A INSERÇÃO DA SEGURANÇA CIBERNÉTICA NA AGENDA DE SEGURANÇA DOS EUA NO SÉCULO XXI

THE INSERTION OF CYBERSECURITY IN THE UNITED STATES OF AMERICA SECURITY AGENDA IN THE 21st CENTURY

Vinicius G.Ribeiro[1]
César G. Rivera[2]

RESUMO:
O objetivo do presente trabalho consiste em descrever como ocorreu o processo de inserção da segurança cibernética na agenda estadunidense de segurança, dentro do recorte histórico referente ao século XXI. O foco deste trabalho concentra-se nas estratégias, principalmente legais, as quais o governo dos Estados Unidos da América adota, visando um melhor enfrentamento das crescentes ameaças ao seus sistemas de informação internos.

ABSTRACT:
The objective of this study is to describe the process which cybersecurity became inserted in the American security agenda, within the historical period regarding the 21st century. This paper focus specially on the strategies, particularly legal, which the government of the United States of America adopts, seeking a better affront to the growing threats to their internal information systems.

PALAVRAS-CHAVE:
Século XXI. Estados Unidos da América. Segurança Cibernética. Guerra Cibernética.

KEYWORDS:
21st Century. United States of America. Cybersecurity. Cyberwar

Introdução

O avançado estágio no qual o mundo se encontra atualmente, no quesito tecnológico, acarretou mudanças nas mais variadas áreas. A tecnologia trouxe novos conceitos e preocupações, principalmente quanto a novas formas de

1 Doutor em Ciência da Computação pela Universidade Federal do Rio Grande do Sul. Professor da UniRitter Laureate International Universities e da ESPM-Sul. (vinicius.ribeiro@espm.br).
2 Bacharel em Relações Internacionais pela Escola Superior de Propaganda e Marketing de Porto Alegre (ESPM-SUL). (cesargrivera@hotmail.com).

comunicação e interação entre os estados nacionais. Em relação aos conflitos entre estados, as guerras passaram a ser cada vez mais assimétricas, dada a disparidade entre a capacidade tecnológica das nações. Consequentemente surgem os recentes conceitos de Guerra Cibernética e da Segurança da Informação. Esses têm por base a utilização de maneira ofensiva e defensiva, ofensiva majoritariamente, utilizando-se de informações e sistemas de comunicação para corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes computadorizadas. Pode-se afirmar que novos aspectos da agenda clássica das nações terminaram por mudar e, na área da segurança nacional, o resultado não é diferente.

O conceito de segurança possui um aspecto peculiar: o mesmo é constantemente modificável, ficando à mercê das características e aspectos únicos do período histórico em questão. Logo, apenas recentemente a preocupação com a segurança cibernética surge como novo paradigma nas preocupações dos estados - em especial, dos Estados Unidos. Tendo em vista quanto a nação estadunidense necessita de novas estratégias para assegurar sua condição no novo ambiente cibernético, o estudo quanto às providências do Estado se torna pertinente (BUZAN; HANSEN, 2011).

O estudo da forma como a segurança cibernética passa a fazer parte da agenda de segurança dos Estados Unidos da América reside no fato da escassez de material de pesquisa acadêmica relacionada ao assunto segurança cibernética - não em relação à conceituação, mas sim quanto à contextualização e ao histórico do processo pelo qual os Estados Unidos passam. O estudo visa ao preenchimento desta lacuna, uma vez que o tema da segurança cibernética ganha relevância devido ao avançado estado tecnológico atual do mundo. Para atingir seu objetivo, o estudo deve cobrir a evolução do conceito de segurança nacional, as novas guerras cibernéticas e, por fim, as atitudes legais e ilegais do governo, a exemplo da *National Security Agency* (NSA) estadunidense relativas à inserção da cibersegurança na agenda de segurança nacional. Tendo em vista que as doutrinas que mais privilegiaram as questões cibernéticas foram as de Bush e Obama, o presente artigo se manterá sob o recorte histórico do século XXI.

Assim, o trabalho mantém uma linha de estudo cronológica em relação à segurança cibernética, considerando os fatos históricos pertinentes quanto a sua abrangência. Em seguida, apresenta o contexto atual de conflitos cibernéticos, tanto envolvendo atores estatais como não estatais. Na última parte, volta-se para as ações tomadas pelo governo dos EUA ante as novas ameaças cibernéticas.

Contexto Cibernético

A chamada cibersegurança trata de um conceito tão controverso quanto o de segurança nacional. Apesar disso, Jentleson (2010) cunha o termo

como sendo conjunto de meios e tecnologias criadas pelo estado que visam proteger - de danos e intrusão ilícita-, programas, computadores, redes, dados, propriedade intelectual, etc. Debates em torno da cibersegurança apresentaram certa intensificação em meados dos anos 1990 nos Estados Unidos da América. Tal fato possui como origem principal a chamada Revolução da Informação ou Terceira Revolução Industrial. A enorme presença das tecnologias da informação envolvidas em absolutamente todos os aspectos da atividade humana acarretou a informatização, não só do sistema financeiro internacional, mas principalmente dos sistemas de defesa governamentais.

