UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

MARIA CRISTINA DE CASTRO MOREIRA

A PARCERIA PÚBLICO-PRIVADA NA CIBERESTRATÉGIA NORTE-AMERICANA: UMA ANÁLISE COMPARATIVA ENTRE AS AÇÕES DOS GOVERNOS BUSH E OBAMA (2001-2017)

Porto Alegre
2019

MARIA CRISTINA DE CASTRO MOREIRA

A PARCERIA PÚBLICO-PRIVADA NA CIBERESTRATÉGIA NORTE-AMERICANA: UMA ANÁLISE COMPARATIVA ENTRE AS AÇÕES DOS GOVERNOS BUSH E OBAMA (2001-2017)

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Relações Internacionais.

Orientador: Prof. Dr. Érico Esteves Duarte

Porto Alegre

2019

CIP - Catalogação na Publicação

Moreira, Maria Cristina de Castro
A PARCERIA PÚBLICO-PRIVADA NA CIBERESTRATÉGIA NORTE-AMERICANA: UMA ANÁLISE COMPARATIVA ENTRE AS AÇÕES DOS GOVERNOS BUSH E OBAMA (2001-2017) / Maria Cristina de Castro Moreira. -- 2019.
89 f.
Orientador: Érico Esteves Duarte.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Relações Internacionais, Porto Alegre, BR-RS, 2019.

1. Parceria Público-Privada. 2. Ciberestratégia. 3. Cibersegurança. 4. Estados Unidos . I. Duarte, Érico Esteves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

MARIA CRISTINA DE CASTRO MOREIRA

A PARCERIA PÚBLICO-PRIVADA NA CIBERESTRATÉGIA NORTE-AMERICANA: UMA ANÁLISE COMPARATIVA ENTRE AS AÇÕES DOS GOVERNOS BUSH E OBAMA (2001-2017)

Trabalho de conclusão submetido ao Curso de Graduação em Economia da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Relações Internacionais.

Aprovada em: Porto Alegre, _____de _____de 2019.

BANCA EXAMINADORA:

Prof. Dr. Érico Esteves Duarte – Orientador
UFRGS

Prof. Dr. Eduardo Munhoz Svartman
UFRGS

Prof. Dr. Marco Aurélio Chaves Cepik
UFRGS

À minha família.

AGRADECIMENTOS

Gostaria de agradecer, em primeiro lugar, a Deus por me dar o dom da vida e também me agraciar com todas as oportunidades e bens que recebi. Agradeço à Divina Providência por ter me preservado, até o momento, e ter traçado caminhos para minha vida melhores do que eu jamais poderia imaginar. Agradeço a Deus por ter me guiado e me sustentado nesta estrada até aqui, trajetória que não foi fácil e tranquila, mas que me fez crescer intelectualmente, humanamente e espiritualmente. Dou graças a Deus por ter me feito nascer na minha família e estendo o agradecimento a ela também, pois foi minha base do início ao fim, em todas as minhas jornadas, mas em especial na faculdade, sempre acolhendo, ouvindo, aconselhando – e às vezes trabalhando junto também! Agradeço a Deus pelo meu namorado, também, que me acompanhou na reta final deste trabalho, especialmente, me relembrando diariamente como devemos fazer nossas tarefas com alegria e comprometimento, sem deixar de lado o que mais importa: a nossa fé. Dou graças a Deus pelos meus amigos, todos eles, de anos atrás e de dias atrás, cada um à sua maneira acompanhou, influenciou e encheu de alegria e sorrisos minha caminhada nestes anos de faculdade. Obrigada por cada apoio, conversa, risada, estudo e convivência, me fizeram e fazem ser quem eu sou, me fazem uma pessoa melhor! Agradeço a Deus a oportunidade de estudar na UFRGS e encontrar tantos professores que partilharam generosamente seus conhecimentos, e especialmente pelo meu prof. orientador, pelos ensinamentos, apoio, paciência e dedicação. Agradeço, por fim, a Deus por ter me apresentado meu grande amigo do Céu, São Josemaría Escrivá, que me ensinou, principalmente ao longo da construção desse trabalho, que as pequenas coisas são grandes quando feitas com amor e que, fazendo essas pequenas coisas bem e com todo nosso esforço empenhado nelas, diante dos olhos do Pai elas se tornam coisas enormes e valiosas! Amo muito e me espelho em todos vocês!

Àquele que puder ser sábio,
não lhe perdoamos que não o seja.

São Josemaría Escrivá

RESUMO

O presente trabalho tem como objetivo analisar a ciberestratégia de segurança dos governos Bush e Obama, especificamente no que tange a presença da parceria público-privada nas suas ações relativas ao ciberespaço. O ambiente ciber apresenta peculiaridades e situações únicas, com mudanças constantes, que afetam a segurança dos países de uma maneira abrangente nunca antes verificada, envolvendo infraestruturas críticas, responsabilidade tanto do governo, como do setor privado. Busca-se identificar a existência de um padrão de comportamento dos governos ao trabalharem a parceria ou verificar se há mudanças marcantes entre as ações de um presidente ou de outro. O método de pesquisa qualitativo de pesquisa documental foi utilizado, a partir da análise de conteúdo de quatro documentos emitidos pelos governos Bush e Obama. Verificou-se uma quantidade maior do que a esperada das menções relacionadas à parceria público-privada nos documentos do Governo Bush. Essa situação é explicada pelo contexto de confronto ao ciberterrorismo e proteção das infraestruturas críticas. Pela análise quantitativa, verifica-se que no Governo Obama a parceria foi mais valorizada e procurou-se organizá-la de forma a auxiliar e envolver ainda mais o setor privado. No entanto, o Governo Obama encontrou dificuldades em realizar as mudanças propostas, apenas dando continuidade às ações iniciadas no Governo Bush, pois, neste período, transparência e respeito à privacidade dos cidadãos passaram a ser os tópicos centrais dos temas de cibersegurança. Concluiu-se que, ao longo do período, a parceria público-privada se desenvolveu de forma desorganizada e sem objetivos comuns, o que dificultou o engajamento das empresas privadas. Ao fim da análise, chega-se à conclusão de que, para que a parceria se desenvolvesse a ponto de suprir todas as deficiências encontradas na comunicação e compartilhamento de tecnologias entre os setores público e privado, seria necessário um aprimoramento ou, até mesmo, uma ruptura com a estratégia adotada pelos governos.

