PANORAMA EUA

VOL. 3, Nº 6, AGOSTO DE 2013

OPEU
OBSERVATÓRIO POLÍTICO DOS ESTADOS UNIDOS

INCT INEU
INSTITUTO NACIONAL DE CIÊNCIA E TECNOLOGIA PARA ESTUDOS SOBRE OS ESTADOS UNIDOS
NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY FOR STUDIES ON THE UNITED STATES

PANORAMA EUA
OBSERVATÓRIO POLÍTICO DOS ESTADOS UNIDOS
INSTITUTO NACIONAL DE CIÊNCIA E TECNOLOGIA
PARA ESTUDOS SOBRE OS ESTADOS UNIDOS – INCT-INEU

ISSN 2317-7977

VOL. 3, Nº 6, AGOSTO DE 2013

http://www.opeu.org.br

SUMÁRIO

SEGURANÇA

OS ESTADOS UNIDOS E A AMEAÇA À SEGURANÇA CIBERNÉTICA

Por Tatiana Teixeira

Atualmente, a ameaça cibernética é considerada um dos grandes desafios para a segurança nacional dos Estados Unidos. Termos como *Digital 9/11* e *Cyber Pearl Habor* vêm sendo usados para simbolizar este possível novo campo de batalha, já reconhecido inclusive pelo Departamento da Defesa (DOD, na sigla em inglês). Em sua confirmação como secretário de Estado, John Kerry disse que os ciberataques são as armas nucleares do século XXI. Tal mudança de percepção de ameaça vem acompanhada de um novo perfil de inimigo e pode levar à militarização do espaço virtual. Traz, ainda, implicações diretas na definição de soberania no ciberespaço, na percepção de palco de guerra e na transformação da natureza de conflito.

Pela primeira vez, os Estados Unidos admitiram, em março de 2013, estar em preparação para uma guerra virtual. Em audiência no Comitê de Serviços Armados da Câmara, o diretor do *Cyber Command* e da Agência de Segurança Nacional (NSA, na sigla em inglês), general Keith Alexander, informou que o governo está montando equipes para tratar de ameaças cibernéticas. Na mesma sessão, o diretor do FBI Robert Mueller disse que os ataques cibernéticos ultrapassarão o perigo do terrorismo em breve. Também presente, o diretor de Inteligência nacional, James Clapper, declarou que as ameaças estão mais interconectadas e virais. Ele destacou os ciberataques, acrescentando o seu potencial para paralisar a economia e a infraestrutura do país.

Essas ameaças, que já existiam em administrações anteriores, tornaram-se prioridade no governo de Barack Obama. Segundo Clapper, a maior parte da infraestrutura crítica do país está em risco. Setores de geração elétrica, redes de transporte, e sistemas financeiros e de comunicações não contam com proteção suficiente, podendo entrar em colapso diante de um ciberataque. Outro problema é que os governos locais e estaduais não têm recursos financeiros e humanos ou conhecimento técnico para lidar com tal realidade.

Em 2011, o Departamento de Segurança Doméstica (DHS, na sigla em inglês) registrou um aumento de 383% nos ataques à infraestrutura. Em julho de 2013, a McAfee e o *Center for Strategic and International Studies* divulgaram um relatório que quantifica o impacto econômico do crime cibernético. São, pelo menos, US$ 100 bilhões ao ano em danos à economia e perda de 508 mil empregos devidos à atividade *online* criminosa. Os prejuízos se relacionam a perdas de propriedade intelectual e à obtenção de informação empresarial sigilosa; aos custos com a interrupção da atividade na rede; às despesas extras para garantir a segurança na Internet e ao dano à reputação da empresa atacada. Um exemplo deste último caso foi o ataque sofrido, em abril de 2013, pela agência de notícias AP em sua conta no *Twitter*. Uma falsa notícia atribuída à AP divulgou que o presidente Barack Obama teria sido fisicamente ferido, fato que derrubou as bolsas de valores em questão de minutos.

A percepção do governo encontra eco na opinião pública. Segundo a pesquisa *The New York Times/CBS News*, entre 31 de maio e 4 de junho de 2013, 64% dos entrevistados veem os ciberataques como uma ameaça “muito séria” para os sistemas de computadores, e 57% acreditam que o país não esteja preparado para lidar com a questão. Como explica o ex-subsecretário de Defesa William Lynn III, trata-se de um conflito assimétrico, difícil de prever e classificar. Outra dificuldade é rastrear a origem e determinar a natureza do ataque, bem como as motivações dos agressores. Em meio às incertezas, o FBI relaciona os agentes de ciberameaças (grupos criminosos organizados e Estados patrocinadores) à espionagem e ao roubo de propriedade intelectual. Em contrapartida, os grupos terroristas tradicionais seriam motivados por ideologias.