Acima de tudo, os governos nacionais tentam gerir os problemas de segurança – como, por exemplo, espionagem e crime - nos quadros jurídicos nacionais, embora a volatilidade tecnológica do domínio cibernético faça com que as leis e regulamentos estejam sempre perseguindo um alvo em movimento. O domínio do ciberespaço é frequentemente descrito como um bem público ou um bem comum global, mas esses termos são um ajuste imperfeito. Um bem público é aquele do qual todos podem se beneficiar e que nenhum seja excluído, por mais que isso possa descrever alguns dos protocolos de informação da internet, não descreve de maneira fiel a infraestrutura física, que é um recurso escasso localizado dentro dos limites de Estados soberanos. E o ciberespaço não é um bem comum - como os oceanos, por exemplo - , já que partes dele estão sob o controle soberano (BOOZ ALLEN HAMILTON, 2011).

A migração da prioridade norte-americana agora passa a ocupar o chamado quinto domínio. Após conflitos terrestres, marítimos, aéreos e espaciais, o governo estadunidense começa a focar não só sua agenda de segurança dando prioridade à segurança cibernética mas também ao meio não físico como mecanismo de difusão de poder (NYE, 2012).

Alguns países como China e, principalmente, Coreia do Norte, já possuem doutrinas de segurança cibernética mais avançadas que os Estados Unidos. Ambos já possuem soldados especializados para o combate em meio cibernético, os chamados *cyberwarriors.* Como já relatado anteriormente, o aspecto evolutivo da segurança possui forte relação com o contexto global (político, financeiro, etc) no qual o país se encontra. No caso dos Estados Unidos da América no século XXI, a ameaça cibernética e o processo, talvez definitivo, de migração de conflitos para o domínio cibernético evidenciam, em parte, o porquê da presença da segurança nacional do quinto domínio agora como tema permanente na agenda estadunidense (JENTLESON, 2010).

Para Rosenzweig (2013), existem três problemas da internet que a tornam um ambiente propício para ataques. O primeiro é a questão anonimato, que o vasto domínio cibernético possibilita. Em alguns países há um controle maior em relação a esse aspecto, como no caso do Brasil com o Marco Civil

da Internet, que busca uma maior regulamentação da internet brasileira. A segunda vulnerabilidade encontra-se na dificuldade de distinção entre diferentes atividades cibernéticas. O setor responsável pela parte defensiva(setor de segurança nacional mais especificadamente) do Estado possui grande dificuldade em distinguir entre espionagem e um ataque cibernético em grande escala, já que frequentemente esses se parecem com as comunicações autorizadas e inofensivas. A diferença se torna perceptível apenas quando uma intrusão ocorre. O terceiro problema aparece devido ao atual alcance universal da internet em praticamente todo mundo, consequentemente, os Estados lidam com a insurgência em larga escala de novos atores. O ambiente cibernético favorece a ação de não só estados menores mas também principalmente de grupos não estatais. Em relação a isso, Joseph Nye (2012) retrata o espaço cibernético como gerador de um equilíbrio de poder no sistema internacional, e é de fato, o que se observa atualmente. Dada a presente proliferação de conflitos no ciberespaço, as chamadas *cyberwars* já são tratadas como realidade. Essas podem ser consideradas como conflitos reais, com a equivalência de um conflito armado no mundo físico, devido ao fator conhecido como resultado cinético.

> O espaço cibernético como um domínio de guerra moderna cria uma série de complexibilidades que inexistem nos outros domínios físicos. Você não pode identificar visualmente o inimigo, tampouco confirmar a sua nacionalidade. [...] Portanto, uma boa estratégia em qualquer investigação cibernética é seguir o rastro do dinheiro deixado para trás pela logística necessária para organizar um ataque no domínio cibernético, serviços de hospedagem, aquisição de software, quantidade de banda e assim por diante (CARR, 2011, p. 103, tradução do autor).

Para Jorge (2012), existem duas dimensões quanto ao uso do poder cibernético para alcançar os objetivos de política externa da nação estadunidense: uma, aberta ao público, visível para a opinião pública; e uma segunda secreta, a qual faz uso de ataques com armas cibernéticas de maneira ofensiva a outros países. Quanto à primeira dimensão, essa se encontra singularizada na figura de Richard Clarke. Clarke e Knake (2012) protagoniza o clamo por uma política de segurança nacional com foco crescente no domínio cibernético. De fato, sua vontade apresenta-se apoiada na constatação de que os Estados Unidos são o país mais dependente de sistemas computadorizados para o funcionamento da sua sociedade e, principalmente, economia. Consequentemente, a nação estaria mais vulnerável a ataques cibernéticos: portanto os Estados Unidos seriam os menos interessados em uma "guerra cibernética". Outrossim, o principal intuito - segundo Jorge (2012) -, dessa constatação é realmente desviar a atenção da verdadeira dimensão norte-americana de atos cibernéticos.

A segunda dimensão diz respeito ao uso das guerras cibernéticas - ou de armas cibernéticas - para alcançar fins de política externa, os quais dificilmente

seriam conquistados por outros meios. No caso específico das ações perante o Irã, por exemplo, o intuito estadunidense é atrasar o programa nuclear iraniano, já que a nação persa é vista como ameaça por Washington devido ao seu potencial nuclear. Há que levar em consideração o fato dos recentes avanços do Irã, principalmente quanto ao desenvolvimento da tecnologia nuclear para obtenção de energia a partir da divisão do átomo. Esse fato faz com que os EUA passem a considerar a guerra aberta e declarada como uma opção arriscada, o que faz com que ações no domínio cibernético se tornem mais atrativas e seguras para a nação (JORGE, 2012).

