O Cap Jason Smith e o Sgt Clinton atualizam software de antivírus de Unidades da Força Aérea para a prevenção de hackers no ciberespaço, na base aérea de Barksdale, Louisiana. (Força Aérea dos EUA/Sgt Cecílio Ricardo)

A Cibersegurança
Já Não é Apenas para Oficiais de Comunicações

Ten Cel (Res) D. Bruce Roeder, Exército dos EUA

O Ten Cel D. Bruce Roeder, da Reserva Remunerada do Exército dos EUA, é instrutor no Departamento de Ensino a Distância no U.S. Army Command and General Staff College, no Forte Leavenworth, Kansas. É bacharel pela Academia Militar dos EUA e mestre pela Webster University. Serviu anteriormente em várias funções operacionais, de Polícia do Exército e de segurança.

"SIGO!" ("O Com!") foi o BRADO que surgiu no jantar da Unidade quando o microfone estridente não funcionou, durante um discurso público na plataforma do salão de baile no clube dos oficiais. O pessoal das Armas combatentes sorriu aliviado enquanto o coitado do O Com (*signal officer* — oficial de comunicações [O Com]) se esforçou determinadamente para conseguir que o componente defeituoso no equipamento funcionasse como deveria. Isso é como alguns de nós abordam o assunto de

cibersegurança: é o campo de atividade de um *nerd*. E graças a Deus!

Ora, se era assim, agora já não é mais. Quando o Diretor da Inteligência Nacional, James R. Clapper, promulgou a *Worldwide Threat Assessment of the US Intelligence Community* ("Avaliação de Ameaças Mundiais da Comunidade de Inteligência dos EUA", em tradução livre), de 2013, para o Comitê Seleto de Inteligência do Senado dos EUA, a ameaça cibernética aparecia na frente do terrorismo e das armas de destruição em massa em sua lista de ameaças globais à Segurança Nacional do país[1]. De fato, os ataques cibernéticos estão constantemente nas notícias. Perito em cibersegurança, o oficial da Reserva finlandesa Mikko H. Hyppönen postula que, nos países em desenvolvimento, é provável que as pessoas estejam sendo vítimas de crime on-line, em vez de crimes "verdadeiros"[2]. Com a natureza onipresente das interações *on-line* na vida moderna, a ameaça cibernética, ou ciberameaça, é uma ameaça de maior importância à segurança dos indivíduos e da nação. Então, como se saiu aquele O Com desesperado e seus esforços para fazer com que o equipamento funcionasse devidamente?

Bem, vamos dar uma olhada na situação difícil que o nosso O Com enfrenta. Primeiro, em termos simples, três tipos básicos de atacantes cibernéticos representam uma ameaça: os criminosos, os ideólogos e os Estados-nação. Geralmente, os criminosos profissionais estão motivados pela ganância. Eles se encaixam sob a jurisdição da lei, embora a tecnologia que empregam costume estar além das capacidades das agências policiais comuns. A próxima categoria é dos ideólogos e os assim chamados "hacktivistas", como *WikiLeaks* ou *Anonymous*, que geralmente estão motivados por uma visão mundial política ou filosófica, ou talvez pelo ceticismo. Frequentemente, anunciam seus alvos e, às vezes, conduzem ataques simplesmente para ganhar atenção ou para serem engraçados. A lei os trata como criminosos, também. O terceiro tipo é dos Estados-nação que são usualmente motivados pela segurança, pela economia, ou por outros interesses, podendo planejar e executar ataques cibernéticos coordenados contra seus inimigos, pois, geralmente, têm acesso a mais recursos do que os criminosos e os ideólogos.

Contudo, não é sempre fácil relacionar atacantes cibernéticos a categorias definidas. O que mais gera dúvida é a questão aberta de saber se um ciberataque é um emprego da força ou não.

Além disso, é difícil determinar quais ameaças cibernéticas são mais perigosas para a Segurança Nacional dos EUA e quais são as mais prováveis de causar prejuízo. As ciberameaças específicas surgem de formas inesperadas. Por exemplo, o *Stuxnet*, o *malware* diabolicamente destrutivo que visou os centrifugadores na instalação de enriquecimento de urânio em Natanz, no Irã, hoje representa uma ameaça bem maior, além do seu propósito original. Isso é porque o código usado para construir o *Stuxnet* (descoberto em 2010 e amplamente considerado como um ciberataque patrocinado por um Estado) foi vazado inadvertidamente na internet. Alguns analistas acreditam que seus descendentes (como Duqu e Flame) já podem estar residindo nos bancos de dados de infraestruturas críticas por todo o mundo[3]. As coisas más que estão acontecendo estão além do conjunto de habilidades ou de recursos de qualquer O Com. Como devemos responder a esta questão?