Palavras-chave: Parceria Público-Privada. Ciberestratégia. Cibersegurança. Estados Unidos. Ciberespaço. Barack Obama. George J. Bush.

ABSTRACT

This paper aims to analyze the Bush and Obama administrations cybersecurity strategy, specifically regarding the presence of public-private partnership in their cyberspace actions. The cyber environment presents unique peculiarities and situations with constant changes that affect the security of countries in a comprehensive way never verified before, involving critical infrastructures, responsibility of both the government and the private sector. This analysis aims to identify the existence of a behavioral pattern of the two administrations when working on the partnership and to verify if there are marked changes between the actions of one president to another. The qualitative research method of documentary research was used, based on the content analysis of four documents issued by the Bush and Obama administrations. There were more than expected mentions of public-private partnership in the Bush administration documents. This situation is explained by the context of confrontation with cyberterrorism and protection of critical infrastructures. From the quantitative analysis, it appears that the Obama administration valued the partnership more and sought to organize it in such a way as to assist and further involve the private sector. However, the Obama administration found it difficult to make the proposed changes, only continuing the actions initiated under the Bush administration, as transparency and respect for citizens' privacy became the central topics of cybersecurity in this period. It was concluded that, over the period, the public-private partnership developed in a disorganized way and without common goals, which made it difficult for private companies to engage. At the end of the analysis, it is concluded that, in order for the partnership to develop to the point of addressing all the deficiencies found in the communication and sharing of technologies between the public and private sectors, it would be necessary to improve or even break with the strategy adopted by the administrations.

Keywords: Public-Private Partnership. Cyber Strategy. United States. Cybersecurity. Cyberspace. Barack Obama. George J. Bush.

LISTA DE ABREVIATURAS E SIGLAS

ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
ASEAN	*Association of Southeast Asian Nations*
CNCI	*Comprehensive National Cybersecurity Initiative*
CTIIC	*Cyber Threat Intelligence Integration Center*
DCS/SCADA	*Digital Control Systems/Supervisory Control and Data Acquisition Systems*
DHS	*United States Department of Homeland Security*
DoD	*United States Department of Defense*
EFF	*Eletronic Frontier Foundation*
EUA	Estados Unidos da América
GPO	*Government Printing Office*
INTERNET	*International Net*
ISACs	*Information Sharing and Analysis Centers*
ITMF	*Information Technology Modernization Fund*
ITU	*International Telecommunications Union*
NASA	*National Aeronautics and Space Administration*
NISAC	*National Infrastructure Simulation and Analysis Center*
NIST	*National Institute for Standards and Technology*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OMB	*Office of Management and Budget of the White House*
PCCIP	*President's Comission for Critical Infrastructure Protection*
PCSs	*Process Control Systems*
PPP	*Public Private Partnership* / Parceria público-privada
SAM	*Stakeholders, activities and motives*
SOX	*Sarbanes-Oxley Act*
TABC	*Trans-Atlantic Business Council*
TABD	*Transatlantic Business Dialogue*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TI	Tecnologia da Informação
USA	*United States of America*

SUMÁRIO

1 INTRODUÇÃO

O debate sobre cibersegurança e estratégia para o ciberespaço tem adquirido maior relevância no estudo das Relações Internacionais, visto que o desenvolvimento do ciberespaço – esse cenário com características únicas, com oportunidades e desafios novos para a ação estatal e demais atores – tem acontecido de forma cada vez mais rápida, englobando o dia a dia de mais indivíduos, organizações e Estados (NYE, 2010). Segundo Mary Ellen O'Connell (2012), professora e pesquisadora em Direito Internacional na Universidade de Notre Dame (Indiana, EUA), o termo "ciber" tem presença constante nas discussões que tratam sobre segurança internacional na atualidade e as ameaças cibernéticas têm se tornado uma preocupação presente nas agendas de políticas públicas e política externa dos países. A relevância estratégica vem sendo verificada, principalmente no campo da defesa, em economias desenvolvidas como Estados Unidos, Reino Unido e Austrália, de acordo com Choo (2011), professor da Universidade do Texas em Santo Antonio (Texas, EUA). Lewis (2002, p. 1, tradução nossa)[1] sinaliza na primeira página de seu artigo que os "Ataques cibernéticos, segurança de rede e informações colocam problemas complexos que atingem novas áreas de segurança nacional e políticas públicas", sendo natural esse foco crescente dos Estados em criar políticas de defesa que protejam seu país dos perigos enfrentados no ciberespaço.

Verificando-se a relevância que o tema do ciberespaço vem adquirindo na agenda de defesa e segurança dos mais diversos Estados no globo, torna-se relevante uma análise primária do desenvolvimento da estratégia para o tema de uma das principais potências do século XXI. Os Estados Unidos, apresentam-se deste modo, como ponto de referência para se entender o movimento de outros países, sejam eles potências ou países em desenvolvimento no Sistema Internacional. Vem sendo identificada como uma prática comum a países que ainda não tiveram graves problemas com ciberataques, basear-se no histórico e reação de outros países que já tiveram maior contato com o assunto (ACÁCIO; LOPES, 2012) para definir suas políticas de cibersegurança, mostrando-se assim, novamente, a importância do estudo do caso norte-americano.

---

[1] *"Cyber attacks, network security and information pose complex problems that reach into new areas for national security and public policy."* (LEWIS, 2002, p. 1).

