Como entender as denúncias de vigilantismo global

*Por **Pedro Antonio Dourado de Rezende**, professor do Departamento de Ciências da Computação, Universidade de Brasília*

View the full image

Data da publicação:

Novembro de 2013

A divulgação de documentos obtidos pelo ex-funcionário de empresa contratada pela NSA, Edward Snowden, surpreendem mais pela conduta dele e pelas reações que essa conduta provocou. Snowden está soprando em um castelo de cartas que quanto mais cedo cair menos mal fará, ao menos para as vítimas mais indefesas do consequente caos. Caos que de um jeito ou de outro virá, e que está sendo gerado não por ele, mas pela alquimia financeira das treze casas bancárias que controlam a economia no mundo. Elas estão criando dinheiro sem lastro, via malabarismos eletrônicos contábeis, que furtam da moeda circulante sua função de reserva de valor enquanto a mesma é ainda mais rapidamente acumulada em contas de poucos.

Em entrevista ao portal RT o analista financeiro Max Keiser[1], experiente inovador em táticas especulativas para pregões eletrônicos, aponta para o cenário dessas revelações como ele o vê: a compania onde Snowden trabalhava, Booz Allen, junto com algumas outras parceiras são mentoras da manipulação que ocorre em importantes mercados globais de juros e de câmbio, como o LIBOR e o FOREX, e essa manipulação é o combustível que mantém o "império militar" funcionando, supondo eu que Keiser se refere aí à OTAN.

A economia dos EUA por si só não consegue mais manter suas ambições militares, e para isso essas ambições precisam manipular mercados. O tipo de inteligência que Snowden pode mostrar como se agrega, é fundamental para essas manipulações. Elas podem instrumentar a Booz Allen e suas parceiras a canalizar bilhões de dólares para irrigar campanhas militares norte-americanas. Então, essa fúria contra Snowden na verdade seria por causa de dinheiro, e não de segurança. Keiser prossegue nos lembrando que a Casa Branca é refém de Wall Street, dos fundos hedge, de banqueiros corruptos e também da Booz Allen, e que as empresas parceiras no PRISM[2] têm incentivos financeiros para participar desse programa, além dos possíveis pedágios para acesso a dados pessoais dos seus clientes.

Os índices cobiçados são sensíveis a dados econômicos. Se a Booz Allen e certas parceiras podem manipular

esses dados, podem com isso manobrar os índices que guiam os mercados – incluindo preços de ações em pregões voláteis, inclusive das suas próprias. Se a Booz Alen e certas parceiras coletam informações privilegiadas, outras parceiras podem, com tais informações, ganhar bilhões e bilhões de dólares para o esquema através de operações algorítmicas em pregões automatizados, que são efetuadas por software em altíssima velocidade, com enormes volumes e quase sempre disparadas por diminutas variações de preços, uma novidade tecnológica ainda infiscalizável e sujeita a sérias falhas[3]. É claro – para Keiser – que os grandes bancos de Wall Street e de Londres estão fazendo isso.

Assim, toda esta fúria persecutória contra Snowden pode ter causa em manobras virtuais que só darão lucro – fraudulento – enquanto houver confiança coletiva em moedas sem lastro. Não é por causa do vazamento de segredos de Estado em si, já que isso ocorre a toda hora sem que os delatores sejam importunados, inclusive a respeito deste caso[4], ou mesmo mentindo[5], se o efeito pretendido na grande mídia for o de maquiar a imagem do governo. Infelizmente, os EUA não têm mais dinheiro para financiar suas guerras e aí o governo precisa recorrer à manipulação de mercados via bisbilhotagem. Esta realidade é última coisa que aquele país quer ver vindo à tona de forma crível[6], por atos de um “insider” em fuga candidato a mártir. Pois o filão secreto de ouro (de tolo) que Keiser aponta seria, na lógica do capital, assim “roubado.”

