatores, juntos, constituem os principais motivos que levam os Estados Unidos a manter sua posição dominante na vigilância global.



É ISSO AÍ…

Basta juntar dinheiro, interesse nacional e ego, e aí, sim, se pode falar em moldar o mundo da maneira mais ampla possível. / Que país não quer transformar o mundo em um lugar melhor… para si mesmo?

O autor observa que a dominação da internet pelos Estados Unidos proporcionou ao país poder e influência significativos, além de gerar grandes lucros:

QUAL É A AMEAÇA?

Sejamos claros: o mundo ocidental (sobretudo os Estados Unidos) conquistou influência e ganhou muito dinheiro graças ao estabelecimento de padrões anteriores / Os Estados Unidos foram o principal responsável por moldar a internet atual. Isso resultou em uma exportação generalizada da cultura e da tecnologia norte-americanas. Resultou também em muito dinheiro ganho por entidades norte-americanas.

Esse lucro e esse poder, é claro, intensificaram inevitavelmente a indústria da vigilância em si, proporcionando outro motivo para sua expansão sem fim. A era pós-11 de Setembro testemunhou uma explosão maciça dos recursos dedicados à vigilância. A maioria desses recursos foi transferida dos cofres públicos (ou seja, dos contribuintes norte-americanos) para o bolso de corporações privadas de vigilância defensiva.

Empresas como Booz Allen Hamilton ou AT&T empregam batalhões de ex-altos funcionários do governo, enquanto batalhões de atuais altos funcionários na área da defesa já passaram (e é provável que ainda passem) por essas mesmas corporações. Aumentar constantemente o tamanho do Estado de vigilância é uma forma de garantir que os recursos do governo continuem fluindo, que a engrenagem permaneça lubrificada. Essa também é a melhor forma de garantir que a NSA e suas agências relacionadas conservem sua importância institucional e sua influência em Washington.

Conforme a escala e a ambição do setor de vigilância cresceram, o mesmo aconteceu com o perfil daqueles considerados seus adversários. Ao listar as diversas ameaças supostamente enfrentadas pelos Estados Unidos, a NSA – em um documento intitulado "Agência de Segurança Nacional: Visão Geral de Briefing" – inclui alguns itens previsíveis: "hackers", "elementos criminosos" e "terroristas". De forma reveladora, contudo, também amplia seu escopo com a inclusão nessa lista de *tecnologias*, entre as quais a própria internet:

A AMEAÇA HOJE

Hackers; Insiders; Internet; Wireless; Circuitos de alta velocidade; Pagers; Fac-símile; Satélite; Elementos criminosos; Terroristas

A internet tem sido propalada há tempos como um instrumento sem precedentes de democratização, liberalização e até emancipação. No entanto, aos olhos do governo dos Estados Unidos, essa rede global e outros tipos de tecnologia de comunicação ameaçam minar o poderio norte-americano. Vista nesses termos, a ambição da NSA de "coletar tudo" torna-se finalmente coerente. É vital que a NSA monitore todas as partes da internet, bem como de quaisquer outros meios de comunicação, para que nenhum deles possa escapar ao controle do governo dos Estados Unidos.

Em última instância, além da manipulação diplomática e das vantagens econômicas, um sistema de espionagem onipresente permite aos Estados Unidos manter seu controle sobre o mundo. Quando o país consegue saber tudo o que todos estão fazendo, dizendo, pensando e planejando – seus próprios cidadãos, populações estrangeiras, corporações internacionais, líderes de outros governos –, seu poder sobre eles é maximizado. Isso é duplamente verdadeiro quando o governo opera em níveis de sigilo cada vez mais altos. O sigilo cria um espelho de apenas uma direção: o governo dos Estados Unidos vê tudo o que o resto do mundo faz, inclusive sua própria população, mas ninguém sabe de suas ações. É o cúmulo do desequilíbrio, que dá lugar à mais perigosa de todas as condições humanas: o exercício de um poder ilimitado sem transparência nem prestação de contas.

As revelações de Edward Snowden subverteram essa perigosa dinâmica ao revelar a existência do sistema e seu modo de funcionamento. Pela primeira vez, pessoas do mundo inteiro puderam ter conhecimento da verdadeira extensão das capacidades de vigilância usadas contra elas. A notícia provocou um debate mundial intenso e sustentado justamente porque essa vigilância representa uma grave ameaça à governança democrática. Ela também gerou propostas de reformas, uma discussão

global sobre a importância da liberdade na internet e da privacidade na era eletrônica, além de uma conscientização sobre a pergunta vital: o que a vigilância sem limites significa para nós como indivíduos, em nossa própria vida?

4

OS DANOS DA VIGILÂNCIA

Governos do mundo inteiro têm se esforçado fortemente para treinar seus cidadãos a desdenhar a própria privacidade. Uma ladainha de lugares-comuns hoje conhecidos de todos convenceu as pessoas a tolerarem invasões brutais a seu universo privado; as justificativas foram tão bem-sucedidas que muitos aplaudem enquanto as autoridades coletam grandes quantidades de informação sobre o que dizem, leem, compram e fazem – e com quem.

Essas autoridades estatais foram auxiliadas em seu ataque à privacidade por uma série de magnatas da internet, os parceiros indispensáveis da vigilância do governo. Quando Eric Schmidt, CEO do Google, foi questionado durante uma entrevista à CNBC em 2009 sobre as preocupações em relação à retenção de dados dos usuários praticada por sua empresa, sua famigerada resposta foi: "Se você tiver alguma coisa que não quer que ninguém saiba, talvez não a devesse estar fazendo, para começo de conversa." Com igual descaso, o fundador e CEO do Facebook, Mark Zuckerberg, afirmou em uma entrevista de 2010 que "todos já se sentem à vontade não só compartilhando mais informações de diferentes tipos, mas também de modo mais aberto e com mais pessoas". A privacidade na era digital não é mais uma "norma social", alegou ele, conceito que beneficia convenientemente os interesses de uma empresa de tecnologia que trabalha com informações pessoais.

A importância da privacidade, porém, é evidenciada pelo fato de que nem mesmo aqueles que a desvalorizam, que a declararam extinta ou dispensável, acreditam no que dizem. Os mesmos que se manifestam contra a privacidade várias vezes se esforçaram, e muito, para controlar a visibilidade de seu comportamento e de suas informações. O próprio governo dos Estados Unidos usou medidas extremas para proteger suas ações do olhar do público, erguendo um muro cada vez mais alto de sigilo por trás do qual opera. Como já afirmava um relatório da ACLU em 2011: "Hoje em dia, grande parte das ações de nosso governo é conduzida em segredo." Esse mundo de sombras é tão secreto, "tão grande e impenetrável", como descreveu o *Washington Post*, "que ninguém sabe quanto ele custa, quantas pessoas emprega, quantos programas engloba ou exatamente quantas agências fazem o mesmo trabalho".

De modo semelhante, os magnatas da internet tão dispostos a violar nossa privacidade se mostram protetores ao extremo quando se trata de sua vida privada. O Google insistiu na política de não falar com jornalistas do site de notícias de tecnologia CNET depois que este publicou detalhes pessoais sobre Eric Schmidt, entre os quais seu salário, doações de campanha feitas por ele e seu endereço, todas informações públicas obtidas usando o próprio Google de modo a ilustrar a ameaça invasiva representada pela empresa.

Enquanto isso, para garantir sua privacidade, Mark Zuckerberg comprou as quatro casas adjacentes à sua em Palo Alto, na Califórnia, gastando para isso 30 milhões de dólares. Como disse o CNET: "A sua vida pessoal agora é conhecida como dados do Facebook. A vida pessoal do CEO da empresa agora é conhecida como vá cuidar da sua vida."

A mesma contradição é expressada pelos muitos cidadãos comuns que desdenham o valor da privacidade, mas mesmo assim protegem com senhas suas contas de e-mail ou de mídias sociais. Essas pessoas põem trinco na porta de seus banheiros e lacram os envelopes nos quais enviam suas cartas. Quando ninguém está olhando, fazem coisas que jamais cogitariam fazer quando totalmente expostas. Dizem coisas aos amigos, psicólogos e advogados que não querem que ninguém mais saiba. Expressam opiniões on-line que não desejam ver associadas ao seu nome.

Os muitos defensores da vigilância com quem conversei desde que Snowden fez suas revelações logo repetiram a opinião de Eric Schmidt: a privacidade é para quem tem algo a esconder. Só que nenhum deles se mostrou disposto a me informar a senha de seu e-mail ou permitir câmeras de vídeo dentro de suas casas.

Quando a presidente do Comitê de Inteligência do Senado, Dianne Feinstein, insistiu que a coleta de metadados pela NSA não configura vigilância – uma vez que não inclui o conteúdo de nenhuma comunicação –, houve protestos na internet exigindo que ela respaldasse sua afirmação com atos: estaria disposta a publicar uma vez por mês uma lista completa das pessoas para quem havia mandado e-mails e telefonado, com a duração das chamadas e a localização física de seus interlocutores na ocasião? Era inconcebível ela aceitar fazê-lo, justamente porque essas informações são profundamente reveladoras: torná-las públicas significaria uma verdadeira invasão do universo privado da pessoa.

A questão não é a hipocrisia daqueles que minimizam o valor da privacidade alheia ao mesmo tempo que se esmeram para proteger a própria, embora isso seja revelador. O fato é que o desejo de privacidade é compartilhado por todos nós como parte essencial, e não secundária, do que significa ser humano. Nós todos compreendemos de forma instintiva que a esfera privada é onde podemos agir, pensar, falar, escrever, experimentar e decidir como ser longe do olhar avaliador dos outros. A privacidade é uma das condições centrais para ser livre.

Talvez a formulação mais famosa do que significa privacidade e por que ela é desejada de forma tão universal e preeminente tenha sido feita em 1928 pelo juiz da Suprema Corte dos Estados Unidos Louis Brandeis no caso "Olmstead contra a União": "O direito de ser deixado sozinho [é] o mais abrangente dos direitos, e o mais valorizado por um povo livre", escreveu ele. O valor da privacidade "tem um escopo muito mais amplo" do que as simples liberdades civis. Ela é fundamental:

> Os redatores da nossa Constituição buscaram garantir condições favoráveis à busca da felicidade. Eles reconheceram o significado da natureza espiritual do homem, de seus sentimentos e de seu intelecto. Entenderam que apenas parte das agruras, do prazer e da satisfação da vida pode ser encontrada em objetos materiais. Buscaram proteger os americanos em seus pensamentos, crenças, emoções e sensações. Em contraste com o governo, eles lhes conferiram o direito de ser deixados em paz.

Mesmo antes de ser nomeado para a Suprema Corte, Brandeis já era um ardente defensor da importância da privacidade. Em parceria com o advogado Samuel Warren, assinou em 1890 o inspirador artigo da *Harvard Law Review* intitulado "O direito à privacidade", no qual argumentava que despojar alguém de sua privacidade era um crime de natureza bem distinta do roubo de um bem material. "O princípio que protege os escritos pessoais e outras produções individuais não contra o

roubo e a apropriação física, mas contra a publicação em qualquer formato, na verdade não é o princípio da propriedade privada, mas sim o de uma personalidade inviolável."

Quase nunca se discutem os motivos que tornam a privacidade essencial à liberdade e felicidade humanas, mas eles são compreendidos de forma instintiva pela maioria das pessoas, como demonstra o esforço feito por cada uma delas para proteger sua vida privada. Para começar, o comportamento humano se modifica radicalmente quando se sabe estar sendo observado. As pessoas se esforçam para fazer o que se espera delas; querem evitar a vergonha e a condenação. Para tanto, aderem com firmeza às práticas sociais aceitas, atendo-se aos limites impostos e evitando ações que possam ser consideradas desviantes ou anormais.

Assim, o leque de escolhas que elas consideram quando acham que estão sendo observadas é bem mais estreito do que as suas possíveis ações em âmbito privado. A negação da privacidade tem por efeito uma severa restrição da liberdade de escolha.

Há muitos anos, fui ao *bat mitzvah* da filha de um de meus melhores amigos. Durante a cerimônia, o rabino ressaltou que "a lição central" que a menina deveria aprender era que "estava sempre sendo observada e julgada". Disse-lhe que Deus sempre sabia o que ela estava fazendo e conhecia cada escolha sua, cada ato e cada pensamento, por mais particular que fosse. "Você nunca está sozinha", afirmou, o que significava que ela deveria sempre fazer a vontade de Deus.

O que o rabino queria dizer era claro: se você nunca pode escapar ao olhar atento de uma autoridade suprema, não tem outra escolha senão respeitar os ditames por ela impostos. Não pode sequer cogitar trilhar o próprio caminho além dessas regras; se você acredita que está sendo sempre vigiado e julgado, na realidade não é um indivíduo livre.

Todas as autoridades opressoras – políticas, religiosas, sociais, parentais – têm por base essa verdade vital e usam-na como ferramenta importante para impor ortodoxias, forçar o cumprimento das regras e eliminar a dissidência. É de seu interesse transmitir a mensagem de que elas não deixarão de saber nada que seus súditos façam. Muito mais eficaz do que uma força policial, a eliminação da privacidade neutraliza qualquer tentação de se desviar das regras e normas.

Com a exclusão do universo privado, perdem-se muitos dos atributos tipicamente associados à qualidade de vida. A maioria das pessoas já experimentou na pele como a privacidade permite se livrar das restrições. E todos nós também já tivemos a experiência de externar comportamentos privados quando pensávamos estar sozinhos – dançar, confessar-se, explorar alguma expressão sexual, compartilhar ideias não testadas – e depois nos envergonhar por termos sido vistos.

Só quando acreditamos que ninguém mais está observando é que nos sentimos livres – livres para de fato experimentar, testar limites, explorar novas formas de pensar e de ser, descobrir o que significa ser nós mesmos. O que tornou a internet tão atraente foi justamente o fato de proporcionar a possibilidade de falar e agir de forma anônima, algo vital para a exploração individual.

Por esse motivo, é no universo privado que germinam a criatividade, a dissidência e a contestação da ortodoxia. Uma sociedade em que todo mundo sabe que pode ser vigiado pelo Estado – na qual o universo privado é eliminado de forma eficaz – é uma sociedade na qual esses atributos se perdem, tanto no nível social quanto no individual.

A vigilância estatal em massa traz, portanto, uma repressão inerente, mesmo no caso improvável de não haver abusos por parte de autoridades vingativas no intuito, por exemplo, de obter informações privadas sobre adversários políticos. Independentemente de como a vigilância é usada ou

abusada, os limites impostos por ela à liberdade são intrínsecos à sua existência.

Evocar o *1984* de George Orwell é um certo clichê, mas as semelhanças entre o mundo sobre o qual o autor alertou e o Estado de vigilância da NSA são inegáveis: ambos se apoiam na existência de um aparato tecnológico capaz de monitorar as ações e as palavras de cada cidadão. O paralelo é negado pelos defensores da vigilância – segundo eles, não estamos sendo vigiados *o tempo todo* –, mas seu argumento passa ao largo da questão. No livro, os cidadãos não eram necessariamente monitorados o tempo inteiro; na verdade, não faziam ideia de que estivessem sendo monitorados. Mas o Estado tinha capacidade para observá-los a qualquer momento. O que mantinha todos na linha eram a incerteza e a possibilidade de uma vigilância onipresente:

> A tela da TV recebia e transmitia ao mesmo tempo. Qualquer som produzido por Winston mais alto do que um leve sussurro era captado por ela; além disso, enquanto ele permanecesse dentro do campo de visão dominado pela placa de metal, podia ser visto também. É claro que não dava para saber se você estava sendo vigiado em um momento específico. Com que frequência ou por meio de que sistema a Polícia do Pensamento se conectava a determinado indivíduo não passava de conjectura. Era até possível pensar que todos fossem vigiados o tempo inteiro, mas de qualquer forma ela podia conectar seu fio a você sempre que quisesse. Você precisava viver – e vivia, por um hábito que se tornava instinto – na suposição de que todos os sons que produzia eram ouvidos e, a não ser no escuro, todos os seus movimentos, monitorados.

Nem mesmo a NSA, com toda a sua capacidade, seria capaz de ler todos os e-mails, escutar todos os telefonemas e rastrear todas as ações de cada indivíduo. O que torna um sistema de vigilância eficaz no controle do comportamento humano é a consciência de que as palavras e ações das pessoas são passíveis de monitoramento.

Esse princípio está no cerne do conceito proposto pelo filósofo setecentista britânico Jeremy Bentham chamado Panopcticon: um projeto de prédio que, segundo ele, permitiria às instituições controlarem de forma eficaz o comportamento humano. Nas suas palavras, a estrutura seria usada em "qualquer tipo de estabelecimento no qual pessoas de qualquer descrição devam ser mantidas sob inspeção". A principal inovação arquitetônica do Panopticon era uma grande torre central a partir da qual todos os cômodos – fossem celas de prisão, salas de aula ou enfermarias de hospitais psiquiátricos – podiam ser monitorados por guardas o tempo todo. Seus ocupantes, porém, não podiam ver o que havia dentro da torre, e portanto não tinham como saber quando estavam ou não sendo vigiados.

Como as instituições – qualquer instituição – não eram capazes de observar todo mundo o tempo todo, a solução de Bentham foi criar "a aparente onipresença do inspetor" na mente dos ocupantes. "As pessoas a serem inspecionadas devem sempre se sentir sob inspeção, ou pelo menos sentir que têm uma grande chance de estarem sendo inspecionadas." Assim, elas agiriam como se estivessem sempre sendo vigiadas, mesmo quando não fosse o caso. O resultado seria docilidade, obediência e conformidade com as expectativas. Bentham previa que essa criação fosse se alastrar muito além das prisões e dos hospitais psiquiátricos até atingir todas as instituições sociais. Em sua opinião, inculcar

na mente dos cidadãos que eles podem sempre estar sendo monitorados iria revolucionar o comportamento humano.

Nos anos 1970, Michel Foucault observou que o princípio do Panopticon de Bentham era um dos mecanismos fundadores do Estado moderno. Em *Vigiar e punir*, ele afirma que o panopticonismo é "um tipo de poder aplicado aos indivíduos na forma de uma supervisão individual contínua, na forma de controle, punição e compensação, e na forma de correção, ou seja, a moldagem e transformação dos indivíduos segundo determinadas normas".

Foucault explica, ainda, que a vigilância onipresente não só aumenta o poder das autoridades e propicia obediência como também induz os indivíduos a internalizarem aqueles que os vigiam. Quem acredita estar sendo vigiado instintivamente decidirá fazer o que se quer que ele faça, sem nem perceber que está sendo controlado – o Panopticon "induz no prisioneiro um estado de visibilidade consciente e permanente que garante o funcionamento automático do poder". Com o controle assim internalizado, os indícios explícitos de repressão desaparecem, pois não são mais necessários: "O poder externo pode se desfazer de seu peso físico; ele tende a ser incorpóreo; quanto mais se aproxima do limite, mais constante, profundo e permanente são os seus efeitos: trata-se de uma vitória profunda, que evita qualquer confronto físico e já está sempre decidida de antemão."

Além disso, esse modelo de controle tem a grande vantagem de criar, ao mesmo tempo, a ilusão de liberdade. A compulsão de obedecer passa a existir na cabeça de cada um. Por medo de estarem sendo observados, os indivíduos resolvem, por conta própria, obedecer. Isso elimina a necessidade de todos os símbolos visíveis de coerção, permitindo o controle de pessoas que equivocadamente se julgam livres.

Por esse motivo, todos os Estados repressivos consideram a vigilância em massa um de seus instrumentos de controle mais importantes. Ao descobrir que a NSA havia passado anos interceptando chamadas feitas com seu celular pessoal, a chanceler alemã Angela Merkel, em geral contida, falou com o presidente Obama e, irritada, comparou a vigilância dos Estados Unidos à Stasi, o célebre serviço de segurança da Alemanha Oriental, onde ela fora criada. Merkel não estava querendo dizer que os Estados Unidos fossem equivalentes ao regime comunista, mas sim que o cerne de um Estado de vigilância ameaçador – seja ele representado pela NSA, pela Stasi, pelo Grande Irmão ou pelo Panopticon – é a percepção de que, a qualquer momento, pode-se estar sendo monitorado por autoridades invisíveis.

Não é difícil entender por que as autoridades dos Estados Unidos e de outros países ocidentais têm sido tentadas a construir um sistema onipresente de espionagem direcionado a seus próprios cidadãos. O agravamento da desigualdade econômica, transformado em uma verdadeira crise pelo colapso financeiro de 2008, gerou graves instabilidades internas. Até mesmo democracias relativamente estáveis, como Espanha e Grécia, tiveram distúrbios perceptíveis. Em 2011, houve dias de protestos de rua em Londres. Nos Estados Unidos, tanto a direita – manifestações do Partido Republicano em 2008 e 2009 – quanto a esquerda – movimento Occupy – iniciaram duradouros protestos de cidadãos. Pesquisas nesses países revelaram níveis surpreendentemente fortes de descontentamento com a classe política e com a forma de dirigir a sociedade.

Face a perturbações sociais, as autoridades em geral têm duas alternativas: aplacar a população com concessões simbólicas ou fortalecer seu controle de modo a minimizar os possíveis danos aos

seus interesses. As elites ocidentais parecem preferir a segunda alternativa – fortalecer o próprio poder –, talvez o único curso de ação viável para proteger sua posição. A reação ao movimento Occupy foi esmagá-lo pela força, com gás lacrimogêneo, spray de pimenta e condenações. A paramilitarização das forças policiais domésticas pôde ser vista claramente nas cidades americanas: policiais sacaram armas usadas nas ruas de Bagdá para sufocar protestos organizados dentro da legalidade e em grande parte pacíficos. A estratégia – instilar nas pessoas o medo de comparecer às manifestações e protestos – de modo geral deu certo. O objetivo mais amplo era cultivar a ideia de que esse tipo de resistência contra uma força estabelecida maciça e impenetrável é inútil.

Um sistema de vigilância onipresente atinge o mesmo objetivo, mas com potência ainda maior. Quando o governo observa tudo o que as pessoas estão fazendo, o simples fato de organizar movimentos dissidentes é dificultado. Mas a vigilância em massa também elimina a dissidência em um lugar mais profundo e mais importante: na mente, que o indivíduo treina para pensar apenas de acordo com o que é esperado e exigido dele.

A história não deixa dúvidas de que coerção e controle coletivos são ao mesmo tempo a intenção e o efeito de um Estado de vigilância. Walter Bernstein, roteirista de Hollywood incluído na lista negra e submetido a monitoramento durante o macarthismo, forçado a escrever sob pseudônimo para continuar a trabalhar, descreveu a dinâmica da autocensura opressiva que advém da sensação de estar sendo vigiado o tempo todo:

> Todo mundo tomava cuidado. Não era época para se expor demais. Havia roteiristas, gente não incluída na lista negra, que faziam coisas, não sei como se poderia chamar isso, coisas "de vanguarda", mas nada político. Eles mantinham distância da política. Acho que havia uma sensação generalizada de "não é bom se arriscar muito".
>
> Esse não é um ambiente que incentive a criatividade ou que solte a imaginação. Você sempre corre o perigo de se autocensurar, de dizer "ah, não, não vou tentar isso porque sei que ninguém vai querer fazer ou que o governo vai achar ruim", ou algo desse tipo.

Um relatório publicado pela fundação PEN American Center em novembro de 2013, intitulado *Efeitos arrepiantes: vigilância da NSA leva escritores americanos à autocensura*, retoma de forma sinistra as observações de Bernstein. A organização fez um levantamento para verificar os efeitos das revelações sobre a NSA em seus membros e descobriu que muitos autores hoje "partem do princípio de que suas comunicações estão sendo monitoradas" e mudaram seu comportamento de uma forma que "limita sua liberdade de expressão e restringe o livre fluxo de informação". Mais especificamente, "24% evitaram de propósito determinados assuntos em conversas por e-mail ou por telefone".

O pernicioso poder de controle da vigilância onipresente e a autocensura dele resultante são confirmados por uma série de experimentos em ciências sociais, e vão muito além do ativismo político. Vários estudos mostram como essa dinâmica funciona nos níveis pessoais e psicológicos mais profundos.

Uma equipe de pesquisadores, cujas conclusões foram publicadas no periódico *Evolutionary Psychology*, apresentou aos participantes da pesquisa atos moralmente questionáveis, como, por exemplo, embolsar uma quantia considerável de dinheiro encontrada em uma carteira na rua ou saber que um amigo incluiu informações falsas em seu currículo. Os pesquisadores solicitaram às

pessoas que avaliassem o grau de transgressão desses exemplos. O estudo observou que os indivíduos aos quais eram mostradas imagens sugestivas de vigilância, como um grande par de olhos vidrados, classificavam os atos como "mais repreensíveis" do que aqueles aos quais se mostrava uma imagem neutra. Os pesquisadores concluíram que a vigilância incentiva quem está sendo vigiado a "afirmar sua aprovação das normas sociais dominantes" em uma tentativa de "administrar a própria reputação de forma ativa".

Um experimento abrangente conduzido em 1975 por dois psicólogos da Universidade Stanford – Gregory White e Philip Zimbardo – e intitulado "Os efeitos arrepiantes da vigilância" buscou avaliar se o fato de ser observado tinha algum impacto na expressão de opiniões políticas controversas. O estudo foi impulsionado pelas preocupações dos americanos com a vigilância conduzida pelo governo:

> O escândalo de Watergate, revelações de grampos na Casa Branca e investigações no Congresso sobre a espionagem doméstica conduzida pela CIA serviram para destacar a temática cada vez mais paranoica da vida americana: o Grande Irmão pode estar observando você! Propostas de bancos de dados nacionais, o uso de helicópteros de vigilância por forças de polícia urbanas, a presença de câmeras em bancos e supermercados e as revistas de pessoas e bens feitas em aeroportos são alguns dos indícios de que nossa vida privada está submetida a um escrutínio cada vez mais intenso.

Os participantes foram sujeitados a diversos níveis de vigilância e orientados a dar sua opinião sobre a legalização da maconha.

Ficou claro que os indivíduos "ameaçados" – aqueles cujas afirmações seriam compartilhadas com a polícia para "fins de treinamento" – tinham mais chances de condenar o uso da maconha e de usar em seu discurso pronomes de segunda e terceira pessoas ("você", "eles", "as pessoas"). Apenas 44% dos participantes sob vigilância defenderam a legalização, contra 77% daqueles que não estavam sob ameaça. Foi revelador o fato de 31% dos participantes monitorados terem buscado, de forma espontânea, a aprovação dos pesquisadores (com a pergunta "tudo bem?", por exemplo), enquanto apenas 7% do outro grupo terem feito o mesmo. Participantes "ameaçados" demonstraram níveis muito maiores de ansiedade e inibição.

Na conclusão do artigo, White e Zimbardo observaram que "a ameaça ou realidade de uma vigilância governamental pode inibir psicologicamente a liberdade do discurso". Os autores acrescentaram ainda que, embora seu "modelo de pesquisa não oferecesse a possibilidade de 'evitar reuniões'", eles imaginavam que "a ansiedade gerada pela ameaça de vigilância levaria muitas pessoas a evitar por completo situações" nas quais pudessem ser monitoradas. "Como essas suposições são limitadas apenas pela imaginação de cada um e incentivadas todos os dias por revelações de invasão de privacidade pelo governo e pelas instituições", escreveram eles, "o limite entre ilusões paranoicas e cautelas justificadas torna-se de fato muito tênue".

É verdade que a vigilância às vezes pode promover o que alguns talvez considerem um comportamento desejável. Um estudo constatou que as arruaças nos estádios de futebol suecos – torcedores jogando garrafas e isqueiros no campo – diminuíram 65% após a introdução de câmeras de segurança. E a literatura de saúde pública sobre o ato de lavar as mãos confirmou repetidas vezes

que a melhor maneira de aumentar a probabilidade de alguém lavar as mãos é pôr outra pessoa por perto.

No entanto, o efeito esmagador de ser observado é uma restrição severa das escolhas individuais. Mesmo no mais íntimo dos ambientes – em família, por exemplo –, a vigilância transforma ações insignificantes em fonte de autojulgamento e ansiedade pelo simples fato de a pessoa estar sendo observada. Em um experimento conduzido no Reino Unido, pesquisadores deram aos participantes aparelhos de rastreamento que permitiam controlar o paradeiro de parentes. Era possível acessar a qualquer momento a localização precisa de qualquer familiar e, caso esta fosse visualizada, a pessoa recebia uma mensagem. Sempre que um parente rastreava outro, ele também recebia um questionário perguntando por que o havia feito e se a informação recebida tinha correspondido às expectativas.

Nos depoimentos posteriores ao experimento, os participantes afirmaram que, embora às vezes considerassem o rastreamento reconfortante, também se preocupavam com a possibilidade de que, caso estivessem em um lugar inesperado, seus parentes pudessem "tirar conclusões precipitadas" quanto ao seu comportamento. E a opção "ficar invisível" – ou seja, bloquear o mecanismo de compartilhamento da própria localização – não solucionava essa ansiedade: muitos participantes disseram que o próprio ato de evitar a vigilância iria gerar desconfiança. Os pesquisadores concluíram:

> Há caminhos trilhados em nossa vida cotidiana que não somos capazes de justificar e que podem ser totalmente insignificantes. No entanto, sua representação em um aparelho de rastreamento (...) lhes confere significado, parecendo exigir um grau extraordinário de prestação de contas. Isso gera ansiedade, sobretudo em relacionamentos íntimos, nos quais as pessoas podem se sentir mais pressionadas a justificar coisas que são simplesmente incapazes de justificar.

