informações que lhe ajudem a decidir sobre a terceirização da segurança e a localizar serviços de terceirizados de segurança.

- Apresente um breve resumo dos argumentos a favor e contra a terceirização da segurança computacional para sua empresa.
- Selecione duas empresas que ofereçam esse tipo de serviço, comparando as empresas e seus serviços.
- Prepare uma apresentação eletrônica para a gerência, resumindo suas conclusões. Sua apresentação deverá indicar por que acredita que deveriam optar (ou não) pela terceirização da segurança computacional da empresa. Se você acredita que sua empresa deve terceirizar, a apresentação deve identificar quais serviços de terceirização escolheu e justificar sua decisão.

RESOLVENDO PROBLEMAS ORGANIZACIONAIS

A ameaça iminente de uma guerra cibernética

"Agora os nossos inimigos também estão buscando capacitação para sabotar nossa rede elétrica, nossas instituições financeiras e nossos sistemas de controle de tráfego aéreo. Não podemos olhar para trás daqui alguns anos e perguntar por que não fizemos nada diante dessas reais ameaças à nossa segurança e à nossa economia."

Com essas palavras, em seu discurso para os Estados da União, em 2013, Barack Obama tornou-se oficialmente o primeiro presidente norte-americano da guerra cibernética. Obama estava prestes a assinar a ordem de execução das melhorias da segurança cibernética da infraestrutura crítica, que permite que as empresas associadas à supervisão de redes elétricas, barragens e instituições financeiras participem voluntariamente de um programa para receber informações confidenciais e não confidenciais sobre ameaças de segurança cibernéticas, anteriormente disponíveis apenas aos fornecedores de produtos utilizados para defesa pelo governo. A principal desvantagem é que só a legislação pode impor os requisitos da segurança mínima para as empresas do setor privado, que opera a maior parte da infraestrutura crítica dos Estados Unidos. Infelizmente, em 2012, o Congresso norte-americano não conseguiu aprovar dois projetos de lei sobre segurança cibernética que eram muito mais sólidos, curvando-se à pressão de empresas preocupadas com o crescente custo de segurança além de preocupações levantadas pelos defensores da privacidade.

A guerra cibernética é mais complexa do que as guerras convencionais. Embora muitos alvos potenciais sejam militares, as redes de energia, os sistemas financeiros e as redes de comunicação de um país também podem ficar inoperantes. Agentes não estatais, como grupos de terroristas ou de criminosos, podem planejar ataques, sendo muitas vezes difícil identificar quem é o responsável. As nações devem estar constantemente alertas com relação a novos *malwares* e outras tecnologias que poderiam ser usados contra elas, e algumas dessas tecnologias desenvolvidas por grupos de hackers habilidosos são abertamente oferecidas para venda aos governos interessados.

A escala e a velocidade dos ataques cibernéticos têm aumentado nos Estados Unidos e em outras partes do mundo. De setembro de 2012 a março de 2013, pelo menos 12 instituições financeiras dos Estados Unidos — Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, HSBC, J.P. Morgan Chase e American Express — foram alvo de ataques que tornaram seus servidores mais lentos, em razão de um rastreamento, e depois derrubaram esses servidores. A severidade reduziu a magnitude dos ataques distribuídos aos anteriores de recusa de serviços (DDoS). Os data centers dessas organizações tinham sido infectados com um *malware*, disponível por muito tempo, chamado Itsoknoproblembro, que cria botnets de servidores escravos, apelidados de bRobots, porque eles são muito difíceis de serem rastreados de modo reverso a um servidor que os comanda e os controla (C&C). Os bRobots sobrecarregaram os sites dos bancos com dados criptografados. Uma sobrecarga de solicitações criptografadas intensifica imensamente a eficácia do ataque, permitindo que os atacantes derrubem o site com um número menor de requisições.

O objetivo dos ataques foi provocar um nível de tensão inédito no maior número de instituições financeiras possível. Nenhuma informação sobre as contas foi roubada e nenhum lucro financeiro foi visado, levando os peritos a pensar que foi um ataque patrocinado pelo Estado. O grupo de hackers Izzad-Din al-Qassam Fighters reivindicou a responsabilidade, afirmando que foi uma retaliação por um vídeo contra o Islamismo. Os oficiais do governo norte-americano acreditam que o agressor é, na verdade, o Irã, promovendo uma retaliação às sanções econômicas impostas para deter seu programa nuclear e ao que ele acredita terem sido ataques cibernéticos dos Estados Unidos.