Um despiste que circula, no argumento de que ele é traidor e por isso não merece crédito, tenta tapar o sol com peneira. Se não merece crédito, por que tanta fúria persecutória contra o jovem supostamente desequilibrado e delirante, produzindo crises diplomáticas mais parecidas com tiros no pé? A humilhação aérea ao mais digno índio aimara, o presidente Evo Morales, por exemplo, aparentemente instigada pelo embaixador americano na Áustria William Eacho[7], esbarrou no fiel de uma balança delicada do xadrez diplomático, cuja sacudida legitimou a acolhida de Snowden pelo governo da Rússia. Esse quebracabeças portanto ainda tem mais peças a encaixar.

Entre os mecanismos utilizados pelos EUA para interceptar comunicações, as backdoors de programas e sistemas operacionais proprietários são apenas uma das vulnerabilidades exploradas. Desde 2001 é sabido que o programa Echelon[8] interceptava sinais de satélite, mas hoje sabemos mais: que as backdoors agora exigidas por lei americana (CALEA)[9] nos roteadores de grande porte homologados nos EUA estendem esse vigilantismo também para quase todas as rotas de fibra óptica, centralizadas na arquitetura atual das espinhas dorsais (backbones) transcontinentais, que por decisões empresariais bordeiam os pontos de troca de tráfego nacionais. O que cobre praticamente todos os meios de transmissão digital a longa distância hoje em uso.

Mas hoje sabemos também, por revelações de Snowden[10], o que em 2001 apenas suspeitávamos (com o caso NSAKEY)[11]: que a vigilância se estende também, em capilaridade, a quase toda plataforma individual e computador pessoal, àquelas e àqueles que usam sistema operacional proprietário Microsoft Windows, neutralizando nelas e neles a única possível defesa restante, que seria a criptográfica; e capilarmente estendido também a quase todo serviço global agregado, via programa PRISM.

Uma backdoor funciona como uma porta virtual secreta, embutida em software, acionável remotamente por quem a conhece para dar passagem sorrateira a dados. Isso funciona tanto para dados copiados de dentro do sistema e enviados para quem controla remotamente a backdoor, como também para dados enviados por quem controla remotamente a backdoor para dentro do sistema, visando alterá-lo ou manipulá-lo à sorrelfa (inclusive, se for o caso, para apagar ou alterar dados de algum usuário do sistema). Em um roteador destinado a distribuir o tráfego de dados entre rotas de saída, por satélite ou por fibra óptica, por exemplo, uma backdoor pode ser programada para grampear por atacado o fluxo que por ali passe, em todo ou em partes selecionáveis por áreas de origem ou de destino, com a cópia do fluxo enviada para repositórios de agências como a NSA, que para recebê-los inaugura o maior centro de dados jamais construído para esse fim[12].

É impossível impedir a interceptação, mesmo empregando criptografia (por mais robusta que seja), se o sistema operacional rodando no computador de um dos interlocutores for fornecido por uma parceira do PRISM. E é justamente uma empresa que proíbe em contrato a engenharia reversa dos seus sistemas proprietários, blindando-se de admitir publicamente que os mesmos embutem backdoors, e que implode os mais recentes diante de qualquer tentativa de sanitizálos contra backdoors embutidos, que fornece mais de 90% desses sistemas.

Por outro lado, sem empregar criptografia é impossível impedir a interceptação, seja com sistema operacional livre ou proprietário, se a rota entre os interlocutores tiver algum ponto de passagem obrigatória por um roteador que tenha backdoor. Seja backdoor embutida pelo fabricante, o que é obrigatório nesse tipo de equipamento se o fabricante quiser que seja homologado nos EUA, seja instalado por empresa de telecomunicação que os opera, situação previsível onde tais empresas sejam parceiras de algum dos inúmeros programas de espionagem global

ou de vigilantismo militar.

É possível impedir a interceptação apenas entre plataformas auditáveis, portanto com sistemas livres e de código aberto, que sendo livres não requerem cadastramento para serem habilitadas, sanitizadas contra backdoors nas duas pontas da comunicação, combinada com o uso correto de criptografia robusta. Mas isso é relativamente possível apenas, pois tais condições são difíceis de serem garantidas, já que são relativas à competência técnica de potenciais adversários com interesse em interceptar no varejo, haja vista as ferramentas virtuais de ataque conhecidas como “zero-day exploits”[13], que proliferam num comércio cinzento aquecido pelas verbas ocultas que sustentam esses esquemas[14].