Desde 2002, principalmente após os atentados do 11 de Setembro, é possível verificar a preocupação crescente dos Estados Unidos com a defesa frente às ameaças presentes no ciberespaço, com a adoção de uma série de medidas e políticas para aumentar a segurança do país em relação ao ciberespaço nos últimos 17 anos. Muitas dessas medidas estão registradas em documentos oficiais, onde se observa a percepção americana e também se identifica a evolução da abordagem ao longo desse período, também em relação à parceria público-privada. A partir destes documentos é possível verificar que a cibersegurança nacional esteve em pauta de maneira presente e constante nos governos Bush e Obama – apesar de sua divergência em termos políticos e ideológicos, visto que o Governo Bush era guiado pelos ideais republicano e já o Governo Obama tinha viés democrata -, destacando-se o relacionamento entre os governos e as empresas privadas. Um dos principais diferenciais das políticas de ciberdefesa é este caráter fundamental da comunicação e parceria entre o setor público-privado, alinhando interesses e fomentando o conhecimento do campo para desenvolver a estratégia do governo de defesa nacional e internacional no ciberespaço. Segundo McCarthy (2018), a parceria público-privada pode ser considerada a melhor ferramenta para se enfrentar os desafios da cibersegurança atualmente. Essa relevância se dá principalmente pelo fato de a maior parte das infraestruturas críticas estarem sob domínio de empresas privadas.

O presente trabalho buscou contribuir com o fomento do estudo sobre cibersegurança, que vem conquistando importância ano a ano no cenário das Relações Internacionais. Para tanto, foi realizada uma análise comparativa e balanço da evolução da parceria público-privada na estratégia de cibersegurança dos governos dos Estados Unidos nos anos de 2001 a 2017, sendo este país pioneiro e líder no envolvimento estatal nas questões do ciberespaço. A partir desta análise, discorreu-se sobre a correlação entre a expansão do ciberespaço[2] (ESTADOS UNIDOS, 2006) no período, com um melhor delineamento[3] da estratégia governamental norte-americana em relação à parceria público-privada neste espaço,

[2] Define-se “expansão do ciberespaço” como o alcance global que a infraestrutura da tecnologia da informação atingiu, de acordo com documento do governo federal dos Estados Unidos (ESTADOS UNIDOS, 2006), crescendo, sem precedentes: o volume de informações eletrônicas, a proliferação de novas aplicações e serviços, e a troca de informações dentro do que se chama “ciberespaço”.

[3] Define-se “melhor delineamento” como a verificação de melhorias tanto quantitativas – de investimento e direcionamento de recursos humanos e materiais –, quanto qualitativas – de análise do emprego desses fatores quantitativos e seus resultados subjetivos.

visando acompanhar a evolução identificada anteriormente. O trabalho foi elaborado de forma a, em primeiro lugar, contextualizar e conceituar a temática do ciberespaço, para então proceder-se com a construção de um panorama da evolução do mesmo no período e aprofundar-se no recorte definido dentro da estratégia norte-americana para o ciberespaço: a parceria público-privada. Neste sentido, buscou-se analisar de modo mais detalhado algumas ações dos governos vigentes no período em questão, revisando documentos emitidos pelos Governo de Bush e, posteriormente, de Obama.

Essa análise foi feita através de descrição e avaliação dos elementos contextuais da construção e execução de cada estratégia, por meio da revisão de quatro documentos específicos ao tema, emitidos por cada governo, a saber: *The National Strategy to Secure Cyberspace (2003)* e *Federal Plan for Cyber Security and Information Research and Development: Report by the Interagency Working Group on Cyber Security and Information Assurance* (2006) do Governo Bush; *Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) e *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011) referentes ao Governo Obama. Além disso, também buscou-se identificar o grau de causalidade do contexto, estrutura e interações. Desta forma, a análise teve como objetivo, ainda, identificar os principais pontos das estratégias para o ciberespaço da parceria público-privada, procurando concluir a existência ou não de um padrão, uma estabilidade ou uma evolução/involução na conduta dos governos norte-americanos. Concluindo a análise, realizou-se uma comparação entre as estratégias de cada governo, de modo a inferir se houve realmente uma mudança no *modus operandi* da estratégia norte-americana para o ciberespaço em relação à parceria público-privada, identificando as variáveis causais da ocorrência ou não dessa mudança. Por fim, também era objetivo do trabalho trazer uma abordagem preliminar do tema, visto que esse não se apresentou como uma aplicação teórica, por falta de teorias consolidadas sobre o ciberespaço e as Relações Internacionais.

Para realizar essa análise, o método de pesquisa qualitativo de pesquisa documental foi utilizado, tomando como exemplo o trabalho de Souza Junior e Streit (2017) na sua avaliação da política brasileira para a cibersegurança em comparação com a experiência internacional de países como Estados Unidos, Índia, África do Sul e Reino Unido. Essa abordagem, segundo Godoy (1995), prevê como meio de

análise o exame de documentos/artigos que não tiveram tratamento analítico profundo ou que podem ser novamente analisados, para se construir novas interpretações ou complementos às pesquisas já existentes, mostrando-se a abordagem mais adequada a ser empreendida neste trabalho. Por esta razão, aplicou-se a ordem de organização de aplicação do método exposta por Godoy (1995): em primeiro lugar os documentos citados acima foram identificados e selecionados para serem codificados e analisados – sendo a análise de conteúdo uma das técnicas mais utilizadas (BARDIN, 1977). Dentro da análise de conteúdo, realizaram-se os 3 passos propostos: (i) a pré-análise, fase de organização e levantamento de documentos; (ii) a categorização, codificação e classificação das informações, focando para análise quantitativa na quantidade de vezes que o tema é citado, e para a qualitativa, que forma/qual a relevância da citação do cerne do trabalho: a parceria público-privada, sendo assim *"public-private"* o principal termo analisado, por ser atrelado à parceria analisada; e, por fim, (iii) a soma das informações "brutas" dos documentos oficiais ao conhecimento advindo dos estudos desenvolvidos na área, de maneira a dar significado ao material construído. A partir dessa análise, foi possível a identificação dos movimentos e evoluções do governo norte-americano ao longo do período analisado, sinalizando padrões e tendências da relação analisada no trabalho (GODOY, 1995).