De acordo com o DOD, o ciberespaço é uma rede interdependente de infraestruturas de tecnologia da informação, que inclui Internet, telecomunicações e sistemas de computadores, com seus usuários conectados independentemente da geografia física. Na acepção

do Departamento da Justiça, ciberataques são crimes que têm um sistema de computadores como alvo e ocorrem por meio de vírus (vermes e cavalos de troia), ataques de denial-of-service (DOS), vandalismo e sabotagem eletrônica. Além das ferramentas ofensivas, as ciberarmas incluem ferramentas de uso duplo (ataque e monitoramento de rede) e ferramentas defensivas (encriptação e firewalls). No caso do ciberterrorismo, o objetivo seria colapsar a Internet e a infraestrutura nacional. Este seria o caso, por exemplo, do verme Stuxnet, supostamente criado pelos Estados Unidos em parceria com Israel. Aquele foi o primeiro malware (software malicioso) de uso destrutivo designado para atacar os sistemas de controle de um complexo industrial, no caso, as instalações de energia nuclear no Irã.

Ameaças aos Estados Unidos

O conceito de guerra cibernética vem sendo adotado como o uso ofensivo e defensivo de sistemas de informação para negar, explorar, corromper ou destruir valores do adversário baseados em redes computadorizadas. O analista do *Council on Foreign Relations* Adam Segal sugere cautela com o termo, já que ainda não houve destruição física ou mortes decorrentes dos ataques virtuais. Até o presente, as maiores ameaças aos Estados Unidos ainda são espionagem e cibercrime, com ataques voltados para roubo ou corrupção de dados, e interrupção no uso de informações e no funcionamento dos sistemas de controle. Nenhuma delas se configuraria como um ato de guerra. William Lynn III alerta, porém, que, *"embora a ameaça à propriedade intelectual seja menos dramática do que a ameaça à infraestrutura nacional, ela será o maior desafio virtual para os Estados Unidos no longo prazo"*.

Em 2012 e 2013, empresas como Wells Fargo, JP Morgan, Chase, Citigroup, U.S. Bancorp, PNC Financial Services, American Express e Bank of America sofreram ataques de hackers. Em 2010, o Google viu contas de emails de dissidentes chineses serem invadidas supostamente pelo governo da China. No mesmo ano, o grupo Anonymous cometeu ataques do tipo DOS aos sites PayPal, Mastercard e Amazon, em apoio ao Wikileaks. Criada em 2006, essa plataforma foi responsável pela publicação de documentos sobre a prisão de Guantánamo e pela disseminação do vídeo de soldados norte-americanos matando civis em Bagdá. Em seguida, o site divulgou mais de 450 mil documentos sobre as guerras no Iraque e no Afeganistão, e aproximadamente 250 mil comunicações diplomáticas dos Estados Unidos, no que ficou conhecido como Cablegate. Seriam as pessoas envolvidas com o Wikileaks criminosas ou ciberativistas?

Apesar de os analistas apontarem a China como uma das origens das investidas digitais contra os Estados Unidos, no primeiro mandato do governo Obama, adotou-se um tom cauteloso em relação ao país asiático. O objetivo era evitar antagonismos e preservar canais de cooperação em temas sensíveis, como o programa nuclear da Coreia do Norte ou as sanções ao Irã no Conselho de Segurança da ONU.

A partir de 2013, porém, nota-se uma retórica mais direta após a publicação do *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* e do relatório da consultoria Mandiant Corp. Ambos apontam a China e seu Exército de Libertação Nacional como os principais responsáveis pelos ciberataques aos Estados Unidos e acusam os chineses de roubo de tecnologia industrial com objetivos estratégicos. Em março, o então assessor de segurança nacional, Tom Donilon, criticou as invasões cibernéticas originadas na China e pediu um diálogo bilateral construtivo sobre o tema.

A China alega que as acusações são discriminatórias e sem fundamento. Em junho de 2013, Obama e o presidente chinês, Xi Jinping, reuniram-se em Washington, em uma primeira tentativa de aproximação diplomática sobre cibersegurança. A expectativa é a de que esse primeiro encontro leve a discussões mais profundas na comunidade internacional sobre como aplicar os princípios do Direito Internacional para esse novo domínio.

Hoje, China (34%), Indonésia (21%) e Estados Unidos (8,3%) seriam as principais fontes de ataques cibernéticos. "*Quando dissemos ciberespionagem, essencialmente, é a China*", afirma o ex-diretor da CIA, Michael

Hayden, acusando os chineses de motivações. Hayden admite que os Estados Unidos também praticam esse tipo de espionagem, mas com o objetivo de "*proteger e manter os cidadãos seguros*".