Não é por acaso que o braço brasileiro do cartel das grandes empresas de software proprietário demoniza tanto o software livre[15], que é a única alternativa para se usar a Internet de forma efetivamente protegível contra interceptação de varejo, quando devidamente sanitizada nas pontas de uma comunicação corretamente criptografada.

Não é de hoje que os braços legais dos agentes deste esquema incitam todos à devassidão digital autoconsentida, enquanto seus lobbies pressionam legislativos contra o uso autônomo da criptografia, com os quatro cavaleiros do ciberapocalipse – pornografia infantil, terrorismo, pirataria e cibercrime – servindo sempre de espantalhos.

Medidas de infraestrutura anunciadas pelo governo brasileiro (lançamento de satélite nacional, construção de cabos submarinos próprios aos EUA, Europa e África) não são suficientes para impedir a espionagem do tráfego de dados envolvendo serviços globais oferecidos por parceiros privados do programa PRISM.

Em casos envolvendo o uso de serviços globais, não há medida neutralizadora possível a não ser a do usuário optar por serviços alternativos ou semelhantes instalados e operados com tecnologia livre e adequadamente implementada e gerenciada.

Mesmo assim, o efeito de proteção será aí relativo ao poder de fogo disponível ao vigilantismo global, modulado pelo interesse nele despertável pelo perfil rastreável de quem queira se proteger. No caso de redes sociais, essa adequação requer redes federadas colaborativas[16] e ferramentas criptográficas próprias para anonimização, como aquelas oferecidas por softwares e serviços do projeto Tor[17]. Satélite nacional e cabos submarinos controlados pelo país só agregariam efeito neutralizador da espionagem e do vigilantismo global quando as duas pontas de uma comunicação internacional estiverem operando com computadores protegidos contra interceptação de varejo, ou seja, com software livre sanitizado de backdoors para conexões corretamente criptografadas.

Sem criptografia, ou com ela fraca ou incorretamente usada, o efeito neutralizador dessas medidas, no caso de comunicação doméstica, só pode ser efetivo se combinado à sanitização dos roteadores na rota do tráfego dos dados. E isso ainda não é possível aqui, devido à privatização total da infraestrutura de telecomunicações que o Brasil sofreu e à forma atual com que os equipamentos, tais como centrais comutadoras e roteadores, são homologados pela Anatel – que só checa as especificações de funcionalidade declaradas pelo fabricante. Portanto, as medidas anunciadas têm grande chance de serem, sozinhas, na prática inócuas ou irrisórias, no máximo apenas encarecendo um pouco a bisbilhotagem desbragada.

Com a arquitetura propositadamente devassa das telecomunicações no Brasil, hoje totalmente privatizada e muito mal fiscalizada, perante o alcance e o escopo do esquema de espionagem e vigilantismo denunciado por Snowden, o que se revela é um cenário de grave vulnerabilidade para o país. Um cenário cujo efeito prático nessa área é o de facilitar e baratear a bisbilhotagem, e cuja gravidade se deve a muito desleixo e descaso – não só quando somos repetidamente tungados no pré-sal[18], mas também em relação a princípios constitucionais pétreos.

Ainda, as várias ferramentas de coleta e processamento empregados nesse esquema instrumentam não só a espionagem militar clássica, a industrial e a comercial em favor das empresas do esquema e suas parceiras, mas também aplicações militares até então inéditas, como por exemplo a mineração de dados para os signature strikes, em que aeronaves remotamente controlada (VANTs ou drones) matam suspeitos rastreando-os por padrões digitais de comportamento[19], sem identificação positiva do alvo. Testados no Afeganistão e no Paquistão em mais de mil civis, esses métodos de ataque estão em amplo desenvolvimento e generalização, com mais de 40 países buscando lançar tecnologias similares[20].