2 CIBERESPAÇO: UM PANORAMA

Emitir opiniões a respeito de Internet – bem como do espaço que utilizamos ao "navegar" por ela – parece muito natural e simples à maioria das pessoas, nos dias de hoje, uma vez que se tem um acesso bastante difundido dessa rede de comunicações ao redor de todo globo. Previa-se que, no ano de 2018, atingir-se-ia a marca de 51% da população utilizando a Internet em todo o mundo, segundo dados apresentados pelo diretor da *International Telecommunications Union* (ITU), Houlin Zhou (MAIS DA METADE, 2018) e é esse tipo de afirmação que pode acabar gerando uma falsa impressão de conhecimento e entendimento do tema, dada a extrema facilidade de acesso à rede mundial de computadores. Não é o que, de fato, acontece, visto que a internet é um ambiente complexo, com diversas particularidades e situações únicas, não presenciadas no mundo "real". Embora a internet seja acessível a muitos, poucos são os que compreendem a sua complexidade, principalmente quando se busca analisá-la do ponto de vista da cibersegurança nas Relações Internacionais.

Neste capítulo, buscar-se-á discutir alguns conceitos e princípios básicos para empreender uma análise própria de Relações Internacionais sobre o tema. Também serão apresentadas, também, algumas das abordagens de Teoria das Relações Internacionais voltadas ou adaptadas ao ciberespaço e cibersegurança, bem como os problemas identificados em tentativas de utilização de teorias já consolidadas, aplicadas a um ambiente totalmente novo e diferente dos anteriormente abordados nas teorias mais difundidas. Por fim, discorrer-se-á sobre o pioneirismo e liderança dos Estados Unidos, em se tratando de ciberespaço e cibersegurança, bem como a relevância das parcerias público-privadas no desenvolvimento de uma estratégia abrangente de cibersegurança.

2.1 CONCEITO E DEFINIÇÃO DE CIBERESPAÇO E CIBERSEGURANÇA

O estudo do ciberespaço tem sido uma tarefa empreendida há mais de 3 décadas e ainda hoje é difícil identificar uma definição que seja bem aceita e utilizada de maneira ampla por diversos autores e estudiosos do tema. É questão recorrente, identificada nas pesquisas relativas ao ciberespaço, a discussão sobre a dificuldade de conceituar e abordar determinados fatores ou pontos fundamentais na

análise do ciberespaço – quando a dificuldade não se dá em definir o próprio ciberespaço – de maneira precisa (ACÁCIO; LOPES, 2012; HARKNETT; STEVER, 2011; NYE, 2010; PORTELA, 2016; SCHNEIER, 2015; SOUZA JUNIOR; STREIT, 2017). De todo modo, apesar das dificuldades e, muitas vezes, das imprecisões dos conceitos apresentados, é necessário que o presente trabalho se apoie em uma definição mais delimitada e razoável diante da proposição do que se busca discutir e apresentar.

Em 2009, Daniel Kuehl, em um esforço de melhor definir o termo, empreendeu uma análise de 14 definições diferentes de "ciberespaço" coletadas ao longo dos anos e postulou uma nova definição, a partir de desenvolvimento de ideias extraídas dessas definições e demais elementos identificados em sua pesquisa. De acordo com Kuehl (2009, p. 4, tradução nossa)[4],

> [...] ciberespaço é um domínio global dentro do ambiente de informação, cujo caráter único e distinto é enquadrado pelo uso de eletrônicos e espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de comunicação de informação.

Essa definição se adequa ao presente trabalho, visto que destaca os aspectos tecnológicos e eletrônicos fundamentais ao caráter único deste ambiente sem, no entanto, utilizar termos técnicos específicos de Tecnologia da Informação. O uso de tais vocábulos apenas dificultaria a compreensão daqueles que, interessados no ciberespaço no campo das Relações Internacionais, não têm a necessidade de deter-se em questões técnicas referentes a redes e protocolos da internet. Interessa destacar também que, apesar de dispormos de diversas definições de ciberespaço – que não serão apresentadas aqui –, variando de acordo com a ótica com a qual se analisa o mesmo, ainda assim existe um ponto comum entre a maioria das definições desenvolvidas: a ideia de comunicação via dispositivos de computação (BRYANT, 2016).

Sob o olhar das Relações Internacionais, o ciberespaço, então, faz parte dos cinco domínios onde os Estados disputam poder e soberania: o domínio terrestre, marítimo, aéreo, espacial e agora ciberespacial, cada qual com suas particularidades

---

[4] *"[...] cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."* (KUEHL, 2009, p. 4)

e diferenças, mas todos interligados pela necessidade de utilização de tecnologia para atuação eficiente em cada um dos ambientes (KUEHL, 2009). No entanto, é apenas no ciberespaço que se observa essa relação com a tecnologia como fundante do próprio espaço de atuação, sendo necessária essa conexão para haver interação no espaço. A interconexão e interdependência de redes de informação e sistemas inerentes ao ciberespaço se deve ao fato de este ser um domínio que reside simultaneamente no campo físico e no virtual, e que permite um trânsito instantâneo dos seus usuários ao redor do mundo sem que existam muitas barreiras limitantes ou fronteiras definidas (KUEHL, 2009). Propriamente dito, dentro do campo virtual do ciberespaço, é praticamente impossível definir uma fronteira e, muitas vezes, também torna-se difícil distinguir a nacionalidade de cada um dos usuários, bem como as localidades de origem de ameaças que podem emergir dentro desse campo.