Em um experimento finlandês responsável por uma das simulações mais radicais de vigilância já feitas, câmeras foram colocadas nas casas dos participantes – exceto banheiros e quartos –, e todas as suas comunicações eletrônicas foram monitoradas. Embora a propaganda do estudo tenha se transformado em viral nas mídias sociais, os pesquisadores tiveram dificuldade para encontrar dez residências que aceitassem participar.

Entre as que se candidataram, as reclamações relacionadas ao projeto se concentravam na invasão de partes banais de sua vida diária. Uma das mulheres se sentiu pouco à vontade para ficar pelada dentro de casa; outra se incomodou com as câmeras enquanto arrumava o cabelo depois do banho; outro participante pensou na vigilância enquanto aplicava uma injeção de remédios em si mesmo. Ao serem vigiadas, ações inócuas ganharam camadas de significado.

No início, os participantes descreveram a vigilância como incômoda, mas logo "se acostumaram" com ela. O que no começo era profundamente invasivo se normalizou, transformando-se no estado normal e deixando de ser percebido.

Como mostram os experimentos citados, existem vários tipos de ações que as pessoas desejam manter privadas, mesmo que não constituam "fazer algo errado". A privacidade é indispensável para uma ampla gama de atividades humanas. Se alguém liga para um S.O.S. Suicídio, vai a uma clínica de aborto, frequenta um site de sexo virtual, marca uma consulta em uma clínica de desintoxicação

ou começa o tratamento de alguma doença, ou então se um delator liga para um jornalista, irá querer manter esses atos na esfera privada por motivos que nada têm a ver com ilegalidade ou mau comportamento.

Resumindo, todo mundo tem algo a esconder. O jornalista Barton Gellman defendeu essa afirmação da seguinte maneira:

> A privacidade é um conceito relacional; depende do seu público. Você não quer que o seu patrão saiba que está procurando outro emprego. Não conta tudo sobre sua vida amorosa a sua mãe ou a seus filhos. Não revela segredos profissionais a seus concorrentes. Nós não nos expomos de forma indiscriminada, e damos importância suficiente à exposição para mentir sem hesitação. Entre cidadãos respeitadores das leis, pesquisadores já mostraram muitas vezes que mentir é "uma interação social diária" (duas vezes ao dia entre estudantes universitários, uma vez por dia no "mundo real"). A transparência total é um pesadelo. Todo mundo tem algo a esconder.

Um dos principais argumentos usados para justificar a vigilância – que ela é para o bem da população – baseia-se na projeção de uma visão de mundo que divide os cidadãos em categorias de pessoas boas e pessoas más. Segundo essa noção, as autoridades usam seus poderes de vigilância apenas contra as pessoas más, as que estão "fazendo algo errado", e só elas têm algo a temer em relação à invasão de sua privacidade. Essa é uma tática antiga. Em matéria publicada na revista *Time* em 1969 sobre a preocupação crescente dos americanos com os poderes de vigilância do governo, o procurador-geral de Nixon, John Mitchell, garantia aos leitores que "qualquer cidadão norte-americano que não esteja envolvido em alguma atividade ilegal não tem absolutamente nada a temer".

O mesmo foi dito por um porta-voz da Casa Branca em reação à controvérsia de 2005 relativa ao programa de grampos ilegal de Bush: "Não se trata de monitorar chamadas feitas para combinar treinos da liga juvenil de beisebol ou que prato levar para um jantar entre amigos. Essas escutas foram pensadas para monitorar ligações de pessoas muito más para outras pessoas muito más." E em agosto de 2013, quando Obama foi ao *Tonight Show* e Jay Leno lhe perguntou sobre as revelações a respeito da NSA, o presidente respondeu: "Nós não temos um programa de espionagem doméstica. O que temos são alguns mecanismos capazes de rastrear um número de telefone ou endereço de e-mail relacionado a algum ataque terrorista."

Para muita gente, esse argumento funciona. A percepção de que a vigilância invasiva se limita apenas a um grupo marginalizado e merecedor formado por quem está "fazendo algo errado" – os maus – garante que a maioria aceite ou até incentive o abuso de poder.

Mas essa visão parte de um grande mal-entendido em relação aos objetivos que movem todas as instituições de autoridade. Aos olhos dessas instituições, "fazer algo errado" abarca muito mais do que atos ilegais, comportamentos violentos e complôs terroristas. Tipicamente, o conceito se estende a qualquer dissidência significativa e qualquer contestação verdadeira. Equiparar a dissidência a estar fazendo algo errado, ou no mínimo a uma ameaça, faz parte da natureza da autoridade.

A história está repleta de exemplos de grupos e indivíduos vigiados pelo governo por causa de suas visões dissidentes e de seu ativismo: Martin Luther King, o movimento em prol dos direitos civis, ativistas contrários à guerra, ambientalistas. Aos olhos do governo e do FBI de J. Edgar Hoover,

todos eles estavam "fazendo algo errado": exercendo uma atividade política que ameaçava a ordem dominante.

Ninguém entendia melhor do que Hoover o poder da vigilância para sufocar a dissidência política, uma vez que ele teve de enfrentar o desafio de impedir o exercício da Primeira Emenda da Constituição – direito à livre expressão e à livre associação –, que proíbe o Estado de prender pessoas por emitirem opiniões impopulares. Nos anos 1960, uma série de casos na Suprema Corte estabeleceram proteções rigorosas para a liberdade de opinião, culminando com a decisão unânime do caso "Brandenburg versus Ohio", que derrubou a condenação de um líder da Ku Klux Klan que, durante um discurso, havia ameaçado de violência autoridades políticas. A Corte decidiu que as garantias de livre expressão e liberdade de imprensa da Primeira Emenda são tão fortes que "não permitem a um Estado proibir ou proscrever a defesa do uso da força".

Devido a essas garantias, Hoover instituiu um sistema para impedir que a dissidência sequer viesse a se desenvolver.

O COINTELPRO, programa de contrainteligência doméstico do FBI, foi denunciado pela primeira vez por um grupo de ativistas antiguerra convencidos de que o movimento tinha sido infiltrado, estava agora submetido a vigilância e era alvo de todo tipo de golpe sujo. Em 1971, na falta de indícios documentais para provar tal afirmação e incapazes de convencer jornalistas a escreverem sobre suas suspeitas, eles arrombaram um escritório do FBI na Pensilvânia e pegaram milhares de documentos.

O material relacionado ao COINTELPRO mostrava como o FBI tivera por alvo grupos e indivíduos considerados subversivos e perigosos, entre os quais a NAACP (Associação Nacional para o Progresso das Pessoas de Cor), movimentos nacionalistas negros, organizações socialistas e comunistas, manifestantes antiguerra e diversos grupos de direita. A organização infiltrara nesses grupos agentes que, entre outras coisas, tentavam manipular seus membros para que estes aceitassem cometer atos criminosos de modo que o FBI pudesse prendê-los e processá-los.

O FBI conseguiu convencer o *New York Times* a suprimir os documentos ou mesmo devolvê-los, mas o *Washington Post* publicou uma série de matérias com base neles. Essas revelações levaram à criação, no Senado, do Comitê Church, cuja conclusão foi:

> [Ao longo de quinze anos] o FBI conduziu uma sofisticada operação de vigilância destinada especificamente à prevenção do exercício dos direitos de expressão e associação relacionados à Primeira Emenda, segundo a noção de que impedir o crescimento de grupos perigosos e a propagação de ideias perigosas protegeria a segurança nacional e inibiria a violência.
>
> Mesmo que todos os alvos em questão estivessem envolvidos em atividades violentas, muitas das técnicas usadas seriam intoleráveis em uma sociedade democrática; o COINTELPRO, entretanto, foi muito além delas. A principal premissa velada dos programas era que uma agência de segurança pública tem o dever de fazer o necessário para combater o que for percebido como ameaça à ordem social e política vigente.

Um memorando-chave do programa explicava que era possível semear a "paranoia" entre os ativistas antiguerra fazendo-os acreditar que "por trás de toda caixa de correio havia um agente do FBI". Assim, os dissidentes, sempre convencidos de estarem sendo vigiados, ficariam amedrontados a

ponto de não exercer o ativismo.

Como era de esperar, a tática deu certo. Em um documentário de 2013 chamado *1971*, vários ativistas descreveram como o FBI de Hoover "tomou conta" do movimento em prol dos direitos civis com vigilância e agentes infiltrados, pessoas que iam às reuniões para depois relatar o que haviam presenciado. Esse monitoramento prejudicava a capacidade de organização e expansão do movimento.

Na época, até mesmo as instituições mais consolidadas de Washington entenderam que a mera existência da vigilância estatal, fosse usada como fosse, sufoca a capacidade de dissidência. Em um editorial de março de 1975 sobre o arrombamento do escritório do FBI, o *Washington Post* alertava justamente para essa dinâmica opressiva:

> O FBI nunca demonstrou grande sensibilidade em relação aos efeitos nocivos que a sua vigilância, e sobretudo sua utilização de informantes anônimos, tem no processo democrático e na prática da livre expressão. Mas é preciso deixar claro que qualquer discussão ou controvérsia relacionada às políticas e aos programas do governo está fadada a ser inibida caso se descubra que o Grande Irmão, disfarçado, está escutando-a e denunciando-a.

O COINTELPRO está longe de ser o único abuso revelado pelo Comitê Church. Segundo o último relatório do comitê, "milhões de telegramas pessoais enviados por, para ou através dos Estados Unidos foram obtidos pela Agência Nacional de Segurança entre 1947 e 1975 graças a um acordo secreto com as três empresas de telégrafo dos Estados Unidos". Além disso, "cerca de 300 mil indivíduos foram indexados em um sistema de computadores da CIA, e arquivos distintos foram criados sobre aproximadamente 7.200 americanos e cerca de cem grupos domésticos" durante uma operação da CIA chamada CHAOS (1967-1973).

Além disso, "estima-se que 100 mil americanos foram objeto de arquivos da inteligência do exército dos Estados Unidos criados entre meados da década de 1960 e o ano de 1971", fora os cerca de 11 mil indivíduos e grupos investigados pelo Serviço da Receita Interna "com base em critérios mais políticos do que fiscais". A CIA também usou grampos para detectar vulnerabilidades, como a atividade sexual, que eram utilizadas na época para "neutralizar" os alvos.

Esses incidentes não foram aberrações da época. Durante a era Bush, por exemplo, documentos obtidos pela ACLU revelaram, como o grupo afirmou em 2006, "novos detalhes da vigilância exercida pelo Pentágono sobre americanos contrários à guerra do Iraque, entre os quais os quacres e grupos estudantis". O Pentágono estava "monitorando manifestantes não violentos por meio da coleta de informações que eram então armazenadas em uma base de dados militar antiterrorista". A ACLU observou ainda que um dos documentos, "catalogado como 'potencial atividade terrorista', enumera ocorrências como a passeata "Stop the War NOW!" ("Parem a guerra agora") em Akron, Ohio".

Ao que tudo indica, as garantias de que a vigilância só está sendo direcionada a quem tiver feito "algo errado" deveria ser um parco consolo, já que um Estado irá considerar errada qualquer contestação ao seu poder.

Em repetidas ocasiões, a oportunidade de caracterizar opositores políticos como "ameaças à

segurança nacional" ou mesmo "terroristas" se mostrou irresistível para os que detêm o poder. Na última década, como em um eco do FBI de Hoover, o governo classificou formalmente dessa maneira ativistas defensores do meio ambiente, várias facções de direita contrárias ao governo, ativistas antiguerra e associações relacionadas aos direitos palestinos. Alguns indivíduos dentro dessas amplas categorias podem até merecer essa designação, mas sem dúvida a maioria não merece, seja ela culpada ou não de ter opiniões políticas opostas às do governo. No entanto, esses grupos são alvos rotineiros de vigilância da NSA e de seus parceiros.

De fato, depois que as autoridades britânicas prenderam meu companheiro, David Miranda, no aeroporto de Heathrow alegando um estatuto antiterrorista, o governo do Reino Unido equiparou de forma explícita meu trabalho jornalístico sobre a vigilância ao terrorismo, alegando que a revelação dos documentos de Snowden "tem por finalidade influenciar um governo e foi feita com objetivos de promover uma causa política ou ideológica. Portanto, ela se encaixa na definição de terrorismo". Não poderia haver maneira mais clara de relacionar uma ameaça aos interesses do poder com o terrorismo.

Nada disso seria surpresa alguma para a comunidade muçulmana dos Estados Unidos, onde o temor da vigilância sob alegações de terrorismo é intenso e disseminado, e não sem motivo. Em 2012, Adam Goldman e Matt Apuzzo, da Associated Press, revelaram um esquema conjunto da CIA e do Departamento de Polícia de Nova York para submeter comunidades muçulmanas inteiras dentro dos Estados Unidos a vigilância física e eletrônica sem qualquer indício de transgressão. Os muçulmanos americanos com grande frequência descrevem os efeitos da vigilância em suas vidas: cada cara nova que aparece em uma mesquita é vista com desconfiança como informante do FBI; amigos e parentes abafam suas conversas por medo de estarem sendo monitorados e por terem consciência de que qualquer opinião considerada hostil aos Estados Unidos pode ser usada como pretexto para um inquérito ou mesmo para uma ação judicial.

Um dos documentos do acervo de Snowden, com data de 3 de outubro de 2012, realça de modo tenebroso esse ponto ao revelar que a agência vem monitorando as atividades na internet de indivíduos que, segundo ela, expressam ideias "radicais" e têm uma influência "radicalizante" sobre os outros. O memorando menciona seis indivíduos em especial, todos muçulmanos, embora enfatize que eles são apenas "exemplos".

A NSA afirma explicitamente que nenhum dos indivíduos escolhidos como alvo integra uma organização terrorista ou está envolvido em qualquer complô. Seu crime são as opiniões que eles expressam: consideradas "radicais", elas justificam a vigilância generalizada e campanhas destrutivas para "explorar vulnerabilidades".

Entre as informações coletadas sobre essas pessoas – pelo menos uma das quais é um "indivíduo dos Estados Unidos" – estão detalhes sobre suas atividades sexuais na rede e sua "promiscuidade na internet", ou seja, os sites pornográficos que visitam e os chats secretos com mulheres que não sejam suas esposas. A agência debate formas de explorar essa informação para destruir a reputação e a credibilidade dessas pessoas (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 27).

HISTÓRICO (U)

(TS//SI//REL A EUA, FVEY) Um relatório anterior de avaliação de SIGINT relacionado à

radicalização indicava que os radicais parecem ser particularmente vulneráveis, no que diz respeito à autoridade, quando seus comportamentos privados e públicos não são consistentes. (A) É provável que algumas das vulnerabilidades, se expostas, questionem a dedicação de um radical à causa do jihad, levando à degradação ou perda de sua autoridade. Exemplos de algumas dessas vulnerabilidades são:

- Visualizar material sexual explícito na internet ou usar linguagem persuasiva e sexualmente explícita ao se comunicar com meninas jovens e inexperientes;
- Utilizar parte das doações recebidas do grupo suscetível para cobrir os gastos pessoais;
- Cobrar uma quantia exorbitante como cachê para dar palestras e se mostrar atraído por oportunidades de aumentar o próprio status; ou
- Ser conhecido por basear suas mensagens públicas em fontes questionáveis ou por usar linguagem de natureza contraditória, o que o torna vulnerável a questionamentos de credibilidade.

(TS//SI//REL A EUA, FVEY) Questões de confiança e reputação são importantes ao se considerar a validade e o apelo da mensagem. É claro que a exploração de vulnerabilidades de caráter, credibilidade, ou ambos, do radical e de sua mensagem poderia ser intensificada por uma compreensão dos veículos que este utiliza na difusão de sua mensagem para o grupo de pessoas suscetíveis e de onde ele é vulnerável em termos de acesso.

Jameel Jaffer, vice-diretor jurídico da ACLU, observou que as bases de dados da NSA "armazenam informações sobre suas opiniões políticas, seu histórico médico, seus relacionamentos íntimos e suas atividades na internet". Segundo a agência, essas informações pessoais não serão alvo de abusos, "mas os documentos em questão mostram que a NSA sem dúvida tem uma definição bem estreita para o termo 'abuso'". Como assinalado por Jaffer, historicamente, a pedido de um presidente, a NSA "usou os frutos da vigilância para desabonar um adversário político, jornalista ou ativista de direitos humanos". Seria "ingênuo", afirma ele, pensar que a agência não é mais capaz "de usar seu poder dessa forma".

Outros documentos descrevem o foco do governo não apenas no WikiLeaks e em Julian Assange, seu fundador, mas também naquilo que a agência chama de "a rede humana que sustenta o WikiLeaks". Em agosto de 2010, o governo Obama instou diversos aliados a entrarem com ações criminais contra Assange devido à publicação de documentos relacionados à guerra no Afeganistão. O debate relativo à pressão para que outros países processassem Assange aparece em um documento da NSA que a agência batizou de "Cronograma de Caça ao Homem". Nele estão detalhados, país a país, os esforços feitos pelos Estados Unidos e por seus aliados para localizar, processar, capturar e/ou matar vários indivíduos, entre os quais supostos terroristas, traficantes de drogas e líderes palestinos. Entre 2008 e 2012, há um cronograma para cada ano (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 28).

(U) Cronograma de Caça ao Homem 2010

Pular para: navegação, busca

Artigo principal: Caça ao homem

Ver também: Cronograma de Caça ao Homem 2011
Ver também: Cronograma de Caça ao Homem 2009
Ver também: Cronograma de Caça ao Homem 2008

(U) **As operações de caça ao homem a seguir ocorreram no ano-calendário de 2010**:
INFORMAÇÃO OMITIDA **Novembro**

Conteúdo

INFORMAÇÃO OMITIDA **Estados Unidos, Austrália, Grã-Bretanha, Alemanha, Islândia**

(U) Em 10 de agosto, os Estados Unidos instaram outras nações com forças no Afeganistão, entre as quais Austrália, Reino Unido e Alemanha, a considerarem processar criminalmente Julian Assange, fundador do site clandestino WikiLeaks e responsável pela publicação não autorizada de mais de 70 mil documentos sobre a guerra no Afeganistão. Os documentos podem ter sido entregues ao WikiLeaks pelo soldado do exército Bradley Manning. O apelo simboliza o início de um esforço internacional para concentrar o elemento judicial do poder nacional no indivíduo sem afiliações nacionais Assange e na rede humana que sustenta o WikiLeaks.

Outro documento da NSA contém o resumo de um debate sobre se o WikiLeaks, bem como o site de compartilhamento de arquivos Pirate Bay, poderiam ser considerados "'entidades estrangeiras maliciosas' para fins de monitoramento". A designação permitiria uma vigilância eletrônica extensa desses sites e de seus usuários. O debate aparece em uma lista ativa de "perguntas e respostas" na qual autoridades do NOC (Escritório de Supervisão e Legalidade do NTOC, Centro de Ameaças e Operações da NSA) e do OGC (Escritório de Assessoria Jurídica Geral) respondem a perguntas apresentadas (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 29).

INFORMAÇÃO OMITIDA **(TS//SI//REL) Entidade estrangeira maliciosa = disseminação de dados americanos?**

Podemos tratar um servidor estrangeiro que armazena ou potencialmente dissemina dados americanos vazados ou roubados como "entidade estrangeira maliciosa" para fins de monitoramento sem recusas? Exemplos: WikiLeaks, thepiratebay.org, etc.

Resposta do NOC/OGC: Entraremos em contato. (Fonte #001)

Uma dessas trocas de mensagens, de 2011, mostra a indiferença da NSA em relação a violar as regras de vigilância. Nos documentos, um operador diz "Fiz bobagem", pois havia monitorado um indivíduo dos Estados Unidos em vez de um estrangeiro. A resposta do escritório de supervisão da

NSA e de sua assessoria jurídica foi: "Não é nada com que precise se preocupar." (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 30)

INFORMAÇÃO OMITIDA **(TS//SI//REL) Monitoramento involuntário de indivíduo dos Estados Unidos**

Fiz bobagem... o seletor tinha fortes indicações de ser estrangeiro, mas no fim das contas era dos Estados Unidos... e agora?

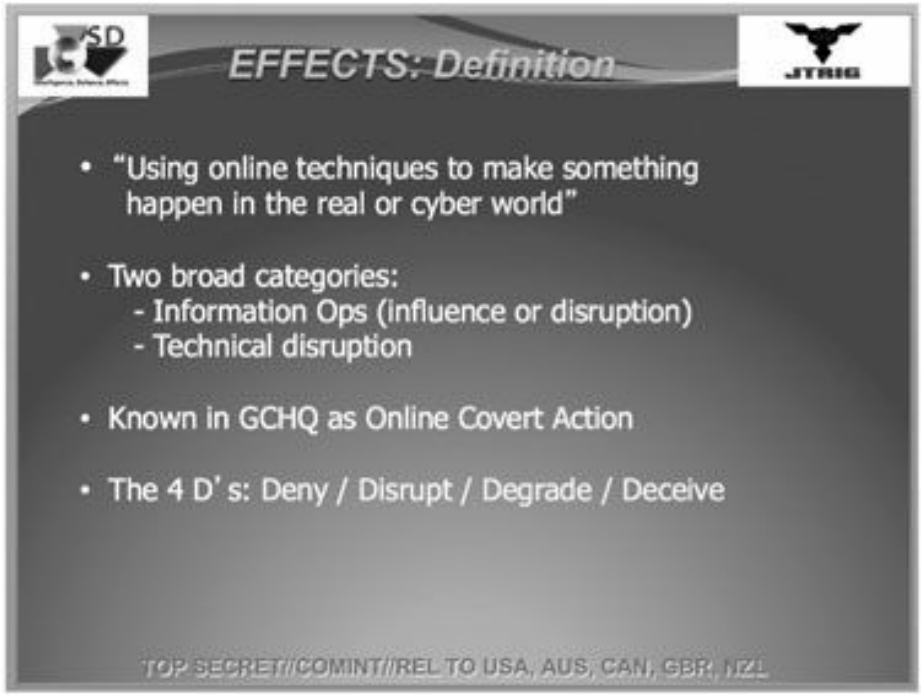
Resposta do NOC/OGC: Em todas as solicitações, se você descobrir que ela é realmente dos Estados Unidos, é preciso pedir autorização e incluí-la no relatório trimestral da OGC... "mas não é nada com que precise se preocupar". (Fonte #001)

A forma de tratar o Anonymous e a categoria vaga de pessoas conhecida como "hacktivistas" é especialmente perturbadora e extrema. Isso porque o Anonymous na verdade não é um grupo estruturado, mas sim uma afiliação solta de indivíduos em torno de uma ideia: pessoas se afiliam ao Anonymous em virtude das opiniões que têm. Pior ainda, a categoria "hacktivistas" não tem significado fixo: pode se referir ao uso de talentos de programação para minar a segurança e o funcionamento da internet, mas também a qualquer um que utilize ferramentas da internet para promover ideias políticas. O fato de a NSA escolher como alvo categorias tão amplas de pessoas equivale a permitir que a agência espione qualquer um, em qualquer lugar – inclusive nos próprios Estados Unidos –, que tenha ideias que o governo julgue ameaçadoras.

Gabriella Coleman, da Universidade McGill, especialista no Anonymous, afirmou que o grupo "não é uma entidade definida", mas "uma ideia que mobiliza ativistas, fazendo-os agir de forma coletiva e externar seu descontentamento político. Trata-se de um movimento social global, com bases amplas, sem estrutura de liderança organizada centralizada ou oficial. Algumas pessoas se uniram em volta desse nome para praticar a desobediência civil digital, mas não é nada que sequer se assemelhe a terrorismo". A maioria dos que abraçaram a ideia fizeram-no "visando sobretudo à expressão política normal. Ter o Anonymous e os hacktivistas como alvo é o mesmo que ter como alvo cidadãos que estão expressando suas crenças políticas, e tem por resultado o sufocamento da dissidência legítima", explica ela.

Apesar disso, o Anonymous foi escolhido como alvo por uma unidade da GCHQ que emprega algumas das táticas mais controversas e radicais conhecidas no mundo da espionagem: "operações de bandeira falsa", "armadilhas sexuais", vírus e outros ataques, estratégias de engodo e "operações de informação para arruinar reputações".

Um slide de PowerPoint apresentado por autoridades de vigilância da GCHQ na conferência de Desenvolvimento de Sinais de 2012 descreve duas formas de ataque: "operações de informação (influência ou perturbação)" e "perturbação técnica". A GCHQ designa esses métodos como "Ação Sigilosa na Internet", dedicada a alcançar o que o documento chama de "os quatro Ds": *deny*, negar/ *disrupt*, perturbar/ *degrade*, degradar/ *deceive*, enganar.



EFEITOS: DEFINIÇÃO

"Usar técnicas on-line para fazer algo acontecer no mundo real ou cibernético" / Duas grandes categorias: / Operações de informação (influência ou perturbação) / Perturbação técnica / Conhecida na GCHQ como Ação Sigilosa na Internet / Os 4 Ds: negar/perturbar/degradar/enganar

Outro slide descreve as táticas usadas para "desabonar um alvo". Entre elas estão "montar uma armadilha sexual", "mudar suas fotos em sites de redes sociais", "escrever um blog fazendo-se passar por uma de suas vítimas" e "mandar e-mails/torpedos para seus colegas, vizinhos, amigos, etc.".

COMO DESABONAR UM ALVO

Montar uma armadilha sexual / Mudar suas fotos em sites de redes sociais / Escrever um blog fazendo-se passar por uma de suas vítimas / Mandar e-mails/torpedos para seus colegas, vizinhos, amigos, etc.

Em observações que acompanham os slides, a GCHQ explica que a "armadilha sexual" – velha tática da Guerra Fria que consiste em usar mulheres bonitas como forma de atrair alvos masculinos para situações comprometedoras e desabonadoras – foi atualizada para a era digital: hoje, um alvo é atraído para um site ou para um encontro on-line comprometedor. O comentário ainda acrescenta: "Ótima opção. Quando funciona, dá muito certo." Da mesma forma, métodos tradicionais de infiltração em grupos são agora adotados na internet (ver documento original no capítulo ANEXO: DOCUMENTOS ORIGINAIS, figura 31):

TOP SECRET//COMINT//REL A EUA, AUS, CAN, GBR, NZL

CK

Armadilha sexual: uma ótima opção. Quando funciona, dá muito certo.

- Conseguir que alguém vá a algum lugar da internet, ou a um local físico, para encontrar "um rosto conhecido".

- O JTRIG (Grupo Conjunto de Pesquisa em Ameaças de Inteligência) tem capacidade para "moldar" o ambiente em determinadas ocasiões.

Troca de fotos; você foi avisado, "o JTRIG está na área!"

Pode alçar a "paranoia" a um outro nível.

E-mail/mensagem de texto:

- Trabalho de infiltração

- Ajuda o JTRIG a obter credibilidade junto a grupos na internet, etc.

- Ajuda a unificar SIGINT/Efeitos.

Outra técnica envolve impedir "alguém de se comunicar". Para tanto, a agência pode "bombardear seu telefone com torpedos", "bombardear seu telefone com chamadas", "apagar sua presença na internet" e "bloquear seu aparelho de fax".