Em tempos ainda de paz, propostas recentes do Ministério das Comunicações podem parecer motivo para

pilhérias em audiências legislativas, do tipo “marido traído”, mas mesmo assim tal conduta não parece prudente para membros do governo de um pais já tão espoliado como o Brasil. Se já havia no governo brasileiro quem soubesse do esquema em 2008, como indicam matérias na imprensa, sobre quem advogava e advoga terceirização frouxa para tudo tecnológico, e debocha de estratégias para defesa da soberania via autonomia tecnológica, cabe perguntar a quem interessa manter o atual ministro das Comunicações.

Cabe perguntar por que esse ministro sabotou o Programa Nacional de Banda Larga, o que fez com a infraestrutura nele erguida, e por que demitiu o mentor e gestor desse programa, um dos mais tarimbados estrategistas brasileiros com bagagem técnica para negociações internacionais. Por que enterrou esse programa, cuja importância estratégica para neutralizar a exposição de toda a comunicação digital brasileira ao esquema denunciado está muito bem explicada, em matéria de Luiz Grossman no portal Convergência Digital por exemplo[22].

Se traição à pátria no Brasil não é assunto de interesse jornalístico para a mídia corporativa, se não for mais crime, ou se é crime só para certa cor ideológica do suposto beneficiado inimigo, então podemos ao menos dizer que tal conduta de um servidor público revela vassalagem neocolonial, como denunciada em recente audiência pública no Senado sobre o tema[23], para usar um termo recém-empregado em declaração conjunta dos chefes de Estado na cúpula do Mercosul[24].

Este texto é adaptado de uma entrevista a Tadeu Breda publicada em julho de 2003 no portal de notícias Rede Brasil Atual[25]

---

1. Ver http://rt.com/op-edge/keiser-international-confidence-crumbling-snowden-182

2. Ver http://rt.com/op-edge/nsa-network-global-fascism-167/. Sobre o PRISM, ver http://pt.wikipedia.org/wiki/PRISM_%28programa_de_vigil%C3%A2ncia%29

3. Ver http://www.cnbc.com/id/48443271

4. Ver http://www.reuters.com/article/2013/06/26/us-usa-security-tactics-idUSBR...

5. Ver http://nymag.com/nymetro/news/media/features/9226

6. Ver http://br.reuters.com/article/topNews/idBRSPE96C02B20130713

7. Ver http://www.correntewire.com/obamas_austrian_ambassador_was_source_of_bad...

8. Ver http://pt.wikipedia.org/wiki/Echelon

9. Sobre a CALEA, ver http://pt.wikipedia.org/wiki/CALEA

10. Ver http://revistaforum.com.br/blog/2013/07/snowden-microsoft-colabora-ativa...

11. Sobre a backdoor NSAKEY no sistema Windows, ver http://en.wikipedia.org/wiki/NSAKEY

12. Ver https://www.youtube.com/watch?v=xLTXRF4w-Cc

13. Ver http://en.wikipedia.org/wiki/Zero-day_attack

14. Ver http://mobile.nytimes.com/2013/07/14/world/europe/nations-buying-as-hack...

15. Ver http://www.dignow.org/post/associa%C3%A7%C3%A3o-brasileira-dasempresas-d...

16. Ver http://iaesjournal.com/online/index.php/IJ-CLOSER/article/download/Cairo...

17. Ver https://www.torproject.org/index.html.en

18. Ver http://www.fazenda.gov.br/resenhaeletronica/MostraMateria.asp?cod=441160

19. Ver http://rt.com/usa/cia-drone-strikes-unknown-targets-293

20. Ver http://www.wired.com/dangerroom/2012/06/drones-south-america. Sobre o futuro da guerra baseada em "drones", ver Nick Turse e Tom Engelhardt, Terminator Planet: The First History of Drone Warfare 2001-2050, e-book

21. Ver http://www1.folha.uol.com.br/mundo/2013/07/1309366-brasil-sabedesde-2001... e também http://www.youtube.com/watch?v=aPV0kebN8o4

22. Ver http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoi...

23. Ver http://www.youtube.com/watch?v=wfPGArGoxcg

24. Ver http://www.secretariageral.gov.br/noticias/ultimas_noticias/2013/07/12-0...

25. Ver http://www.redebrasilatual.com.br

Categoria:

- poliTICs 16