Mesmo com o sentimento gerado pelo onze de setembro na nação norte-americana, o foco e a prioridade do Departamento de Defesa dos Estados Unidos da América começam a mudar. No ano de 2013, as chamadas guerras cibernéticas passaram a ocupar a liderança do ranking de ameaças à segurança nacional dos Estados Unidos da América, tomando a frente da organização terrorista Al-Qaeda. De fato, trata-se de um consenso no Departamento de Defesa dos Estados Unidos da América que o país se encontra em um momento pleno de guerra, um conflito nem físico ou declarado, apenas cibernético (DILANIAN, 2013).

Basicamente, esse é o ambiente que os Estados Unidos e muitos outros países irão enfrentar nos anos que virão. Após os ataques do onze de setembro, o maior ataque terrorista de sua história, além das consequências sociais, econômicas e políticas, a agenda americana de segurança passou por um processo radical de mudança em seus norteadores de política externa. Segundo o relato do Washington Post (2013) no dia 29 de agosto de 2013, até mesmo a NSA possui seu próprio time de hackers de elite. Essa equipe é responsável pela criação de um programa altamente secreto da NSA, que recolhe informações sobre alvos estrangeiros através da invasão de seus computadores, roubo de dados e monitoramento de comunicações principalmente. Existe também o TAO (*Tailored Access Operations*) que desenvolve programas que poderiam destruir ou danificar computadores e redes estrangeiras via ciberataques, caso haja ordem do presidente. O TAO "permitiu que a NSA coletasse dados a partir de telefones móveis que foram usados por agentes da Al-Qaeda e outras pessoas de interesse na caça a Osama Bin Laden " (THE WASHINGTON POST, 2003).

Os Estados Unidos da América estão em um novo processo de câmbio de suas relações bilaterais. O conflito cibernético torna-se um fator de grande importância quanto à redefinição dos processos - não só de relações bilaterais, mas principalmente de relações econômicas e militares. O novo ambiente cibernético e, consequentemente, o conflito intrínseco no mesmo representa uma mudança no quesito segurança internacional. O que estamos vivenciando é uma mudança maior na segurança internacional. Devido às enormes diferenças entre China e Estados Unidos, especialmente no aspecto militar e econômico, no que tange a momento e objetivos futuros, não existe um vasto espaço para cooperação na cibersegurança. Agora, ambas as nações se encontram diante do

importante processo que é o ajuste de suas políticas quanto à infraestrutura de informações que é o ciberespaço. Em relação aos Estados Unidos, as decisões-chave estão relacionadas a evitar os danos econômicos que poderão vir de crimes cibernéticos e, principalmente, da ciberespionagem. Ressalta-se a importância da criação de barreiras antiespionagem devido à grande concentração de propriedade intelectual que os Estados Unidos possuem. Quanto a China, a proteção do conhecimento intelectual também é necessária, principalmente devido às tecnologias desenvolvidas de forma nativa, que podem vir a interessar os países ocidentais (BILLO, 2004).

Um aspecto contemporâneo relativo à temática da segurança é a inclusão de cada vez mais novas facetas, garantindo assim uma maior abrangência quanto a questões de defesa nacional. O novo ambiente cibernético mundial proporcionou o surgimento de novas ameaças a[à] integridade de todas as nações mundiais. Como principal resultado, temos novas questões como as guerras cibernéticas e o terrorismo cibernético surgidos majoritariamente no século XXI. No caso do ciberterrorismo, já é tratado como uma ameaça à segurança nacional já existente, apesar de não haver consenso a respeito de sua atual situação. A evolução da ameaça denota a necessidade da reinvenção e adaptação das políticas externas para que possam lidar com esse novo tipo de fator (ANDRESS; WINTERFELD, 2011).

A princípio, a política norteadora de segurança cibernética norte-americana baseia-se principalmente nos princípios de liberdade fundamental, privacidade e fluxo livre de informações. As chamadas "liberdades fundamentais" remetem à capacidade de procurar, receber e transmitir informações e ideias por qualquer meio e de uma forma transfronteiriça. A estratégia básica de segurança está fortemente ligada à obrigação de proteger os cidadãos norte-americanos, tendo em vista o maior envolvimento dos mesmos com a internet. O fundamento da política ciberespaço internacional dos Estados Unidos reside na crença de que o mesmo contém potencial imenso para o país norte-americano e, em segundo plano, para o mundo. Ao longo das últimas três décadas, os Estados Unidos assistiram à revolução tecnológica impulsionar a economia do país. Ameaças à segurança cibernética representam um dos mais sérios riscos à segurança nacional, segurança pública, e a econômia de qualquer país. Ataques cibernéticos de *hackers*, organizações terroristas e Estados-nações se tornam cada vez mais comuns (UNITED STATES OF AMERICA, 2011).

A busca por um espaço cibenético seguro por parte do governo estadunidense fica evidente quando observadas as devidas publicações e atitudes legais que o governo efetiva. A nova política de *Framework* de Obama, focada no compartilhamento de informações entre empresas privadas e o governo, também demonstra grande interesse do governo em uma maior presença no ambiente

cibernético nacional. Da mesma forma, as informações reveladas por Edward Snowden também demonstram o mesmo enorme interesse, a ponto de invadir não só a privacidade de seus próprios habitantes, como a "soberania" cibernética de outras nações, trazendo enormes consequências diplomáticas para os EUA.