Em agosto de 2012, o vírus Shamoon infectou 30 mil máquinas em uma empresa de petróleo da Arábia Saudita, a Aramco. Ele destruiu as estações de trabalho, sobrescrevendo o *Master Boot Record* (MBR — registro de inicialização mestre), que armazena informações importantes sobre a unidade de disco rígido para ajudar a inicialização do sistema do computador. Shamoon também excluiu dados em servidores e sobrescreveu determinados arquivos com uma imagem da bandeira norte-americana em chamas. Autoridades dos Estados Unidos atribuíram o ataque ao Irã.

Menos de duas semanas depois, a empresa de gás natural do Qatar, a RasGas, foi forçada a desativar seu site e sistemas de e-mail por conta de um ataque atribuído inicialmente também ao Shamoon. Uma equipe de investigação concluiu que era bem provável ser uma cópia do ataque anterior, tentando se parecer com o mesmo invasor. Funcionários do governo dos Estados Unidos culparam os hackers iranianos. Autoridades israelenses atribuíram ambos os ataques à guarda cibernética do Irã, formada após o *worm* Stuxnet.

O *worm* Stuxnet foi descoberto em junho de 2010, e acredita-se que ele foi desenvolvido por uma operação secreta conjunta entre os Estados Unidos e Israel. Ele foi projetado para desativar o software que controla as centrífugas da Siemens para enriquecer urânio, o que supostamente iria atrasar a capacidade do Irã de fabricar armas nucleares em até cinco anos. O Irã também tem sido alvo de outro *malware*. O *worm* Duqu, descoberto em setembro de 2011, rouba certificados digitais usados para autenticação a fim de ajudar futuros vírus a parecerem um software seguro. Em abril de 2012, outro *malware* de espionagem, intimamente relacionado com Stuxnet e Duqu, chamado Flame, foi descoberto quando os discos rígidos do Ministério do Petróleo do Irã e da Companhia Nacional do Petróleo iraniano foram apagados. Quatro meses mais tarde, os investigadores descobriram que o agente de eliminação de dados que eles estavam procurando, quando foi descoberto o Flame, era um agente de *malware* separado chamado Wiper. Os investigadores acreditam que o objetivo principal do Wiper era erradicar o *malware* criado por esse grupo.

Crimes cibernéticos surgem com uma desvantagem considerável. *Malwares* lançados anteriormente são recuperáveis e podem ser adaptados e reutilizados tanto por inimigos do Estado-nação como por criminosos cibernéticos não afiliados. O código do Stuxnet foi adaptado para uso em crime cibernético financeiro. Outra desvantagem é a falta de controle. Cerca de 60% das infecções conhecidas do Stuxnet ocorreram no Irã, mas 18% foram na Indonésia, 8% na Índia e os 15% restantes espalhados em todo o mundo. Em novembro de 2012, a Chevron admitiu que sua rede foi infectada com o Stuxnet pouco tempo depois de ele se espalhar para além do Irã.

Para as autoridades norte-americanas, os ataques ao setor financeiro, à Aramco da Arábia Saudita e à Rasgas sinalizaram uma mudança na política iraniana de defesa contra o crime cibernético. Depois de investir aproximadamente US$ 1 bilhão em sua guarda cibernética em 2012 (o que ainda representa apenas um terço dos gastos dos Estados Unidos), o Irã pode ter se tornado uma potência cibernética de primeiro nível.

A China tem sido uma potência cibernética de primeiro nível há vários anos. Alvos norte-americanos de suspeitas de ataques cibernéticos chineses incluem departamentos federais (segurança interna, Estado, energia, comércio); altos funcionários (Hillary Clinton, Almirante Mike Mullen); laboratórios de armamento nuclear (Los Alamos, Oak Ridge); fabricantes de produtos usados para defesa (Northrup Grumman, Lockheed Martin); organizações jornalísticas (*The Wall Street Journal*, *The New York Times*, *Bloomberg*); empresas de tecnologia (Google, Adobe, Yahoo); multinacionais (Coca-Cola, Dow Chemical); e simplesmente quase todos os outros nós do comércio, infraestrutura ou autoridade norte-americana. Os hackers obtiveram informações sensíveis, tais como estratégias de negociação de grandes corporações; projetos de mais de 24 dos principais sistemas de armamento dos Estados Unidos, incluindo o avançado sistema de mísseis Patriot, os sistemas de defesa de mísseis balísticos Aegys, da Marinha, o avião de combate F/A-18, o V-22 Osprey, o helicóptero Black Hawk e o F-35 Joint Strike Fighter; além do funcionamento da rede de energia elétrica norte-americana, possivelmente estabelecendo bases para atos de sabotagem. Ataques cibernéticos oriundos da China e de outras nações têm persistido porque os Estados Unidos apresentam dificuldades em defender os seus sistemas de informação; o ciberespaço ainda não está sujeito às normas internacionais, e anos de invasões provocaram pouca reação norte-americana.