Em entrevista ao CFR, Hayden sugere que seu governo compartilhe informações e forme alianças para estabelecer uma estrutura de cibersegurança. Defende mais apoio ao setor privado e maior participação do Departamento de Estado (DOS, na sigla em inglês). Em sentido oposto, Stewart Baker, subsecretário para Políticas e Tecnologia no DHS durante a administração Bush, ironiza a efetividade do Direito Internacional e seu papel na segurança cibernética.

O senador John McCain (R-AR) também é contrário a colocar mais autoridade nas mãos do DHS, defendendo que o Cyber Command e a NSA controlem as operações. Segundo o general Keith Alexander, ambos possuem mais conhecimento técnico do que o DHS. Organizações como American Civil Liberties Union, Center for Democracy and Technology e Electronic Frontier Foundation alegam que, por ser uma agência civil, o DHS possibilitaria melhor supervisão sobre as decisões do governo.

Entre outras recomendações dos especialistas, estão um maior debate público sobre as capacidades cibernéticas como instrumentos de segurança nacional, e mais engajamento dos Estados Unidos em fóruns multilaterais e bilaterais, com o país liderando pelo exemplo. Em 2006, o Senado ratificou a Convenção de Budapeste sobre Cibercrime de 2001, proposta pelo Conselho Europeu e o único tratado multilateral existente para tratar da questão, embora seja um documento sem efeito vinculante e com muitas lacunas. Os Estados Unidos se comprometeram a respeitá-lo desde que esteja de acordo com suas leis federais.

Em editorial, o The New York Times ressalta que os Estados Unidos não discutem seu próprio papel na expansão da *cyberwarfare*. A falta de uma política coerente e consensual, a competição interagências, o excesso de classificação de informação e o baixo nível de compartilhamento agravam o cenário. Sendo o direito internacional ainda incapaz de lidar com os problemas de atribuição e jurisdição, e o uso da força no mundo cibernético, crimes virtuais e reais tendem a ser retaliados da mesma forma, ou seja, "por aproximação". Mary O'Connell, da Universidade de Notre Dame, explica que, por ser um espaço internacional, as atividades no ciberespaço e as respectivas legislações domésticas devem estar de acordo com o direito internacional e sem ênfase na esfera militar.

O problema é que, nos Estados Unidos, torna-se corrente o pensamento militar convencional para atacar problemas cibernéticos. Nesse caso, priorizar a destruição física pode ferir o preceito de proporcionalidade previsto em instrumentos do direito internacional, como a Carta da ONU, e as Convenções de Haia e de Genebra. Nenhum deles foi atualizado para especificar ataque armado, uso da força ou agressão no ciberespaço.

William Lynn III afirma que os modelos de contenção da Guerra Fria não se aplicam ao ciberespaço, principalmente pela dificuldade de se identificar o agressor. Tradicionais regimes de controle de armas também seriam ineficazes para conter os ataques devido às dificuldades de atribuição, que tornam a verificação do cumprimento das normas quase impossível. Para o especialista, é preciso desenvolver um novo modelo.

Cybersegurança no governo

Em 2009, quando assumiu a presidência, Obama determinou a atualização da *Comprehensive National Cybersecurity Initiative,* implementada por George W. Bush. Nela, o DHS constava como o principal responsável pela defesa das redes governamentais (domínio ".gov"), e por desenvolver um plano de cibercontrainteligência e estratégias de contenção. Foi somente em 2011 que o Congresso começou a debater uma nova legislação para dar mais autoridade ao DOD, em detrimento do DHS.

Em 2010, o Departamento de Defesa criou o *Cyber Command*. Os Estados Unidos garantem que o órgão é sobretudo defensivo, mas a resistência do governo à ideia de um tratado sobre desarmamento no espaço cibernético coloca em dúvida a posição dos Estados Unidos. Reforça essa suspeita a sanção da

Presidential Policy Directive 20, em 2012, que estabeleceu princípios para o uso de operações cibernéticas, incluindo ações ofensivas a computadores.

Na *National Security Strategy* de 2010, os EUA reconheceram sua vulnerabilidade no espaço cibernético e a importância da cibersegurança. Apesar disso, o país ainda não apresenta uma estratégia específica para enfrentar o problema. Divulgada em 2011, a *International Security for Cyberspace* sugeriu criar o cargo de coordenador de segurança cibernética para atuar com a Casa Branca; investir mais em inovação e educação; e elaborar uma ampla estrutura para coordenar respostas entre as agências após ataques virtuais. Há um forte componente de contenção, com o país respondendo a atos hostis no ciberespaço como reagiriam a qualquer outra ameaça, o que significa que a resposta não se limitará ao universo cibernético, estendendo-se aos meios econômicos, diplomáticos e militares.