Doutrina Bush

A doutrina Bush teve como marco principal a forma com que o governo dos Estados Unidos da América passaram a encarar o terrorismo. Em 11 de setembro de 2001, dois aviões foram lançados com tripulação, seus passageiros e terroristas suicidas sobre as duas torres do *World Trade Center* na cidade Nova Iorque. Além disso, um terceiro avião atingiu o Pentágono, com intuito de destruir o centro de comando militar dos Estados Unidos. A partir desse dia foi declarada guerra ao terror, acarretando intervenções militares tanto no Afeganistão quanto no Iraque.

Entende-se que a repercussão e também a gravidade dos ataques terroristas em solo norte-americano, somada ao sentimento da população, culmina com a declaração do *Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism).* A lei veio como uma resposta praticamente imediata aos ataques do onze de setembro, o que reflete na velocidade com que a mesma foi aprovada. O Ato Patriota teve um processo de aprovação peculiar, já que desde sua apresentação a *House of Representatives*[3] no dia 23 de outubro de 2001, por Frank J. Sensenbrenner, após apenas 24 horas, a lei seguiu para aprovação do senado estadunidense. No dia 25 de outubro de 2001, a lei foi aprovada com larga vantagem(contrariando a opinião pública norte-americana) para seguir em frente para obtenção da sanção final do presidente Bush (UNITED STATES OF AMERICA, 2001).

Como esperado, apenas um dia depois, George W. Bush assina o Ato Patriótico em 26 de outubro de 2001. Apesar de toda a contradição da opinião pública em relação aos perigos que a lei representaria às liberdades individuais de seus cidadãos, o Ato Patriótico se configura como uma lei fundamental no estudo da doutrina de segurança do governo Bush (UNITED STATES OF AMERICA, 2004). O estudo e interpretação do Ato Patriótico é de grande relevância, já que a preocupação do governo com terrorismo cibernético e possíveis ameaças à setores estrututurais do país aparecem de forma explícita no corpo da lei. O documento, publicado pelo *Government Printing Office*[4] (GPO), possui partes específicas tratando da segurança estrutural do país.

3 A *House of Representatives* dos Estados Unidos da América, conforme consta na Constituição norte-americana, cria e aprova leis federais. Ela é uma das duas câmaras do Congresso(seguida pelo Senado), e integra o Legislativo do governo dos EUA.

4 O GPO é uma agência do ramo legislativo do governo federal dos Estados Unidos da América. O escritório é responsável pela impressão de documentos produzidos ou destinados ao governo federal, incluindo a Corte Suprema, o Congresso, etc (THE WASHINGTON POST, 2006).

O título VIII do Ato patriótico, denominado *Strengthening the Criminal Laws Against Terrorism*[5], possui um número total de dezessete artigos (801 até 817), que abordam temas como terrorismo doméstico (artigo 802), jurisdição estadunidense em território estrangeiro(artigo 804), etc. Ainda sob o título VIII, nesse contexto, duas seções se destacam: *Deterrence and prevention of cyberterrorism* (artigo 814) e a *Development and support of cybersecurity forensic capabilities,* o artigo 816 (UNITED STATES OF AMERICA, 2001).

Já o artigo 814 teve como principal intuito o aumento das penalidades contra crimes de ciberterrorismo. A seção aumentou a pena máxima para quem causar danos a um computador protegido pelo governo federal, estendendo a pena máxima de dez anos para vinte anos de reclusão. Ainda no artigo 814, o Congresso tratou de ampliar o alcance da proteção oferecida a computadores de propriedade do governo federal. Antes da aprovação do Ato Patriótico, havia quatro categorias de danos possíveis que terminariam por causar a condenação da pessoa envolvida: o artigo 814 cria uma quinta categoria de danos. Esse seria o caso de haver dano em qualquer sistema ou computador usado pelo o governo ou para o mesmo, em prol da defesa nacional ou da segurança nacional. Além disso, a seção deixou de maneira clara o significado de "perda" em relação aos crimes cibernéticos, agora incluindo custos necessários para responder à ofensa qualquer que seja. Essa alteração visa garantir que, aqueles que intencionalmente decidam invadir sistemas de computadores e causar danos aos mesmos, sejam responsabilizados de acordo com o dano econômico causado por seus atos (UNITED STATES OF AMERICA, 2004).

Ainda no título XVIII, há o artigo 816 (UNITED STATES OF AMERICA, 2001) intitulado de *Development and Support of Cybersecurity Forensic Capabilities.* Basicamente, a seção autoriza a verba com valor total de 50 milhões de dólares para criação e suporte de uma rede regional forense de computadores. Apesar do título, a rede de instalações não terá como propósito exclusivo a condução forense de atividades relacionadas à segurança cibernética. Os laboratórios também serão utilizados como centros de treinamentos para pessoal subordinado a qualquer setor policial (local, estadual e federal) quanto a ações de defesa contra terrorismo cibernético. Segundo Peterson (2002), a criação dos laboratórios em questão também possuía a intenção de facilitar a comunicação entre os diferentes setores responsáveis pela vigilância dos sistemas de computadores do governo.