Os investigadores acreditam que, em setembro de 2012, um dos grupos de hackers de elite do Exército de Libertação Popular da China (*People's Liberation Army* — P.L.A.) atacaram a Telvent, empresa que monitora empresas de serviços públicos, estações de

tratamento de água e mais da metade dos oleodutos e gasodutos na América do Norte. Seis meses depois, os peritos da Telvent e do governo ainda não sabiam se o motivo era espionagem ou sabotagem. Especialistas de inteligência dos Estados Unidos acreditam que os investimentos da China nos Estados Unidos, particularmente os investimentos recentes e substanciais em petróleo e gás, impedirão os ataques da China à infraestrutura. A economia chinesa não poderia escapar das consequências negativas resultantes de uma parada significativa dos sistemas de transportes dos Estados Unidos ou dos mercados financeiros. O Irã, sem investimentos nos Estados Unidos, é uma ameaça muito maior. Além disso, os canais diplomáticos estão abertos em relação à China.

Menos de uma semana depois do Discursos sobre o Estado da União, por Obama, a empresa de segurança Mandiant divulgou detalhes sobre um grupo, que eles apelidaram de "APT1". A Mandiant rastreou o APT1 até um prédio em Xangai. Documentos da China Telecom indicavam ter sido construído ao mesmo tempo em que surgiu a unidade 61398 do P.L.A., que é a unidade militar de *hacking* — o segundo escritório do terceiro departamento do General Staff Department da China. Equipado com uma infraestrutura de fibra óptica de alta tecnologia, esse edifício branco de 12 andares de escritórios foi considerado a origem de uma ofensiva que durou seis anos e que se infiltrou em 141 empresas em 20 setores.

A preocupação crescente do governo Obama com os riscos de segurança econômica e nacional impostos por invasões cibernéticas tem sido repetidamente expressa às principais autoridades chinesas. Em maio de 2013, o relatório anual do Pentágono dirigido ao Congresso norte-americano acusou diretamente, pela primeira vez, o governo chinês e a P.L.A. de atacar o governo dos Estados Unidos e a rede de fabricantes de produtos de defesa. O confronto direto havia sido contornado porque os Estados Unidos querem a ajuda da China a lidar com a ameaça nuclear e militar da Coreia do Norte e com as sanções contra o Irã. Obama voltou a levantar a questão durante sua cúpula informal com o primeiro ministro chinês Xi Jinping em junho de 2013.

Dois meses antes, no entanto, a Coreia do Norte, outro adversário da guerra cibernética embrionária, foi acusada de ter deflagrado seu ataque mais prejudicial até então. Apesar dos obstáculos que limitam a sua capacidade de desenvolver competências, incluindo sanções que restringem seu acesso à tecnologia, e um talento limitado em decorrência das políticas escassas de penetração da Internet e de acesso restrito, acredita-se que a Coreia do Norte teria deflagrado ataques às instituições comerciais, educacionais, governamentais e militares, tanto da Coreia do Sul quanto dos Estados Unidos. Em março de 2013, 32 mil computadores em três grandes bancos sul-coreanos e as duas maiores emissoras de televisão foram afetados. Sites de bancos foram temporariamente bloqueados, telas de computador ficaram em branco, os caixas eletrônicos falharam e o comércio foi interrompido.

Os atacantes usaram o *exploit kit* (conjunto de ferramentas que exploram vulnerabilidades) Gondad, escrito em chinês, para infectar PCs com um cavalo de Troia que fornece uma porta de entrada para que o invasor assuma o controle da máquina, criando um bot ou computador zumbi. Uma vez que a "porta dos fundos" digital é criada, o controlador pode depositar uma carga de *malware*, nesse caso, um agente limpador chamado Dark Seul. Como o Shamoon, o Dark Seul sobrescreve o *master boot record* (MBR). Não há nenhuma prova conclusiva implicando a Coreia do Norte, mas as tensões tinham se agravado entre os dois países. A administração de Kim Jong-un havia manifestado sua raiva nos dias que antecederam o ataque em questão, em relação aos exercícios de treinamento militar de rotina realizados em conjunto pela Coreia e pelos Estados Unidos, agravados pela participação da Coreia do Sul nas sanções promovidas pelas Nações Unidas, sob a liderança dos Estados Unidos, contra a Coreia do Norte em virtude de seu teste nuclear conduzido no mês anterior. Seoul afirma que Pyongyang teria efetuado seis ataques cibernéticos anteriores, desde 2009. Os especialistas em segurança do recém-formado centro de comando de segurança cibernética da Coreia do Sul acreditam que a Coreia do Norte vem reunindo e treinando uma equipe de milhares de indivíduos na guerra cibernética, e os Estados Unidos concordam. Para a Coreia do Norte, a ameaça de retaliação cibernética é insignificante. O acesso à Internet somente agora está se estendendo a um número maior do que alguns poucos privilegiados, as empresas estão apenas começando a adotar o uso de banco on-line, e alvos valiosos são praticamente inexistentes.