IMPEDIR ALGUÉM DE SE COMUNICAR

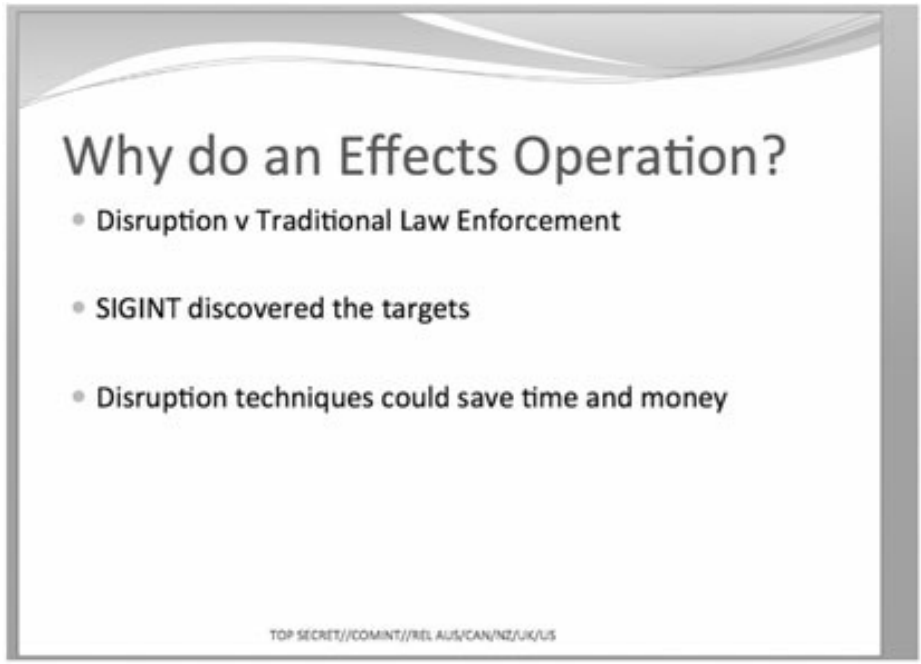
Bombardear seu telefone com torpedos / Bombardear seu telefone com chamadas / Apagar sua presença na internet / Bloquear seu aparelho de fax

IMPEDIR O COMPUTADOR DE ALGUÉM DE FUNCIONAR

Enviar-lhe um vírus: / AMBASSADORS RECEPTION – criptografa a si mesmo, apaga todos os e-mails, criptografa todos os arquivos, faz a tela tremer, impede *log on* / Conduzir um ataque de Serviço Negado no computador

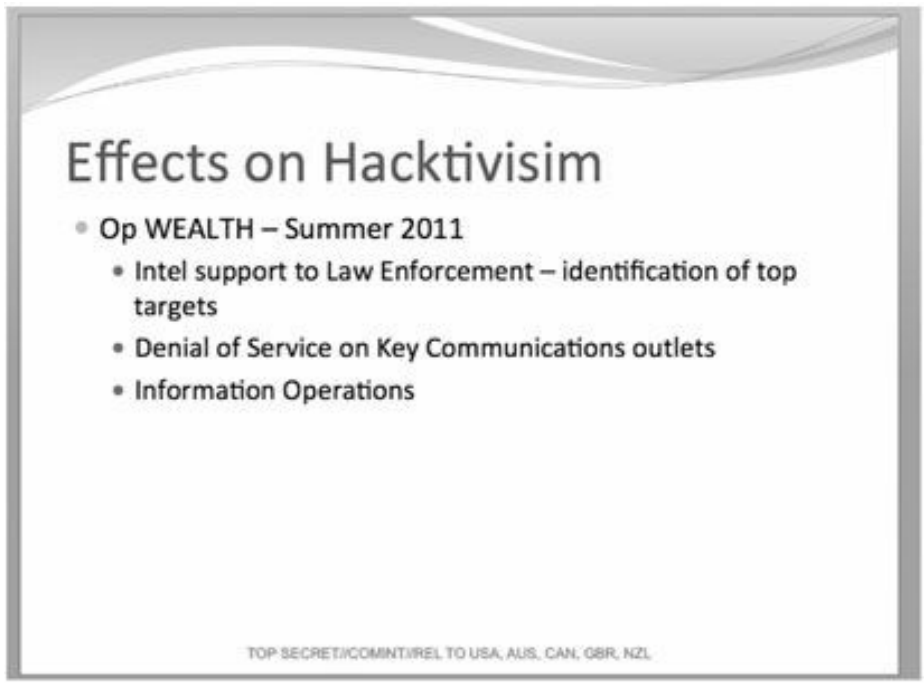
A GCHQ também gosta de usar técnicas de "perturbação" no lugar daquilo que chama de

"segurança pública tradicional", como coleta de indícios, tribunais e processos judiciais. Em um documento chamado "Sessão de ciberofensiva: como ampliar os limites e executar ações contra o hacktivismo", a GCHQ discute a escolha de "hacktivistas" como alvos usando, ironicamente, ataques de "serviço negado", tática em geral associada a hackers.



POR QUE CONDUZIR UMA OPERAÇÃO DE EFEITOS?

- Perturbação versus segurança pública tradicional / Alvos descobertos por SIGINT / Técnicas de perturbação podem poupar tempo e dinheiro



EFEITOS NO HACKTIVISMO

Operação WEALTH – Verão de 2011 / Suporte de inteligência à segurança pública – identificação de alvos principais / Negação de serviço em canais de comunicação-chave /

A agência de vigilância britânica também usa uma equipe de cientistas sociais, que conta com alguns psicólogos, para desenvolver técnicas de "HUMINT (*human intelligence*, ou inteligência humana) na internet" e "perturbação de influência estratégica". O documento "A arte do engodo: como treinar uma nova geração de operações sigilosas na internet" é dedicado a essas táticas. Preparado pelo setor da agência chamado HSOC (Célula de Operações em Ciências Humanas), alega utilizar conceitos de sociologia, psicologia, antropologia, neurociência e biologia, entre outros, para maximizar as habilidades de engodo da GCHQ na internet.

Um slide mostra como realizar a "Dissimulação – Ocultar o real" ao mesmo tempo que se propaga a "Simulação – Mostrar o falso", antes de examinar as "etapas psicológicas do engodo" e o "mapa de tecnologias" usado para praticá-lo, entre as quais estão Facebook, Twitter, LinkedIn e "páginas da internet".

Enfatizando que "as pessoas tomam decisões por motivos emocionais, não racionais", a GCHQ argumenta que o comportamento na internet é movido por "efeito demonstração" ("as pessoas copiam umas às outras durante as interações sociais"), "acomodação" e "mímica" ("adoção, pela pessoa que se comunica, de traços sociais específicos do interlocutor").

O documento apresenta, então, o que chama de "Manual Operacional de Perturbações". Estas incluem "operação de infiltração", "operação de estratagema", "operação de bandeira falsa" e "operação de picada", e o manual promete um "desenvolvimento completo" do programa de perturbação "no início de 2013", quando "mais de 150 funcionários [tiverem recebido] treinamento integral".

MANUAL OPERACIONAL DE PERTURBAÇÕES

Operação de infiltração / Operação de estratagema / Operação ensaiada / Operação de bandeira falsa / Operação de resgate falso / Operação de perturbação / Operação de picada

Com o título "Técnicas mágicas & experimento", o documento menciona a "Legitimação da violência", a "Construção da experiência na mente dos alvos, que deve ser aceita sem que eles percebam", e a "Otimização dos canais de engodo".

Esse tipo de plano do governo para monitorar e influenciar as comunicações na internet e para disseminar falsas informações na rede já vem dando margem a especulações há algum tempo. O professor de direito de Harvard Cass Sunstein, assessor próximo de Obama e ex-diretor do Escritório de Informação e Assuntos Regulatórios da Casa Branca que foi nomeado para o conselho da Casa Branca responsável por supervisionar as atividades da NSA, escreveu em 2008 um controverso artigo propondo que o governo dos Estados Unidos empregasse equipes de agentes disfarçados e defensores "pseudoindependentes" da "infiltração cognitiva" em grupos da internet, salas de bate-papo, redes sociais e sites, bem como em grupos de ativistas off-line.

Esses documentos da GCHQ mostram pela primeira vez que essas controversas técnicas para enganar e prejudicar reputações passaram do estágio das propostas para o da implementação.

Todos os indícios ressaltam a proposta implícita feita aos cidadãos: não contestem e não terão nada com que se preocupar. Se cuidarem da própria vida e apoiarem, ou pelo menos tolerarem, o que nós fazemos, ficarão bem. Em outras palavras, caso queiram ser considerados isentos de transgressões, devem evitar provocar as autoridades que exercem poderes de vigilância. Trata-se de um acordo que incentiva a passividade, a obediência e a conformidade. O comportamento mais seguro, a forma de garantir que vão "deixá-lo em paz" é ficar quieto e se mostrar dócil, e não ameaçador.

Para muitos, esse é um acordo atraente, que convence a maioria de que a vigilância é inofensiva ou mesmo benéfica. Eles pensam: nós somos sem graça demais para atrair a atenção do governo. Já escutei coisas do tipo "Duvido muito que a NSA esteja interessada em mim. Se eles quiserem escutar minha vida sem graça, podem ficar à vontade". Ou então: "A NSA não está interessada na sua avó falando sobre receitas ou no seu pai combinando a partida de golfe."

São pessoas que se convenceram de que jamais serão escolhidas como alvo – por não representarem ameaça e por serem dóceis – e que, portanto, negam a existência da vigilância, não ligam para ela ou se mostram explicitamente dispostas a suportá-la.

Durante uma entrevista comigo pouco depois de as matérias sobre a NSA começarem a ser publicadas, Lawrence O'Donnell, apresentador da MSNBC, zombou do conceito da NSA como "um grande e assustador monstro da vigilância". Ao resumir sua opinião, ele concluiu:

> Minha sensação até agora é que (...) Eu não estou com medo (...) o fato de o governo estar coletando [dados] em um nível tão gigantesco, tão maciço, significa que é ainda mais difícil que eles me encontrem (...) e eles não têm incentivo nenhum para chegar a mim. Portanto, eu, neste estágio, não me sinto de forma alguma ameaçado por isso.

Hendrik Hertzberg, da revista *New Yorker*, também externou opiniões igualmente despreocupadas sobre os perigos da vigilância. Após admitir que "há motivos para se sentir apreensivo em relação ao alcance exagerado das agências de inteligência, com o sigilo excessivo e com a falta de transparência", ele escreveu que "também há razões para manter a calma", e em especial que a ameaça representada "para as liberdades civis, do jeito que as coisas estão hoje, é abstrata, conjectural e inespecífica". E a colunista do *Washington Post* Ruth Marcus, minimizando a inquietação com os poderes da NSA, anunciou – de forma absurda – que "é quase certo que os meus metadados não foram examinados".

Em um sentido importante, O'Donnell, Hertzberg e Marcus têm razão. O governo dos Estados Unidos de fato não tem "incentivo nenhum" para escolher como alvo pessoas como eles, para as quais a ameaça de um Estado de vigilância pouco mais é do que "abstrata, conjectural, inespecífica". Isso é verdade porque jornalistas que dedicam a carreira a venerar a autoridade mais poderosa do país – o presidente, que é o comandante-geral da NSA – e a defender seu partido político raramente, para não dizer nunca, correm o risco de desagradar aqueles que ocupam o poder.

É claro que defensores zelosos e leais do presidente e de suas políticas, bons cidadãos que nada fazem para atrair a atenção negativa dos poderosos, não têm qualquer motivo para temer o Estado de vigilância. É assim em qualquer sociedade: é difícil que aqueles que não representam contestação alguma sejam alvo de medidas repressoras; logo, do seu ponto de vista eles podem se convencer de que a opressão na verdade não existe. Mas a verdadeira medida de quanto uma sociedade é livre não é a forma como ela trata seus defensores, mas como trata os dissidentes e outros grupos marginalizados. Mesmo nas piores tiranias do mundo, defensores zelosos estão imunes aos abusos do poder público. No Egito de Mubarak, quem saiu às ruas para exigir sua saída foi preso, torturado, abatido a tiros; quem o defendeu e ficou em casa quietinho, não. Nos Estados Unidos, quem se viu alvo da vigilância de Hoover foram os líderes da NAACP, os comunistas e os ativistas de direitos civis e antiguerra, não os cidadãos bem-comportados que se calaram diante da injustiça social.

Não deveria ser preciso defender os poderosos com lealdade para estar a salvo da vigilância estatal. Tampouco o preço da imunidade deveria ser evitar a dissidência antagônica ou provocadora. Não deveríamos querer uma sociedade na qual a mensagem transmitida é que você só será deixado em paz caso imite o comportamento complacente e os conselhos convencionais de um colunista famoso.

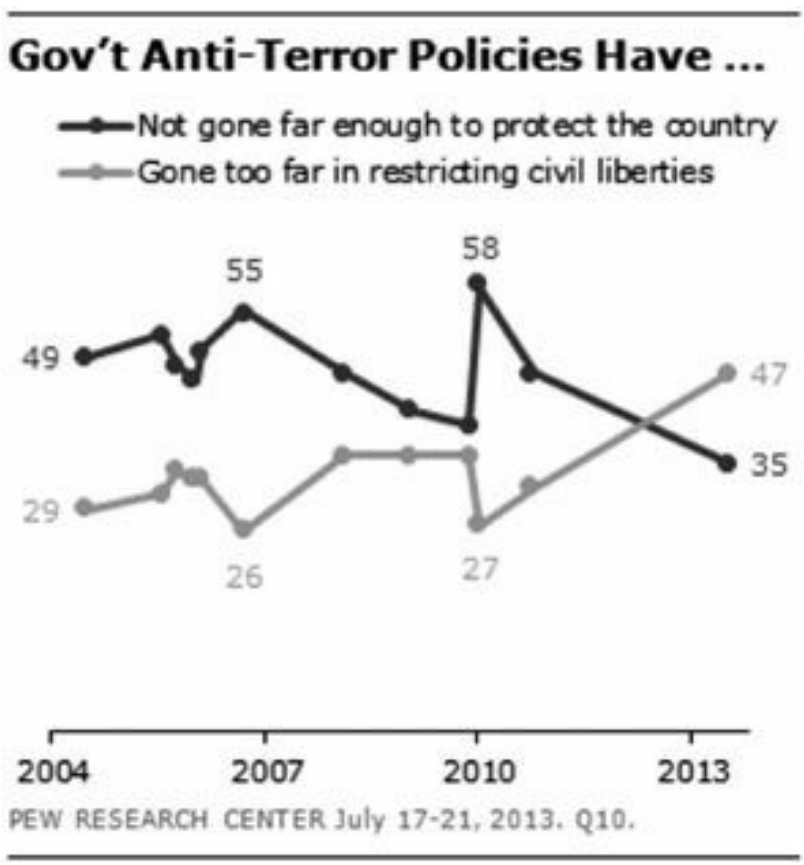
Além do mais, a sensação de imunidade experimentada por um grupo específico atualmente no poder está fadada a ser ilusória. Isso fica claro quando observamos como as afiliações partidárias moldam a apreensão dos perigos da vigilância estatal. A conclusão é que os entusiastas de ontem podem, muito rápido, se tornar os dissidentes de hoje.

Em 2005, época do escândalo sobre os grampos não autorizados da NSA, quase todos os liberais e democratas consideravam o programa de vigilância da agência ameaçador. Parte disso, é claro, era uma típica picuinha partidária: o presidente era George W. Bush, e os democratas viam naquilo uma oportunidade para infligir danos políticos a ele e seu partido. No entanto, parte significativa de seu medo era genuína: como eles consideravam Bush malicioso e perigoso, a percepção que tinham da vigilância estatal por ele conduzida era ameaçadora, e na condição de adversários políticos eles se consideravam particularmente ameaçados. Da mesma forma, os republicanos tinham uma visão mais inofensiva ou mais defensiva das ações da NSA. Em dezembro de 2013, por outro lado, democratas e progressistas tinham se tornado os principais defensores da agência.

Numerosos dados de pesquisas refletem essa mudança. No fim de julho de 2013, o Centro de Pesquisas Pew publicou um levantamento mostrando que a maioria dos americanos não acreditava nas defesas proporcionadas pelas ações da NSA. Em especial, "a maioria da população – 56% – diz que os tribunais federais não conseguem oferecer limites adequados aos dados de telefonia e internet que o governo coleta como parte de seus esforços antiterroristas". E "uma porcentagem ainda maior (70%) acha que o governo usa esses dados para outros fins que não investigar o terrorismo". Além disso, "63% pensam que o governo também está coletando informações sobre o conteúdo das comunicações".

O mais surpreendente é que os americanos agora consideram a ameaça da vigilância mais inquietante do que a do terrorismo:

> Ao todo, 47% afirmam que sua maior preocupação em relação às políticas antiterrorismo do governo é que elas foram longe demais na restrição das liberdades civis da pessoa comum, enquanto 35% afirmam estar mais preocupados com o fato de as políticas não terem feito o suficiente para proteger o país. Nas pesquisas conduzidas pelo Centro Pew, nunca antes, desde que a pergunta foi feita pela primeira vez, em 2004, o número de pessoas mais preocupadas com as liberdades civis foi maior que o das preocupadas com a proteção contra o terrorismo.



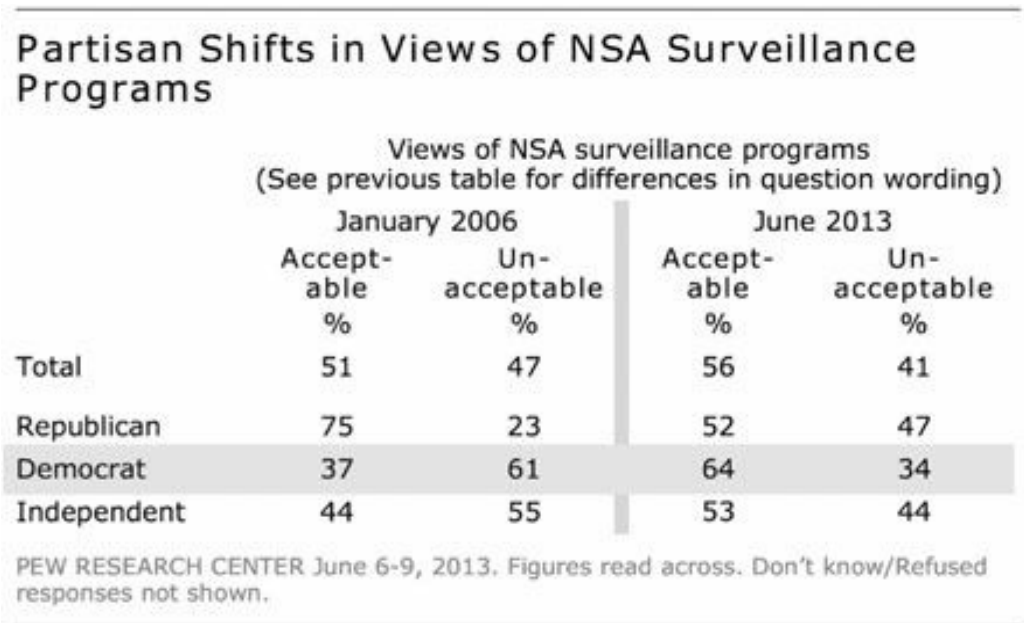
AS POLÍTICAS ANTITERROR DO GOVERNO...

Não foram longe o suficiente para proteger o país / Foram longe demais na restrição das liberdades civis / Centro de Pesquisas Pew, 17-21 de julho de 2013

Os dados dessa pesquisa foram uma boa notícia para qualquer um que estivesse alarmado com o uso excessivo de poder por parte do governo e com a exageração crônica da ameaça representada pelo terrorismo. Mas assinalavam também uma reveladora inversão: os republicanos, que no governo Bush defendiam a NSA, foram superados pelos democratas depois que o sistema de vigilância passou a ser controlado por Obama, um dos seus. "No país inteiro, há mais apoio ao programa de coleta de dados do governo entre os democratas (57% de aprovação) do que entre os republicanos (44%)."

Números semelhantes de uma pesquisa feita pelo *Washington Post* revelaram que os conservadores estavam muito mais preocupados com a espionagem da NSA do que os liberais. Quando questionados com a pergunta "Qual é o seu grau de preocupação, se houver, com a coleta e o uso de suas informações pessoais pela NSA?", 48% dos conservadores se disseram "muito preocupados", contra apenas 26% dos liberais. Conforme observou o professor de direito Orin Kerr, isso representa uma mudança fundamental: "É uma inversão interessante se comparada a 2006, quando o presidente era republicano, e não democrata. Na época, uma pesquisa do Pew revelou que 75% dos republicanos aprovavam a vigilância da NSA, contra apenas 37% dos democratas."

Um gráfico do centro de pesquisas deixa clara essa mudança:



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.

MUDANÇAS PARTIDÁRIAS NA OPINIÃO SOBRE OS PROGRAMAS DE VIGILÂNCIA DA NSA

Opiniões sobre os programas de vigilância da NSA
(ver tabela anterior para diferenças na formulação da pergunta)
Coluna da esquerda: Total / Republicanos / Democratas / Independentes
Coluna do meio: Janeiro de 2006 / Aceitável / Inaceitável
Coluna da direita: Junho de 2013 / Aceitável / Inaceitável
Abaixo: Centro de Pesquisas Pew, 6-9 de junho de 2013. Os números devem ser lidos na horizontal. Não sei / Não quero responder foram excluídos.

Os argumentos a favor e contra a vigilância apresentam uma rotatividade descarada dependendo de que partido esteja no poder. Em 2006, a coleta em massa de metadados pela NSA foi denunciada de forma veemente por um senador no programa *The Early Show*:

> Eu não preciso escutar seus telefonemas para saber o que você está fazendo. Se eu souber todos os telefonemas que você deu, posso determinar cada uma das pessoas com quem falou. Posso criar um padrão muito, muito intrusivo sobre a sua vida (...) E a verdadeira pergunta é: o que eles fazem com essa informação coletada que não tem nada a ver com a Al-Qaeda? Nós vamos confiar que o presidente e o vice-presidente dos Estados Unidos estão fazendo a coisa certa? Não me incluam nessa.

O senador que atacou de maneira tão dura a coleta de metadados era Joe Biden, que mais tarde, como vice-presidente, passou a integrar um governo democrata que usou exatamente os mesmos argumentos antes menosprezados por ele.

O ponto relevante aqui não é apenas o fato de muitos defensores partidários serem hipócritas sem princípios e sem qualquer outra convicção verdadeira que não a busca do poder, embora isso com certeza seja verdade. Mais importante é o que essas afirmações revelam sobre a natureza do que as pessoas pensam sobre a vigilância estatal. Como com tantas injustiças, elas se mostram dispostas a descartar o medo de um alcance excessivo do governo quando acreditam que aqueles que detêm o controle são benevolentes e confiáveis. Só consideram a vigilância perigosa ou digna de preocupação quando se sentem ameaçadas por ela.

Expansões radicais de poder são muitas vezes iniciadas assim, persuadindo-se as pessoas de que elas afetam apenas um grupo específico e isolado. Os governos há muito tempo convencem populações a não darem atenção a condutas opressivas, levando-as a acreditar, com ou sem razão, que apenas certos indivíduos marginalizados são escolhidos como alvo e que todos os outros podem permitir ou mesmo apoiar essa opressão sem medo de que ela se aplique a eles próprios. Sem falar nas evidentes falhas morais dessa posição – nós não ignoramos o racismo porque ele se dirige a uma minoria, nem desdenhamos a fome usando o pretexto de que dispomos de uma oferta generosa de alimentos –, ela é quase sempre mal direcionada com base em alegações pragmáticas.

A indiferença ou o apoio daqueles que se acreditam isentos invariavelmente permite que o mau uso do poder se alastre para muito além de sua aplicação original, até os abusos se tornarem impossíveis de controlar – como é inevitável que aconteça. Os exemplos são profusos demais para serem enumerados, mas talvez o mais recente e poderoso seja a exploração da Lei Patriota. Após o 11 de Setembro, o Congresso aprovou quase por unanimidade um aumento significativo da vigilância e dos poderes de detenção, convencido pelo argumento de que isso permitiria detectar e impedir futuros atentados.

A pressuposição implícita era que os poderes seriam usados sobretudo contra muçulmanos com ligações terroristas – uma expansão clássica de poder, confinada a um grupo restrito dedicado a um tipo de ato específico –, e esse foi um dos motivos que fizeram a medida ter um apoio avassalador. Mas o que aconteceu foi bem diferente: a Lei Patriota foi aplicada muito além de seus objetivos explícitos. Na realidade, desde sua implementação, ela foi usada principalmente em casos que nada tinham a ver com terrorismo ou segurança nacional. A *New York Magazine* revelou que, de 2006 a

2009, o "espiar e olhar" autorizado pela lei (permissão para cumprir um mandado de busca sem informar de imediato o alvo) foi usado em 1.618 casos relacionados a drogas, 122 casos ligados a estelionato e apenas 15 envolvendo terrorismo.

No entanto, uma vez que os cidadãos aceitem um novo poder acreditando que ele não os afeta, este se torna institucionalizado e legítimo, e a objeção passa a ser impossível. De fato, a principal lição aprendida por Frank Church em 1975 foi o tamanho do perigo representado pela vigilância em massa. Em entrevista concedida ao programa *Meet the Press*, ele afirmou:

> A qualquer momento, essa capacidade pode ser voltada contra a população, e a capacidade de monitorar tudo – conversas telefônicas, telegramas, qualquer coisa – é tamanha que nenhum americano teria mais privacidade alguma. Seria impossível se esconder. Se esse governo um dia virasse um tirano (...) a capacidade tecnológica proporcionada pela comunidade de inteligência poderia lhe permitir impor uma tirania total, e não haveria como lutar contra isso, pois mesmo o mais cuidadoso esforço para se unir e resistir (...) seria passível de conhecimento pelo governo. Tal é a capacidade dessa tecnologia.

Em 2005, James Bamford observou no *New York Times* que a ameaça da vigilância estatal é hoje bem mais forte do que nos anos 1970: "Como as pessoas expressam seus pensamentos mais íntimos em mensagens de e-mail, como expõem seus históricos médicos e financeiros na internet e conversam com frequência por celular, a agência é quase capaz de entrar na sua mente."

A preocupação de Church de que qualquer capacidade de vigilância "poderia se voltar contra a população americana" é justamente o que a NSA fez depois do 11 de Setembro. Apesar de a agência operar com base na Lei de Vigilância de Inteligência Estrangeira, e embora a proibição de espionagem doméstica esteja contida em sua missão desde o início, muitas de suas atividades de vigilância estão agora concentradas em cidadãos norte-americanos em território nacional.

Mesmo sem haver abusos, e ainda que alguém não seja um alvo específico, um Estado de vigilância que coleta tudo prejudica a sociedade e a liberdade política em geral. Tanto nos Estados Unidos quanto em outros países, o progresso só foi conquistado por meio da habilidade de contestar o poder e as ortodoxias e de inaugurar novas maneiras de pensar e viver. Todo mundo sofre quando essa liberdade é sufocada pelo medo de estar sendo observado, mesmo quem não pratica a defesa da dissidência ou o ativismo político. Hendrik Hertzberg, que minimizou as preocupações com os programas da NSA, admitiu, no entanto, que "o estrago já estava feito. É um estrago cívico. Um estrago coletivo. Um estrago na arquitetura da confiança e da prestação de contas que sustenta uma sociedade aberta e um sistema político democrático".

Os defensores da vigilância têm, em essência, um único argumento a favor da vigilância em massa: ela só é feita para deter o terrorismo e manter as pessoas seguras. Evocar uma ameaça externa é, de fato, uma das táticas preferidas para manter a população submissa aos poderes do governo. O governo dos Estados Unidos vem alardeando os perigos do terrorismo há mais de uma década para justificar uma infinidade de atos radicais, de detenções e tortura a assassinatos e à invasão do Iraque. Desde os atentados do 11 de Setembro, autoridades norte-americanas utilizam por reflexo a palavra

"terrorismo". Isso é muito mais um slogan, uma tática, do que um argumento verdadeiro ou uma justificativa convincente para agir. E, no caso da vigilância, uma enxurrada de indícios mostra quão dúbia essa justificativa é na verdade.

Para começar, é claro que grande parte da coleta de dados conduzida pela NSA nada tem a ver com terrorismo ou segurança nacional. Interceptar as comunicações da gigante Petrobras, espionar sessões de negociação em uma cúpula econômica, ter como alvo os líderes democraticamente eleitos de países aliados ou coletar todos os registros de comunicações dos americanos não tem qualquer relação com o terrorismo. No que diz respeito à atual vigilância praticada pela agência, está evidente que deter o terrorismo é um pretexto.

Além disso, ficou provado que o argumento de que a vigilância em massa impediu complôs terroristas – alegação feita por Obama e por uma série de autoridades de segurança nacional – é falso. Como observou o *Washington Post* em dezembro de 2013 em artigo intitulado "Defesa do programa telefônico da NSA por autoridades pode estar desmoronando", um juiz federal declarou o programa de coleta de metadados de telefonia "quase certamente" inconstitucional, dizendo também que o Departamento de Justiça foi incapaz de "citar um só caso em que a análise da coleta em massa de metadados pela NSA tenha de fato impedido um atentado terrorista iminente".

No mesmo mês, a comissão consultiva de Obama, formada por pessoas escolhidas a dedo (entre elas um ex-vice-diretor da CIA e um ex-assessor da Casa Branca) e reunida para estudar o programa da NSA por meio do acesso a informações confidenciais, concluiu que o programa de metadados "não era essencial à prevenção de ataques e poderia, com facilidade, ter sido obtido convenientemente utilizando-se um mandado [judicial] convencional".

O *Post* ainda dizia: "Em depoimentos no Congresso, [Keith] Alexander disse que o programa ajudou a detectar dezenas de complôs tanto dentro quanto fora dos Estados Unidos", mas o relatório da comissão consultiva "abalava de maneira profunda a credibilidade dessas afirmações".

E mais: como os senadores democratas Ron Wyden, Mark Udall e Martin Heinrich – todos membros do Comitê de Inteligência – afirmaram sem rodeios ao *New York Times*, a coleta em massa de registros telefônicos não melhorou a proteção dos americanos contra a ameaça do terrorismo.

> A utilidade do programa de coleta em massa foi muito exagerada. Ainda precisamos ver alguma prova de que ele tenha um valor real e singular na proteção da segurança nacional. Apesar de nossas repetidas solicitações, a NSA não apresentou indícios de qualquer caso em que tenha usado esse programa para examinar registros telefônicos que não poderiam ter sido obtidos com um mandado judicial normal ou uma autorização de emergência.