Esse campo totalmente novo e emergente é resultado de características únicas do Século XXI, como comunicação instantânea e desenvolvimento de tecnologias e inteligência artificial; e a preocupação com as oportunidades e desafios que surgem com esse novo domínio, fazendo com que os Estados se interessem em buscar uma boa adaptação das ações para um cenário desconhecido e pouco explorado, até agora. O ciberespaço representa um novo domínio estratégico e fundamental para a manutenção da soberania de cada Estado (ACÁCIO; LOPES, 2012), porém ainda são muitas as dificuldades com que se deparam os Estados ao explorarem esse novo domínio, pois o ciberespaço traz consigo uma dicotomia intrínseca. Segundo Nye (2010), é um ambiente que propicia o desenvolvimento, pois abre caminhos, traz acessibilidade e melhora a comunicação e compartilhamento de conhecimento para todas as camadas da sociedade. Em contraponto, por ser ter praticamente uma ausência de fronteiras e o anonimato ser facilitado neste ambiente, é muito mais fácil de se cometer crimes e ataques sem uma punição, o que acaba criando um “clima” de insegurança e a expectativa de se estar sofrendo ameaças recorrentemente (NYE, 2010). Tendo-se essa sensação de insegurança e ameaça pairando sobre o ar, tende-se a esperar que o Estado procure desenvolver meios de defender sua nação e sua população de possíveis ataques e perigos que sofram através dos meios *online* (HARKNETT; STEVER, 2011). Para suprir essa necessidade, os Estados têm procurado desenvolver e formular estratégias para a segurança no ciberespaço, surgindo,

assim, conceitos de cibersegurança e ciberdefesa na rotina da construção das políticas internas e externas dos países. No entanto, muitas vezes, falta aos governos *expertise* e tecnologia desenvolvida para a área de atuação, sendo o aspecto de maior conhecimento destes, o fato de que existem muitas vulnerabilidades na área de segurança cibernética, sem ter meios para identificação e contenção desses riscos de maneira efetiva, como já têm desenvolvidos em outras áreas. Neste contexto, identificamos a primeira situação em que se percebe que uma parceria com o setor privado é necessária e desejada pelos governos, visto que muitas empresas privadas já vêm desenvolvendo tecnologia específica de segurança no ciberespaço há mais tempo e se dedicando a esse tópico em específico. É do interesse dos governos, deste modo, entender de que maneira agem individualmente as empresas no quesito cibersegurança, a fim de aplicar o que for pertinente às estratégias nacionais de maneira ampla e geral.

Por ser o ciberespaço, conforme já exposto, muito complexo, abrangendo tanto o ambiente físico como o digital, existem diversos problemas de delimitação de alguns dos componentes-chave desse ambiente. A própria essência do ciberespaço acaba criando uma dificuldade de identificação de padrões de previsibilidade, problemática enfrentada tanto pelos pesquisadores – que visam formular teorias – quanto pelos estadistas e interessados na temática do ciberespaço e da cibersegurança – que buscam criar estratégias e métodos de combate a ameaças cibernéticas. Os principais pontos de destaque levantados nesse debate, em que se observa as diferenças e peculiaridades identificadas no ciberespaço, são: o custo, os atores, as assimetrias, as responsabilidades, as questões geográficas e o anonimato (HARKNETT; STEVER, 2011; NYE, 2010). Todos esses pontos também devem ser referenciados de maneira uniforme, pois se verifica que se interligam e são necessários na compreensão uns dos outros no contexto do ciberespaço.

Diferente de outros domínios – como, por exemplo, o espaço – o acesso ao ciberespaço é facilitado e difundido, tendo um custo bastante abaixo da média de investimento, quando comparado com outros domínios. Não são necessários grandes recursos ou *expertise* para explorar o ciberespaço. Segundo Sheldon (2015, p. 309, tradução nossa)[5], “Qualquer pessoa com acesso a tecnologias de comunicação de informação em rede pode usá-lo (o ciberespaço)”. Os Estados

[5] *“Anyone with access to networked Information-communication technologies can use it.”* (SHELDON, 2015, p. 309).

acabam exercendo uma atuação mais limitada, visto que esse espaço é compartilhado entre os setores públicos e privados e explorado por indivíduos (LOBATO; KENKEL, 2015). São diversos os atores envolvidos e relevantes agindo e conquistando seu espaço no domínio ciber: indivíduos, coletivos, grupos, organizações, empresas e Estados (KREMER; MÜLLER, 2014). Cada um deles tem seus próprios interesses e modos de atuação, nem sempre condizentes com os dos demais, dos quais surgem alguns dos problemas de assimetrias. Apesar de verificarmos a existência de muitos atores coexistindo no ciberespaço e muitos dos atores menores, como Estados pequenos e mesmo indivíduos ou organizações/grupos, por certas vezes, ganhando espaço, ainda é clara a soberania dos Estados frente aos demais. Há, dessa forma, uma maior difusão de poder e existe uma possibilidade maior de acesso aos recursos de poder por diferentes tipos de atores. No entanto, Nye (2010) relembra diversas vezes ao longo dos seus trabalhos sobre ciberespaço e ciberpoder, que difusão de poder não é o mesmo que equalização de poder, de modo que ainda há assimetrias neste espaço. Existe uma maior inclusão de atores e formas de atuação, embora ainda existam fatores como acesso facilitado a recursos e tecnologia de ponta, que beneficiam os grandes e tradicionais atores.