O governo Obama já começou a ajudar aliados da Ásia e do Oriente Médio a construir as suas defesas de rede de computadores contra o Irã e a Coreia do Norte, incluindo fornecimento de hardware, software e programas de treinamento avançado. Futuros jogos de guerra conjunta incluiriam ataques cibernéticos simulados, mas dissuadir ataques cibernéticos é um problema muito mais complexo do que a guerra convencional, e os funcionários dos Estados Unidos admitem que esse esforço é uma experiência.

Enquanto o aumento da pressão diplomática e da natureza entrelaçada das duas maiores economias do mundo pode produzir um acordo possível entre a China e os Estados Unidos, a forma de lidar com os chamados "atores irracionais" — Irã e Coreia do Norte — é mais espinhosa. Como a China é o maior parceiro comercial da Coreia do Norte e seu aliado mais

importante, elaborar um acordo com a China pode ser o primeiro passo em direção à condução da Coreia do Norte. Enquanto o Irã está isolado diplomaticamente, a China depende dele para satisfazer as suas necessidades energéticas. A China anda na corda bamba entre a economia iraniana ou seguir as sanções das Nações Unidas pelas quais votou. É bem provável que o caminho para acordos entre Pyongyang e Teerã passe por Pequim. Enquanto isso, o comando militar responsável pela maior parte dos esforços de guerra cibernética dos Estados Unidos, o U.S. Cyber Command (Cybercom), terá um aumento previsto de 500% de mão de obra entre 2014 e 2016.

Fontes: Julian E. Barnes, Siobhan Gorman, e Jeremy Page, "U.S., China Ties Tested in Cyberspace", *Wall Street Journal*, 19 fev. 2013; David Feith, "Why China Is Reading Your Email", *Wall Street Journal*, 19 mar. 2013; Thom Shanker e David E. Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers", *New York Times*, 8 jun. 2013; Mark Clayton, "New clue in South Korea cyberattack reveals link to Chinese criminals", *Christian Science Monitor*, 21 mar. 2013; Siobhan Gorman e Siobhan Hughes, "U.S. Steps Up Alarm Over Cyberattacks," Wall Street Journal, March 12, 2013; Siobhan Gorman e Julian E. Barnes, "Iran Blamed for Cyberattacks: U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy Firms", *Wall Street Journal*, 12 out. 2012; Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks", *New York Times*, 20 mar. 2013; Rachael King, "Stuxnet Infected Chevron's IT Network", *Wall Street Journal*, 8 nov. 2012; Mark Landler e David E. Sanger, "U.S. Demands China Block Cyberattacks and Agree to Rules", *New York Times*, 11 mar. 2013; Youkyung Lee, "Experts: NKorea training teams of 'cyber warriors", Associated Press, 24 mar. 2013; Nicole Perlroth, David E. Sanger e Michael S. Schmidt, "As Hacking Against U.S. Rises, Experts Try to Pin Down Motive", *New York Times*, 3 mar. 2013; Nicole Perlroth e Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", *New York Times*, 8 jan. 2013; Nicole Perlroth e David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt", *New York Times*, 28 mar. 2013; David E. Sanger, David Barboza e Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.", *New York Times*, 18 fev. 2013; David E. Sanger, "U.S. Blames China's Military Directly for Cyberattacks", *New York Times*, 6 mai. 2013; David E. Sanger e Nicole Perlroth, "Cyberattacks Against U.S. Corporations Are on the Rise", *New York Times*, 12 mai. 2013; Michael S. Schmidt e Nicole Perlroth, "Obama Order Gives Firms Cyberthreat Information", *New York Times*, 12 fev. 2013.

PERGUNTAS SOBRE O ESTUDO DE CASO

8.10 A guerra cibernética é um problema sério? Justifique.

8.11 Avalie os fatores humanos, organizacionais e tecnológicos responsáveis por esse problema.

8.12 Quais soluções estão disponíveis para esse problema? Você acha que elas serão eficazes? Justifique.