Em fevereiro de 2013, Obama assinou a ordem executiva *Improving Critical Infrastructure Cybersecurity* (n. 13636) para promover o compartilhamento de informação entre o governo e o setor privado responsável pela infraestrutura crítica do país. Dez anos antes, a *National Strategy to Secure the Cyberspace* pedia a liderança do setor privado sobre a segurança virtual da infraestrutura nacional. Apelo parecido já havia sido feito na primeira estratégia nacional de cibersegurança, a *Presidential Decision Directive 63* (PDD 63), divulgada em maio de 1988, no governo Clinton. O plano focava a proteção da infraestrutura e parcerias público-privadas. Aparentemente, as políticas vinham se repetindo em diferentes governos, sem clara eficácia.

Alguns esforços legislativos foram feitos, também sem grandes avanços, devido à forte polêmica em relação ao excesso de regulação federal, invasão de privacidade dos cidadãos e ataque à liberdade de expressão. Este foi o caso do *Cyber Intelligence Sharing and Protection Act* (CISPA), do *Cybersecurity Act* de 2012, na Câmara, e do *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Tecnhology Act* de 2012 (SECURE IT), no Senado. O *Cybersecurity Act* não recebeu voto suficiente para seguir no Senado. O CISPA passou na Câmara em 2013, mas Obama ameaça vetá-lo, tornando incerto seu futuro. Igualmente polêmicos, os *Stop Online Piracy Act* (SOPA) e *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PIPA) estão paralisados. O *Protecting Space as a National Asset Act* de 2010 foi apresentado no Senado (S. 3480) e na Câmara (H.R.5548), embora ainda sem definição.

* * * * *

Documentos e declarações oficiais mostram que ainda não há consenso nos Estados Unidos sobre como tratar a questão da segurança cibernética. A consequência é o uso intercambiável de ciberguerra, ciberterrorismo e cibercrime, contribuindo para sensacionalismo e pânico interno sobre ameaças que seriam específicas de segurança pública, e não de segurança nacional. Atribuições inadequadas resultarão em respostas desproporcionais a um ataque.

Embora 2013 tenha sido o ano de maior proatividade e endurecimento de postura do governo, os Estados Unidos se mantêm bastante vulneráveis, pouco avançando em alguns pontos básicos. No setor privado, empresas recorrem muitas vezes a sistemas de segurança antiquados e ineficazes. No âmbito público, o Poder Legislativo age com excessiva lentidão à premência de desafios tão velozes. Também permanece a dificuldade de se encontrar um equilíbrio entre segurança e proteção dos interesses nacionais, e as demandas da sociedade civil para que isso seja feito com maior transparência e respeito à privacidade dos usuários da rede.

Outra desvantagem do país é quanto à capacitação de profissionais da área de cibersegurança, ao contrário do que vem ocorrendo em países como China e Índia. Ao focar excessivamente na ameaça virtual externa, o governo também minimiza o risco humano interno, evidenciado nos recentes e espetaculares vazamentos de informação sigilosa por cidadãos norte-americanos, como Bradley Manning e Edward Snowden.

Além disso, a concentração do poder decisório no DOD, somada às incongruências entre

teoria e prática, aumentam a resistência e a desconfiança dos demais países em atuar conjuntamente com os Estados Unidos. Outro problema é a percepção da comunidade internacional de que os Estados Unidos tentarão dominar o ciberespaço.

É preciso atualizar as normas internacionais para um mundo mais interconectado e dependente de tecnologia, que pode criar mais flancos vulneráveis e espaços de desentendimento. Países como Estados Unidos, Grã-Bretanha, Alemanha, França, China e Rússia já veem o meio cibernético como uma nova dimensão de combate, junto com mar, terra, ar e espaço sideral. Trata-se de um esforço necessariamente multilateral.

De acordo com a agência da ONU, *International Telecommunication Union*, em 2013, o número de internautas no mundo todo chegará a 2,749 bilhões. O *Networking Index* da Cisco prevê 18,9 bilhões em 2016 – um salto significativo. Não é possível contar, portanto, com analogias jurídicas que serão, inevitavelmente, sujeitas a interpretações e interesses de cada ator do sistema internacional. Como lembrou a Força Tarefa do CFR, os Estados Unidos não poderão, isoladamente, determinar as fronteiras da ciberguerra.


OPEU
OBSERVATÓRIO POLÍTICO
DOS ESTADOS UNIDOS
INCT
INEU
INSTITUTO NACIONAL DE CIÊNCIA
E TECNOLOGIA PARA ESTUDOS
SOBRE OS ESTADOS UNIDOS
NATIONAL INSTITUTE OF SCIENCE
AND TECHNOLOGY FOR STUDIES
ON THE UNITED STATES