Um estudo conduzido pela fundação centrista New America para testar a veracidade das justificativas oficiais em relação à coleta de metadados também estabeleceu que o programa "não teve nenhum impacto discernível na prevenção de atos terroristas". Pelo contrário, conforme observado no *Washington Post*, na maioria dos casos em que complôs foram desmantelados o estudo apontou que "a segurança pública e métodos investigativos tradicionais forneceram os primeiros indícios que permitiram dar início ao caso".

De fato, o histórico é bem pobre. O sistema "coletar tudo" não fez nada para detectar, muito menos

desbaratar, o atentado a bomba de 2012 durante a Maratona de Boston. Tampouco detectou a tentativa de bombardeio de um avião que sobrevoava Detroit no Natal, ou o plano para bombardear a Times Square, ou ainda o complô para atacar a rede de metrô da cidade de Nova York – todos esses incidentes foram evitados graças a alertas de passantes ou à ação das forças de polícia tradicionais. O sistema com certeza não fez nada para deter a série de matanças a tiros nos Estados Unidos, de Aurora a Newtown. Atentados internacionais importantes, de Londres a Mumbai ou Madri, passaram despercebidos mesmo quando envolviam, no mínimo, dezenas de pessoas.

E, apesar das alegações oportunistas da NSA, a vigilância em massa não teria proporcionado aos serviços de inteligência ferramentas melhores para impedir os atentados de 11 de setembro de 2001. Em um pronunciamento diante do Comitê de Inteligência do Senado, Keith Alexander afirmou "preferir mil vezes estar aqui hoje discutindo" o programa "a tentar explicar como não conseguimos evitar um outro 11 de Setembro". (O mesmo argumento, *ipsis litteris*, constava em instruções distribuídas pela NSA a seus funcionários para que eles pudessem se esquivar de perguntas.)

A implicação disso é uma intimidação baseada na hierarquia, e é extremamente enganadora. Como o analista de segurança da CNN Peter Bergen mostrou, a CIA tinha vários relatórios sobre um complô da Al-Qaeda e "bastante informação sobre dois dos sequestradores e sua presença nos Estados Unidos", que "não compartilhou com outras agências do governo até já ser tarde demais para tomar qualquer providência".

Lawrence Wright, especialista em Al-Qaeda da *New Yorker*, também derrubou a sugestão da NSA de que a coleta de metadados poderia ter impedido o 11 de Setembro ao explicar que a CIA "reteve informações cruciais do FBI, que tem autoridade máxima para investigar terrorismo dentro dos Estados Unidos e ataques a americanos no exterior". Segundo ele, o FBI poderia ter impedido o 11 de Setembro.

> O FBI tinha mandados para vigiar todas as pessoas relacionadas à Al-Qaeda nos Estados Unidos. Podia segui-las, grampear seus telefones, clonar seus computadores, ler seus e-mails e solicitar por intimação seus históricos médicos, bancários e de cartão de crédito. Tinha o direito de exigir das empresas de telefonia os registros de qualquer chamada feita por elas. Um programa de coleta de metadados não era necessário. Necessária mesmo era a cooperação com outras agências federais, mas por motivos tanto mesquinhos quanto obscuros essas agências decidiram ocultar provas vitais dos investigadores mais propensos a impedir os ataques.

O governo tinha a inteligência necessária, mas não soube entendê-la nem tomar as devidas providências. A solução pela qual optou em vez disso – coletar tudo de forma indiscriminada – nada fez para sanar essa falha.

Inúmeras vezes, de várias direções diferentes, a evocação da ameaça terrorista para justificar a vigilância foi denunciada como fraude.

Na realidade, a vigilância em massa teve praticamente o efeito contrário: ela torna mais difícil detectar e deter atos terroristas. O deputado democrata Rush Holt, que é físico e um dos poucos cientistas do Congresso, argumentou que coletar tudo relacionado às comunicações de todo mundo só faz ocultar os verdadeiros complôs organizados por terroristas de verdade. Uma vigilância focada, e não indiscriminada, renderia informações mais específicas e mais úteis. A abordagem atual soterra

as agências de inteligência com tantos dados que é impossível analisá-los de forma eficaz.

Além de fornecer informação demais, os esquemas de vigilância da NSA acabam aumentando a vulnerabilidade do país: os esforços da agência para burlar os métodos de criptografia que protegem transações normais na internet – on-line banking, históricos médicos, comércio – deixaram esses sistemas expostos à infiltração por hackers e entidades hostis.

Em um artigo na *Atlantic* em janeiro de 2014, o especialista em segurança Bruce Schneier observou:

> Uma vigilância onipresente não só é ineficaz, mas também extraordinariamente dispendiosa. Ela prejudica nossos sistemas técnicos, uma vez que os próprios protocolos da internet deixam de ser confiáveis. Não é só com os abusos domésticos que devemos nos preocupar, mas com o resto do mundo também. Quanto mais decidirmos bisbilhotar a internet e outras tecnologias de comunicação, menos a salvo da bisbilhotice alheia estaremos. Nossa escolha não é entre um mundo digital onde a NSA pode bisbilhotar e outro onde a NSA é impedida de bisbilhotar, mas sim entre um mundo digital vulnerável a qualquer agressor e outro seguro para todos os usuários.

Talvez o fato mais notável em relação à exploração exaustiva da ameaça do terrorismo é que esta é obviamente superdimensionada. O risco de qualquer americano morrer em um atentado terrorista é infinitesimal, muito menor do que a chance de ser fulminado por um raio. Em 2011, John Mueller, professor da Universidade Estadual de Ohio que escreveu extensamente sobre o equilíbrio entre riscos e despesas na luta contra o terror, explicou: "O número de pessoas no mundo inteiro que são mortas fora das zonas de guerra por terroristas do tipo muçulmano, candidatos à Al-Qaeda, deve ser de poucas centenas. É basicamente o mesmo número de pessoas que morrem por ano afogadas na banheira."

Mais cidadãos americanos "sem dúvida" morreram "no exterior em acidentes de trânsito ou de doenças intestinais", noticiou a agência McClatchy, "do que devido ao terrorismo".

A ideia de que deveríamos desmantelar as proteções que constituem o âmago de nosso sistema político para erigir um Estado de vigilância generalizada em nome desse risco é o cúmulo da irracionalidade. No entanto, a ameaça continua a ser exagerada de modo incansável. Pouco antes dos Jogos Olímpicos de 2012, em Londres, surgiu uma controvérsia relacionada a uma suposta falta de segurança. A empresa contratada para cuidar da segurança não havia providenciado o número de guardas estipulado em contrato, e vozes esganiçadas mundo afora insistiram que os jogos estariam vulneráveis a um atentado terrorista.

Depois de uma Olimpíada sem incidentes, Stephen Walt observou na *Foreign Policy* que a indignação, como de hábito, fora causada por um profundo exagero em relação à ameaça. Em sua matéria, ele citou um ensaio de John Mueller e Mark G. Stewart, publicado no periódico *International Security*, no qual os autores analisaram cinquenta casos de supostos "complôs terroristas islâmicos" contra os Estados Unidos apenas para concluir que "praticamente todos os responsáveis eram 'incompetentes, ineficazes, pouco inteligentes, idiotas, ignorantes, desorganizados, equivocados, confusos, amadores, drogados, irrealistas, débeis mentais, irracionais e tolos'". Mueller e Stewart citavam Glenn Carle, ex-vice-representante de inteligência nacional para ameaças transnacionais, que afirmou: "Devemos ver os jihadistas como os oponentes pequenos, letais, desestruturados e dignos de

pena que são", observando que as "capacidades [da Al-Qaeda] são muito inferiores aos seus desejos".

O problema, porém, é que há um número excessivo de facções de poder com interesses velados no temor do terrorismo: o governo, que busca justificar os próprios atos; as empresas de vigilância e armamentos, afogadas em subsídios públicos; e os grupos de poder permanentes de Washington, que fazem questão de decidir as próprias prioridades sem nenhuma contestação real. Stephen Walt observou o seguinte:

> Mueller e Stewart estimam que os gastos com segurança doméstica (ou seja, sem contar as guerras no Iraque e no Afeganistão) cresceram mais de 1 trilhão de dólares desde o 11 de Setembro, embora o risco anual de morrer em um ataque terrorista doméstico seja próximo de um em 3,5 milhões. Usando estimativas conservadoras e metodologias convencionais de avaliação de riscos, os autores estimam que, para essas despesas valerem a pena, "elas teriam de interromper, impedir, frustrar ou proteger o país de 333 atentados de grande porte que, de outro modo, ocorreriam anualmente". Por fim, eles se mostram preocupados com o fato de essa noção de perigo exagerada ter sido "internalizada": mesmo quando os políticos e "especialistas em terrorismo" não estão exagerando o perigo, o público continua a considerar a ameaça grande e iminente.

Enquanto o temor relacionado ao terrorismo foi manipulado, os perigos comprovados de se permitir ao Estado operar um imenso aparato de segurança secreto foram seriamente minimizados.

Ainda que a ameaça do terrorismo existisse no nível alegado pelo governo, nem por isso os programas de vigilância da NSA estariam justificados. Há outros valores tão importantes quanto a segurança física, se não mais. Esse conceito faz parte da cultura política norte-americana desde a criação do país, e também é crucial para outras nações.

Com frequência, países e indivíduos fazem escolhas que põem os valores da privacidade e, de forma implícita, da liberdade, acima de outros objetivos como a segurança física. De fato, o próprio objetivo da Quarta Emenda à Constituição dos Estados Unidos é proibir determinadas ações policiais, mesmo que estas possam reduzir a criminalidade. Se a polícia pudesse invadir qualquer residência sem mandado, talvez fosse mais fácil prender assassinos, estupradores e sequestradores. Se o Estado pudesse instalar monitores em nossas casas, a taxa de criminalidade provavelmente sofreria uma queda significativa (sem dúvida no caso de assaltos a residências, mas a maioria das pessoas ficaria indignada com essa possibilidade). Se o FBI tivesse autorização para escutar nossas conversas e apreender nossas comunicações, talvez um amplo leque de crimes fosse evitado e solucionado.

No entanto, a Constituição foi redigida para impedir essas invasões do Estado sem suspeita plausível. Ao estabelecer esse limite, nós admitimos, de forma voluntária, a probabilidade de mais crimes. Mas ainda assim o estabelecemos, expondo-nos a um grau maior de perigo, porque a busca da segurança física absoluta nunca foi nossa única e mais importante prioridade do ponto vista social.

Acima até do bem-estar físico, um valor central mantém o Estado fora do nosso universo privado – nossas "pessoas, casas, documentos e bens", segundo os termos da Quarta Emenda. Fazemos isso justamente porque esse universo é o berço de muitos dos atributos associados à qualidade de vida: criatividade, exploração, intimidade.

Abrir mão da privacidade na busca da segurança absoluta é tão prejudicial à saúde da psique e da

vida dos indivíduos quanto à da cultura política. Para o indivíduo, pôr a segurança em primeiro lugar significa uma vida de paralisia e medo: nunca embarcar em um carro ou avião, nunca valorizar a qualidade de vida mais do que a quantidade e pagar qualquer preço para evitar o perigo.

Fomentar o medo é uma tática prezada pelas autoridades exatamente porque o medo racionaliza, de forma muito convincente, a expansão do poder e a limitação dos direitos. Desde o início da Guerra ao Terror, a população norte-americana ouviu muitas vezes que deveria abrir mão de seus direitos políticos básicos se quisesse ter qualquer esperança de evitar uma catástrofe. Pat Roberts, presidente do Comitê de Inteligência do Senado, afirmou, por exemplo: "Sou um forte defensor da Primeira Emenda, da Quarta Emenda e das liberdades civis. Mas ninguém tem liberdades civis se estiver morto." E o senador republicano John Cornyn, que se candidatou à reeleição no Texas com um vídeo no qual aparecia como um valentão de chapéu de caubói, fez uma defesa covarde dos benefícios de abrir mão dos próprios direitos: "Nenhuma das suas liberdades civis tem muita importância depois que você morre."

O apresentador de *talk show* Rush Limbaugh também contribuiu, demonstrando ignorância histórica ao perguntar a seu numeroso público: "Qual foi a última vez que vocês ouviram um presidente declarar guerra sob o pretexto de que precisamos proteger nossas liberdades civis? Não consigo me lembrar de nenhum (...) As nossas liberdades civis não valem nada se estivermos mortos! Se você estiver morto e enterrado, se estiver coberto de terra dentro de um caixão, sabe quanto valem as suas liberdades civis? Zero, nadica de nada."

Uma população, um país que dê mais importância à segurança física do que a qualquer outro valor acabará abrindo mão da liberdade e sancionando qualquer poder assumido pelas autoridades em troca da promessa de segurança total, por mais ilusória que seja. No entanto, a segurança absoluta não passa de uma quimera, perseguida mas jamais obtida. Essa busca degrada tanto aqueles que a conduzem quanto qualquer país que se deixe definir por ela.

O perigo representado pelo fato de o Estado operar um imenso aparato de vigilância secreta é bem mais ameaçador agora do que em qualquer outro período da história. Enquanto o governo, graças à vigilância, sabe cada vez mais o que seus cidadãos estão fazendo, os cidadãos sabem cada vez menos o que o governo está fazendo, uma vez que este é protegido por um muro de sigilo.

É difícil exagerar quão radicalmente essa situação reverte a dinâmica que define uma sociedade saudável, ou quão fundamentalmente ela modifica o equilíbrio de poder a favor do Estado. O Panopticon de Bentham, imaginado para depositar um poder inquestionável nas mãos das autoridades, baseava-se nessa reversão: "Sua essência", escreveu o filósofo, repousa "na centralidade da situação do inspetor" combinada com "as mais eficazes ferramentas para ver sem ser visto".

Em uma democracia saudável acontece o contrário. Democracia exige prestação de contas e consentimento dos governados, o que só é possível quando os cidadãos sabem o que está sendo feito em seu nome. A pressuposição, com raras exceções, é de que eles saberão tudo o que suas autoridades políticas estiverem fazendo; é por isso que essas autoridades são chamadas de funcionários públicos e trabalham no setor público, no serviço público e em órgãos públicos. De forma inversa, também com raras exceções, a pressuposição é que o governo não saberá nada que os cidadãos respeitadores da lei estiverem fazendo. É por isso que somos chamados de indivíduos privados, que operam na esfera privada. A transparência é para quem cumpre funções públicas e exerce um poder público. A privacidade é para todos os demais.

5

O QUARTO PODER

Uma das principais instituições ostensivamente dedicadas a monitorar e supervisionar o poder do Estado é a imprensa especializada em política. A teoria de um "quarto poder" visa garantir a transparência do governo e proporcionar um mecanismo para conter abusos, dos quais a vigilância secreta de populações inteiras sem dúvida é um dos exemplos mais radicais. No entanto, essa contenção só funciona se os jornalistas agirem contra aqueles que detêm o poder político. Nos Estados Unidos, contudo, a mídia com frequência abdicou desse papel, mostrando-se subserviente aos interesses do governo e até mesmo amplificando suas mensagens em vez de examiná-las, além de fazer o seu trabalho sujo.

Nesse contexto, eu sabia que a hostilidade da imprensa em relação às minhas reportagens sobre as revelações de Snowden era inevitável. Em 6 de junho, dia seguinte à publicação da primeira matéria sobre a NSA no *Guardian*, o *New York Times* levantou a possibilidade de um inquérito criminal. "Depois de anos escrevendo de forma intensa, obsessiva, até, sobre a vigilância do governo e processos contra jornalistas, Glenn Greenwald de repente se posicionou bem na interseção entre essas duas questões, e quem sabe na mira de promotores federais", afirmou o jornal em um perfil sobre mim. Minhas reportagens sobre a NSA, acrescentava o texto, "devem atrair a atenção do Departamento de Justiça, que vem perseguindo delatores de forma agressiva". O perfil citava o neoconservador Gabriel Schoenfeld, do Hudson Institute, que há muito tempo defende o indiciamento de jornalistas por publicarem informações secretas, chamando-me de "apologista altamente profissional de qualquer tipo de antiamericanismo, seja quão extremo for".

O indício mais revelador das intenções do *Times* partiu do jornalista Andrew Sullivan, citado no mesmo perfil: "Quando se começa um debate [com Greenwald], pode ser difícil ter a última palavra", e "acho que ele compreende muito mal o que de fato significa governar um país ou conduzir uma guerra". Incomodado pelo uso de seus comentários fora de contexto, Andrew depois me mandou a entrevista completa que havia concedido à jornalista do *Times* Leslie Kaufman, na qual fazia elogios ao meu trabalho que o jornal deliberadamente decidiu omitir. Mais reveladoras ainda, porém, foram as perguntas originais que Kaufman tinha lhe enviado:

- "Está claro que ele tinha opiniões fortes, mas que tipo de jornalista ele é? Confiável? Honesto? Cita os outros de forma fiel? Descreve de forma fiel as suas posições? Ou é mais defensor do que jornalista?"
- "Ele afirma que o senhor é amigo dele, é verdade? Tenho a sensação de que ele é meio solitário e de que tem o tipo de opinião radical que torna difícil manter amizades, mas posso estar enganada."

De certa forma, a segunda pergunta – que diz que sou um cara "meio solitário", que tem

dificuldade em manter amizades – é ainda mais significativa do que a primeira. Denegrir o mensageiro e taxá-lo de desajustado para prejudicar a credibilidade da mensagem é uma tática antiga quando se trata de delações, e muitas vezes funciona.

A energia dedicada a me denegrir pessoalmente ficou bem clara quando recebi o e-mail de um jornalista do *New York Daily News*. Ele disse estar investigando diversos aspectos do meu passado, entre eles minhas dívidas, pendências com o fisco e o fato de, oito anos antes, eu ter tido ações de uma empresa privada que era sócia de outra companhia de distribuição de vídeos pornôs. Como o *Daily News* é um jornaleco especializado em explorar os podres das pessoas, decidi que não havia por que chamar mais atenção ainda para as questões levantadas dando qualquer tipo de resposta.

Nesse mesmo dia, porém, recebi um e-mail de um repórter do *Times*, Michael Schmidt, também interessado em escrever sobre minhas antigas dívidas fiscais. Como os dois periódicos tinham ficado sabendo ao mesmo tempo de um detalhe tão obscuro era um mistério, mas estava claro que o *Times* julgava minhas dívidas antigas dignas de notícia – embora se recusasse a fornecer qualquer explicação para justificar tal fato.

Essas questões eram obviamente sem importância e destinadas a manchar minha reputação. O *Times* acabou não dando a matéria, ao contrário do *Daily News*, que chegou a incluir detalhes de uma disputa que eu tivera no meu prédio, dez anos antes, devido a alegações de que o meu cachorro ultrapassava o limite de peso permitido pela convenção do condomínio.

Embora a campanha para me denegrir fosse previsível, o esforço para negar meu status de jornalista, não, e suas potenciais ramificações eram drásticas. Dessa vez, a campanha também foi iniciada pelo *New York Times*, no mesmo perfil publicado em 6 de junho. No título, o jornal fez questão de se referir a mim usando um substantivo não jornalístico: "Blogueiro especializado em vigilância no centro de controvérsia". Por pior que fosse esse título, o original que saiu na internet era ainda pior: "Ativista antivigilância no centro de novo vazamento".

Margaret Sullivan, ombudsman do periódico, criticou o título, afirmando considerá-lo "menosprezador". Segundo ela: "Não há nada de errado em ser blogueiro, é claro – eu mesma sou. Mas, quando a mídia corporativa usa essa palavra, de alguma forma parece estar dizendo: 'Você não é exatamente um de nós.'"

Na matéria, fui qualificado diversas vezes como algo diferente de um "jornalista" ou "repórter". Segundo o jornal, eu era "advogado e blogueiro de longa data" (não exerço a advocacia há seis anos, e quando as matérias começaram a sair já trabalhava havia muito tempo como colunista em veículos importantes, além de ter publicado quatro livros). Nas ocasiões em que eu atuara como "jornalista", afirmava o texto, minha experiência era "pouco usual", não devido às minhas "opiniões claras", mas porque eu "quase nunca [tinha me] reportado a um editor".

A imprensa toda, então, iniciou um debate sobre se eu era mesmo um "jornalista" ou alguma outra coisa. A alternativa sugerida com maior frequência era "ativista". Ninguém se deu ao trabalho de definir nenhuma dessas palavras e todos se contentaram em confiar em clichês vagos, como a mídia tende a fazer, sobretudo quando o objetivo é demonizar. A partir daí, esse rótulo vago e desprovido de significado passou a ser usado de forma rotineira.

A palavra usada para me qualificar era importante em vários níveis. Em primeiro lugar, a remoção da etiqueta "jornalista" reduz a legitimidade da notícia. Além disso, transformar-me em "ativista" poderia ter consequências jurídicas, ou seja, criminais. Os jornalistas dispõem de proteções

legais, tanto formais quanto informais, que não se aplicam a mais ninguém. Enquanto em geral se considera legítimo que um jornalista publique segredos do governo, por exemplo, isso não vale para alguém agindo em qualquer outra condição.

Intencionalmente ou não, as pessoas que promoviam a ideia de que eu não era um jornalista – apesar de eu escrever para um dos mais antigos e maiores jornais do mundo ocidental – estavam facilitando a condenação de minhas reportagens como criminosas pelo governo. Depois que o *New York Times* me taxou de "ativista", a ombudsman Sullivan admitiu que "essas questões adquiriram um significado maior no clima atual, e podem vir a se revelar cruciais para o Sr. Greenwald".

A expressão "clima atual" era uma referência sucinta a duas grandes controvérsias ocorridas em Washington com relação ao tratamento de jornalistas pelo governo. A primeira foi a aquisição secreta, pelo Departamento de Justiça, de e-mails e registros telefônicos de repórteres e editores da Associated Press para identificar sua fonte em uma reportagem.

O segundo incidente, mais extremo, envolvia o esforço do Departamento de Justiça para descobrir a identidade de outra fonte que tinha vazado informações secretas. Para isso, o departamento apresentou uma declaração juramentada em um tribunal federal solicitando um mandado para ler os e-mails do chefe de redação da Fox News em Washington, James Rosen.

Na solicitação, advogados do governo taxaram Rosen de "cúmplice de conspiração" nos delitos cometidos pela fonte, uma vez que ele obtivera material confidencial. A declaração foi um choque porque, como disse o *New York Times*, "nenhum jornalista americano jamais foi processado por reunir e publicar informações confidenciais, de modo que os termos usados apontavam para a possibilidade de o governo Obama estar alçando a um novo patamar sua operação para pôr fim aos vazamentos".

Todos os comportamentos citados pelo Departamento de Justiça para justificar a acusação de "cúmplice de conspiração" feita a Rosen – ter trabalhado junto com a fonte para obter documentos, estabelecido um "plano de comunicação sigilosa" para que suas conversas não fossem interceptadas e "usado a bajulação e a manipulação da vaidade e do ego [da fonte]" para convencê-la a vazar as informações – eram rotina para jornalistas investigativos.

Como afirmou o veterano jornalista de Washington Olivier Knox, o Departamento de Justiça tinha "acusado Rosen de violar a lei antiespionagem com um comportamento que – conforme descrito na própria declaração apresentada ao tribunal – se atém aos limites do jornalismo tradicional". Considerar a conduta dele um delito equivalia a criminalizar o jornalismo em si.

Essa manobra talvez tenha sido menos surpreendente do que poderia ser não fosse o contexto mais amplo dos ataques da administração Obama a delatores e fontes. Em 2011, o *New York Times* revelou que o Departamento de Justiça, na tentativa de localizar a fonte de um livro escrito por James Risen, obteve "extensos registros de seus telefonemas, histórico financeiro e viagens", incluindo "suas 'informações bancárias e de cartão de crédito e determinados registros de viagens aéreas feitas por ele', além de três relatórios de crédito detalhando sua situação financeira".

O Departamento de Justiça também estava tentando forçar Risen a revelar a identidade de sua fonte, com uma provável perspectiva de prisão caso ele se recusasse a fazê-lo. Jornalistas país afora ficaram apavorados com a forma como Risen foi tratado: se um dos mais renomados e institucionalmente protegidos repórteres investigativos americanos podia ser submetido a um ataque tão agressivo, qualquer jornalista corria esse risco.

Muitos na imprensa reagiram alarmados. Um artigo típico, publicado no *USA Today*, observou que "o presidente Obama enfrenta acusações de que o seu governo de fato declarou guerra aos jornalistas" e citou o ex-repórter de segurança nacional do *Los Angeles Times*, Josh Meyer: "Existe um limite que nenhum outro governo havia cruzado, e que o governo Obama simplesmente ignorou." Jane Mayer, admirada repórter investigativa da *New Yorker*, alertou na revista *New Republic* que o ataque a delatores conduzido pelo Departamento de Justiça de Obama estava funcionando como um ataque ao jornalismo em si: "É um impedimento enorme ao trabalho jornalístico, portanto não se deve falar em esfriamento; é mais forte do que isso, é mais um congelamento e uma imobilização total do processo."

A situação levou o Comitê de Proteção aos Jornalistas – organização internacional que monitora ataques do Estado à liberdade de imprensa – a publicar o primeiro relatório de sua história sobre os Estados Unidos. Escrito por Leonard Downie Jr., ex-editor executivo do *Washington Post*, o documento, publicado em outubro de 2013, concluiu:

> A guerra contra os vazamentos e outros esforços para controlar informações por parte do governo são os mais agressivos (...) desde o governo Nixon (...). Os trinta experientes jornalistas entrevistados para este relatório, que trabalham em Washington para diversos veículos (...), foram incapazes de recordar qualquer precedente.

A dinâmica ultrapassava o âmbito da segurança nacional até incluir, segundo um chefe de redação, um esforço para "prejudicar notícias sobre a prestação de contas de *agências* governamentais".

Os jornalistas norte-americanos, que haviam passado anos completamente apaixonados por Barack Obama, agora com frequência se referiam a ele nos seguintes termos: uma espécie de grave ameaça à liberdade de imprensa, e sob esse aspecto o líder mais repressor desde Richard Nixon. Uma virada e tanto para um político que subiu ao poder prometendo "o governo mais transparente da história dos Estados Unidos".

Para abafar o escândalo crescente, Obama ordenou ao procurador-geral Eric Holder que se reunisse com representantes da mídia para reavaliar o regulamento relativo ao tratamento de jornalistas pelo Departamento de Justiça. O presidente se disse "perturbado com a possibilidade de que investigações sobre vazamentos possam arrefecer o jornalismo investigativo que garante a prestação de contas do governo" – como se não houvesse comandado justamente esse tipo de ataque ao processo de apuração jornalística nos últimos cinco anos.

Em uma audiência no Senado em 6 de junho de 2013 (dia seguinte à publicação da primeira matéria sobre a NSA pelo *Guardian*), Holder prometeu que o Departamento de Justiça jamais processaria "nenhum repórter por fazer o seu trabalho". Seu objetivo, acrescentou, era apenas "identificar e processar os funcionários do governo que põem em risco a segurança nacional ao violarem seus juramentos, e não atacar membros da imprensa ou desencorajá-los a realizar seu trabalho vital".

De certa forma, era um desdobramento bem-vindo: estava claro que a administração sentira uma pressão suficiente para gerar pelo menos um arremedo de preocupação com a liberdade de imprensa. No entanto, a promessa de Holden tinha um rombo imenso: no caso de Rosen, da Fox News, o

Departamento de Justiça havia determinado que trabalhar junto a uma fonte para "roubar" informações confidenciais ultrapassava o escopo do "trabalho do repórter". Assim, a garantia de Holder dependia da visão do Departamento de Justiça do que constitui jornalismo e do que ultrapassa as fronteiras legítimas da atividade.

Nesse contexto, o esforço de alguns personagens da mídia para me alijar do "jornalismo" – para insistir que o que eu estava fazendo era "ativismo", não apuração e divulgação de notícias, e portanto um crime – era um perigo em potencial.

O primeiro sinal explícito de que eu seria processado veio do deputado republicano por Nova York Peter King, que fora presidente do Subcomitê contra o Terrorismo da Câmara de Representantes e convocara audiências dignas do macarthismo sobre o terror "interno" representado pela comunidade muçulmana dos Estados Unidos (por ironia, King era um antigo defensor do IRA). O deputado confirmou para Anderson Cooper, da CNN, que os jornalistas que estivessem trabalhando nas matérias sobre a NSA deveriam ser processados "caso estivessem cientes de que a informação era confidencial (...) sobretudo tratando-se de algo dessa magnitude". Ele ainda acrescentou: "Existe uma obrigação moral, mas também jurídica, acredito eu, que proíbe um jornalista de revelar algo que comprometa de forma tão grave a segurança nacional."

Mais tarde, na Fox News, King esclareceu estar se referindo especificamente a mim:

> Estou falando de Greenwald (...) Ele não apenas revelou essas informações como afirmou ter nomes de agentes e colaboradores da CIA no mundo todo, e ele está ameaçando revelar isso. A última vez que algo assim foi feito neste país, o chefe da CIA na Grécia foi assassinado (...) Eu acho que [os processos contra jornalistas] devem ter alvos muito específicos, ser muito seletivos e, com certeza, uma exceção muito rara. Mas nesse caso, quando alguém revela segredos como esses e ameaça revelar mais ainda, sim, é preciso (...) é preciso que haja ações legais contra essa pessoa.