Mais Burocracia?

A resposta típica, e até obrigatória, do governo é proporcionar a um órgão ou agência a responsabilidade e os recursos para remediar o problema. Essa abordagem previsível, lenta e de cima para baixo para resolver problemas no nível nacional é ineficaz contra um problema incerto, de mudanças rápidas e de baixo para cima. Por exemplo, o Departamento de Defesa estabeleceu o Comando Cibernético dos Estados Unidos (USCYBERCOM), um comando subunificado e subordinado ao Comando Estratégico dos EUA, sendo as Forças Singulares organizadas devidamente para prover o apoio necessário: o Exército com o Comando Cibernético do Exército, a Marinha com o Comando Cibernético da Frota dos EUA, a

Força Aérea com a 24ª Força Aérea (Cibernética das Forças Aéreas) e o Corpo de Fuzileiros Navais com o Comando Cibernético das Forças de Fuzileiros Navais. No entanto, independentemente das capacidades dessas Unidades, elas concentram-se principalmente nas ameaças de cibersegurança às redes de informações da Defesa dos EUA. Por outro lado, "o governo frequentemente não se percebe das atividades maliciosas que visam a atingir nossa infraestrutura crítica", disse o Gen Ex Keith Alexander, antigo Diretor da Agência de Segurança Nacional e do USCYBERCOM[4].

Quando se trata do setor civil, o Deputado dos EUA Mike Rogers, do Estado de Michigan, diz que "hoje, estamos engajados em uma guerra cibernética [...] e estamos perdendo"[5]. Contudo, não há dúvida de que os chefes empresariais dos EUA estão percebendo que a ameaça cibernética é verdadeira e que caberia a eles trabalhar estreitamente com o governo para evitar um grande ataque ou estar pronto para responder efetivamente. Para eles, se algo afeta seus lucros, torna-se importante. Mesmo assim, as empresas atualmente têm pouco incentivo para alertar as autoridades federais, depois de serem alvos de um *hacking* (ataque cibernético), pois o governo logo compartilharia essa informação com seus competidores. Além do mais, se as empresas compartilham certas informações com alguns de seus competidores, arriscam ser processados pelo governo baseado nas leis *antitrust* [Leis nos EUA que têm por objetivo eliminar práticas anticompetitivas e diminuir os monopólios — N. do T]. Portanto, a não ser que as empresas tenham alguma proteção da responsabilidade legal ou contra a perda da vantagem competitiva, é improvável que trabalhem juntos voluntariamente. As proteções legais precisam ser estabelecidas pelo Congresso, porém nenhuma legislação de segurança cibernética foi aprovada desde 2002. Em 12 de fevereiro de 2013, o Presidente Obama promulgou a ordem do poder executivo chamada "Improving Critical Infrastructure Cybersecurity" ("Melhorando a Infraestrutura Crítica da Cibersegurança", em tradução livre). Mesmo quando o Congresso age, a participação permanecerá sendo, com quase toda a certeza, de carácter voluntário por parte dos proprietários civis da infraestrutura econômica[6]. O cuidado e o sustento do aparelho de cibersegurança do governo (incluindo os terceirizados afiliados), quase com certeza, nos

Foto de Jeff Scaparra

Dois cadetes da Academia da Força Aérea discutem defesas de redes durante uma competição regional chamada Defesa Cibernética Universitária Nacional, 06 Mar 11.

capacitarão a obter e a manter o contato com a ameaça cibernética, mas é improvável que esse aparelho seja capaz de eliminar a iniciativa do inimigo. Parece que estamos atacando o problema como um macaco solto em uma loja de louças. A solução do problema requererá algo mais.