Essa vantagem dos Estados em relação aos demais atores presentes no ciberespaço existe, porém, em contrapartida, há uma série de responsabilidades que acabam tornando-se parte do escopo das preocupações do Estado no ciberespaço. Espera-se que, por ter maiores recursos e deter mais poder, os governos protejam suas nações também nesse âmbito, além de procurarem estabelecer objetivos no ciberespaço que contemplem sua população. Desse modo, ocorre uma maior mobilização e participação por parte dos governos estaduais, governos locais e empresas privadas na construção das estratégias para cibersegurança dos Estados, visto que cada um deseja defender seus interesses próprios pertinentes a cada setor de atuação (HARKNETT; STEVER, 2011; THOMAS, 2013). Um dos maiores desafios dos Estados em proteger satisfatoriamente sua nação no ciberespaço é a dificuldade de se responsabilizar os autores de ameaças sofridas internamente. Essa situação explica-se por que o ciberespaço, conforme apontado anteriormente, tem um certo nível de presença física, passível de obter-se uma localização geográfica bem definida correlata a algum país, porém, a porção maior do ciberespaço se encontra fora do espaço físico. Falta uma delimitação precisa desse

ambiente, que tende a crescer cada dia mais, sem fronteiras, sem uma geografia bem definida (HARKNETT; STEVER, 2011). Nye (2010) também trata sobre a dificuldade de se delimitar o ciberespaço, por sua geografia mutável, com menos barreiras e custos, que compromete até a identificação de “distâncias” dentro desse espaço.

Por fim, outra questão que traz complicações à responsabilização de ataques no ciberespaço é o anonimato. A arquitetura do ciberespaço mundial, com características de interligação, geografia fluida, falta de normas e rapidez de troca de informação, propicia e facilita que os atacantes neste meio se escondam atrás de camadas de proteção e “mascarem” a verdadeira origem dos ataques (LOBATO; KENKEL, 2015). Uma das particularidades do ciberespaço é justamente essa: atores pequenos, como uma pessoa sozinha, com algum recurso adquirido com baixo custo conseguem afetar recursos físicos – que têm maior custo – de grandes atores (NYE, 2010). Localiza-se nesta, a questão da responsabilidade dos ataques no ciberespaço: quando ocorre um ataque via internet que afeta estruturas físicas, sejam públicas ou privadas, espera-se uma resposta do governo do país atingido. Porém, existe essa dificuldade de identificação dos verdadeiros responsáveis pelo ataque e falta definição de regras sobre como agir e punir esse tipo de situação. O que acaba ocorrendo é uma responsabilização do Estado de onde o ataque originou-se, quando é possível identificar (KREMER; MÜLLER, 2014), levando o âmbito de discussão e “combate” para a relação entre Estados diretamente.

Com a definição das principais características particulares do ciberespaço e também da cibersegurança verifica-se que, “o novo ambiente cibernético mundial proporcionou o surgimento de novas ameaças à integridade de todas as nações mundiais” (RIBEIRO; RIVERA, 2014, p.140). Observa-se que os Estados enfrentam tanto riscos de serem atacados e prejudicados nos níveis virtuais e físicos, tendo prejuízos inimagináveis antes do advento do ciberespaço, quanto de também estarem sempre passíveis de serem responsabilizados por atos e ataques que têm origem em empresas e indivíduos situados em seu país.

2.2 STATUS DOS ESTUDOS TEÓRICOS NA ÁREA

A maior dificuldade e o maior consenso nas análises sobre o ciberespaço e a cibersegurança dos países é o fato de que não se encontra, dentre as Teorias de Relações Internacionais "tradicionais"[6], uma teoria que abarque adequadamente o ciberespaço, seus atores, suas relações e peculiaridades. Acácio e Lopes (2012) propõem uma tentativa de fazer um balanço geral sobre essa temática específica, analisando como as teorias mais utilizadas – Realismo, Escola Inglesa, Neoliberalismo e Escola de Copenhague – se aplicariam/aplicam ao ciberespaço.

No Realismo, mostram que haveria uma continuidade do pensamento que já foi exposto pelos principais autores da teoria, como Waltz (2002), onde os Estados constituiriam suas capacidades cibernéticas com a finalidade de maximizar seus interesses nesse novo cenário de atuação. Em complemento, mencionam o "*National Accountability*", conceito que explica que os Estados teriam responsabilidade sobre qualquer ataque oriundo do seu país em direção a outro através da utilização do ciberespaço, mesmo que não se trate de uma ação governamental. Sobre a Escola Inglesa, apresentam reflexões sobre o que seria possível utilizar da teoria para entender o ciberespaço e suas novas dinâmicas, visto que os principais autores dessa teoria não viveram para verificarem os avanços da Internet. A principal delas vem a ser a abordagem de como a guerra está vinculada à política do poder e como o histórico de ação de um Estado influencia nas decisões estratégicas de outro.

Abordando a Escola de Copenhagen, reportam a questão da segurança como algo que é uma ameaça existencial, o que leva as autoras desta corrente – Hansen e Nissenbaum (2009) – a buscarem desenvolver um adendo à teoria, com a criação de um Setor de Segurança Cibernética. Este deve abordar a "[...] hipersecuritização, práticas cotidianas e tecnificações – porque estes não podem ser encontradas na dinâmica de outro Setor apresentado pela Escola de Copenhague." (ACÁCIO; LOPES, 2012, p. 20). Na abordagem Neoliberal, por ter autores mais contemporâneos, tem-se um desenvolvimento do assunto de maneira mais contextualizada, onde entende-se os Estados como principais atores do Sistema Internacional – o que inclui o ciberespaço –, sem, no entanto, excluir a existência de

[6] Por tradicionais pretende-se referir-se às teorias já consolidadas e reconhecidas no campo.

outros atores relevantes e influentes, mas secundários. Esta corrente teórica traz a ideia de que existe a possibilidade dos Estados cooperarem para obterem ganhos conjuntos. Acácio e Lopes (2012) citam Nye (2011), importante autor neoliberal e pesquisador na área, para tratar sobre o significado de poder no ciberespaço, expondo a ideia de que o poder é o mesmo que vemos em outras esferas do Sistema Internacional, sendo modificada, na realidade, sua natureza e a maneira como ele é difundido. Por fim, essa corrente levanta também a ideia de que é possível que aconteça uma promoção de regimes internacionais no ciberespaço, onde os Estados buscariam coletivamente obter vantagens frente a outros regimes e/ou blocos.