Dizer que eu havia ameaçado revelar nomes de agentes e colaboradores da CIA era uma mentira deslavada, inventada por King. Mesmo assim, as declarações dele abriram as comportas, e os comentaristas continuaram o ataque. Marc iessen, do *Washington Post*, ex-redator de discursos para Bush e autor de um livro que justifica o programa de torturas dos Estados Unidos, defendeu King em um artigo intitulado "Sim, publicar segredos da NSA é crime". Acusando-me de "infringir o título 18 do Código Legal dos Estados Unidos, §798, que torna ilegal a publicação de informações confidenciais que revelem criptografia ou inteligência de comunicações do governo", ele acrescentou: "Greenwald claramente violou essa lei (assim como o *Post*, aliás, ao publicar detalhes confidenciais sobre o programa PRISM)."

Alan Dershowitz foi à CNN e declarou: "Na minha opinião, é óbvio que Greenwald cometeu uma infração." Conhecido defensor das liberdades civis e da imprensa, Dershowitz mesmo assim afirmou que meu trabalho de jornalismo "não está no limite da criminalidade, mas bem no centro dela".

O coro cada vez mais numeroso foi engrossado pelo general Michael Hayden, que chefiou a NSA e depois a CIA no governo Bush e implementou o programa de escuta ilegal sem mandado da agência. "É provável que Edward Snowden", escreveu ele no site CNN.com, "se revele o delator de segredos norte-americanos mais custoso na história da República", e acrescentou que "Glenn Greenwald merece muito mais a caracterização de cúmplice de conspiração do Departamento de Justiça do que James

Rosen, da Fox, já mereceu".

A princípio limitado, em grande parte, a figuras de direita, de quem se poderia esperar a visão do jornalismo como um crime, o coro de vozes clamando para que eu fosse processado aumentou durante minha participação – agora infame – no programa semanal *Meet the Press*, do canal NBC.

A própria Casa Branca já elogiou o *Meet the Press* como um veículo cômodo para políticos de Washington e outros membros da elite transmitirem sua mensagem sem muita resistência. O programa foi descrito por Catherine Martin, ex-diretora de comunicação do vice-presidente Dick Cheney, como "nosso melhor formato", pois nele Cheney podia "controlar a mensagem". Pôr o vice-presidente no *Meet the Press*, segundo ela, era "uma tática que usamos com frequência". De fato, um vídeo do apresentador David Gregory no palco durante o Jantar de Correspondentes na Casa Branca, dançando desengonçado mas com grande animação, atrás de Karl Rove enquanto este cantava rap, tornou-se um viral na internet por simbolizar de maneira muito vívida o que o programa realmente é: um veículo que os detentores de poder político frequentam para ganhar repercussão e ser bajulados, no qual só se ouvem as declarações mais convencionais e rígidas, no qual só é permitido o mais restrito escopo de opiniões.

Fui convidado a participar do programa na última hora, e apenas por necessidade. Horas antes, estourara a notícia de que Snowden deixara Hong Kong e estava agora em um avião com destino a Moscou, reviravolta espetacular que inevitavelmente iria dominar o noticiário dali em diante. O *Meet the Press* não teve escolha senão transformar essa notícia no seu lide, e eu, por ser uma das poucas pessoas a ter tido contato com Snowden, fui chamado para ser o convidado principal do programa.

Já tinha feito ásperas críticas a Gregory ao longo dos anos, e previa uma entrevista belicosa. Só que não esperava a seguinte pergunta do apresentador: "Na medida em que o senhor auxiliou e facilitou as ações de Snowden, inclusive em seus desdobramentos atuais, por que não deveria ser acusado de um crime, Sr. Greenwald?" Eram tantas coisas erradas na pergunta que levei um minuto inteiro para processar o fato de que ele realmente a tinha feito.

O problema mais gritante era a quantidade de suposições sem fundamento embutidas na pergunta. A afirmação "na medida em que" eu havia auxiliado e facilitado "as ações de Snowden, inclusive em seus desdobramentos atuais" equivalia a dizer: "Na medida em que o Sr. Gregory assassinou seus vizinhos"... Aquilo era apenas um exemplo óbvio da formulação "Quando foi que o senhor parou de espancar sua esposa?".

Por trás da falácia de retórica, porém, um jornalista televisivo acabara de avalizar o conceito de que outros jornalistas podiam e deveriam ser processados por praticarem o jornalismo, uma afirmação extraordinária. A pergunta de Gregory insinuava que todos os repórteres investigativos nos Estados Unidos que trabalham com fontes e recebem informações confidenciais são criminosos. Era justamente essa teoria e esse ambiente que haviam tornado o jornalismo investigativo tão precário.

De forma previsível, Gregory me retratou repetidas vezes como algo que não um "jornalista". Introduziu uma das perguntas dizendo: "O senhor gosta de polêmicas, tem opinião, é colunista." E anunciou: "A questão sobre quem é jornalista talvez esteja aberta a discussão com relação ao que o senhor está fazendo."

Mas Gregory não foi o único a usar esses argumentos. Nenhum integrante do grupo reunido pelo *Meet the Press* para comentar minha conversa com o apresentador fez qualquer ressalva à ideia de

que um jornalista pudesse ser processado por trabalhar com uma fonte. Chuck Todd, da NBC, reforçou a teoria levantando, de forma ameaçadora, "questões" sobre o que chamava de meu "papel" no "complô":

> Glenn Greenwald (...) até que ponto ele estava envolvido no complô? (…) Será que teve algum outro papel que não o de simples receptor dessas informações? E será que ele vai ter de responder a essas perguntas? Porque existe um conceito legal em jogo (...) existe, existe sim.

Um programa da CNN chamado *Reliable Sources* (Fontes Confiáveis) debateu a questão enquanto mantinha um gráfico o tempo todo na tela com os dizeres: "Glenn Greenwald deve ser processado?"

Walter Pincus, do *Washington Post* – que espionou estudantes norte-americanos no exterior para a CIA nos anos 1960 –, assinou uma coluna com fortes sugestões de que Laura, eu e Snowden estávamos agindo como parte de uma trama secreta comandada pelo fundador do WikiLeaks, Julian Assange. A coluna continha tantos erros factuais (documentados por mim em uma carta aberta a Pincus) que o *Post* foi forçado a anexar uma correção de três parágrafos e duzentas palavras, bem maior do que o normal, reconhecendo vários deles.

Em seu programa na CNBC, Andrew Ross Sorkin, colunista financeiro do *New York Times*, afirmou:

> Sinto que, um, nós pisamos na bola pelo simples fato de permitir que [Snowden] fosse para a Rússia. E, dois, está claro que os chineses nos odeiam só por tê-lo deixado sair do país (...). Eu o prenderia, e a esta altura quase prenderia também Glenn Greenwald, o jornalista que parece estar querendo ajudá-lo a chegar ao Equador.

Que um jornalista do *Times* – periódico que chegara a recorrer à Suprema Corte para poder publicar os documentos do Pentágono – defendesse a minha prisão era um forte sinal da devoção que muitos repórteres corporativos nutrem pelo governo dos Estados Unidos; afinal de contas, criminalizar o jornalismo investigativo teria um grave impacto no jornal e em seus funcionários. Sorkin me pediu desculpas depois, mas seus comentários demonstraram a velocidade e a facilidade com que essas afirmações ganham força.

Felizmente, essa opinião está longe de ser unânime entre os membros da imprensa norte-americana. Na verdade, a ameaça de criminalização levou diversos jornalistas a se unirem para defender o meu trabalho, e em muitos grandes programas televisivos os apresentadores estavam mais interessados no teor das minhas revelações do que em demonizar os envolvidos. Nas semanas que se seguiram à minha participação no *Meet the Press*, inúmeros deles manifestaram sua condenação à pergunta feita por Gregory. O *Huffington Post* publicou: "Ainda não conseguimos acreditar direito no que David Gregory acabou de perguntar a Glenn Greenwald." Toby Harnden, chefe do escritório do *Sunday Times* britânico em Washington, tuitou: "Eu já fui preso no Zimbábue de Mugabe por 'praticar jornalismo'. David Gregory está dizendo que os Estados Unidos de Obama devem fazer o mesmo?" Vários repórteres e colunistas do *New York Times*, do *Post* e de outros veículos me defenderam em público e em particular. Mas nem todo o apoio podia neutralizar o fato

de que os próprios repórteres haviam defendido a possibilidade de perigo jurídico.

Advogados e outras pessoas que consultei concordaram que, se eu voltasse para os Estados Unidos, havia um risco real de ser preso. Tentei encontrar uma única pessoa em cuja opinião confiasse para me dizer que essa probabilidade não existia, que era inconcebível o Departamento de Justiça me processar. Ninguém disse isso. A opinião generalizada era que o Departamento de Justiça não me atacaria explicitamente por causa do meu trabalho jornalístico, pois iria querer evitar a aparência de estar perseguindo jornalistas. A preocupação, no caso, era de que o governo fabricasse uma teoria dizendo que os supostos crimes cometidos por mim estavam fora do âmbito do jornalismo. Ao contrário de Barton Gellman, do *Washington Post*, eu fora a Honk Kong encontrar Snowden antes de publicar as matérias; falara com ele várias vezes depois que ele chegara à Rússia, e publicara matérias sobre a NSA como freelancer em jornais do mundo todo. O Departamento de Justiça poderia tentar alegar que eu havia "auxiliado e facilitado" o vazamento dos documentos por Snowden, ou ajudado um "fugitivo" a escapar da justiça, ou então que o meu trabalho com jornais estrangeiros configurava algum tipo de espionagem.

Além disso, meus comentários sobre a NSA e o governo dos Estados Unidos tinham sido deliberadamente agressivos e insolentes. O governo sem dúvida devia estar desesperado para punir alguém pelo que já fora chamado de o vazamento mais prejudicial da história do país, se não para aliviar a raiva institucional, pelo menos para desencorajar futuros atos semelhantes. Como a cabeça que mais se queria ver na ponta de uma estaca agora se encontrava na segurança de um asilo político em Moscou, Laura e eu éramos uma segunda opção desejável.

Durante meses, vários advogados com contatos de alto nível no Departamento de Justiça tentaram obter garantias informais de que eu não seria processado. Em outubro, cinco meses após a publicação da primeira matéria, o deputado Alan Grayson escreveu para o procurador-geral Holder observando que políticos proeminentes haviam pedido a minha prisão e que eu tivera de recusar um convite para depor no Congresso sobre a NSA devido ao risco de um possível processo. Concluiu a carta dizendo:

> Considero isso uma lástima, porque (1) a prática do jornalismo não é crime; (2) pelo contrário, é protegida explicitamente pela Primeira Emenda constitucional; (3) as reportagens do Sr. Greenwald sobre esses assuntos na realidade informaram a mim, a outros integrantes do Congresso e ao público em geral sobre violações sérias e abrangentes da lei e dos direitos constitucionais cometidas por agentes do governo.

A carta indagava se o Departamento de Justiça tinha a intenção de me indiciar e, no caso de eu tentar ingressar nos Estados Unidos, se "o Departamento de Justiça, o Departamento de Segurança Doméstica ou qualquer outro órgão do governo federal pretendia deter, interrogar, prender ou processar" a minha pessoa. No entanto, conforme noticiou em dezembro o *Orlando Sentinel*, jornal da cidade natal de Grayson, sua carta nunca foi respondida.

Do final de 2013 até o início de 2014, a ameaça de um processo só fez aumentar conforme funcionários do governo sustentavam um ataque claramente articulado para criminalizar meu trabalho. No fim de outubro, Keith Alexander, diretor da NSA, em óbvia referência às minhas contribuições como freelancer pelo mundo, reclamou de "os repórteres de jornal terem todos esses documentos, cinquenta mil... seja lá quantos forem, e os estarem vendendo", e fez a estarrecedora

exigência de que "nós" – o governo – "deveríamos dar um jeito de impedir isso". Em uma audiência no mês de janeiro, o presidente do Comitê de Inteligência da Câmara dos Representantes, Mike Rogers, disse repetidas vezes ao diretor do FBI James Comey que alguns dos jornalistas estavam "vendendo propriedade roubada", o que fazia deles "intermediários" ou "ladrões", e então especificou estar se referindo a mim. Quando comecei a noticiar a espionagem canadense junto com a CBC, o porta-voz do Parlamento do governo de direita de Stephen Harper me denunciou como um "pornoespião" e acusou a CBC de comprar de mim documentos roubados. Nos Estados Unidos, o diretor da Inteligência Nacional, James Clapper, começou a usar o termo criminal "cúmplices" em referência a jornalistas que cobriam o caso da NSA.

Eu achava que a chance de ser preso caso voltasse aos Estados Unidos era inferior a 50%, ainda que apenas por uma questão de imagem e controvérsia mundial. Calculei que a mácula potencial no legado de Obama como primeiro presidente norte-americano a processar um jornalista por praticar o jornalismo fosse um obstáculo suficiente. No entanto, se o passado recente provava alguma coisa, era que o governo dos Estados Unidos estava disposto a cometer todo tipo de ato repreensível sob a alegação de proteger a segurança nacional, sem ligar para como o resto do mundo via esses atos. As consequências de uma avaliação errada – acabar algemado e acusado de infringir leis relacionadas à espionagem, ser processado por um Judiciário federal que havia se mostrado vergonhosamente subserviente a Washington em relação a essas questões – eram graves demais para serem descartadas com despreocupação. Eu estava decidido a voltar aos Estados Unidos, mas só após ter uma compreensão clara dos riscos. Enquanto isso, minha família, meus amigos e vários tipos de oportunidades importantes para falar no país sobre o trabalho que eu estava fazendo permaneciam fora de alcance.

O fato de advogados e um membro do Congresso considerarem o risco real já era por si só extraordinário, um poderoso indicador da erosão da liberdade de imprensa. E o fato de jornalistas terem se unido ao coro que tratava o meu trabalho como uma infração era um triunfo notável de propaganda para todos os poderes do governo, que podiam confiar em profissionais formados para fazer o trabalho por eles e equiparar o jornalismo investigativo contrário às suas posições a um crime.

Os ataques a Snowden, é claro, foram muito mais virulentos. Foram também bizarramente idênticos no que diz respeito ao tema. Comentaristas importantes que nada sabiam sobre ele adotaram de imediato o mesmo roteiro de clichês para denegri-lo. Horas depois de ficarem sabendo seu nome, marcharam a uma só cadência para desabonar seu caráter e suas motivações. Segundo eles, Snowden fora movido não por uma convicção genuína, mas por um "narcisismo em busca de fama".

Bob Schieffer, âncora do noticiário *CBS News*, denunciou Snowden como um "rapaz narcisista" que "se acha mais esperto do que os outros". Jeffrey Toobin, da *New Yorker*, diagnosticou-o como "narcisista megalômano que merece ir para a cadeia". Richard Cohen, do *Washington Post*, sentenciou que Snowden "não é paranoico; é apenas narcisista", em referência à notícia de que ele se protegia com um cobertor para impedir que suas senhas fossem filmadas pelas câmeras no teto. De forma bizarra, Cohen afirmou ainda que Snowden "vai entrar para a história como um homem que se traveste de Chapeuzinho Vermelho", e que "o seu suposto desejo de ser famoso será frustrado".

Essas caracterizações eram claramente ridículas. Snowden estava decidido a sumir do mapa,

como ele mesmo disse, e a não conceder entrevistas. Ele sabia que a mídia adora levar qualquer notícia para o lado pessoal, e queria manter o foco na vigilância da NSA, não nele mesmo. Cumprindo o que havia afirmado, recusou todos os convites da imprensa. Todos os dias, durante muitos meses, recebi telefonemas e e-mails de quase todos os programas de TV, personalidades do noticiário televisivo e jornalistas famosos dos Estados Unidos implorando por uma chance de conversar com ele. Matt Lauer, apresentador do *Today Show*, ligou várias vezes para tentar nos convencer; o *60 Minutes* foi tão insistente em seus pedidos que parei de atender as ligações; Brian Williams despachou vários representantes diferentes para defender seu caso. Se quisesse, Snowden poderia ter passado dia e noite nos programas de TV mais influentes, com o mundo inteiro assistindo.

Mas ele se mostrou irredutível. Eu transmitia os pedidos e ele os recusava, para evitar desviar a atenção das revelações. Estranho comportamento para um narcisista em busca de fama.

Em seguida vieram outros ataques à personalidade de Snowden. David Brooks, colunista do *New York Times*, zombou dele dizendo que "ele foi incapaz de concluir o ensino superior básico". Snowden, decretou Brooks, é "o típico exemplo de homem sem filtro", símbolo da "maré crescente de desconfiança, do alastramento corrosivo do cinismo, do esgarçamento do tecido social e da ascensão de pessoas com uma visão tão individualista que não entendem realmente como integrar os indivíduos e cuidar do bem comum".

Para Roger Simon, do *Politics*, Snowden era "um fracassado" porque havia "largado o ensino médio". Debbie Wasserman Schultz, deputada democrata e presidente do Comitê Nacional Democrata, censurou Snowden, que acabara de arruinar a própria vida para fazer as revelações sobre a NSA, taxando-o de "covarde".

Inevitavelmente, o patriotismo dele foi questionado. Como ele tinha ido para Hong Kong, afirmaram que era provável que estivesse trabalhando como espião para o governo chinês. "Não é difícil imaginar que Snowden era um agente duplo da China e em breve irá desertar", anunciou o veterano consultor de campanha do Partido Republicano Matt Mackowiak.

Quando Snowden deixou Hong Hong rumo à América Latina com escala na Rússia, porém, a acusação no mesmo instante passou de espião chinês a espião russo. Gente como o deputado Mike Rogers fez essa acusação sem qualquer tipo de indício, ignorando o fato óbvio de que Snowden só estava na Rússia porque os Estados Unidos haviam revogado seu passaporte e depois pressionado países como Cuba a revogar sua promessa de salvo-conduto. Além do mais, que tipo de espião russo iria a Hong Kong ou trabalharia com jornalistas e se identificaria publicamente, em vez de transmitir os documentos a seus superiores em Moscou? A alegação nunca fez qualquer sentido e não tinha por base nenhum fragmento sequer de fato, mas isso não impediu que se espalhasse.

Uma das acusações mais levianas e sem embasamento contra Snowden veio do *New York Times*, segundo o qual ele fora autorizado a deixar Hong Kong pelo governo chinês, não pelas autoridades de Hong Kong, e que ainda fez uma especulação indecente e prejudicial: "Dois especialistas ocidentais em inteligência, que já trabalharam para grandes agências de espionagem do governo, afirmaram acreditar que o governo chinês conseguira esvaziar o conteúdo dos quatro laptops que o Sr. Snowden afirmou ter levado para Hong Kong."

O jornal não tinha qualquer prova de que o governo chinês tivesse conseguido obter os dados de Snowden sobre a NSA, e simplesmente levava seus leitores a concluir que isso tinha acontecido com

base em dois "especialistas" anônimos que "acreditavam" que isso pudesse ter acontecido.

Na época em que essa notícia foi publicada, Snowden estava no aeroporto de Moscou, sem possibilidade de entrar na internet. Assim que reapareceu, negou com veemência, em matéria publicada no *Guardian*, que tivesse passado quaisquer dados para a China ou a Rússia. "Nunca dei nenhuma informação a nenhum desses dois governos, e eles nunca tiraram nada dos meus laptops", afirmou ele.

Um dia depois de publicado o desmentido de Snowden, Margaret Sullivan criticou o *Times* pela matéria. Entrevistou Joseph Kahn, da editoria internacional do jornal, que declarou: "É importante ver esse trecho da matéria como o que de fato é: uma suposição quanto ao que poderia ter acontecido, baseada em especialistas que não alegavam ter nenhum conhecimento direto." Sullivan comentou que "duas frases no meio de um artigo do *Times* sobre um tema tão delicado – embora possam não dizer respeito à questão central – têm o poder de mudar o rumo do debate ou de prejudicar uma reputação". Concluindo, ela concordou com um leitor que havia reclamado da matéria dizendo: "Eu leio o *Times* em busca da verdade. Se quiser especulações, posso ler isso em praticamente qualquer lugar."

Em uma reunião para convencer o *Guardian* a colaborar em determinadas matérias sobre a NSA, a editora-executiva do *Times*, Jill Abramson, mandou um recado por Janine Gibson: "Por favor, diga a Glenn Greenwald que concordo inteiramente com ele em relação ao fato de que jamais deveríamos ter publicado aquela alegação sobre a China ter 'esvaziado' os laptops de Snowden. Foi uma irresponsabilidade."

Gibson parecia esperar que eu ficasse contente, mas minha reação foi muito diferente: como a editora-executiva de um jornal podia concluir que um artigo obviamente prejudicial era irresponsável e não deveria ter sido publicado, e não publicar um desmentido ou nem mesmo uma nota do editor?

Além da falta de provas, a alegação de que os laptops de Snowden tinham sido "esvaziados" não se sustentava. Há anos ninguém mais usa laptops para transportar grandes quantidades de dados. Mesmo antes de os computadores portáteis se tornarem comuns, vários documentos eram gravados em discos, como o são hoje em pen drives. É verdade que Snowden tinha quatro laptops em Hong Kong, cada qual com uma função de segurança distinta, mas eles não tinham qualquer relação com a quantidade de documentos que ele carregava consigo. Estes ficavam em pen drives protegidos por sofisticados métodos de criptografia. Uma vez que havia trabalhado como hacker para a NSA, Snowden sabia que eles não poderiam ser acessados nem pela própria NSA, quanto mais por agências de inteligência chinesas ou russas.

Especificar o número de laptops de Snowden era uma forma bastante dissimulada de manipular a ignorância e o medo das pessoas: *ele pegou tantos documentos que precisa de quatro laptops para guardar tudo!* Mesmo que os chineses tivessem dado um jeito de esvaziar seu conteúdo, não teriam conseguido nada de valor.

Igualmente desprovido de sentido era o conceito de que Snowden tentaria se salvar revelando segredos de vigilância a potências estrangeiras. Ele havia desmantelado a própria vida e arriscado um futuro na prisão para revelar ao mundo um sistema de vigilância clandestino que, em sua opinião, precisava acabar. Pensar que pudesse mudar de opinião e ajudar a China ou a Rússia a melhorar sua capacidade de vigilância, tudo para evitar ser preso, era simplesmente estúpido.

A afirmação pode até ter sido uma bobagem, mas seus danos foram significativos e previsíveis.

Qualquer debate sobre a NSA na TV sempre incluía alguém afirmando, sem qualquer oposição, que a China agora dispunha, graças a Snowden, dos segredos mais delicados dos Estados Unidos. Com o título "Por que a China deixou Snowden sair", a *New Yorker* disse a seus leitores: "A utilidade dele estava exaurida quase por completo. Especialistas em inteligência citados pelo *Times* acreditavam que o governo chinês 'houvesse conseguido esvaziar o conteúdo dos quatro laptops que o Sr. Snowden afirmava ter levado para Hong Kong'."

Demonizar a personalidade de quem desafia o poder político é uma tática antiga de Washington, incluindo a imprensa. Um dos primeiros e talvez mais óbvios exemplos dessa artimanha foi o tratamento dado pelo governo Nixon ao delator dos documentos do Pentágono Daniel Ellsberg, que incluiu arrombar o consultório de seu psicanalista para roubar sua ficha e bisbilhotar seu histórico sexual. Por mais sem sentido que o método possa parecer – por que a exposição de informações pessoais constrangedoras neutralizaria provas de comportamento enganador por parte do governo? –, Ellsberg entendeu muito bem o recado: as pessoas não querem ser vinculadas a alguém que foi desabonado ou humilhado publicamente.

A mesma tática foi usada para prejudicar a reputação de Julian Assange muito antes de ele ser acusado de crimes sexuais por duas mulheres na Suécia. E mais: as investidas foram feitas pelos mesmos jornais que haviam trabalhado com ele e se beneficiado das revelações de Chelsea Manning, possibilitadas por Assange e pelo WikiLeaks.

Quando o *New York Times* publicou o que chamou de "Os arquivos da Guerra do Iraque", milhares de documentos confidenciais com detalhes de atrocidades e outros abusos cometidos durante o conflito pelas forças armadas norte-americanas e seus aliados iraquianos, incluiu um artigo de primeira página – mesmo destaque dado às revelações em si – assinado pelo jornalista defensor da guerra John Burns sem qualquer outro objetivo que não retratar Assange como um indivíduo bizarro e paranoico, com uma compreensão restrita da realidade.

O texto descrevia como Assange "se registra em hotéis com nomes falsos, pinta o cabelo, dorme em sofás e no chão e, em vez de cartão de crédito, usa dinheiro vivo, muitas vezes emprestado pelos amigos". Assinalava o que chamava de "comportamento incoerente e autoritário" e "delírios de grandeza", e dizia que seus detratores "acusavam-no de conduzir uma vingança contra os Estados Unidos". Acrescentava, ainda, o seguinte diagnóstico psicológico de um voluntário insatisfeito do WikiLeaks: "Ele não bate bem da bola."

Retratar Assange como louco e delirante tornou-se uma constante do discurso político norte-americano em geral, e em especial do *New York Times*. Em uma das matérias, Bill Keller citou um repórter do jornal que descrevia Assange como um homem "desgrenhado, parecido com um mendigo desses que andam cheios de sacolas de plástico, vestindo um casaco esportivo encardido, uma calça cargo, uma camisa branca suja, tênis surrados e meias brancas imundas e frouxas. Exalava um cheiro de quem não tomava banho havia dias".

O *Times* também puxou o coro em relação à cobertura do caso Manning, insistindo que o que levara o soldado a se tornar um delator de grande porte não fora convicção nem consciência, mas distúrbios de personalidade e instabilidade psicológica. Várias matérias especulavam, sem base alguma, que toda a sorte de coisas – de conflitos relacionados ao gênero a conflitos com o pai, passando por *bullying* antigays no exército – eram os principais motivos por trás da sua decisão de revelar documentos tão importantes.

Atribuir a dissidência a distúrbios de personalidade não chega a ser uma invenção americana. Dissidentes soviéticos eram com frequência confinados em hospitais psiquiátricos, e dissidentes chineses ainda são forçados a receber tratamento para doenças mentais. Há motivos evidentes para fazer ataques pessoais a críticos do status quo. Como já foi assinalado, um deles é tornar o dissidente menos eficaz: poucas pessoas desejam se alinhar com as opiniões de alguém maluco ou esquisito. Outra razão é a contenção: quando dissidentes são expulsos da sociedade e menosprezados como emocionalmente desequilibrados, os outros indivíduos recebem um forte incentivo para não seguirem o seu exemplo.

Mas o motivo mais importante é a necessidade lógica. Para os guardiães do status quo, não há nada de genuína ou fundamentalmente errado com a ordem vigente ou suas instituições dominantes, que são consideradas justas. Portanto, qualquer um que alegue o contrário – sobretudo alguém motivado o suficiente por essa crença para tomar uma atitude radical – deve, por definição, ser emocionalmente instável e psicologicamente incapaz.

Em outras palavras, de modo geral existem duas alternativas: a obediência à autoridade institucional ou a dissidência radical em relação a esta. A primeira só é uma opção racional e válida se a segunda for insana e ilegítima. Para os defensores do status quo, a simples *correlação* entre doença mental e oposição radical à ortodoxia dominante não basta. A dissidência radical deve ser indício, ou mesmo prova, de um grave distúrbio de personalidade.

No cerne dessa formulação há um engodo fundamental, de que a dissidência em relação à autoridade institucional envolve uma escolha moral ou ideológica, enquanto a obediência, não. Uma vez estabelecida essa falsa premissa, a sociedade presta muita atenção na motivação dos dissidentes, mas nenhuma em quem se submete às nossas instituições, seja garantindo que as suas ações permaneçam secretas, seja por algum outro meio. A obediência à autoridade é considerada, de forma implícita, o estado natural.

De fato, tanto a observância quanto a violação das regras envolvem escolhas morais, e ambas as atitudes revelam algo importante em relação ao indivíduo em questão. Em vez da premissa aceita – de que um dissidente radical demonstra um distúrbio de personalidade –, talvez o oposto seja verdadeiro: diante de uma grave injustiça, a recusa à dissidência é sinal de falha de caráter ou fracasso moral.

Foi exatamente isso que afirmou o professor de filosofia Peter Ludlow ao escrever, no *New York Times*, sobre o que chama de "vazamentos, delações e hacking político que vêm constrangendo as forças armadas norte-americanas e as comunidades de inteligência pública e privada" – atividades associadas a um grupo que ele chama de "Geração W", da qual Snowden e Manning são fortes exemplos:

> O desejo da mídia de analisar psicologicamente os integrantes da Geração W é bem natural. Ela quer saber por que essas pessoas estão agindo de um modo que eles, membros da imprensa corporativa, não agiriam. Mas o mesmo vale para os dois lados: se existem motivações psicológicas para delações, vazamentos e hacking político, também existem razões psicológicas para defender a estrutura de poder interna a um sistema – sistema este, no caso, em que a mídia corporativa desempenha um papel importante.
>
> De modo semelhante, é possível que o sistema em si esteja doente, mesmo que os atores da

organização se comportem conforme a etiqueta organizacional e respeitem os vínculos de confiança internos.