Já no título X do Ato Patriótico há uma parte nomeada *Miscellaneous*. O título possui um total de 16 artigos (1001 até 1016), que abordam temáticas mais variadas, como o título sugere. Entretanto, apenas a última seção do título X, intitulado de *Critical Infrastructures Protection* (artigo 1016), traz diretrizes para maior proteção dos sistemas de informação norte-americanos. No artigo

5 Traduzido como "Reforço das Leis Criminais Contra o Terrorismo"

201 do Ato Patriótico (UNITED STATES OF AMERICA, 2001), o Congresso traz a questão da revolução da informação, e de como ela transformou a conduta dos negócios e as operações do governo em relação à segurança nacional e a sua infraestrutura. As empresas privadas e o governo se encontram cada vez mais próximos em uma rede interdependente, tanto física quanto virtual. Redes como telecomunicações, energia e água exemplificam o porquê do esforço do governo em assegurar um contínuo fornecimento de serviços provenientes - tanto de infraestrutura cibernética quanto física. De fato, o foco principal do artigo 201 é a parceria entre empresas privadas e o Estado, através do fornecimento de informações privadas de seus usuários/clientes para o governo norte-americano.

Apesar de o Ato Patriótico possuir explicitamente cautela relacionada à segurança cibernética estrutural do país, a lei não foi o suficiente para conter o aumento de atividade cibernética mal-intencionada no país. Sabe-se que, entre os anos 2000 e 2007, o número de atividades maliciosas cibernéticas flagradas pelo Departamento de Defesa norte-americano apresentou um aumento de 31%, com um total de ataques em torno de cinquenta mil (CARR, 2011). Tendo em vista o aumento de atividade maliciosa, o Departamento de Defesa cria o *Comprehensive National Cybersecurity Initiative* (CNCI).

Com o intuíto de tornar os Estados Unidos mais seguros contra ameaças cibernéticas, o CNCI estabelece a política, estratégia e diretrizes de defesa para proteger os sistemas de rede e servidores federais. Além disso, o CNCI possui como diretriz uma abordagem que antecipa as ameaças cibernéticas e tecnologias que estariam por vir. O mesmo exige que o governo federal utilize de forma otimizada suas capacidades técnicas e organizacionais para identificar tanto ameaças quanto vulnerabilidades que possam vir a representar algum risco. Apesar de a CNCI ter sido criada durante a Doutrina Bush, foi apenas durante a Doutrina Obama que a mesma passou a ter maior importância, tornando-se um dos pilares da política de segurança cibernética do governo Obama (UNITED STATES OF AMERICA, 2009).

Doutrina Obama

A atual doutrina de segurança nacional dos EUA amplia o conceito de segurança para incluir aquecimento global, guerra cibernética e endividamento nacional como ameaças, ao lado de terrorismo doméstico e proliferação nuclear. Essas são as principais características da "Doutrina Obama", que instaura uma ruptura drástica com a abordagem de George W. Bush, que pregava intervenções militares unilaterais.

Já em relação à segurança cibernética, o governo de Barack Obama possui como norteador o documento *Cyber Space Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Esse consistia em uma avaliação

da estrutura vigente dos EUA para a segurança cibernética na época. A *Cyber Space Review* basicamente reafirma o compromisso do governo de lidar com a segurança cibernética. Entende-se que o documento acarretou o desenvolvimento da *Executive Order 13636*, nas modificações da CNCI do governo Obama, ambas importantes para estudo de sua doutrina de segurança. Além disso, a publicação traz a definição de ciberespaço como uma rede interdependente de infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computador e processadores. O termo em questão também se refere ao ambiente virtual de informações e interação entre pessoas (UNITED STATES OF AMERICA, 2014a).

Em maio de 2009, o presidente Barack Obama opta por adotar algumas sugestões presentes no *Cyberspace Policy Review*, incluindo a seleção de um coordenador de segurança cibernética do poder executivo, que terá contato próximo e regular com o presidente. O Poder Executivo dos EUA também recebeu novas diretrizes para trabalhar com elementos-chave da segurança cibernética dos Estados Unidos, incluindo os governos estaduais e municipais e principalmente do setor privado para garantir uma organizada e unificada resposta a incidentes cibernéticos futuros; fortalecer as parcerias público/privado para encontrar soluções que garantam a segurança e a prosperidade dos EUA; investimento em pesquisa e desenvolvimento; e a criação de uma campanha para promover a conscientização de segurança cibernética para dar início à construção de uma força de trabalho digital no século XXI. Em relação ao governo Bush, a contribuição de Obama para a CNCI foi a transparência das iniciativas contidas no documento, que antes eram confidenciais – ou pelo menos muito restritas. O presidente Barack Obama determinou que a CNCI e suas iniciativas deveriam evoluir para gerar uma estratégia de segurança cibernética nacional mais ampla e atualizada. As doze iniciativas, que se reforçam mutuamente, possuem como objetivo principal a proteção do ciberespaço dos Estados Unidos da América. Entretanto, durante a construção dos planos da CNCI, o governo concluiu que esse objetivo não poderia ser alcançado sem haver de fato certo fortalecimento de certas capacidades fundamentais e estratégicas dentro do governo. Portanto, o CNCI passa a incluir o financiamento de diversas estartégias de defesa federais para assim aprimorar áreas-chave como investigação criminal, coleta de informações, processamento e análise de dados. Além disso, a CNCI foi desenvolvida também pensando na privacidade e as liberdades civis, uma vez que há também a questão do financiamento de profissionais dessa área no documento (UNITED STATES OF AMERICA, 2014a)