A característica principal da *World Wide Web* é de que trata-se de uma rede mundial, sendo o seu principal ponto forte o seu caráter internacional. É essa mesma característica que permite que hacktivistas, os criminosos cibernéticos e o seu dinheiro passem rapidamente de um país para outro, enquanto seus sites da internet são meticulosamente identificados e desmantelados. É essencial, para um esforço de cibersegurança efetivo, ter a mesma capacidade de atravessar jurisdições internacionais. As agências precisam ser capazes de coordenar suas ações com as agências semelhantes por todo o mundo com a mesma agilidade dos criminosos. O site da internet do Instituto Inter-regional das Nações Unidas para Pesquisas sobre Delinquência e Justiça (UNICRI) oferece discernimentos sobre como tal abordagem operacional talvez seja capaz de funcionar[7]. Embora o UNICRI seja um órgão pequeno e de recursos limitados dentro das Nações Unidas, essa organização está, no mínimo, olhando na direção certa.

Contratar os Hacktivistas?

O jornalista Misha Glenny entrevistou vários criminosos cibernéticos. Ele não apenas constatou que as instituições incumbidas da tarefa de proteger-nos do crime cibernético fazem um trabalho mal feito em dissuadir, descobrir e investigar casos, mas também que talvez elas resistam em encontrar a chave para uma solução[8]. A avaliação de Glenny é que temos um excesso de tecnologia concentrada no problema, mas uma falta de Inteligência humana. Continuamos a gastar bilhões de dólares em soluções demasiadamente tecnológicas para a cibersegurança, porém ele propõe que analisemos as características e as capacidades dos hacktivistas no cerne do problema. Embora o hacktivista seja apenas uma parte da ameaça geral de cibersegurança, essa pode ser a mais vulnerável. Muitas pessoas na atividade de *hacking* não são mafiosos almejando a vida boa, mas gênios matemáticos acanhados e socialmente desajeitados que, em seu ponto de vista, estão inclinados a serem influenciados por patrocinadores mais sofisticados do que eles. Glenny oferece alguns fatos recentes relacionados com vários criminosos cibernéticos, incluindo o escocês Gary McKinnon, o ucraniano Dimitry Golubov, o cingalês Renukanth Subramaniam, o norte-americano Max Vision, o nigeriano Adewale Taiwo e o turco Cagatay Evyapan. Ele descreve algumas qualidades compartilhadas entre eles e muitos outros hacktivistas. Essas incluem capacidades avançadas de matemática e ciência, bem como habilidades aprimoradas de *hacking* de computadores desenvolvidas durante sua juventude, antes da formação das suas bases morais. Também, curiosamente, ele salienta características coerentes com a síndrome de Asperger, uma forma branda do autismo, bem como sua depressão constante. Frequentemente, essas deficiências no mundo real parecem acompanhar habilidades maravilhosas no mundo virtual de *hacking* de computadores. Ao escolher processar e punir esses gênios, em vez de atraí-los e contratá-los, os Estados Unidos estão punindo e alienando sua melhor chance de encontrar e remediar os problemas que os afligem, diz o argumento. Glenny apresenta um argumento convincente de que, às vezes, ao contrário, devemos considerar contratá-los — como fazem nossos adversários. A China, a Rússia e outros países, ele afirma, recrutam e empregam essas pessoas talentosas antes e depois do seu envolvimento no crime cibernético. Esses países os mobilizam para trabalhar para o Estado, enquanto nós continuamos a depender do nosso sistema penal para investigar e puni-los[9].

Ter um Plano de Contingência?

O experiente engenheiro de informática Danny Hillis advertiu, no início de 2013, que embora gastemos uma grande quantidade de energia e atenção concentrada na proteção de computadores na internet, pensamos pouco sobre a segurança da própria internet como um meio[10]. Hillis considera a internet como um sistema emergente. Ele diz que não a compreendemos completamente, como o tempo e a economia: "ela muda tão rápido que até os peritos não sabem exatamente o que está acontecendo"[11]. Ele diz que devido à maneira como a internet se expandiu, nem sabemos como um ataque efetivo de negação de serviço nos afetaria, então precisamos de "um plano de contingência"[12].

A boa notícia é que um sistema de reserva, baseado em um plano básico alternativo em que os serviços essenciais podem continuar a transmitir e a funcionar, deve ser relativamente fácil de projetar, segundo

Hillis[13]. Embora ele não ofereça detalhes de como pode ocorrer, os planejadores da cibersegurança que trabalhavam durante o susto de Y2K (referindo-se aos efeitos danosos antecipados do *bug* do milênio) podem exumar seu velho plano. Isso proporcionaria um bom começo. Os planos de contingência variariam segundo o setor da infraestrutura envolvida. Ter planos de continuidade independentes das operações baseadas em computadores, e mantê-los atualizados regularmente, pode prover uma mínima proteção na pior das hipóteses. Os planos podem, também, ser meios para soluções criativas de problemas em uma organização. A mentalidade resistente no cerne dos esforços recentes do Exército de melhorar a aptidão abrangente dos soldados pode ser aplicada à nossa infraestrutura crítica nacional, bem como à nossa saúde mental pessoal. O desenvolvimento de setores essenciais de infraestrutura bem equilibrados, fortes e confiáveis, cuja resistência e bem-estar total os capacitam a proliferar em uma era de alta troca de informações e de ameaças constantes, não é difícil de fazer. De fato, é uma meta fidedigna, dentro do nosso alcance.