Joseph Nye é o autor que aparece dentre os nomes mais importantes das Teorias de Relações Internacionais “tradicionais” que vêm desenvolvendo estudos sobre o ciberespaço e as relações internacionais. Tem seu foco principalmente na análise da difusão e funcionamento do monopólio do poder por parte dos Estados nessa realidade (NYE, 2010). Suas principais ideias, que contribuem para as discussões sobre o tema, além da abordagem sobre o poder no ciberespaço, tratam sobre os diversos atores envolvidos e seus recursos para agir neste campo. Dessa forma, sai da ideia do realismo de que apenas os Estados são atores, abordando a ação de organizações e também indivíduos – uma visão que agrega muito mais à análise da cibersegurança, por ter mais semelhança com a lógica e funcionamento das relações dentro do ciberespaço. Além disso, conforme exposto na seção anterior, também trata a dificuldade de delimitar o ciberespaço, por este ter uma geografia mutável, com menos barreiras e custos, fazendo com que seja difícil até se identificar “distâncias” dentro desse espaço. Outra contribuição importante do autor é a colocação de que existe uma certa dicotomia no ciberespaço como ambiente de desenvolvimento. Se de um lado ele abre caminhos, traz acessibilidade e melhora a comunicação e compartilhamento de conhecimento para todas as camadas da sociedade; de outro, por serem nesse âmbito praticamente inexistentes as fronteiras e o anonimato ser facilitado, é muito mais fácil de se cometer crimes e ataques sem uma punição, o que acaba criando um “clima” de insegurança. Nye (2010) ainda aponta para a necessidade de cooperação e de maior regulamentação deste espaço, o que, no entanto, nem sempre é facilitado pelos Estados – que ainda têm maior poder dentre os atores –, por também ser do interesse deles, em parte, esta instabilidade.

Dentre o esforço de se tentar analisar o ciberespaço através da ótica de teorias já existentes, encontram-se também estudos que abordam teorias não tão clássicas nas RI, mas já consolidadas e bem estruturadas. Exemplo disso são o trabalho sobre a cibersegurança e a Escola de Copenhagen (HANSEN; NISSENBAUM, 2009) e também a análise sobre possíveis aplicações de conceitos de poder e violência, segundo a visão de Hannah Arendt, no ciberespaço (BELOW, 2014). Conforme retratado anteriormente por Acácio e Lopes (2012), as autoras do trabalho sobre a Escola de Copenhague sugerem um novo "setor" dentro do estudo, além dos já estipulados tradicionalmente pela corrente teórica: Política, Militar, Econômico, Societal e Ambiental. Fazem, então, esse esforço de caracterizar o "Setor Cibernético", tendo como intuito preencher a lacuna existente nos estudos de segurança sobre a cibersegurança, trazendo três conceitos-chave para a análise do ciberespaço: hipersecuritização, práticas cotidianas e tecnificações. No entanto, no próprio artigo, ainda que defendam seu ponto de vista, as autoras já apontam possíveis críticas que podem ser feitas à sua própria formulação, o que dificulta a ampla aceitação da abordagem teórica proposta. Dentre as críticas, vemos a argumentação de que, teoricamente, a aplicação do Setor Cibernético e seus conceitos deveriam ser gerais e comuns a todas as realidades, porém vê-se que a relevância desses pontos fundamentais da abordagem das autoras varia de importância quando se analisa a cibersegurança sob a perspectiva de um regime não-democrático. Desta forma, entende-se que os conceitos-chave apontados anteriormente são significantes, mas sua formulação e entendimento/relevância vão mudar de acordo com a configuração do regime e da maneira como a sociedade é incluída nessa discussão (HANSEN; NISSENBAUM, 2009).

A outra tentativa de abordagem e conceituação sobre cibersegurança parte de Below (2014), trazendo os conceitos de poder e violência de Arendt para serem aplicados nessa nova área. Hannah Arendt não chegou a viver o suficiente para poder aplicar e adaptar seus estudos ao contexto do ciberespaço. No entanto, Below (2014) se empenha em fazer essa ligação entre os dois campos de estudo, ainda que separados temporalmente, pelo fato dos conceitos de Hannah terem base no humano e sua vida, o que faz sentido quando se tenta transpor ao ciberespaço, visto que a Internet é um ambiente onde muitos atores, dos mais diversos tipos, têm contato constante e direto. Além disso, é um local onde o indivíduo acaba tendo uma relevância única, mesmo quando se analisa o tema a nível das relações

internacionais. Mais uma vez, as análises de Teorias de Relações Internacionais mostram como as teorias clássicas, que veem o Estado como ator único, são falhas quando se busca entender relações cibernéticas, que inevitavelmente envolvem atores de diversos tipos e com relevâncias diferentes. A principal contribuição de Below (2014) é trazer o conceito de poder como um "*espaço de aparência*", espaço de liberdade para os indivíduos, levando muito em conta a participação cívica e engajamento da sociedade na construção da ação do Estado. Below (2014) sugere, então, que o ciberespaço seria um novo espaço para relacionamentos/*networking* políticos livres, afirmando, inclusive, que o acesso à Internet deveria ser visto como um direito humano. Seria nesse espaço que os indivíduos teriam a maior abertura para debaterem sobre os temas de seu interesse, o que leva a autora a afirmar que "Indivíduos atuando em conjunto em assuntos políticos através do discurso representam a concepção de poder de Arendt em contraste com a violência [...]." (BELOW, 2014, p.103, tradução nossa)[7]. A teorização de Below se estabelece em torno desse conceito, no entanto é possível identificar um problema na leitura que se faz da teoria de Arendt, pois o argumento acaba sendo personalista demais e espera que todo cidadão seja consciente e participativo. Ela direciona grande foco ao indivíduo – uma relevância necessária, mas por vezes demasiada –, tratando como se o cidadão médio realmente estivesse interessado e engajado em participar de organizações cívicas, o que nem sempre ocorre. Além disso, para análise deste trabalho, a abordagem torna-se um pouco distante do nicho de interesse, visto que conduz o estudo para a análise da opinião pública e não tanto para a análise de relações de poder entre Estados e outros atores atuantes no ciberespaço.