Trata-se de um debate que as autoridades institucionais desejam ardentemente evitar. A demonização dos delatores por puro reflexo é uma forma de a mídia corporativa dos Estados Unidos proteger os interesses daqueles que detêm o poder. Essa subserviência é tão profunda que muitas das regras do jornalismo são criadas, ou pelo menos aplicadas, para divulgar a mensagem do governo.

Considere-se, por exemplo, a ideia de que vazar informações confidenciais constitui uma espécie de ato malicioso ou criminoso. Os jornalistas de Washington que aplicaram esse conceito a Snowden ou a mim não deploram a revelação de informações secretas em geral, apenas daquelas que desagradam ou prejudicam o governo.

A realidade é que Washington vive soterrada em vazamentos. Os mais celebrados e reverenciados jornalistas da capital norte-americana, como Bob Woodward, garantiram essa posição recebendo e publicando de forma rotineira informações confidenciais obtidas de fontes de alto nível. Autoridades do governo Obama procuraram várias vezes o *New York Times* para revelar dados secretos sobre temas como assassinatos por drones ou o assassinato de Osama bin Laden. O ex-secretário de Defesa Leon Panetta e funcionários da CIA passaram informações secretas à diretora de *A hora mais escura* na esperança de que o filme fosse alardear o maior triunfo político de Obama. (Ao mesmo tempo, advogados do Departamento de Justiça disseram a tribunais federais que, para proteger a segurança nacional, não podiam divulgar informações sobre a caçada a Bin Laden.)

Nenhum jornalista corporativo jamais proporia que as autoridades responsáveis por esses vazamentos ou os jornalistas que os receberam e noticiaram fossem processados. Eles ririam da sugestão de que Bob Woodward – que tem vazado informações ultrassecretas há anos – ou suas fontes de alto nível dentro do governo sejam criminosos.

Isso porque esses vazamentos são sancionados por Washington e servem aos interesses do governo dos Estados Unidos, sendo, portanto, vistos como apropriados e aceitáveis. Os únicos vazamentos que a imprensa de Washington condena são os que contêm informações que os funcionários do governo prefeririam ocultar.

Pensem no que aconteceu poucos segundos antes de David Gregory sugerir no *Meet the Press* que eu fosse preso pelas reportagens sobre a NSA. No início da entrevista, fiz referência a uma decisão judicial ultrassecreta tomada em 2011 pelo tribunal da FISA que qualificava de inconstitucionais e contrárias a estatutos que regulam a espionagem partes significativas do programa de vigilância doméstica da NSA. Eu só sabia dessa decisão porque tinha lido sobre ela nos documentos da NSA que Snowden me dera. No programa, defendi sua divulgação para o público.

Gregory, porém, tentou argumentar que a decisão do parecer da FISA era outra:

> Sobre esse parecer específico da FISA baseado na solicitação do governo, segundo pessoas com quem eu conversei, eles disseram: "Bem, vocês podem obter isso, mas não aquilo. Aquilo na realidade iria além do limite do que vocês têm permissão para fazer." Ou seja, a solicitação foi modificada ou indeferida, e é exatamente isso que o governo está afirmando, que existe uma supervisão judicial nesse caso, e não um abuso.

A questão aqui não são os detalhes do parecer judicial da FISA (embora, quando este foi divulgado, oito semanas depois, tenha ficado claro que a decisão de fato concluía que a NSA agira de forma ilegal). Mais importante é Gregory ter afirmado que sabia da decisão porque suas fontes haviam lhe contado, e então ter divulgado essa informação para o mundo.

Assim, segundos antes de levantar a possibilidade de eu ser preso por causa das reportagens, ele próprio vazou o que considerava uma informação ultrassecreta fornecida por fontes do governo. Só que ninguém jamais sugeriria que o trabalho de Gregory devesse ser criminalizado. Aplicar o mesmo raciocínio ao apresentador do *Meet the Press* e sua fonte seria considerado ridículo.

De fato, Gregory provavelmente seria incapaz de entender que a sua revelação e a minha fossem sequer comparáveis, uma vez que a sua fora feita a mando de um governo que tentava defender e justificar as próprias ações, enquanto a minha fora realizada de forma antagônica, contra os desejos das autoridades.

Isso, claro, é justamente o contrário do que a liberdade de imprensa deveria garantir. A ideia de um "quarto poder" é que aqueles que detêm o maior poder precisam ser desafiados por pressões antagônicas e por uma insistência de transparência; o trabalho da imprensa é desmascarar as falsidades que o poder dissemina, de forma inevitável, para se proteger. Sem esse tipo de jornalismo, abusos são impossíveis de evitar. Ninguém precisa que a Constituição norte-americana garanta a liberdade da imprensa para os jornalistas poderem ser simpáticos e divulgarem e glorificarem os líderes políticos; a garantia é necessária para que os repórteres possam fazer o contrário.

O tratamento desigual com relação à publicação de informações confidenciais é ainda mais patente quando se trata da exigência implícita de "objetividade jornalística". Foi a suposta violação dessa regra que fez de mim um "ativista", não um "jornalista". Como não se cansam de nos repetir, jornalistas não emitem opiniões, apenas relatam os fatos.

Isso é um engodo evidente, uma arrogância da profissão. As percepções e os pronunciamentos de qualquer ser humano têm uma subjetividade inerente. Toda matéria noticiosa é produto de várias pressuposições subjetivas altamente culturais, nacionalistas e políticas. E todo jornalismo serve aos interesses de alguma facção.

A distinção relevante não é entre jornalistas que têm opinião e aqueles que não as têm, pois a segunda categoria não existe. A distinção é, isso sim, entre jornalistas que revelam as próprias opiniões de forma honesta e aqueles que as escondem e fingem não ter nenhuma.

A própria ideia de que os repórteres devem ser isentos de opinião está longe de ser um pré-requisito tradicional da profissão; na realidade, é uma invenção relativamente nova cujo efeito, quando não a intenção, é neutralizar o jornalismo.

Como observou o colunista de mídia da Reuters Jack Shafer, essa recente visão norte-americana reflete "uma triste devoção ao ideal corporativo do que o jornalismo" deve ser, bem como "uma dolorosa falta de compreensão histórica". Desde a criação dos Estados Unidos da América o jornalismo da melhor qualidade e o mais significativo com frequência envolveu repórteres engajados, a defesa de um ponto de vista e a dedicação ao combate à injustiça. O modelo sem opinião, sem cor, sem alma do jornalismo corporativo esvaziou a prática de seus atributos mais louváveis, tornando a grande mídia inconsequente: ela não ameaça ninguém que seja poderoso, exatamente conforme o pretendido.

No entanto, além da falácia inerente de uma cobertura objetiva, a regra quase nunca é aplicada de

forma consistente por quem alega acreditar nela. Jornalistas da grande mídia com frequência expressam suas opiniões sobre uma vasta gama de questões controversas sem verem negado seu status profissional. Se as suas opiniões forem sancionadas pelos funcionários públicos de Washington, eles são percebidos como legítimos.

Ao longo da controvérsia relacionada à NSA, Bob Schieffer, apresentador do *Face the Nation*, denunciou Snowden e defendeu a vigilância da agência, assim como Jeffrey Toobin, correspondente jurídico da *New Yorker* e da CNN. John Burns, correspondente do *New York Times* que cobriu a Guerra do Iraque, reconheceu posteriormente que se manifestara a favor da invasão, chegando a descrever as tropas norte-americanas como "meus libertadores" e "anjos da salvação". Christiane Amanpour, da CNN, passou o verão de 2013 defendendo o uso da força militar norte-americana na Síria. No entanto, essas posturas não foram condenadas como "ativismo", porque, por mais que se reverencie a objetividade, na verdade não existe proibição alguma ao fato de jornalistas terem opinião.

Assim como a suposta norma contra os vazamentos, a "regra" da objetividade não é regra alguma, mas sim uma forma de promover os interesses da classe política dominante. Dessa forma, "a vigilância da NSA é legal e necessária", "a Guerra do Iraque está certa" ou "os Estados Unidos devem invadir tal país" são opiniões aceitáveis para jornalistas expressarem, e eles fazem isso o tempo inteiro.

"Objetividade" nada mais é do que refletir a parcialidade e servir aos interesses de uma Washington entrincheirada. As opiniões só são problemáticas quando ultrapassam os limites aceitáveis da ortodoxia de Washington.

A hostilidade em relação a Snowden não era difícil de explicar. A hostilidade em relação ao jornalista que deu a notícia – eu – talvez seja mais complexa. Em parte competição, em parte o troco por anos de críticas profissionais emitidas contra os astros da mídia norte-americana, além, acredito, de raiva e até vergonha da verdade exposta pelo jornalismo crítico: notícias que irritam o governo revelam o verdadeiro papel de muitos repórteres corporativos, que é amplificar o poder.

O principal motivo para a hostilidade, porém, foi, de longe, o fato de os profissionais da grande mídia terem aceitado o papel de obedientes porta-vozes do poder político, sobretudo no que diz respeito à segurança nacional. Portanto, assim como as autoridades em si, eles desprezam aqueles que contestam ou minam os centros de poder de Washington.

O típico jornalista do passado era definitivamente um outsider. Muitos dos que abraçavam a profissão estavam inclinados não a servir, mas a antagonizar o poder, não apenas por meio da ideologia, mas também da personalidade e da disposição. Optar por uma carreira de jornalista era quase uma garantia do status de outsider: ganhava-se mal, tinha-se pouco prestígio institucional e era-se, em geral, desconhecido.

Isso hoje mudou. Com a compra das empresas de mídia pelas maiores corporações do mundo, a maioria dos astros da imprensa são funcionários de conglomerados com salários altos, iguais a quaisquer outros funcionários do mesmo tipo. Em vez de vender serviços bancários ou instrumentos financeiros, eles oferecem produtos de mídia ao público em nome da empresa para a qual trabalham. Sua trajetória de carreira é determinada pelas mesmas medidas que geram sucesso em um ambiente assim: o grau de satisfação que conseguem dar a seus superiores corporativos e a promoção dos interesses da empresa.

Aqueles que prosperam dentro da estrutura de uma grande empresa tendem a ter mais inclinação a agradar do que a subverter o poder institucional. Consequentemente, quem obtém sucesso no jornalismo corporativo tende a fazer a vontade de quem está no poder. Essas pessoas se identificam com a autoridade institucional e sua habilidade está em servi-la, não em combatê-la.

Fartos indícios apontam para isso. Sabemos da disposição do *New York Times* de omitir, a pedido da Casa Branca, a descoberta do programa ilegal de grampos da NSA feita por James Risen em 2004; na época, o ombudsman do jornal descreveu as desculpas para a omissão como "lamentavelmente inadequadas". Em incidente semelhante no *Los Angeles Times*, em 2006, o editor Dean Baquet derrubou uma matéria de seus repórteres sobre a colaboração secreta entre a AT&T e a NSA baseada em informações fornecidas pelo delator Mark Klein. Este havia apresentado vários documentos que revelavam a construção, pela AT&T, de uma sala secreta em sua sede em São Francisco na qual a NSA pôde instalar *splitters* para desviar telefonemas e tráfego de internet dos clientes da empresa para repositórios da agência.

Nas palavras de Klein, os documentos mostravam que a NSA estava "vasculhando a vida pessoal de milhões de americanos inocentes". No entanto, como declarou Klein ao programa *ABC News* em 2007, Baquet travou a publicação da matéria "a pedido do então diretor da Inteligência Nacional, John Negroponte, e do diretor da NSA na época, general Michael Hayden". Pouco depois, Baquet se tornou chefe do escritório do *New York Times* em Washington, antes de ser promovido ao cargo de chefe de redação do jornal.

O fato de o *Times* promover alguém tão disposto a servir aos interesses do governo não deveria ser nenhuma surpresa. A ombudsman Margaret Sullivan observou que talvez fosse bom o *Times* se olhar no espelho caso seus editores quisessem entender por que fontes que tinham matérias importantes sobre segurança nacional para revelar, como Chelsea Manning e Edward Snowden, não se sentiam seguras ou motivadas para procurar o jornal com suas informações. É bem verdade que o *Times* publicou uma grande quantidade de documentos em parceria com o WikiLeaks, mas logo em seguida o ex-editor-executivo Bill Keller se esforçou para distanciar o jornal de seu parceiro, contrastando publicamente a raiva do governo Obama em relação ao WikiLeaks com seus elogios ao *Times* e à sua cobertura "responsável".

Keller também alardeou, com orgulho, a relação de seu jornal com Washington em outras ocasiões. Em uma aparição em 2010 na BBC para discutir os telegramas obtidos pelo WikiLeaks, ele explicou que o *Times* recebe instruções do governo dos Estados Unidos em relação ao que deve ou não publicar. Incrédulo, o apresentador da BBC falou: "Está dizendo que vocês meio que procuram o governo de antemão e perguntam 'E isto aqui, e aquilo outro, tudo bem fazer isso ou tudo bem fazer aquilo', e aí recebem permissão?" O outro convidado do programa, o ex-diplomata britânico Carne Ross, comentou que as declarações de Keller o faziam pensar que o *New York Times* não era o veículo a se procurar para divulgar os telegramas. "É incrível o jornal estar pedindo aprovação ao governo dos Estados Unidos sobre o que publicar em relação a esse assunto."

Mas não há nada de extraordinário na colaboração desse tipo de mídia com Washington. Por exemplo, é normal jornalistas adotarem a posição oficial norte-americana em disputas com adversários estrangeiros e tomarem decisões editoriais com base naquilo que seja mais benéfico aos "interesses dos Estados Unidos" conforme definidos pelo governo. Jack Goldsmith, advogado do Departamento de Justiça no governo Bush, elogiou o que qualificou de "fenômeno insuficientemente

valorizado: o patriotismo da imprensa norte-americana", ou seja, o fato de a mídia do país tender a se mostrar leal aos objetivos do governo. Citando o diretor da CIA e da NSA na era Bush, Michael Hayden, ele observou que os jornalistas norte-americanos se mostram "dispostos a trabalhar conosco", mas acrescentou que com a imprensa estrangeira "isso é muito, muito difícil".

A identificação da grande mídia com o governo é consolidada por diversos fatores, um dos quais é socioeconômico. Muitos dos jornalistas influentes dos Estados Unidos são hoje multimilionários. Eles moram nos mesmos bairros que os membros da elite política e financeira para os quais atuam ostensivamente como cães de guarda. Frequentam os mesmos eventos, têm os mesmos círculos de amigos e colegas, seus filhos estudam nas mesmas escolas particulares de elite.

Esse é um dos motivos pelos quais jornalistas e funcionários do governo podem trocar de emprego de forma tão natural. Essa dança das cadeiras transfere as figuras da mídia para empregos de alto nível em Washington, da mesma forma que funcionários do governo muitas vezes deixam seus cargos em troca da recompensa de um lucrativo contrato na imprensa. Jay Carney e Richard Stengel, da revista *Time*, estão hoje no governo, enquanto os assessores de Obama David Axelrod e Robert Gibbs são comentaristas do canal MSNBC. Bem mais do que mudanças de carreira, trata-se de transferências laterais: a troca é tão fluida justamente porque os funcionários continuam servindo aos mesmos interesses.

O jornalismo corporativo nos Estados Unidos é tudo, menos um outsider. Ele está integrado por completo ao poder político dominante do país. De um ponto de vista cultural, emocional e socioeconômico, os dois são uma coisa só. Jornalistas influentes, ricos e famosos não querem subverter o status quo que os recompensa de forma tão abundante. Assim como qualquer cortesão, mostram-se ansiosos para defender o sistema que lhes proporciona seus privilégios e desprezam qualquer um que desafie esse sistema.

Falta apenas um curto passo para uma identificação total com as necessidades das autoridades. Nesse contexto, a transparência é ruim; o jornalismo crítico é mau, possivelmente até criminoso. É preciso deixar os líderes políticos exercerem seu poder às escuras.

Em setembro de 2013, todos esses pontos foram defendidos com veemência por Seymour Hersh, vencedor do prêmio Pulitzer responsável por revelar o massacre de Mi Lai e o escândalo de Abu Ghraib. Em entrevista ao *Guardian*, Hersh criticou o que chamou de "timidez dos jornalistas nos Estados Unidos, incapazes de desafiar a Casa Branca e de se tornarem impopulares mensageiros da verdade". Segundo ele, o *New York Times* gasta muito tempo "bancando o lacaio do governo Obama". O governo mente de forma sistemática, argumentou, "mas mesmo assim nenhum dos leviatãs da mídia norte-americana, as redes de televisão ou os grandes veículos impressos" o contestam.

A proposta de Hersh para "consertar o jornalismo" era "fechar as redações da NBC e da ABC, demitir 90% dos editores da mídia impressa e voltar ao trabalho fundamental dos jornalistas", que é ser outsider. "Começar a promover editores que não se possa controlar", defendeu ele. "Os criadores de caso nunca são promovidos", afirmou. Em vez disso, jornalistas e "editores cagões" estão arruinando a profissão, porque a mentalidade dominante é não se atrever a ser outsider.

Depois que um jornalista é identificado como ativista, depois que o seu trabalho é maculado pela acusação de atividade criminosa e que ele é excluído do círculo de proteções de que gozam esses

profissionais, torna-se vulnerável a ser tratado como um criminoso. Isso se tornou claro para mim muito rapidamente depois que as notícias sobre a NSA foram a público.

Minutos após eu chegar em casa no Rio depois da viagem a Hong Kong, David me disse que o seu laptop tinha sumido. Desconfiado de que o desaparecimento tivesse a ver com uma conversa que tivéramos enquanto eu estava fora, ele me lembrou que eu havia lhe telefonado pelo Skype para falar sobre uma grande pasta criptografada de arquivos que pretendia lhe mandar. Quando esta chegasse, instruíra eu, ele deveria guardá-la em algum lugar seguro. Snowden considerara vital que eu entregasse um conjunto completo dos documentos para alguém em quem tivesse plena confiança, para o caso de a minha cópia ser perdida, danificada ou roubada.

"Eu talvez não esteja disponível por muito mais tempo", dissera ele. "E você não sabe como a sua relação de trabalho com Laura vai evoluir. Precisa deixar uma cópia dos documentos com alguém a quem sempre terá acesso, aconteça o que acontecer."

David era a escolha óbvia. Só que eu nunca cheguei a lhe mandar o arquivo. Foi uma das coisas que não tive tempo de fazer enquanto estava em Hong Kong.

"Menos de 48 horas depois que você falou isso, meu laptop foi roubado de casa", contou David.

Resisti à ideia de que o roubo do laptop estivesse ligado à nossa conversa pelo Skype. Comentei com David que fazia questão de que nós não nos transformássemos naquelas pessoas paranoicas que atribuem à CIA qualquer acontecimento inexplicado em suas vidas. Talvez o laptop tivesse sido perdido ou pego por alguém de passagem pela casa, ou quem sabe tivesse sido levado em um roubo não relacionado ao meu trabalho.

David foi derrubando minhas teorias, uma após outra: ele nunca tinha saído de casa com o computador; tinha revirado a casa inteira sem encontrá-lo; nada mais tinha sido levado ou mexido. Segundo ele, eu estava sendo irracional por me negar a considerar o que parecia ser a única explicação.

Àquela altura, vários jornalistas já tinham observado que a NSA não fazia a menor ideia do que Snowden havia pegado ou entregado a mim, não só os documentos específicos, mas também a quantidade. Fazia sentido o governo dos Estados Unidos (ou talvez até outros governos) estar desesperado para saber o que eu tinha. Se pegar o computador de David fosse lhes dar essa informação, por que eles não o roubariam?

Naquele ponto, eu também sabia que uma conversa com David pelo Skype era tudo, menos segura, e estava tão vulnerável ao monitoramento da NSA quanto qualquer outra forma de comunicação. Portanto, o governo tinha capacidade para ouvir que eu planejava lhe mandar os documentos e um forte motivo para se apossar do seu laptop.

O advogado de mídia do *Guardian*, David Schulz, me disse que havia razões para acreditar na teoria de David em relação ao roubo. Contatos na comunidade de inteligência norte-americana tinham lhe avisado que a presença da CIA no Rio era mais forte do que em praticamente qualquer outro lugar do mundo, e que o chefe da agência na cidade era "notoriamente agressivo". Com base nisso, continuou Schulz, "você deveria partir do princípio de que tudo o que disser, tudo o que fizer e todos os lugares aonde for estarão sendo monitorados de perto".

Aceitei o fato de que minha capacidade de comunicação estaria agora muito restrita. Passei a evitar usar o telefone para qualquer outra coisa que não as conversas mais vagas e banais. Só mandava e recebia e-mails através de pesados sistemas de criptografia. Restringi as conversas com

Laura, Snowden e várias outras fontes a programas de chat criptografados. Só conseguia trabalhar em matérias com os editores do *Guardian* e outros jornalistas se estes fossem ao Rio me encontrar. Cheguei até a ficar mais cauteloso ao conversar com David em nossa casa ou em nosso carro. O roubo do laptop tinha nos alertado para a possibilidade de que até mesmo esses espaços mais íntimos poderiam estar sendo vigiados.

Se eu precisava de mais algum indício do clima de ameaça no qual agora trabalhava, este veio na forma de um relato sobre uma conversa entreouvida por Steve Clemons, bem relacionado e conceituado analista político de Washington e editor colaborador da revista *The Atlantic*.

Em 8 de junho, Clemons estava no aeroporto Dulles, na sala VIP da United Airlines, quando escutou quatro funcionários de inteligência do governo dos Estados Unidos dizerem em voz alta que o delator e o jornalista por trás das reportagens sobre a NSA deviam ser "desaparecidos". Afirmou ter gravado um trecho da conversa com seu celular. Segundo Clemons, o diálogo soava como uma simples "bravata", mas ele mesmo assim decidiu publicá-la.

Embora Clemons tenha bastante credibilidade, não levei seu relato muito a sério. No entanto, o simples fato de funcionários do governo poderem jogar conversa fora em público sobre "desaparecer" com Snowden – e com os jornalistas com os quais ele estava trabalhando – era alarmante.

Nos meses seguintes, a possível criminalização das reportagens sobre a NSA passou de ideia abstrata a realidade. Essa drástica mudança foi conduzida pelo governo britânico.

Primeiro, fiquei sabendo por Janine Gibson, através de chat criptografado, de um acontecimento notável ocorrido na redação londrina do *Guardian* em meados de julho. Ela descreveu o que chamou de "mudança radical" no teor das conversas entre o jornal e a GCHQ nas últimas semanas. O que no início tinham sido "conversas muito civilizadas" sobre as notícias veiculadas pelo jornal havia se transformado em uma série de demandas cada vez mais belicosas, e depois em ameaças diretas da agência de espionagem britânica.

Então, de modo mais ou menos repentino, disse-me Gibson, a GCHQ anunciou que não iria mais "permitir" que o jornal seguisse publicando matérias baseadas em documentos ultrassecretos. Exigiu que o *Guardian* de Londres entregasse todas as cópias dos documentos recebidos de Snowden. Se o periódico se recusasse a fazer isso, um mandado judicial iria proibir qualquer nova notícia sobre o tema.

A ameaça não era vazia. No Reino Unido não existe garantia constitucional da liberdade de imprensa. Os tribunais britânicos são tão deferentes às exigências do governo de "restrições prévias" que a mídia pode ser impedida de antemão de noticiar qualquer coisa que supostamente ameace a segurança nacional.

De fato, nos anos 1970, o primeiro jornalista a descobrir e depois noticiar a existência da GCHQ, Duncan Campbell, foi preso e processado. No Reino Unido, os tribunais poderiam a qualquer momento fechar a redação do *Guardian* e confiscar todo o seu material e os equipamentos. "Nenhum juiz negaria se isso lhe fosse solicitado", falou Janine. "Nós sabemos disso, e eles sabem que nós sabemos."

Os documentos de posse do *Guardian* eram apenas uma fração do acervo completo entregue por Snowden em Hong Kong. Ele fizera questão de que as matérias especificamente relacionadas à GCHQ fossem veiculadas por jornalistas britânicos, e em um dos últimos dias em Hong Kong entregou uma cópia desses documentos a Ewen MacAskill.

Durante nossa conversa, Janine me disse que ela e o editor-chefe Alan Rusbridger, além de outros funcionários do jornal, haviam passado o fim de semana anterior em um retiro numa área remota fora de Londres. De repente, ficaram sabendo que agentes da GCHQ estavam a caminho da redação londrina do *Guardian* para confiscar os discos rígidos que continham os documentos. Conforme depois relatou Rusbridger, o argumento foi: "Pronto, vocês já se divertiram, agora queremos os documentos de volta." O grupo estava no retiro havia apenas duas horas e meia quando foi contatado pela GCHQ. "Tivemos de voltar a Londres imediatamente para defender o prédio da redação. Foi bem tenso", contou Janine.

A GCHQ exigiu que o *Guardian* entregasse todas as cópias do acervo. Caso o jornal tivesse obedecido, a agência teria ficado sabendo que documentos Snowden vazara e a situação jurídica dele teria ficado ainda mais ameaçada. Em vez disso, porém, o periódico concordou em destruir todos os discos rígidos relevantes, com funcionários da GCHQ supervisionando tudo para se certificarem de que a destruição fosse conduzida de forma satisfatória para a agência. Nas palavras de Janine, o que aconteceu foi "uma dança muito complexa de corpo mole, diplomacia, contrabando e, por fim, 'destruição cooperativa demonstrável'".

A expressão "destruição demonstrável" foi inventada pela GCHQ para descrever o que ocorreu. Os agentes foram até o subsolo da redação com funcionários do jornal, inclusive o editor-chefe, e ficaram observando enquanto estes quebravam os discos rígidos em pedacinhos, chegando em determinado momento a pedir que insistissem em partes específicas "só para ter certeza de que nada naqueles fragmentos de metal retorcido pudesse ter qualquer interesse para algum agente chinês que estivesse passando por ali", relatou Rusbridger. Ele se lembra de um especialista em segurança ter dito, de brincadeira: "Já podemos mandar os helicópteros pretos embora", enquanto os funcionários do jornal "varriam do chão os restos de um MacBook Pro".

A imagem de um governo que manda agentes a um jornal para destruir à força seus computadores já é, por si só, chocante, o tipo de coisa que os ocidentais ouvem dizer que só acontece em lugares como China, Irã ou Rússia. Mas é espantoso também que um jornal de renome se submeta de modo voluntário e dócil a esse tipo de ordem.

Se o governo estava ameaçando fechar o lugar, por que não pagar para ver e expor a ameaça à luz do dia? Como disse Snowden ao ficar sabendo do acontecido, "a única resposta certa é: vamos lá, fechem o jornal!". Obedecer de forma voluntária e em segredo é permitir que o governo oculte do mundo sua verdadeira natureza: um Estado que intimida jornalistas para impedi-los de divulgar uma das notícias mais significativas para o público.

Pior ainda: o ato de destruir material que uma fonte arriscou a liberdade e até mesmo a vida para revelar foi completamente antiético em relação ao objetivo da profissão de jornalista.

Além da necessidade de expor esse comportamento despótico, o fato de representantes do governo entrarem marchando em uma redação e obrigarem um jornal a destruir informações é algo que sem sombra de dúvida merece ser noticiado. O *Guardian*, porém, parecia inclinado a ficar calado, sublinhando de forma enfática quão precária é a liberdade de imprensa no Reino Unido.

De toda forma, garantiu-me Gibson, o jornal ainda tinha uma cópia do acervo em sua sucursal de Nova York. Ela então me deu uma notícia surpreendente: o *New York Times* agora possuía outra cópia dos mesmos documentos, entregue por Alan Rusbridger à editora-executiva Jill Abramson para garantir que o periódico continuasse com acesso ao material mesmo que um tribunal britânico

tentasse forçar o *Guardian* nos Estados Unidos a destruir sua cópia.

Isso tampouco era uma boa notícia. O *Guardian* não apenas aceitara, em segredo, destruir seus próprios documentos como também, sem consultar ou sequer avisar Snowden ou a mim, entregara uma cópia justamente ao jornal que Snowden decidira excluir por não confiar no seu relacionamento próximo e subserviente ao governo dos Estados Unidos.

Do ponto de vista do *Guardian*, o periódico não podia se dar ao luxo de ignorar as ameaças do governo britânico, uma vez que não dispunha de proteção constitucional e tinha centenas de funcionários e uma instituição centenária a proteger. Destruir os computadores tinha sido melhor do que entregar o acervo à GCHQ. Apesar disso, fiquei incomodado por eles atenderem às exigências do governo, e mais ainda com sua evidente decisão de não alardear o incidente.

No entanto, tanto antes quanto depois da destruição de seus discos rígidos, o *Guardian* continuou agressivo e intrépido em sua maneira de publicar as revelações de Snowden – na minha opinião, mais do que teria sido qualquer outro jornal de tamanho e importância comparáveis. Apesar das táticas de intimidação das autoridades, que só se intensificaram, os editores continuaram a publicar matéria atrás de matéria sobre a NSA e a GCHQ, e merecem grande crédito por isso.