Além dos documentos publicados pelo governo, há outras fontes que disponibilizam informações quanto às prioridades do governco em relação à segurança cibernética nacional, como o website oficial da Casa Branca. Esse

apresenta cinco prioridades que traçam os objetivos do governo: a proteção da infraestrutura essencial do país; aprimoramento das habilidades em identificar/denúnciar incidentes cibernéticos; aproximação com parceiros internacionais para promover a liberdade na internet; proteção das redes federais através do estabelecimento de metas claras de segurança; criação uma força de trabalho especialista em assuntos cibernéticos, avançando além das parcerias do governo com o setor privado (UNITED STATES OF AMERICA, 2014b).

Quanto ao primeiro tópico, o governo percebe a importância da aproximação com o setor privado. Com intuito de fortalecer a cooperação entre os setores, no dia 12 de fevereiro de 2013, o presidente Barack Obama assina a *Executive Order 13636*. O decreto possui foco no compartilhamento de informações em questões de privacidade, e a adoção de práticas de segurança cibernética (UNITED STATES OF AMERICA, 2014c).

O Decreto 13636 deixa encarregado o *National Institute for Standards and Technology* (NIST) de lidar com o setor privado para buscar padrões de segurança dentro de indústrias para assim contruir um quadro geral (*framework)* para segurança cibernética nacional. O governo norte-americano percebe os fortes controles de segurança, políticas, procedimentos e inovações já existentes em empresas. Em resposta ao estado avançado do setor privado, o governo requisita o auxílio voluntário das companhias para moldar infraestrutura cibernética sólida. O *Department of Homeland Security* (DHS), através da voz do presidente Obama, busca estabelecer um programa de participação voluntária para promover a adoção de um quadro geral de práticas gerais de segurança. Sendo assim, a empresa que adere ao quadro aproxima o Estado do objetivo fundamental de identificar, priorizar a execução, gestão e/ou comunicação de riscos de segurança cibernética. Devido a grande parte do setor de comunicações dos Estados Unidos pertencer à iniciativa privada, não há escolha por parte do governo em focar na cooperação para buscar soluções reais para ameaças cibernéticas (UNITED STATES OF AMERICA, 2014d).

Em relação às redes federais internas, a *Cybersecurity Cross Agency Priority* (CCAP) foi criada pela administração do governo Obama para auxiliar setores federais(agências e departamentos) quanto a sua segurança cibernética, mantendo foco especificamente quanto ao tipo de informação que adentra e abandona as redes e em quem possui acesso às redes de informação. A Casa Branca identificou três pontos-chave que necessitam de fortalecimento e investimento: *Trusted Internet Connections*[6](TIC), monitoramento contínuo dos sistemas de informação federais e autentificação forte e segura. A importância de conexões de internet realmente seguras está em controlar o fluxo de informação das agências, e auxiliar no processo de monitoramento dos sistemas

6 Conexões de internet seguras

federais. Entretanto, a mudança proposta pela Casa Branca, nesse caso, seria um monitoramento contínuo que gerasse um controle de segurança em processo constante de atualização. Essa mudança permitiria a agências/departamentos manter uma vigilância em tempo real para avaliar riscos de maneira mais ágil, fornecendo uma resposta adequada à ameaça identificada (UNITED STATES OF AMERICA, 2014d).

Existe também a questão da transnacionalidade do espaço cibernético, o que torna a questão de cooperação internacional essencial para os objetivos estadunidenses. Percebe-se a preocupação do país quanto ao fluxo de capital em formato de dados, e de como o funcionamento da enconômia internacional é dependente de um trânsito livre e seguro. Portanto, há a necessidade de consenso entre diferentes países, quanto a regras, valores e segurança que permeie o sistema cibernético internacional. Por essa razão, os Estados Unidos da América prezam por uma internet livre e transparente, mas principalmente bem regulamentada, com uma legislação internacional. Tudo isso buscando um padrão de comportamento internacional que fomente o comércio entre nações de forma livre e segura. Projetando o futuro do domínio cibernético, o governo Obama pretende desenvolver uma força de trabalho especializada em segurança cibernética. Através de investimentos em pesquisa, desenvolvimento, e tecnologia para assim incentivar inovações no setor privado. Além da já citada aproximação governo-empresa, o governo também percebe a importância da academia. Trabalhos acadêmicos relacionados à segurança cibernética dos Estados Unidos da América são vistos de forma positiva já que encorajam mudanças e inovações nas políticas do governo (UNITED STATES OF AMERICA, 2014b).

Seguindo o estudo dos atos do governo americano em uma linha cronológica, no dia 12 de fevereiro de 2014, o governo de Barck Obama publicou seu mais recente documento voltado para questão de segurança cibernética nacional (até a elaboração do presente estudo), intitulada *Framework for Improving Critical Cyberstruture Cybersecurity* (FICCC). Fazendo uso do conceito de infraestrutura crítica presente no Decreto nº 13636, o documento de 41 páginas basicamente apresenta a consolidação de uma estratégia unificada para a segurança nacional cibernética, através da cooperação entre o governo e empresas particulares (UNITED STATES OF AMERICA, 2014e).

