3.34 • Metamorfoses da violência

O cenário de cibersegurança depois de Snowden e consequências no Brasil

Daniel Oppermann

NOS ÚLTIMOS DEZ ANOS, as discussões sobre segurança cibernética foram se focando principalmente em temas semelhantes, como os ataques *DDoS* à infraestrutura econômica ou pública, fraude online e ataques de *phishing*, mas também em espionagem na esfera política e econômica. Os delinquentes eram geralmente os mesmos, pelo menos nos meios de comunicação ocidentais e na maioria dos debates: *hackers* (muitas vezes retratados como seres antissociais pertencentes ao lado escuro), massas descontroladas de *script kiddies* e, naturalmente, agentes de Estados vilões, principalmente localizados na Europa Oriental e nos continentes asiático e africano. Como os debates sobre a segurança cibernética foram dominados por interesses ocidentais, sempre houve um consenso de que seria necessária uma proteção contra intrusos na infraestrutura ocidental. Quase ninguém estava perguntando o que o Ocidente estava fazendo por conta própria. Embora a análise do código de *Stuxnet* mostrasse que este *worm*, a arma cibernética mais poderosa descoberta até agora, foi provavelmente desenvolvido em escritórios ocidentais para destruir áreas industriais estrangeiras. Enquanto o mundo ainda está esperando que vazem mais notícias sobre o *Stuxnet*, outro incidente grave marcou os debates de segurança cibernética em 2013: as revelações da espionagem online dos EUA contra os representantes políticos, empresas e cidadãos de todo o mundo.

Os vazamentos da NSA

Em junho de 2013, o jornalista norte-americano Glenn Greenwald começou a publicar, no jornal britânico *The Guardian*, as primeiras partes do que iria se tornar o caso mais abrangente de vigilância internacional a partir da internet na história da rede. O mundo já tinha visto ou ouvido falar de algumas formas de vigilância online no passado, mas, desta vez, isso se tornou público por um país que sempre quis aparecer como um guardião da liberdade pessoal e da democracia, enquanto, na verdade, coletava secretamente dados pessoais de milhões de cidadãos de vários países, incluindo a comunicação de governos estrangeiros.

A informação que foi publicada pelo *The Guardian* e outros jornais e revistas foi fornecida por uma fonte que tinha acesso direto à comunicação de dados pessoais na rede: Edward Snowden. Snowden, 29 anos, ex-profissional informático da CIA, trabalhando através da empresa de consultoria americana Booz Allen Hamilton para a Agência de Segurança Nacional (NSA) dos Estados Unidos, explicou em uma entrevista dada a Glenn Greenwald, em Hong Kong, em 6 de junho de 2013 que, durante seu tempo na NSA (2009-2013), teve a autorização oficial para acessar aos dados de comunicação de qualquer pessoa na rede. Depois de ter percebido a dimensão da vigilância realizada pelo governo dos EUA e as condutas irresponsáveis de tratar tais dados privados, Snowden já tinha decidido, em 2008, compartilhar seu conhecimento com o público. Passaram-se mais quatro anos até que ele fez o seu primeiro contato com Glenn Greenwald, e mais alguns meses até junho de 2013, quando os primeiros detalhes foram publicados. Naquele momento, Snowden já tinha ido para Hong Kong para se proteger das autoridades norte-americanas.

Desde junho de 2013, houve frequentes atualizações no programa de vigilância do governo dos EUA. Ficou claro que as agências de segurança na Austrália, Canadá, Nova Zelândia e Reino Unido também estiveram envolvidas, juntamente com os EUA, conhecidas como os *Five Eyes* (FVEY). Varias agências de inteligência destes países estão gerenciando programas de cooperação e bancos de dados, dos quais alguns são chamados PRISM, XKeyscore, Tempora e Boundless Informant.

Programa PRISM: *Big Brother* americano

O programa PRISM (também conhecido como US-984XN) é um seguimento de um projeto de vigilância que foi oficialmente interrompido em 2007 após jornais americanos como o *New York Times* descobrirem e relatarem a interceptação pela NSA de dados de tráfego que entraram e saíram dos Estados Unidos. Com o pretexto de proteger o próprio país contra ataques terroristas, a administração Bush legalizou o PRISM em 2007 através do *Protect America Act* (que foi aprovado no mesmo ano e abriu a porta para as atividades de vigilância dos EUA em todo o mundo sem a necessidade de uma autorização judicial) e o *FISA Amendments Act* de 2008. A quarta emenda da constituição dos EUA, que inclui a proteção do indivíduo contra buscas sem decisão judicial, também foi declarada para não proteger o tráfego de dados uma vez que pertencia a cidadãos não americanos. Isso significa que pelo menos uma parte da comunicação (seja o emissor ou o receptor) pode ser um cidadão não americano. Devido à infraestrutura atual da internet, ambos os parceiros de qualquer comunicação poderiam estar fisicamente localizados fora dos EUA, no entanto, sua comunicação (seja a partir de Maputo para Brasília ou de Lisboa para Luanda) pode certamente passar através do território dos EUA, uma vez que o fluxo de dados não é definido automaticamente pela distância mais curta.