Exército dos EUA, Sgt Candice Harrison

O Sgt Kenneth Tecala e o Oficial Especialista Ben Carmichael, da 2ª Brigada de Combate/1ª Divisão Blindada localizam avarias no sistema de Advertência de Foguetes, Artilharia e Morteiros durante a Avaliação de Integração de Redes 13.1 no Polígono de Tiros McGregor, Novo México, 13 Nov 12.

De fato, Chegamos Atrasados à Festa

Ainda permanece incerto se podemos, ou por quanto tempo podemos, evitar um ataque cibernético. Considerando a natureza da ameaça, a onipresença e a vulnerabilidade da internet e de nossos computadores e os nossos recursos limitados, nossa chance de sucesso talvez pareça mínima. Contudo, alguns de nós, no governo ou nas Forças Armadas, estamos cientes dos assuntos de cibersegurança há muito tempo. Conduzimos instrução anual on-line obrigatória para mostrar nosso conhecimento sobre segurança de computadores e das informações. De fato, para os militares, parece que o velho O Com está se vingando por todos os jantares de Unidade do passado. Portanto, podemos abordar a cibersegurança com a perspectiva de que todos os militares estarão receptivos à antecipação e superação dos desafios da prontidão, se não bem preparados para responder a uma crise de cibersegurança. O relatório de 2013, do Diretor de Inteligência Nacional foi um importante marco e uma convocação para a ação (a atualização

de 2014 ainda coloca ameaças cibernéticas em primeiro lugar na lista). Da mesma forma que a segurança física é uma responsabilidade inerente e não somente o trabalho do chefe da Polícia do Exército, também a cibersegurança não é o campo unicamente dos *nerds*; pertence a todos nós. Qualquer um que, erroneamente, arquivou a cibersegurança na caixa de entrada do O Com deve ligar para seu próprio escritório. O palco é nosso, e o O Com é cada um de nós.

Referências

1. Director of National Intelligence James R. Clapper, statement for the record to the Senate Select Committee on Intelligence, Worldwide Threat Assessment of the US Intelligence Community (12 Mar. 2013), disponível em: https://www.hsdl.org/?view&did=732599.

2. Mikko H. Hypponen, *Three Types of Online Attack* (November 2011), on-line vídeo no site da internet Technology, Entertainment, and Design (TED), disponível em: http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.html.

3. Ralph Langner, *Cracking Stuxnet, a 21st-century Cyber Weapon* (February 2011), on-line vídeo no site da internet Technology, Entertainment, and Design (TED), disponível em: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon; site da internet da Kaspersky Lab website, *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected* (11 Jun. 2012), disponível em: http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

4. Ann Flaherty, "Feds Roll Out Cyber Plan as Hill Vows Legislation," *Associated Press, The Big Story* (13 Feb. 2013), disponível em: http://bigstory.ap.org/article/white-house-revealing-obamas-cybersecurity-plan.

5. Mike Rogers, "America is Losing the Cyber War vs. China," orinalmente no *Detroit News*, 8 Feb. 2013, reproduzido na internete pelo Congressista Mike Rogers, disponível em: http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=319502.

6. President, Executive Order no. 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* (12 Feb. 2013), disponível em: https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

7. Site da internete do United Nations Interregional Crime and Justice Research Institute, *About UNICRI*, disponível em: http://web2012.unicri.it/institute/.

8. Misha Glenny, *Darkmarket: How Hackers Became the New Mafia* (New York: Vintage Books, 2012), p. 271.

9. Ibid., p. 269.

10. Danny Hillis *The Internet Could Crash. We need a Plan B* (February 2013), on-line vídeo do site da internet Technology, Entertainment, and Design (TED), disponível em: http://www.ted.com/talks/danny_hillis_the_Internet_could_crash_we_need_a_plan_b.html.

11. Ibid.

12. Ibid.

13. Ibid.