Além da definição da infraestrutura crítica, a FICCC também utiliza outra diretriz presente no Decreto nº 13636: a necessidade da formulação de uma série de normas, padrões e práticas que auxiliriam empresas a administrar riscos cibernéticos. O resultado foi o desenvolvimento da FICCC, criada através da aproximação do setor privado com o público, resultou em uma linguagem comum entre ambos. O objetivo seria gerenciar os riscos envolvidos na manutenção de uma segurança cibernética eficaz, sem adicionar novas exigências regulatórias

sobre as empresas. A FICCC não requer que a empresa abandone suas existentes práticas de segurança:o que é sugerido pelo governo é que as normas sejam agregadas à estratégia de segurança cibernética já presente na empresa - por isso, a FICCC é um plano de adesão voluntária. No caso de empresas desprovidas de um programa de proteção para seu domínio cibernético, o governo recomenda que as normas sejam utilizadas como norteadoras para desenvolvimento de um programa próprio e único, que seja capaz de atender as necessidades únicas de cada empresa e organização. A flexibilidade das diretrizes da FICCC permite que ela mantenha sua adaptabilidade não apenas em empresas; de fato, o governo norte-americano reconhece a capacidade de seu programa e recomenda sua adoção para outros Estados que possuam interesse em manter seu domínio cibernético seguro. Projetando um possível cenário futuro e fazendo uso da FICCC, os Estados Unidos da América buscam a uniformização do domínio cibernético mundial, dependente da adoção de Estados que estejam dispostos a adoção da *Framework* de Obama. O intuito do governo reside na criação de uma taxonomia comum e um mecanismo para que as empresas possam: descrever sua postura de segurança cibernética vigente; descrever o estágio de cibersegurança desejado; identificar e priorizar oportunidades para melhorias dentro de um contexto baseado na continuidade e repetição; avaliar o progresso em relação à busca do estágio de segurança almejado; e prover comunição estratégica entre as partes interessadas, tanto internamente quanto externamente a empresa (UNITED STATES OF AMERICA, 2014e).

Considerações Finais

Mesmo que os Estados Unidos da América, com sua posição de pioneirismo tecnológico, encontre um sistema internacional formado por nações dotadas de alta capacidade cibernética - visto que Nye (2010) relata a capacidade do poder cibernético de atuar como balanceador de poder nas relações internacionais, a nação estadunidense reconhece a necessidade do implemento de suas capacidades cibernéticas. Independente do caráter ofensivo ou defensivo, os Estados Unidos da América tomam atitudes legais(e ilegais, geralmente operacionalizadas pela NSA) focadas no implemento de suas capacidades de defesa cibernética. Apesar de o consenso quanto à defesa cibernética anteceder as doutrinas Bush e Obama, observa-se que foi apenas durante as administrações do século XXI que a segurança cibernética se torna palpável. De fato, essa começa a interferir na política externa da nação norte-americana, através do uso do poder cibernético. No ambiente interno, medidas legais tomadas pelo governo para supostamente garantir a segurança de sua população causaram grandes controvérsias. A invasão de privacidade, o compartilhamento de informações pessoais e espionagem, todas realizadas pelo governo dos EUA, acabaram sendo expostas ao público por Edward Snowden.

De maneira não declarada, o governo se aproveitou das leis (especialmente o Ato Patriótico) para realizar espionagem interna e externa aos domínios do país. Esse fato apenas acabou vindo a público em junho de 2013, quando ocorreu o vazamento de vários documentos da NSA via as ações de Edward Snowden. As evidências apresentadas por Snowden comprovaram que tanto a questão de transparência, quanto a questão de privacidade de informações da população norte-americana, presentes em suas publicações e discursos presidenciais, não estariam sendo respeitadas pelo governo. Não se limitando apenas a dados da população norte-americana, Snowden trouxe também documentos com informações sobre outros países, estava assim exposta a espionagem internacional realizada pelos Estados Unidos. De fato, a cooperação entre o governo e o setor privado reiterado tantas vezes por Barack Obama estava sendo realizada, mas não de uma maneira transparente como o presidente Obama exaltava. A cooperação entre o governo e empresas internacionais do ramo de comunicações garantiam um intenso fluxo de informações confidenciais a respeito de quem o governo norte-americano achasse necessário. Essa revelação acarretou sérias questões diplomáticas para os Estados Unidos, gerando grande instabilidade não só interna, mas também em suas relações internacionais (THE WASHINGTON POST, 2013).

As consequências do chamado "Efeito Snowden" possibilitam a elaboração de vários estudos na área das relações internacionais. Devido ao alcance global do material revelado por Snowden, vários países deram início a um processo de reformulação de seus sistemas de informação, assim como o questionamento das relações diplomáticas, comerciais e econômicas com os Estados Unidos.

Considerando-se a adaptação da agenda de segurança da nação estadunidense, que se molda de acordo com as necessidades de proteção do Estado, segundo Buzan e Hansen(2011), a adoção da cibersegurança por parte dos EUA ocorre por uma necessidade absoluta e natural. Somado a isso, há a frágil estrutura da internet norte-americana, extremamente ramificada e desprotegida, como afirma Clarke e Knake (2012), sendo apenas um controle estatal mais efetivo das redes internas de internet como sendo uma solução viável.