A comunicação interceptada inclui e-mails, fotos, vídeos, chats, redes sociais e muito mais. Entre os provedores mais afetados estão o Google, a Microsoft e o Yahoo. Mas a Apple, o Facebook, o Skype e outros também estão na lista da NSA. Mesmo os usuários de provedores localizados fora dos EUA não estão totalmente protegidos, uma vez que muitos provedores em todo o mundo usam a infraestrutura de telecomunicação dos EUA. Além disso, há uma variedade de outros programas que são realizados por outros países, em cooperação com os EUA, que entregam informações aos EUA.

A cooperação internacional na vigilância cibernáutica: o programa Tempora...

De acordo com Edward Snowden, não é só a NSA que está envolvida na vigilância na internet, mas também as instituições parceiras em outros países. Um dos mais importantes aliados identificado até o momento é a agência de inteligência britânica *Government Communications Headquarters* (GCHQ) com o seu programa Tempora. Portanto, a GCHQ está trabalhando em cooperação com os principais provedores de telecomunicação para interceptar o tráfego de internet em vários países. Um detalhe interessante é o fato de que, segundo o *The Guardian*, as grandes empresas de telecomunicação no Reino Unido estavam dispostas a entregar mais dados para as agências de segurança do que foram pedidos pelo *Regulation of Investigatory Powers Act* (RIPA). O RIPA está regulando a interceptação de dados de telecomunicação no Reino Unido desde 2000. Este detalhe torna o setor privado um aliado da vigilância de massa da internet, que certamente terá um impacto negativo em sua reputação pública e no relacionamento com seus clientes. A informação fornecida por Snowden mostra, além do mais, que a GCHQ está tão envolvida na vigilância através da internet quanto a NSA, e, provavelmente, ainda mais.

... o projecto XKeyscore...

Outro tijolo no *firewall* de vigilância é o XKeyscore, um projeto de cooperação entre a NSA e outras agências de inteligência como a *Defence Signals Directorate* da Austrália e a *Government Communications Security Bureau* da Nova Zelândia. O XKeyscore é um sistema de análise de dados através da interface de usuário que usa a informação reunida por diferentes meios de vigilância. Uma grande parte destes dados são e-mails capturados por varias agências ao longo dos anos, que podem ser acessados por qualquer usuário no banco de dados. Este projeto mostra perfeitamente como os países participantes estão cooperando para se apoiarem mutuamente com os dados relativos não só aos estrangeiros, mas também aos seus próprios cidadãos. Uma vez que, por exemplo, os EUA não estão necessariamente autorizados a coletar dados de comunicação entre dois cidadãos americanos, somente as

agências de inteligência do Reino Unido podem fazer isso. Como todos os dados são armazenados no mesmo banco de dados, todos os usuários têm acesso a tudo, independentemente da nacionalidade do emissor ou do receptor.

... e o programa Boundless Informant

O Boundless Informant é outra ferramenta usada pela NSA e seus aliados para organizar os dados capturados através de meios diferentes. Sua função principal é a categorização de dados separados por países de origem para torná-los pesquisáveis por qualquer agente de inteligência. Após uma captura de tela da interface do sistema publicada pelo *The Guardian*, em junho de 2013, a NSA estava em posse de mais de 97 bilhões de dados de todos os países do mundo. Pelo menos algumas centenas de milhões deles são provenientes da América do Sul, onde o Brasil é o país com a maioria de dados coletados na região durante a operação chamada *Silverzephyr*, que se concentrou em todos os países latino-americanos. De acordo com a informação publicada por Glenn Greenwald no jornal brasileiro *O Globo*, a NSA tinha um interesse especial nos dados militares e econômicos da região. A coleta de dados foi realizada através do Facebook, do Gmail, do Google (busca), do Hotmail, do Skype, do Yahoo e do YouTube. Embora, como mencionado antes, é muito provável que a comunicação através de outros provedores também tenha sido capturada.

Reações no Brasil

A vasta coleta secreta de dados realizada pela NSA e seus parceiros representa o pior dos cenários de segurança de dados e privacidade. Desde o dia em que Edward Snowden começou a publicar os detalhes sobre as atividades da NSA, as empresas em todo o mundo mais uma vez reconheceram como é vulnerável a estrutura da comunicação global e o que isso significa para os seus próprios segredos corporativos. A espionagem através da internet é muito mais comum do que a maioria das pessoas pode pensar, e está provado que vem também daqueles que pretendem proteger seus aliados através de seu avanço tecnológico, enquanto, na realidade, eles criaram um cenário de insegurança e desconfiança. Não é só a espionagem corporativa, mas também a vigilância sistemática de representantes políticos e das massas de usuários da internet em todo o mundo que contribuíram para um mundo cibernético menos confiável e, portanto, menos seguro.