Mas Laura e Snowden estavam ambos muito zangados, tanto com o fato de o *Guardian* ter se submetido a tamanha intimidação do governo quanto de ter mantido silêncio em relação ao ocorrido. Snowden ficou particularmente furioso ao saber que o acervo da GCHQ acabara indo parar nas mãos do *New York Times*. Considerava isso uma violação de seu acordo com o *Guardian* e de seu desejo de que apenas jornalistas britânicos trabalhassem com os documentos relativos ao Reino Unido, e sobretudo de que o *NYT* não recebesse documento algum. A reação de Laura, por sua vez, acabou tendo consequências dramáticas.

Desde o início de nossa cobertura, a relação de Laura com o *Guardian* foi desconfortável, e depois desses novos desdobramentos a tensão ficou explícita. Durante uma semana de trabalho no Rio, nós dois descobrimos que parte de um dos conjuntos de documentos relacionados à NSA que Snowden havia me passado no dia em que começara a se esconder em Hong Kong (mas que não tivera a chance de entregar a Laura) estava corrompida. Laura não conseguiu recuperar os arquivos no Rio, mas achava que conseguiria fazê-lo quando voltasse a Berlim.

Uma semana depois de voltar à capital alemã, Laura me avisou que os documentos estavam prontos para serem devolvidos a mim. Combinamos que um funcionário do *Guardian* iria de avião até lá, pegaria os documentos e os levaria para mim no Rio. No entanto, evidentemente amedrontado após o drama com a GCHQ, o funcionário do jornal disse a Laura que, em vez de lhe entregar o arquivo pessoalmente, ela deveria despachá-lo para mim pela FedEx.

Isso deixou Laura mais agitada e enfurecida do que eu jamais a vira. "Você não entende o que eles estão fazendo?", perguntou-me ela. "Querem poder dizer: 'Nós não tivemos nada a ver com o transporte desses documentos, quem os enviou e recebeu foram Glenn e Laura.'" Acrescentou ainda que usar a FedEx para enviar documentos ultrassecretos até o outro lado do mundo – e enviá-los no nome dela, em Berlim, para o meu, no Rio, um letreiro de néon para as partes interessadas – era a maior quebra de segurança operacional que conseguia imaginar.

"Nunca mais vou confiar neles", declarou ela.

Mas eu precisava daqueles documentos. Alguns deles eram vitais para matérias nas quais eu

estava trabalhando, e havia muitos outros ainda a serem publicados.

Janine insistiu que o problema era uma falha de comunicação, que o funcionário havia interpretado mal os comentários de seu supervisor, que alguns gerentes de Londres agora estavam receosos de transportar documentos entre mim e Laura. Não havia problema nenhum, disse ela. Alguém do *Guardian* iria de avião até Berlim pegar os documentos naquele mesmo dia.

Mas era tarde demais. "Eu nunca, jamais vou entregar esses documentos para o *Guardian*", disse Laura. "Não confio mais neles."

O tamanho e o caráter delicado dos documentos a deixavam receosa de enviá-los pela internet. Era fundamental que eles fossem entregues a mim pessoalmente por alguém em quem ela confiasse. Essa pessoa foi David, que se ofereceu para ir a Berlim assim que soube do problema. Ambos vimos que essa era a solução ideal. David entendia todas as partes do que estava acontecendo, Laura o conhecia e confiava nele, e ele estava mesmo planejando visitá-la para conversar sobre possíveis novos projetos. Janine concordou alegremente com a ideia e afirmou que o *Guardian* arcaria com o custo da viagem de David.

A agência de viagens do jornal reservou os voos de David na British Airways e lhe mandou o itinerário por e-mail. Jamais nos ocorreu que ele pudesse ter qualquer problema durante a viagem. Jornalistas do *Guardian* que haviam assinado matérias sobre os documentos de Snowden e funcionários que transportaram documentos para lá e para cá tinham pousado no Heathrow e decolado de lá várias vezes sem incidentes. A própria Laura fora de avião a Londres poucas semanas antes. Por que alguém iria pensar que David – um personagem bem mais periférico – estaria correndo perigo?

Ele embarcou no voo com destino a Berlim no domingo 11 de agosto, e deveria voltar uma semana depois com os documentos de Laura. No entanto, na manhã em que ele deveria ter chegado, fui acordado por uma ligação. A voz do outro lado, com um forte sotaque britânico, identificou-se como "agente de segurança do aeroporto de Heathrow" e me perguntou se eu conhecia David Miranda. "Estamos ligando para informá-lo que prendemos o Sr. Miranda de acordo com a Lei sobre Terrorismo de 2000, Cláusula 7."

Não consegui registrar na hora a palavra "terrorismo"; fiquei mais confuso do que qualquer outra coisa. A primeira pergunta que fiz foi quanto tempo havia que ele estava detido, e quando me responderam que já fazia três horas entendi que aquilo não era um controle de imigração habitual. O homem explicou que o Reino Unido tinha o "direito legal" de mantê-lo sob custódia por até nove horas, e depois disso um tribunal poderia estender o tempo de detenção. Ou então ele poderia ser preso. "Ainda não sabemos o que pretendemos fazer", disse o agente de segurança.

Tanto os Estados Unidos quanto o Reino Unido deixaram bem claro que não irão respeitar qualquer limite – seja ele ético, legal ou político – quando alegarem agir contra o "terrorismo". Agora David estava detido com base em uma lei sobre terrorismo. Ele sequer tentara entrar no Reino Unido: estava apenas fazendo uma escala no aeroporto. As autoridades britânicas tinham esticado o braço até um território que tecnicamente nem é britânico para capturá-lo, e alegado os motivos mais assustadores e obscuros para justificar isso.

Advogados do *Guardian* e diplomatas brasileiros intervieram de imediato para tentar garantir a liberação de David. Não fiquei preocupado pensando em como ele iria lidar com o fato de ficar detido. Uma vida extremamente difícil como órfão em uma das favelas mais pobres do Rio de

Janeiro o havia tornado incrivelmente forte, decidido e esperto. Eu sabia que ele entenderia exatamente o que estava acontecendo e por quê, e não tinha dúvidas de que daria pelo menos tanto trabalho aos seus interrogadores quanto estes estavam lhe dando. Mesmo assim, os advogados do *Guardian* observaram que era raro alguém passar tanto tempo detido.

Ao pesquisar a Lei sobre Terrorismo, fiquei sabendo que apenas três em cada mil pessoas são interceptadas e que a maioria dos interrogatórios, mais de 97%, dura menos de uma hora. Apenas 0,06% dos detidos permanece mais de seis horas sob custódia. Parecia haver uma chance significativa de David ser preso quando fosse ultrapassado o limite de nove horas.

Como seu nome sugere, a finalidade declarada da Lei sobre Terrorismo é interrogar pessoas sobre seus vínculos com atividades terroristas. Segundo alega o governo britânico, a autoridade para deter pessoas é usada para "determinar se o indivíduo está ou já esteve envolvido na execução, preparação ou instigação de atos terroristas". Não havia a mais remota justificativa para deter David com base em uma lei dessas, a menos que o meu trabalho jornalístico estivesse agora sendo equiparado ao terrorismo, o que parecia ser o caso.

A cada hora que passava, a situação parecia mais desanimadora. Tudo o que eu sabia era que diplomatas brasileiros, além de advogados do *Guardian*, estavam no aeroporto tentando localizar David e ter acesso a ele, mas sem sucesso. No entanto, dois minutos antes de o prazo de nove horas se esgotar, um e-mail de Janine com uma só palavra me deu a notícia que eu precisava ouvir: "LIBERADO".

A detenção chocante de David foi condenada na mesma hora no mundo inteiro como uma tentativa agressiva de intimidação. Uma matéria da Reuters confirmou que de fato era essa a intenção do governo britânico: "Um agente de segurança norte-americano disse à Reuters que um dos principais objetivos da (...) detenção e interrogatório de Miranda era mandar um recado aos destinatários dos documentos de Snowden, inclusive ao *Guardian*, de que o governo britânico estava levando muito a sério a tentativa de conter os vazamentos."

No entanto, como declarei à horda de jornalistas que se reuniu no aeroporto do Rio para aguardar a chegada de David, a tática de intimidação do Reino Unido não impediria o meu trabalho. Muito pelo contrário: fiquei ainda mais ousado. As autoridades britânicas tinham se mostrado abusivas ao extremo; a única reação adequada, na minha opinião, era intensificar a pressão e exigir maior transparência e prestação de contas. Essa é a principal função do jornalismo. Quando me perguntaram como eu achava que o episódio seria interpretado, respondi acreditar que o governo do Reino Unido iria se arrepender de ter agido daquela forma, porque seus atos o faziam parecer repressivo e abusivo.

Meus comentários – feitos em português – foram distorcidos e mal traduzidos por uma equipe da Reuters, segundo a qual eu teria declarado que, em reação ao que o governo britânico tinha feito com David, eu agora iria publicar documentos sobre o Reino Unido que antes decidira manter em sigilo. Como a Reuters é uma agência de notícias, essa distorção logo foi transmitida mundo afora.

Durante os dois dias seguintes, a mídia noticiou raivosamente que eu jurara exercer um "jornalismo de vingança". Essa foi uma interpretação equivocada e absurda: o que eu quis dizer foi que o comportamento abusivo do Reino Unido só tinha me tornado mais decidido a continuar meu trabalho. No entanto, como eu já havia aprendido em muitas ocasiões, alegar que um comentário foi reproduzido fora de contexto de nada serve para frear a máquina da mídia.

Quer meus comentários tenham sido mal interpretados, quer não, a reação que suscitaram foi reveladora: Reino Unido e Estados Unidos vinham se comportando de forma intimidadora havia anos, reagindo a qualquer contestação com ameaças ou coisa pior. Pouquíssimo tempo antes, as autoridades britânicas tinham forçado o *Guardian* a destruir seus computadores, e haviam acabado de deter meu companheiro com base em uma lei sobre terrorismo. Delatores foram processados e jornalistas, ameaçados de prisão. No entanto, a simples percepção equivocada de uma reação forte a tais agressões provocou grande indignação entre aqueles que defendiam e tentavam desculpar o Estado: *Meu Deus! Ele falou em vingança!* A dócil submissão a uma intimidação oficial é vista como obrigação; uma atitude contestadora, por sua vez, é condenada como um ato de insubordinação.

Depois de enfim conseguirmos escapar das câmeras, David e eu pudemos conversar. Ele me disse ter se mostrado desafiador durante todas as nove horas que passou detido, mas admitiu ter ficado assustado.

As autoridades claramente o haviam identificado como alvo: os passageiros de seu voo foram instruídos a mostrar o passaporte a agentes que aguardavam do lado de fora do avião. Quando viram o seu, ele foi detido com base na Lei sobre Terrorismo e "ameaçado do primeiro ao último segundo", segundo o próprio David, de ser preso caso não demonstrasse "total cooperação". Todo o seu equipamento eletrônico foi confiscado, inclusive o celular com fotos pessoais, seus contatos e chats com amigos, e ele foi forçado a dar a senha do celular sob ameaça de prisão. "Tenho a sensação de que eles invadiram minha vida inteira, como se eu estivesse nu", disse ele.

David não conseguira parar de pensar no que os Estados Unidos e o Reino Unido tinham feito durante a última década sob o pretexto de combater o terrorismo. "Eles raptam pessoas, prendem-nas sem acusação e sem a intervenção de um advogado, fazem-nas desaparecer, mandam-nas para Guantánamo, matam-nas", falou. "Na verdade, não há nada mais assustador do que um desses dois governos dizer que você é terrorista" – algo que não ocorreria com a maioria dos cidadãos norte-americanos ou britânicos. "Você percebe que eles podem fazer o que quiserem com você."

A controvérsia relacionada à detenção de David durou semanas. No Brasil, foi manchete durante vários dias, e a indignação dos brasileiros foi quase unânime. Políticos britânicos pediram uma reforma da Lei sobre Terrorismo. É claro que foi gratificante ver as pessoas identificarem o ato do Reino Unido como o abuso que realmente foi. Ao mesmo tempo, no entanto, já havia muitos anos que a lei era um escândalo, mas, como ela era usada sobretudo contra muçulmanos, pouca gente ligava para isso. A detenção do cônjuge de um jornalista conhecido, branco e ocidental não deveria ter sido necessária para chamar a atenção para o abuso, mas foi.

Sem qualquer surpresa, revelou-se que o governo britânico tinha falado com as autoridades em Washington antes de David ser detido. Quando indagado durante uma coletiva de imprensa, um porta-voz da Casa Branca respondeu: "Fomos avisados com antecedência (...), de modo que era algo que tínhamos a indicação de que poderia ocorrer." A Casa Branca se recusou a condenar a detenção e a reconhecer que não havia tomado qualquer providência para impedi-la ou sequer desencorajá-la.

A maioria dos jornalistas compreendia quão perigoso esse passo era. "Jornalismo não é terrorismo", declarou, indignada, Rachel Maddow em seu programa na rede MSNBC, indo direto ao ponto. Mas nem todo mundo pensava assim. Jeffrey Toobin elogiou o governo do Reino Unido no horário nobre da TV, comparando a conduta de David à de uma "mula que transporta drogas", e acrescentando ainda que ele devia estar grato por não ter sido preso e processado.

Esse risco se tornou um pouco mais plausível quando o governo britânico anunciou ter aberto oficialmente um inquérito criminal sobre os documentos transportados por David. (O próprio David abriu um processo contra as autoridades britânicas, alegando que sua detenção foi ilegal por não ter tido nenhuma relação com o único objetivo da lei com base na qual ele foi detido: investigar os vínculos de um indivíduo com o terrorismo.) Não é de espantar que as autoridades se tornem tão ousadas quando até mesmo os jornalistas mais proeminentes comparam um trabalho jornalístico crucial, feito com o interesse do público em mente, com a abjeta ilegalidade do tráfico de drogas.

Pouco antes de morrer, em 2005, o celebrado correspondente no Vietnã David Halberstam fez um discurso para alunos da Faculdade de Jornalismo da Universidade Colúmbia. O momento de maior orgulho em sua carreira, afirmou, fora quando os generais norte-americanos no Vietnã ameaçaram exigir que seus editores no *New York Times* o afastassem da cobertura da guerra. Em suas próprias palavras, Halberstam "havia enfurecido Washington e Saigon ao enviar despachos pessimistas sobre a guerra". Os generais o consideravam "o inimigo", uma vez que ele também já interrompera suas coletivas de imprensa para acusá-los de estarem mentindo.

Para Halberstam, enfurecer o governo era uma fonte de orgulho, o verdadeiro objetivo e a verdadeira vocação do jornalismo. Ele sabia que ser jornalista significava assumir riscos e confrontar, não se submeter aos abusos de poder.

Hoje, para muitos que praticam a profissão, elogios do governo por um trabalho jornalístico "responsável" – ou seja, por acatarem suas instruções quanto ao que deve e ao que não deve ser publicado – são motivo de honra. Esse fato dá a real medida do nível ao qual o jornalismo crítico norte-americano despencou.

EPÍLOGO

Na primeira conversa on-line que tive com Snowden, ele me falou só ter um medo ao se identificar: que as suas revelações pudessem ser recebidas com apatia e indiferença, o que significaria que ele havia desestruturado a própria vida e corrido o risco de ser preso a troco de nada. Dizer que esse temor não se concretizou é um tremendo eufemismo.

Na realidade, os efeitos da história, ainda em andamento, foram muito maiores, mais duradouros e mais abrangentes do que ele sonhou ser possível. Suas revelações concentraram a atenção do mundo nos perigos da vigilância estatal onipresente e no sigilo generalizado dos governos. Instigaram o primeiro debate global sobre o valor da privacidade individual na era digital e provocaram contestações ao controle hegemônico da internet pelos Estados Unidos. Modificaram a confiabilidade com que pessoas do mundo inteiro recebem qualquer afirmação feita por funcionários do governo norte-americano e transformaram relações entre países. Alteraram de modo radical as opiniões sobre o papel adequado do jornalismo em relação ao poder do governo. Dentro dos Estados Unidos, por fim, deram origem a uma coalizão ideologicamente diversa e suprapartidária que defende uma reforma significativa do Estado de vigilância.

Um episódio, em especial, ressaltou as profundas mudanças provocadas pelas revelações de Snowden. Poucas semanas depois que a primeira matéria sobre ele assinada por mim e publicada no *Guardian* revelou a coleta maciça de metadados pela NSA, dois membros do Congresso dos Estados Unidos apresentaram, juntos, um projeto de lei para retirar o financiamento desse programa da agência. Notavelmente, os dois representantes responsáveis pelo projeto de lei foram John Conyers, liberal de Detroit que estava cumprindo seu vigésimo mandato na Câmara dos Representantes, e Justin Amash, conservador do Partido Republicano que estava apenas no segundo mandato na mesma casa. É difícil imaginar dois membros mais diferentes do Congresso, mas ali estavam eles, unidos na oposição à espionagem doméstica conduzida pela NSA. E o seu projeto logo conquistou dezenas de defensores pertencentes a todo o espectro ideológico, do mais liberal ao mais conservador, além de todos os matizes intermediários – acontecimento raríssimo em Washington.

Quando a lei passou por votação, o debate foi televisionado pelo canal a cabo C-SPAN, e assisti a ele enquanto conversava por chat com Snowden, que também o acompanhava em Moscou, em seu computador. Ficamos pasmos com o que vimos. Acho que foi a primeira vez que ele realmente compreendeu a magnitude do que tinha feito. Os membros da Câmara se levantaram um após outro para denunciar com veemência o programa da NSA, zombando da ideia de que coletar dados sobre as ligações de todos os cidadãos americanos fosse necessário para deter o terrorismo. Aquela era, de longe, a contestação mais agressiva ao Estado de segurança nacional a surgir no Congresso desde os atentados do 11 de Setembro.

Antes das revelações de Snowden, era inconcebível que qualquer projeto de lei criado para destruir um programa de segurança nacional importante recebesse mais do que um punhado de votos. Mas o

resultado final da votação do projeto de lei de Conyers-Amash deixou as autoridades de Washington chocadas: a lei só não foi aprovada por uma margem mínima, 205 votos contra 217. O apoio ao projeto foi totalmente bipartidário: 111 democratas e 94 republicanos votaram a favor. Essa eliminação das divisões partidárias tradicionais foi tão empolgante para Snowden e para mim quanto o apoio significativo para frear a NSA. A Washington oficial é sustentada por um tribalismo cego gerado por uma rígida guerra partidária. Se essa estrutura de vermelho contra azul puder ser minada, e então transcendida, haverá muito mais esperança para a criação de políticas baseadas nos verdadeiros interesses da população.

Ao longo dos meses seguintes, conforme mais e mais matérias sobre a NSA eram publicadas no mundo todo, muitos especialistas previram que o público deixaria de dar importância ao assunto. No entanto, o que ocorreu foi que o interesse pelo debate sobre vigilância continuou a se intensificar, em âmbito não apenas doméstico, mas também internacional. Os acontecimentos de uma única semana em dezembro de 2013 – mais de seis meses após minha primeira matéria sair no *Guardian* – ilustram quanto as revelações de Snowden continuam a produzir consequências e quão insustentável se tornou a posição da NSA.

A semana em questão começou com a drástica opinião emitida pelo juiz federal norte-americano Richard Leon de que a coleta de metadados pela NSA tinha probabilidades de ser considerada uma violação da Quarta Emenda constitucional dos Estados Unidos, e de que sua abrangência era "quase orwelliana". E mais: o jurista, nomeado por Bush, observou de maneira pertinente que "o governo não cita nenhum caso em que a análise da coleta em massa de dados pela NSA tenha de fato impedido uma ação terrorista iminente". Apenas dois dias depois, uma comissão consultiva criada pelo presidente Obama quando o escândalo da NSA veio a público emitiu um relatório de 308 páginas sobre a questão. Esse relatório também rejeitava de forma decisiva as alegações da agência quanto à importância vital de sua espionagem. "Nosso documento sugere que as informações somadas às investigações sobre terrorismo pelo uso da seção 215 [da Lei Patriota] a respeito de metadados de telefonia não foi essencial para impedir atentados", afirmou a comissão, confirmando que em nenhum caso o desfecho teria sido diferente "sem o programa de coleta de metadados de telefonia da seção 215".

Enquanto isso, fora dos Estados Unidos, a semana da NSA também não ia nada bem. A Assembleia Geral da ONU votou por unanimidade a favor de uma resolução – apresentada por Alemanha e Brasil – segundo a qual a privacidade na internet é um direito humano fundamental, aprovação considerada por um especialista como "um recado contundente aos Estados Unidos de que está na hora de reverter o curso e pôr fim à vigilância generalizada da NSA". No mesmo dia, o Brasil anunciou que não escolheria a Boeing, empresa baseada nos Estados Unidos, para um aguardado contrato de compra de jatos de caça no valor de 4,5 bilhões de dólares, mas sim a companhia sueca Saab. A indignação brasileira com a espionagem de seus líderes, empresas e cidadãos conduzida pela NSA foi claramente um fator-chave nessa decisão surpreendente. "O problema da NSA estragou tudo para os americanos", disse à Reuters uma fonte no governo brasileiro.

Nada disso significa que a batalha está ganha. O Estado de segurança é poderosíssimo, talvez mais ainda do que nossas autoridades eleitas do mais alto escalão, e dispõe de um amplo grupo de defensores influentes dispostos a protegê-lo custe o que custar. Assim, não é de espantar que ele também tenha obtido algumas vitórias. Duas semanas após a decisão do juiz Leon, outro juiz federal,

explorando a lembrança do 11 de Setembro, declarou o programa da NSA constitucional em outro caso. Aliados europeus recuaram em relação a demonstrações iniciais de raiva, alinhando-se docilmente aos Estados Unidos, como em tantas outras vezes. O apoio da população norte-americana também foi inconstante: pesquisas mostram que a maioria dos habitantes do país, embora seja contra os programas da NSA revelados por Snowden, ainda quer que ele seja processado pelas revelações. E altas autoridades do governo começaram até a argumentar que não apenas o próprio Snowden, mas também alguns jornalistas com quem ele trabalhou, entre os quais eu, merecem ser processados e presos.

Apesar de tudo isso, é evidente que os defensores da NSA enfrentaram um revés, e seus argumentos contra uma reforma têm sido cada vez mais fracos. Por exemplo, os partidários da vigilância em massa sem suspeita muitas vezes insistem que alguma espionagem é sempre necessária. Só que esse raciocínio não significa nada; ninguém discorda dele. A alternativa à vigilância em massa não é a total eliminação da vigilância. É, em vez disso, uma vigilância com alvo definido, apenas nos casos em que haja indícios significativos de que a pessoa está de fato cometendo algum delito. Este tipo de espionagem tem muito mais probabilidades de impedir complôs terroristas do que a atual abordagem de "coletar tudo", que soterra os órgãos de inteligência com tamanha quantidade de dados a ponto de impedir os analistas de processá-los de forma eficaz. Além disso, ao contrário de uma vigilância em massa indiscriminada, esse enfoque respeita os valores da Constituição norte-americana e os preceitos básicos da justiça ocidental.

De fato, na esteira dos escândalos de abuso de vigilância desvendados pelo Comitê Church nos anos 1970, foi justamente este o princípio que levou à criação do tribunal da FISA: a noção de que o governo deve apresentar algum indício de infração ou status de agente estrangeiro antes de poder escutar as conversas de alguém. Infelizmente, esse tribunal foi transformado em um mero carimbador, e não exerce qualquer supervisão significativa nas solicitações de vigilância do governo. A ideia essencial, porém, é sólida, e mostra um caminho a ser seguido. Converter o tribunal da FISA em um órgão judicial de verdade, em vez da atual configuração parcial na qual só o governo pode argumentar seu caso, seria uma reforma positiva.

Por si sós, é improvável que essas mudanças legislativas domésticas sejam o suficiente para solucionar o problema da vigilância, uma vez que o Estado de segurança nacional muitas vezes coopta as entidades encarregadas de supervisioná-lo. (Como vimos, por exemplo, os comitês de inteligência no Congresso a esta altura já foram cooptados por completo.) Mas mudanças legislativas desse tipo podem ao menos fortalecer o princípio de que não há lugar para vigilância em massa indiscriminada em uma democracia ostensivamente guiada por garantias constitucionais de privacidade.

Outros passos também podem ser dados para recuperar a privacidade na internet e limitar a vigilância estatal. Esforços internacionais – hoje conduzidos por Alemanha e Brasil – para construir uma nova infraestrutura de internet, evitando que a maioria do tráfego tenha de transitar pelos Estados Unidos, poderiam ter efeitos significativos na redução do controle norte-americano sobre a rede. E os indivíduos também têm um papel a cumprir no sentido de recuperar sua privacidade on-line. Recusar-se a usar os serviços de empresas de tecnologia que colaborem com a NSA e seus aliados pressionará essas empresas a deixarem de colaborar, e incentivará a concorrência a se dedicar à proteção da privacidade. Várias companhias de tecnologia europeias já estão anunciando seus

serviços de e-mail e chat como uma alternativa superior àquelas propostas por Google e Facebook, alardeando o fato de que não fornecem – nem virão a fornecer – dados de usuários à NSA.

Além disso, para impedir os governos de se intrometerem em suas comunicações e em sua atividade pessoal na internet, todos os usuários deveriam adotar ferramentas de criptografia e de anonimato para a navegação. Isso é particularmente importante para quem trabalha em áreas sensíveis, como jornalistas, advogados e ativistas de direitos humanos. E a comunidade de tecnologia deve continuar a desenvolver programas de anonimato e criptografia mais eficazes e mais fáceis de usar.

Em todas essas frentes, ainda há muito trabalho a fazer. No entanto, menos de um ano depois que fui me encontrar com Snowden em Hong Kong, não resta dúvida de que as revelações já provocaram mudanças fundamentais e irreversíveis em muitos países e setores. Além das reformas específicas da NSA, as ações de Snowden também contribuíram de forma significativa para a causa da transparência e de reformas em geral no governo. Ele criou um modelo para inspirar os outros, e é provável que futuros ativistas sigam seus passos e aperfeiçoem os métodos que ele utilizou.

O governo Obama, que processou mais delatores do que todos os outros presidentes norte-americanos somados, tentou criar um clima de medo capaz de sufocar qualquer tentativa de vazamento. Mas Snowden destruiu esse projeto. Ele conseguiu continuar livre, fora do alcance dos Estados Unidos. E mais: recusou-se a permanecer escondido e se identificou com orgulho. O resultado é que a imagem que as pessoas têm dele não é a de um condenado de macacão laranja preso por correntes, mas de um indivíduo independente e articulado, capaz de falar por si e de explicar o que fez e por quê. O governo dos Estados Unidos não pode mais disfarçar a mensagem simplesmente demonizando o mensageiro. Eis uma importante lição para futuros delatores: falar a verdade não precisa destruir sua vida.

Para o restante de nós, o efeito inspirador dos atos de Snowden é igualmente profundo. Dito de forma bem simples, ele lembrou a todos a extraordinária capacidade que qualquer ser humano tem de mudar o mundo. Mesmo sendo uma pessoa comum sob todos os aspectos exteriores – criado por pais sem qualquer riqueza ou poder especiais, sem ter sequer se formado no ensino médio, trabalhando como funcionário obscuro de uma corporação gigantesca –, ele conseguiu, por meio de um único ato ditado pela própria consciência, literalmente alterar o curso da história.

Até mesmo os ativistas mais comprometidos muitas vezes se sentem tentados a sucumbir ao derrotismo. As instituições vigentes parecem poderosas demais para serem desafiadas; as ortodoxias, arraigadas demais para serem eliminadas, e há sempre muitos participantes com interesses velados na manutenção do status quo. Mas são os seres humanos em conjunto, e não uma pequena quantidade de elites operando em segredo, que podem decidir o tipo de mundo no qual nós queremos viver. Promover a capacidade humana de raciocinar e tomar decisões: é esse o objetivo da delação, do ativismo, do jornalismo político. E, graças às revelações de Edward Snowden, é isso que está acontecendo agora.

ANEXO

DOCUMENTOS ORIGINAIS

FIGURA 1:

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

FIGURA 2:

Future Plans (U)

(TS//SI//REL) In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers.

These targets are ideally suited for software demodulation. Additionally, MSOC has developed a capability to automatically scan and demodulate signals as they activate on the satellites. There are a multitude of possibilities, bringing our enterprise one step closer to "collecting it all."

FIGURA 3:

(S//SI//REL TO USA, FVEY) SHELLTRUMPET Processes it's One Trillionth Metadata Record

By NAME REDACTED on 2012-12-31 0738

(S//SI//REL TO USA, FVEY) On December 21, 2012 SHELLTRUMPET processed its One Trillionth metadata record. SHELLTRUMPET began as a near-real-time metadata analyzer on Dec 8, 2007 for a CLASSIC collection system. In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring, direct E-Mail tip alerting, TRAFFICTHIEF tipping, and Real-Time Regional Gateway (RTRG) filtering and ingest. Though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year, and half of that volume was from SSO's DANCINGOASIS. SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems), MUSKETEER, and Second Party systems. We will be expanding its reach into other SSO systems over the course of 2013. The Trillion records processed have resulted in over 35 Million tips to TRAFFICTHIEF.