Como destacado por Rosenzweig (2013), um grave fator de insegurança cibernética no caso dos EUA é o alto grau de privatização dos sistemas. Com uma rede altamante ramificada, e um controle estatal praticamente inexistente, os EUA encontram-se em uma posição extremamente vulnerável, frente a ameaças cibernéticas. De certa forma, entende-se que o foco da política de *framework,* o FICCC de Obama, visa ao controle e compartilhamento de informações de empresas privadas com o governo, seja a resposta do presidente à ausência do governo no controle de suas redes de comunicação (UNITED STATES OF AMERICA, 2014e).

REFERÊNCIAS BIBLIOGRÁFICA

ANDRESS, Jason; WINTERFELD, Steve. **Cyber Warfare:** Techniques, tactics and tools for security practitioners.[S.L] Elsevier, 2011.

BILLO, Charles G.. **Cyber Warfare**: An Analysis of the Means and Motivations of Selected Nation States. 2004. Disponível em: <http://www.ists.dartmouth.edu/library/212.pdf>. Acesso em: 15 dez. 2013.

BOOZ ALLEN HAMILTON. **The Road to Cyberpower**: Seizing Opportunity While Managing Risk in the Digital Age. 2011. Disponível em: < http://www.boozallen.com/media/file/road-to-cyberpower.pdf&ei=QF2lUsDZD8qfkAfZ44G4CA&usg=AFQjCNGXNlfjpYyX94-kTW-W7tbmJgdZuQ&sig2=wxwvwG9stxDtk5zcOItsbw&bvm=bv.57752919,d.eW0>. Acesso em: 2 dez. 2013.

BUZAN, Barry; HANSEN, Lene. **The Evolution of International Studies**. Disponível em: <http://guessoumiss.files.wordpress.com/2011/08/the-evolution-of-international-security-studies.pdf>. Acesso em: 01 out. 2013.

CARR, Jeffrey. **Inside Cyber Warfare:** Mapping the Cyber Underworld, 2011.

CLARKE, Richard A.; KNAKE, Robert K. **Cyberwar**: The Next Threat to National Security and What to Do About It. Nova Iorque: Harper Collins, 2012.

DILANIAN, Ken. **Cyber-attacks a bigger threat than Al Qaeda, officials say**: Top intelligence officials say the foreign assaults are growing. They also sound an alarm about North Korea. Los Angeles, mar. 2013. Disponível em: <http://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313>. Acesso em: 10 jun. 2014

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. 5. ed. São Paulo: Atlas, 1999.

JORGE, Bernardo Wahl G. de Araújo. 2012. Estados Unidos, poder cibernético e a "guerra cibernética": Do Worm Stuxnet ao Malware Flame/Skywiper – e além.

NYE, Joseph. Cyber Power. 2010. Disponível em: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. Acesso em: 12 out. 2013.

NYE, Joseph. O Futuro do Poder. São Paulo: Benvira, 2012. Tradução de Magda Lopes.

ROSENZWEIG, Paul. **Cyber Warfare**: How Conflicts in Cyberspace are Challenging America and Changing the World. Santa Bárbara: Praeger, 2013

JENTLESON, Bruce W. **American Foreign Policy:** The Dynamics of Choice in the 21st Century. 4. ed. Nova Iorque: Norton & Company, 2010.

THE WASHINGTON POST. **Timeline:** The U.S. Government and Cybersecurity. 2003. Disponível em: <http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html>. Acesso em: 20 ago. 2014

THE WASHINGTON POST. **Edward Snowden Comes Forward as Source of NSA Leaks**. 2013. Disponível em: <http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html#>. Acesso em: 07 out. 2013.

THE WASHINGTON POST. **Confronting Digital Age Head-On**. 2006. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2006/03/12/AR2006031200938.html>. Acesso em: 11 set. 2014.

UNITED STATES OF AMERICA. 2001. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism** (USA PATRIOT ACT) Act of 2001. 107th Congress, 1st Session, H.R. 3162. October 25, 2001. Disponível em: <http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>. Acesso em: 10 set. 2014.

UNITED STATES OF AMERICA. 2004, Department of Justice. **The USA Patriot Act:** Preserving Life and Liberty. Disponível em: http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf. Acesso em 8 set. 2014

UNITED STATES OF AMERICA. 2009. Congress. **Comprehensive National Cybersecurity Initiative:** Legal Authorities and Policy Considerations. [S.I.]. Disponível em: <http://fas.org/sgp/crs/natsec/R40427.pdf>. Acesso em: 20 ago.2014.

UNITED STATES OF AMERICA. White House Office. **Cyberspace policy Review**: Assuring a Trusted and Resilient Information and Communications Infrastructure. Disponível em: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf . Acesso em : 27 set. 2014a

UNITED STATES OF AMERICA. White House Office. **Foreign policy**: cybersecurity. Disponível em: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity. Acesso em: 21 set. 2014b.

UNITED STATES OF AMERICA. White House Office. **Foreign Policy**: cybersecurity — Executive Order 13636. Disponível em: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636. Acesso: 21 set. 2014c.

UNITED STATES OF AMERICA. White House Office. **Cross-Agency Priority Goal**: cybersecurity. Disponível em: http://goals.performance.gov/content/cybersecurity. Acesso em: 23 set. 2014d.

UNITED STATES OF AMERICA. National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Cybersecurity.** Disponível em: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. Acesso em: 11 out. 2014e.

Recebido em Novembro de 2014
Aprovado em Dezembro de 2014