Em 24 de setembro de 2013, a presidente brasileira Dilma Rousseff declarou sua indignação durante seu discurso de abertura na frente da 68ª Assembleia Geral das Nações Unidas em Nova Iorque, sobre as atividades de vigilância dos Estados Unidos no mundo. Durante seu discurso, ela também criticou as atividades de vigilância organizadas contra o Brasil. Ela sublinhou que o argumento de proteção largamente usado contra ameaças terroristas não justifica o comportamento dos EUA, uma vez que o Brasil não estava apoiando o terrorismo e vive em paz com os países vizinhos há mais de 140 anos. Segundo seu discurso, o ciberespaço não deveria ser utilizado incorretamente como um instrumento de guerra, espionagem ou sabotagem contra outros países. O conteúdo de seu discurso já tinha sido aguardado pelos analistas, uma vez que não foi a primeira vez que a Dilma abordou o tema. Em julho de 2013, o jornal *O Globo* publicou um artigo explicando como a internet brasileira e a comunicação telefônica estavam interceptadas pela NSA. No dia 1 de setembro, o jornal *O Globo* publicou outro artigo, incluindo arquivos internos da NSA que afirmavam que os EUA tinham interceptados *e-mails* e comunicações telefônicas da Presidente Dilma. Uma semana depois, no dia 8 de setembro, o mesmo jornal surgiu com a informação de que as redes de computadores da Petrobras também foram alvos da NSA. Demorou pouco mais que uma semana para o governo brasileiro analisar a situação e enviar uma resposta para Washington: em 17 de setembro, a presidente declarou oficialmente que tinha cancelada sua visita oficial a Washington, que seria no dia 23 de outubro.

> “A governança da internet é baseada na abordagem de governança multissetorial dando igual espaço para todos os atores da sociedade civil, do setor privado e dos governos.”

Também em casa, o governo brasileiro tomou medidas para prevenir uma ulterior interceptação de redes de comunicação nacionais. Em 02 de setembro, o Ministério das Comunicações declarou que estava trabalhando em um sistema nacional de e-mail que seria desenvolvido pelos serviços postais estatais, os Correios, juntamente com o Serviço Federal de Processamento de Dados (Serpro). A ideia original era desenvolver um serviço de comunicação segura para a transmissão de documentos digitais, que seria garantido por um certificado digital e que estava sendo preparado mesmo antes de as atividades da NSA se tornarem públicas. Este serviço estava se concentrando principalmente nas empresas privadas e na comunicação governamental, enquanto um sistema semelhante para os cidadãos iria ser desenvolvido depois. Devido à gravidade da situação, este plano foi modificado e, atualmente, os Correios estão trabalhando em ambos os sistemas para estar pronto em meados de 2014.

Além da criptografia de comunicação, o governo também quer reduzir o fluxo de dados de usuários brasileiros da internet através de servidores com base nos EUA. Por esta razão, a presidente Dilma pediu à Câmara dos Deputados, por meio de nota oficial em 11 de setembro, para decidir sobre o Marco Civil da Internet, um projeto de lei que inclui passagens relativas à privacidade, liberdade de expressão e neutralidade da rede, mas também regras para o serviço de provedores estrangeiros, para armazenar dados de clientes brasileiros no Brasil, em vez de transferi-los para servidores fora do país. No entanto, é muito provável que especialmente esta última ideia tenha sido desenvolvida mais em luz da próxima campanha eleitoral presidencial de 2014, do que pela competência técnica.

Depois de sua reunião em Brasília em 9 de outubro, a presidente Dilma anunciou, juntamente com o CEO da ICANN, Fadi Chehadé, a intenção de convidar os representantes de todos os setores da sociedade a participar em um congresso internacional sobre a governança da internet, a decorrer em 2014. A ICANN, a *Internet Corporation for Assigned Names and Numbers*, está atualmente em um processo de reestruturação para entregar mais influência para os atores de países que no passado não foram igualmente representados na organização. As posições firmes do Brasil em relação às atividades da NSA estão oferecendo à ICANN um parceiro forte na América do Sul. Embora seja uma abordagem positiva pela ICANN transferir partes de seu trabalho para países como a Singapura, a Índia, a Turquia e o Uruguai (como aconteceu nos últimos meses) e, em seguida, abrir um diálogo com novos parceiros, como o Brasil, é importante considerar um detalhe crucial. A governança da internet é baseada na abordagem de governança multissetorial dando igual espaço para todos os atores da sociedade civil, do setor privado e dos governos. Quando a presidente Dilma falou na frente da ONU, ela se referiu a uma abordagem multilateral, em vez de uma abordagem multissetorial. Embora ela tenha mencionada a importância de outros atores, sua escolha de palavras também apontou para uma determinada direção, que não está principalmente a favor da sociedade civil, do setor privado e dos usuários de internet. Parecia mais uma tentativa de tomar o controle de certas partes da infraestrutura da internet das mãos de um governo, mas não com a intenção de entregá-lo à sociedade e ao setor privado, mas para outros governos. Se este for o caso, as consequências da vigilância da NSA poderiam se tornar uma nacionalização da infraestrutura fundamental de TI em vários países. Já existe um número crescente de governos que começaram nos últimos anos a assumir o controle sobre a internet em seus próprios países, desenvolvendo certas medidas de controle técnico. Caso as atividades da NSA sejam usadas pelos governos para justificar medidas nacionais para proteger seus próprios dados, a internet se tornará um lugar cada vez mais restrito em um futuro próximo. ■