FIGURA 4:

FAIRVIEW - Corp partner since 1985 with access to int. cables, routers, switches. The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs. Aggressively involved in shaping traffic to run signals of interest past our monitors.

FIGURA 5:

(TS//SI//NF) ORANGECRUSH, part of the OAKSTAR program under SSO's corporate portfolio, began forwarding metadata from a third party partner site (Poland) to NSA repositories as of 3 March and content as of 25 March. This program is a collaborative effort between SSO, NCSC, ETC, FAD, an NSA Corporate Partner and a division of the Polish Government. ORANGECRUSH is only known to the Poles as BUFFALOGREEN. This multi-group partnership began in May 2009 and will incorporate the OAKSTAR project of ORANGEBLOSSOM and its DNR capability. The new access will provide SIGINT from commercial links managed by the NSA Corporate Partner and is anticipated to include Afghan National Army, Middle East, limited African continent, and European communications. A notification has been posted to SPRINGRAY and this collection is available to Second Parties via TICKETWINDOW.

FIGURA 6:

SILVERZEPHYR FAA DNI Access Initiated at NSAW (TS//SI//NF)

By NAME REDACTED on 2009-11-06 0918

(TS//SI//NF) On Thursday, 11/5/09, the SSO-OAKSTAR SILVERZEPHYR (SZ) access began forwarding FAA DNI records to NSAW via the FAA WealthyCluster2/Tellurian system installed at the partner's site. SSO coordinated with the Data Flow Office and forwarded numerous sample files to a test partition for validation, which was completely successful. SSO will continue to monitor the flow and collection to ensure a ny anomalies are identified and corrected as required. SILVERZEPHYR will continue to provide customers with authorized, transit DNR collection. SSO is working with the partner to gain access to an additional 80Gbs of DNI data on their peering network, bundled in 10 Gbs increments. The OAKSTAR team, along with support from NSAT and GNDA, just completed a 12 day SIGINT survey at site, which identified over 200 new links. During the survey, GNDA worked with the partner to test the output of their ACS system. OAKSTAR is also working with NSAT to examine snapshots taken by the partner in Brazil and Colombia, both of which may contain internal communications for those countries.

FIGURA 7:

(TS//SI//NF) PRISM (US-984XN) expanded its impact on NSA's reporting mission in FY12 through increased tasking, collection and operational improvements. Here are some highlights of the FY12 PRISM program:

PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA's 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FY11). PRISM was cited in 13.4% of all 1st, 2nd, and 3rd Party NSA reporting (up from 11.9% in FY11), and is also the top cited SIGAD overall

Number of PRISM-based end-product reports issued in FY12: 24,096, up 27% from FY11

Single-source reporting percentage in FY12 and FY11: 74%

Number of product reports derived from PRISM collection and cited as sources in articles in the President's Daily Brief in FY12: 1,477 (18% of all SIGINT reports cited as sources in PDB articles - highest single SIGAD for NSA); In FY11: 1,152 (15% of all SIGINT reports cited as sources in PDB articles - highest single SIGAD for NSA)

Number of Essential Elements of Information contributed to in FY12: 4,186 (32% of all EEIs for all Information Needs); 220 EEIs addressed solely by PRISM

Tasking: The number of tasked selectors rose 32% in FY12 to 45,406 as of Sept 2012

Great success in Skype collection and processing; unique, high value targets acquired

Expanded PRISM taskable e-mail domains from only 40, to 22,000

FIGURA 8:

(TS//SI//NF) SSO HIGHLIGHT – Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection

By NAME REDACTED on 2013-03-08 1500

(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)

FIGURA 9:

(TS//SI//NF) New Skype Stored Comms Capability For PRISM

By NAME REDACTED on 2013-04-03 0631

(TS//SI//NF) PRISM has a new collection capability: Skype stored communications. Skype stored communications will contain unique data which is not collected via normal real-time surveillance collection. SSO expects to receive buddy lists, credit card info, call data records, user account info, and other material. On 29 March 2013, SSO forwarded approximately 2000 Skype selectors for stored communications to be adjudicated in SV41 and the Electronic Communications Surveillance Unit (ECSU) at FBI. SV41 had been working on adjudication for the highest priority selectors ahead of time and had about 100 ready for ECSU to evaluate. It could take several weeks for SV41 to work through all 2000 selectors to get them approved, and ECSU will likely take longer to grant the approvals. As of 2 April, ESCU had approved over 30 selectors to be sent to Skype for collection. PRISM Skype collection has carved out a vital niche in NSA reporting in less than two years with terrorism, Syrian opposition and regime, and exec/special series reports being the top topics. Over 2800 reports have been issued since April 2011 based on PRISM Skype collection, with 76% of them being single source.

FIGURA 10:

(TS//SI//NF) SSO Expands PRISM Skype Targeting Capability

By NAME REDACTED on 2013-04-03 0629

(TS//SI//NF) On 15 March 2013, SSO's PRISM program began tasking all Microsoft PRISM selectors to Skype because Skype allows users to log in using account identifiers in addition to Skype usernames. Until now, PRISM would not collect any Skype data when a user logged in using anything other than the Skype username which resulted in missing collection; this action will mitigate that. In fact, a user can create a Skype account using any e-mail address with any domain in the world. UTT does not currently allow analysts to task these non-Microsoft e-mail addresses to PRISM, however, SSO intends to fix that this summer. In the meantime, NSA, FBI and Dept of Justice coordinated over the last six months to gain approval for PRINTAURA to send all current and future Microsoft PRISM selectors to Skype. This resulted in about 9800 selectors being sent to Skype and successful collection has been received which otherwise would have been missed.

FIGURA 11:

(TS//SI//NF) Microsoft releases new service, affects FAA 702 collection

By NAME REDACTED on 2012-12-26 0811

(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all current FISA and 702/PRISM requirements - no changes to UTT tasking procedures were required. The SSL solution does not collect server-based voice/video or file transfers. The MS legacy collection system will remain in place to collect voice/video and file transfers. As a result there will be some duplicate collection of text-based chat from the new and legacy systems which will be addressed at a later date. An increase in collection volume as a result of this solution has already been noted by CES.

FIGURA 12:

(TS//SI//NF) Expanding PRISM Sharing With FBI and CIA

By NAME REDACTED on 2012-08-31 0947

(TS//SI//NF) Special Source Operations (SSO) has recently expanded sharing with the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) on PRISM operations via two projects. Through these efforts, SSO has created an environment of sharing and teaming across the Intelligence Community on PRISM operations. First, SSO's PRINTAURA team solved a problem for the Signals Intelligence Directorate (SID) by writing software which would automatically gather a list of tasked PRISM selectors every two weeks to provide to the FBI and CIA. This enables our partners to see which selectors the National Security Agency (NSA) has tasked to PRISM. The FBI and CIA then can request a copy of PRISM collection from any selector, as allowed under the 2008 Foreign Intelligence Surveillance Act (FISA) Amendments Act law. Prior to PRINTAURA's work, SID had been providing the FBI and CIA with incomplete and inaccurate lists, preventing our partners from making full use of the PRISM program. PRINTAURA volunteered to gather the detailed data related to each selector from multiple locations and assemble it in a usable form. In the second project, the PRISM Mission Program Manager (MPM) recently began sending operational PRISM news and guidance to the FBI and CIA so that their analysts could task the PRISM system properly, be aware of outages and changes, and optimize their use of PRISM. The MPM coordinated an agreement from the SID Foreign Intelligence Surveillance Act Amendments Act (FAA) Team to share this information weekly, which has been well-received and appreciated. These two activities underscore the point that PRISM is a team sport!

FIGURA 13:

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)

(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.

FIGURA 14:

While we have invested significant analytic and collection effort of our own to find and exploit these communications, the difficulties we face in obtaining regular and reliable access to such communications impacts on our ability to detect and prevent terrorist acts and diminishes our capacity to protect the life and safety of Australian citizens and those of our close friends and allies.

We have enjoyed a long and very productive partnership with NSA in obtaining minimised access to United States warranted collection against our highest value terrorist targets in Indonesia. This access has been critical to DSD's efforts to disrupt and contain the operational capabilities of terrorists in our region as highlighted by the recent arrest of fugitive Bali bomber Umar Patek.

We would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities – in particular Australians involved with AQAP.

FIGURA 15:

(TS//SI//REL) There are also a few surprises... France targets the US DoD through technical intelligence collection, and Israel also targets us. On the one hand, the Israelis are extraordinarily good SIGINT partners for us, but on the other, they target us to learn our positions on Middle East problems. A NIE [National Intelligence Estimate] ranked them as the third most aggressive intelligence service against the US.

Balancing the SIGINT exchange equally between US and Israeli needs has been a constant challenge in the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party CT relationship being driven almost totally by the needs of the partner.

FIGURA 16:

Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2012, the Government made 1,856 applications to the Foreign Intelligence Surveillance Court (the "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,856 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,789 applications included requests for authority to conduct electronic surveillance.

Of these 1,789 applications, one was withdrawn by the Government. The FISC did not deny any applications in whole or in part.

FIGURA 17:

(U) **NSA Washington Mission**

(U) **Regional**

(TS//SI) ISI is responsible for 13 individual nation states in three continents. One significant tie that binds all these countries together is their importance to U.S. economic, trade, and defense concerns. The Western Europe and Strategic Partnerships division primarily focuses on foreign policy and trade activities of Belgium, France, Germany, Italy, and Spain, as well as Brazil, Japan and Mexico.

(TS//SI) The Energy and Resource branch provides unique intelligence on worldwide energy production and development in key countries that affect the world economy. Targets of current emphasis are [redacted]. Reporting has included the monitoring of international investment in the energy sectors of target countries, electrical and Supervisory Control and Data Acquisition (SCADA) upgrades, and computer aided designs of projected energy projects.

FIGURA 18:

The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.

FIGURA 19:

(S//SI) BLARNEY Team Provides Outstanding Support to Enable UN Security Council Collection

By NAME REDACTED on 2010-05-28 1430

(TS//SI//NF) With the UN vote on sanctions against Iran approaching and several countries riding the fence on making a decision, Ambassador Rice reached out to NSA requesting SIGINT on those countries so that she could develop a strategy. With the requirement that this be done rapidly and within our legal authorities, the BLARNEY team jumped in to work with organizations and partners both internal and external to NSA.

(TS//SI//NF) As OGC, SV and the TOPIs aggressively worked through the legal paperwork to expedite four new NSA FISA court orders for Gabon, Uganda, Nigeria and Bosnia, BLARNEY Operations Division personnel were behind the scenes gathering data determining what survey information was available or could be obtained via their long standing FBI contacts. As they worked to obtain information on both the UN Missions in NY and the Embassies in DC, the target development team greased the skids with appropriate data flow personnel and all preparations were made to ensure data could flow to the TOPIs as soon as possible. Several personnel, one from legal team and one from target development team were called in on Saturday 22 May to support the 24 hour drill legal paperwork exercise doing their part to ensure the orders were ready for the NSA Director's signature early Monday morning 24 May.

(S//SI) With OGC and SV pushing hard to expedite these four orders, they went from the NSA Director for signature to DoD for SECDEF signature and then to DOJ for signature by the FISC judge in record time. All four orders were signed by the judge on Wednesday 26 May! Once the orders were received by the BLARNEY legal team, they sprung into action parsing these four orders plus another "normal" renewal in one day. Parsing five court orders in one day – a BLARNEY record! As the BLARNEY legal team was busily parsing court orders the BLARNEY access management team was working with the FBI to pass tasking information and coordinate the engagement with telecommunications partners.

FIGURA 20:

TOP SECRET//COMINT//NOFORN

August 2010

(U//FOUO) Silent Success: SIGINT Synergy Helps Shape US Foreign Policy

(TS//SI//NF) At the outset of these lengthy negotiations, NSA had sustained collection against France Japan, Mexico, Brazil

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) The resolution was adopted by twelve votes for, two against (Brazil and Turkey), and one abstention from Lebanon. According to USUN, SIGINT "helped me to know when the other Permreps [Permanent Representatives] were telling the truth.... revealed their real position on sanctions... gave us an upper hand in negotiations... and provided information on various countries 'red lines.'"

FIGURA 21:

TOP SECRET//COMINT//NOFORN

June 2010

SID today

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) NAME REDACTED, Chief, Access and Target Development (S3261)

(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.

FIGURA 22:

(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

FIGURA 23:

(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.

FIGURA 24:

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) Entered**

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 when we attempt to upgrade a node that is affected by the bug.

Last CCB Entry: 04/10/13 16:08:11 NAME REDACTED

09 Apr Blarney CCB - Blarney ECP board approved

ECP lead: NAME REDACTED

Programs Affected: Blarney Fairview Oakstar Stormbrew

No Related Work Tasks

FIGURA 25:

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…

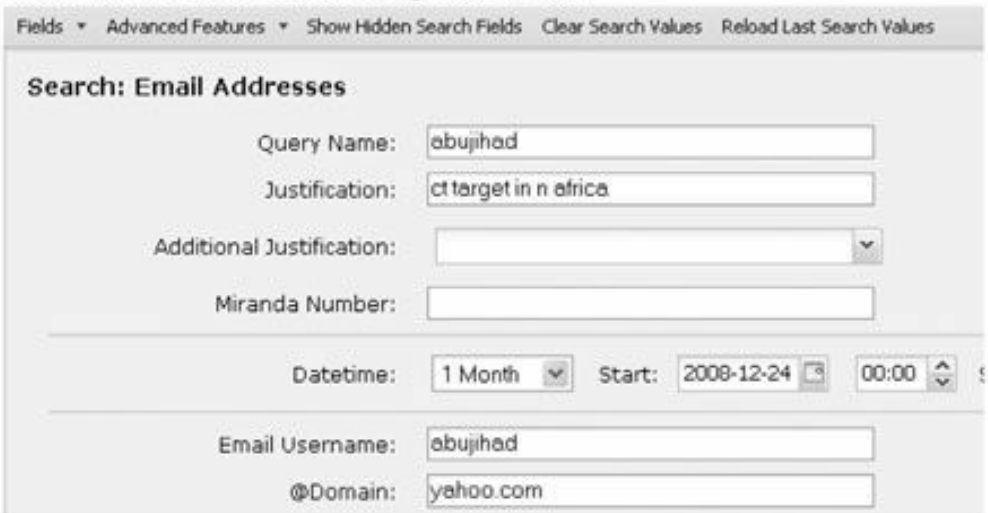


FIGURA 26:

(TS//SI//NF) BLARNEY Exploits the Social Network via Expanded Facebook Collection

By NAME REDACTED on 2011-03-14 0737

(TS//SI//NF) SSO HIGHLIGHT - BLARNEY Exploits the Social Network via Expanded Facebook Collection

(TS//SI//NF) On 11 March 2011, BLARNEY began delivery of substantially improved and more complete Facebook content. This is a major leap forward in NSA's ability to exploit Facebook using FISA and FAA authorities. This effort was initiated in partnership with the FBI six months ago to address an unreliable and incomplete Facebook collection system. NSA is now able to access a broad range of Facebook data via surveillance and search activities. OPIs are excited about receiving many content fields, such as chat, on a sustained basis that had previously only been occasionally available. Some content will be completely new including subscriber videos. Taken together, the new Facebook collection will provide a robust SIGINT opportunity against our targets – from geolocation based on their IP addresses and user agent, to collection of all of their private messages and profile information. Multiple elements across NSA partnered to ensure the successful delivery of this data. An NSA representative at FBI coordinated the rapid development of the collection system; SSO's PRINTAURA team wrote new software and made configuration changes; CES modified their protocol exploitation systems and the Technology Directorate fast-tracked upgrades to their data presentation tools so that OPIs could view the data properly.

FIGURA 27:

BACKGROUND (U)

(TS//SI//REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particularly vulnerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these vulnerabilities include:

- Viewing sexually explicit material online or using sexually explicit persuasive language when communicating with inexperienced young girls;
- Using a portion of the donations they are receiving from the susceptible pool to defray their own personal expenses;
- Charging an exorbitant amount of money for their speaking fees and being singularly attracted by opportunities to increase their stature; or
- Being known to base their public messaging on questionable sources or using language that is contradictory in nature, leaving them open to credibility challenges.

(TS//SI//REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting vulnerabilities of character, credibility, or both, of the radicalizer and his message could be enhanced by an understanding of the vehicles he uses to disseminate his message to the susceptible pool of people and where he is vulnerable in terms of access.

FIGURA 28:

(U) Manhunting Timeline 2010

TOP SECRET//SI/TK//NOFORN

Jump to: navigation, search

Main article: Manhunting

See also: Manhunting Timeline 2011
See also: Manhunting Timeline 2009
See also: Manhunting Timeline 2008

(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 filing 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.[16]

FIGURA 29:

[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

FIGURA 30:

[edit] (TS//SI//REL) Unknowingly targeting a US person

I screwed up...the selector had a strong indication of being foreign, but it turned out to be US...now what?

NOC/OGC RESPONSE: With all querying, if you discover it actually is US, then it must be submitted and go in the OGC quarterly report...'but it's nothing to worry about'. (Source #001)

FIGURA 31:


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
CK
Honey-trap; a great option. Very successful when it works.
- Get someone to go somewhere on the internet, or a physical location to be met by a "friendly face".
- JTRIG has the ability to "shape" the environment on occasions.
Photo change; you have been warned, "JTRIG is about!!"
Can take "paranoia" to a whole new level.
Email/text:
- Infiltration work.
- Helps JTRIG acquire credibility with online groups etc.
- Helps with bringing SIGINT/Effects together.

OBSERVAÇÃO SOBRE AS FONTES

Mais informações sobre as fontes deste livro podem ser encontradas em www.glenngreenwald.net.

AGRADECIMENTOS

Nos últimos anos, os esforços dos governos ocidentais para ocultar dos próprios cidadãos seus atos mais significativos foram repetidamente frustrados por uma série de revelações notáveis feitas por delatores destemidos. Em várias ocasiões, pessoas que trabalhavam dentro de agências do governo ou do aparato militar dos Estados Unidos e de seus aliados decidiram que não podiam permanecer caladas depois de descobrir sérias transgressões. Em vez disso, optaram por tornar públicos os atos equivocados das autoridades, às vezes contrariando a lei de forma consciente para isso, e sempre com grande custo pessoal, pondo em risco suas carreiras, seus relacionamentos íntimos e sua liberdade. Qualquer um que viva em uma democracia, qualquer um que valorize a transparência e a prestação de contas tem para com esses delatores uma imensa dívida de gratidão.

A extensa linhagem de predecessores que inspirou Edward Snowden começa com Daniel Ellsberg, responsável pelo vazamento dos Documentos do Pentágono, um de meus mais antigos heróis pessoais e meu atual amigo e colega, cujo exemplo tento seguir em todo o trabalho que faço. Outros delatores corajosos, que suportaram perseguições por revelar ao mundo verdades vitais, são Chelsea Manning, Jesselyn Radack e omas Tamm, bem como os ex-altos funcionários da NSA omas Drake e Bill Binney. Essas pessoas também inspiraram as ações de Edward Snowden de forma crucial.

Expor o sistema onipresente de vigilância sem suspeita que vinha sendo construído em segredo pelos Estados Unidos e seus aliados foi um ato ditado pela consciência de Snowden ao custo de um grande sacrifício. Ver um homem de 29 anos, comum sob todos os outros aspectos, se arriscar de modo consciente a passar a vida na prisão em nome de um princípio e agir em defesa dos direitos humanos básicos foi simplesmente estarrecedor. Seu destemor e sua tranquilidade inabalável – baseada na convicção de estar fazendo a coisa certa – foram o motor de todo o meu trabalho jornalístico a respeito do assunto, e terão profunda influência sobre mim pelo resto da vida.

O impacto das revelações teria sido impossível sem minha incomparavelmente corajosa e brilhante parceira jornalística e amiga Laura Poitras. Apesar de ter passado anos sendo assediada pelo governo dos Estados Unidos por causa de seus filmes, ela jamais hesitou sequer uma vez antes de divulgar de forma agressiva as notícias sobre a NSA. Sua insistência na própria privacidade e sua aversão aos holofotes às vezes ocultaram quão indispensável ela foi para todo o nosso trabalho. Mas sua experiência, seu tino estratégico, seu senso crítico e sua coragem estiveram sempre no âmago de tudo o que fizemos. Nós nos falamos quase todos os dias e tomamos todas as decisões importantes em conjunto. Eu não poderia ter desejado parceria mais perfeita ou amizade mais encorajadora e inspiradora do que a dela.

Como Laura e eu sabíamos que aconteceria, a coragem de Snowden acabou se revelando contagiosa. Vários jornalistas se mostraram intrépidos na publicação de notícias relacionadas ao vazamento, entre eles os editores do *Guardian* Janine Gibson, Stuart Millar e Alan Rusbridger, bem

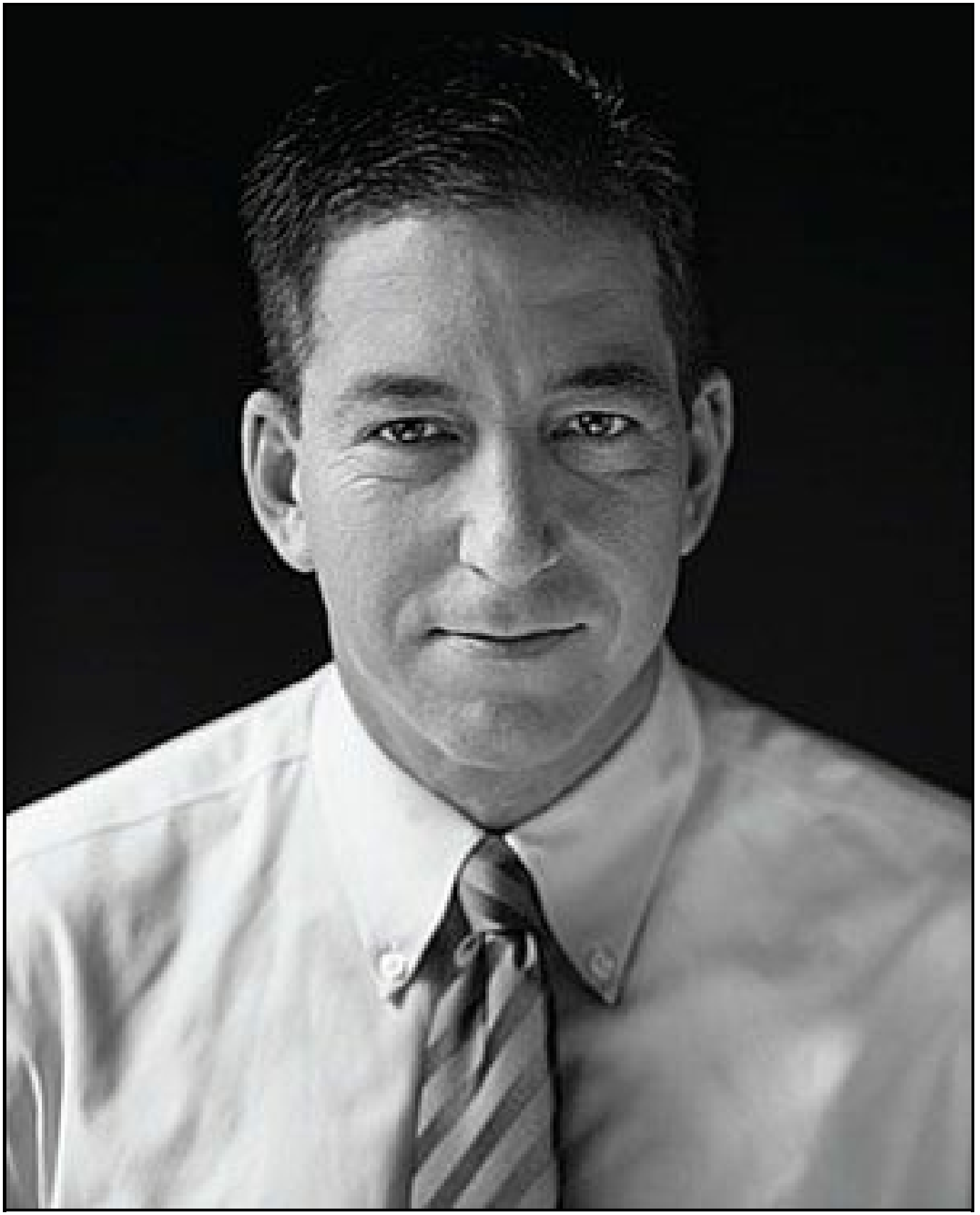
como vários repórteres do mesmo jornal, liderados por Ewen MacAskill. Snowden pôde continuar livre, e portanto capaz de participar do debate que ajudou a suscitar, graças ao apoio ousado e indispensável do WikiLeaks e de sua representante Sarah Harrison, que o ajudou a sair de Hong Kong e depois permaneceu com ele em Moscou durante quatro meses, pondo em risco sua capacidade de retornar com segurança ao seu país, o Reino Unido.

Vários amigos e colegas me deram conselhos muito sensatos e apoio em diversas situações difíceis, entre os quais Ben Wizner e Jameel Jaffer, da ACLU; meu melhor amigo da vida inteira, Norman Fleisher; um dos melhores e mais corajosos jornalistas investigativos do mundo, Jeremy Scahill; a decidida e competente jornalista brasileira Sonia Bridi, da Rede Globo; e o diretor-executivo da Freedom of the Press Foundation, Trevor Timm. Minha família, que muitas vezes se mostrou preocupada com o que estava acontecendo (como só a família pode se mostrar), ainda assim foi sempre firme em seu apoio (como só a família pode ser): meus pais, meu irmão Mark e minha cunhada Christine.

Não foi fácil escrever este livro, sobretudo dadas as circunstâncias, e por isso sou verdadeiramente grato à Metropolitan Books: a Connor Guy, por sua supervisão eficaz; a Grigory Tovbis, pelas contribuições editoriais sensíveis e pela proficiência técnica; e sobretudo a Riva Hocherman, cuja inteligência e cujos altos padrões fizeram dela a melhor editora possível para o livro. Este é o segundo título consecutivo que publico com Sara Bershtel e sua mente sábia e criativa, e não posso me imaginar sequer querendo escrever outro sem ela. Meu agente literário, Dan Conaway, foi mais uma vez uma voz firme e sábia ao longo de todo o processo. Meu profundo agradecimento também a Taylor Barnes, pela ajuda fundamental na feitura deste livro; seus talentos de pesquisadora e sua energia intelectual não deixam dúvidas quanto à carreira jornalística estelar que a aguarda.

Como sempre, no centro de tudo o que faço está meu parceiro de vida, meu marido há nove anos, minha alma gêmea David Miranda. O calvário que ele teve de enfrentar por causa de nosso trabalho foi grotesco e enfurecedor, mas a vantagem foi que o mundo pôde ver que ser humano extraordinário ele é. A cada passo do caminho, David me instilou destemor, me tornou mais decidido, guiou minhas escolhas, deu opiniões que me fizeram ver com mais clareza e esteve sempre ao meu lado, inabalável, me dando apoio e amor incondicionais. Uma parceria como essa é inestimável, pois elimina o medo, destrói limites e torna tudo possível.

© Jimmy Chalk



Glenn Greenwald publicou, mais recentemente, os livros *With Liberty and Justice for Some* e *A Tragic Legacy*, ambos inéditos no Brasil. Ex-advogado e colunista do jornal *e Guardian* até outubro de 2013, recebeu diversos prêmios por suas reportagens investigativas, entre eles o Online Journalism Awards, da Online News Association, em 2013, o Esso de Melhor Reportagem de 2013 – junto com Roberto Kaz e José Casado, o Pioneer Award, da Electronic Frontier Foundation, e o George Polk Awards, ambos também em 2013. Além disso, o conjunto de reportagens sobre os documentos da NSA assinadas por Greenwald, Laura Poitras, Ewen MacAskill e Barton Gellman deu aos periódicos *The Guardian e The Washington Post* o Pulitzer 2014 na categoria Serviço ao Público.

Seus textos foram publicados em vários jornais e revistas de política, como *e New York Times* , *Los Angeles Times* e *e American Conservative*. Em fevereiro de 2014, Greenwald criou, junto com Laura Poitras e Jeremy Scahill, o Intercept, um novo veículo de mídia, no site First Look Media.

INFORMAÇÕES SOBRE A SEXTANTE

Para saber mais sobre os títulos e autores
da EDITORA SEXTANTE,
visite o site www.sextante.com.br
e curta as nossas redes sociais.
Além de informações sobre os próximos lançamentos,
você terá acesso a conteúdos exclusivos
e poderá participar de promoções e sorteios.

 www.sextante.com.br

 facebook.com/esextante

 twitter.com/sextante

 instagram.com/editorasextante

 skoob.com.br/sextante

Se quiser receber informações por e-mail,
basta se cadastrar diretamente no nosso site
ou enviar uma mensagem para
atendimento@esextante.com.br

Editora Sextante
Rua Voluntários da Pátria, 45 / 1.404 – Botafogo
Rio de Janeiro – RJ – 22270-000 – Brasil
Telefone: (21) 2538-4100 – Fax: (21) 2286-9244
E-mail: atendimento@esextante.com.br

SUMÁRIO