Paralelamente à exposição sobre os estudos e análises de possibilidades de aplicação das teorias mais "tradicionais" ou, pelo menos, consolidadas das Relações Internacionais, verifica-se também a tentativa de dois autores contemporâneos de formularem um arcabouço teórico específico para entender os desafios dos Estados no ciberespaço. Kremer e Müller (2014), assim como Nye (2010) e, como visto, a maioria dos autores que se empenham em trabalhar com o ciberespaço e as relações internacionais, colocam a dicotomia existente no ciberespaço como ponto de partida da formulação de suas ideias. De um lado existe um grande leque de oportunidades para economia, maior comunicação, dentre outros aspectos positivos

---

[7] *"Individuals acting in concert on political affairs through speech represents Arendt's conception of power in contrast to violence […]."* (BELOW, 2014, p.103).

proporcionados por esse ambiente, no entanto, de outro lado, existe a emergência de novas ameaças que afetam a segurança nacional, privada e comercial. Em atenção a esse ponto negativo do ciberespaço, os atores desenvolvem suas estratégias posicionando como uma demanda estatal e privada controlar e contra-atacar as ameaças existentes nesse âmbito.

A justificativa de por que se propõem à construção de um novo arcabouço analítico e não utilizam um já existente é que Kremer e Müller (2014) consideram as abordagens existentes insatisfatórias quanto às suas classificações. Sua crítica afirma que a literatura já desenvolvida é incoerente, visto que misturam categorias atores e motivações, por isso se faz relevante a proposta de uma teorização que não faça isso e que corrija esses problemas. Estabelecem, então, o SAM – *Stakeholders, activities and motives* –, preocupando-se em relacionar de maneira adequada os atores às suas motivações, mas não de maneira direta e padronizada, visto que existem diversos tipos de *stakeholders* (indivíduos, coletivos, grupos, organizações, empresas, Estados e organizações). Além disso, cada incidente dentro do ciberespaço pode envolver mais de um tipo de ator e os autores defendem que, teoricamente, estes atores, dependendo de seus recursos, têm as mesmas possibilidades de deter poder neste espaço. Outra ideia importante desenvolvida pelos autores diz respeito à análise do total de ataques feitos/sofridos no ciberespaço, onde uma parcela muito pequena envolve diretamente Estados, no entanto, não é descartada a responsabilidade dos governos sobre essas questões. Kremer e Müller (2014) argumentam que a relevância da ameaça para cada Estado dependerá da circunstância em que esta ocorrer, sugerindo que "Quanto maior for a relevância de um incidente de cibersegurança relatado [...] e menor as competências das autoridades para reagir ao incidente, maior é a ameaça global para o Estado e maior é a necessidade de ação." (KREMER; MÜLLER, 2014, p. 53-54, tradução nossa)[8]. Daí surge a importância de um desenvolvimento forte de uma cooperação entre o setor público e privado dentro de um país, já que nenhum dos atores tem competência suficiente para vencer sozinho nestas questões, nem mesmo o Estado.

[8] *"The greater the relevance of a cyber security related incident [...] and the lesser the competences of the authorities in regard to react to this incident, the greater is the overall threat for the state and the greater is the need for action."* (KREMER; MÜLLER, 2014, p. 53-54).

Destacando um ponto positivo quanto ao trabalho desenvolvido por Kremer e Müller (2014), podemos ver que o esforço por formular um princípio de teoria é válido e, acompanhando o raciocínio dos autores, percebe-se uma análise de fato voltada para o contexto ímpar do ciberespaço. No entanto, uma crítica que se identifica ao trabalho é que os autores afirmam querer superar as classificações insatisfatórias, no entanto, quando tratam sobre “motivações” do arcabouço analítico, não elaboram uma lista conclusiva de categorias. Argumentam que as motivações são versáteis e não exclusivas, porém não as definem bem. Esse tipo de ponto acaba mostrando que a justificativa inicial da necessidade de um novo ponto de vista para analisar o ciberespaço faz sentido, mas que os autores em questão não conseguem desenvolver uma estratégia totalmente nova de análise, porque acabam encontrando problemas semelhantes aos que outros autores também tiveram.

Visto que ainda não se formularam teorias de relações internacionais que possibilitem a aplicação ao ciberespaço de maneira completa, é possível utilizar-se para análise de temas de relações internacionais a pesquisa documental, quando não se pretende estabelecer uma teoria pioneira no campo, mas apenas empreender um estudo em menor profundidade. Como exemplo desse método, temos Souza Junior e Streit (2017) na sua avaliação da política brasileira para a segurança cibernética em comparação com a experiência internacional de países como Estados Unidos, Índia, África do Sul e Reino Unido.

2.3 PIONEIRISMO DOS ESTADOS UNIDOS E A RELEVÂNCIA DA PARCERIA PÚBLICO-PRIVADA

É necessário, para melhor entender a complexidade do ciberespaço, utilizar-se de casos e exemplos concretos que permitam visualizar as peculiaridades citadas anteriormente de maneira a propiciar que se formulem novas ideias e teorias a partir de fatos reais e não de simulações ou situações hipotéticas. Os Estados Unidos se configuram como país com mais conteúdo e história para ser analisada em se tratando do ciberespaço e de cibersegurança, sendo conhecido por seu pioneirismo e maior desenvolvimento consolidado na área. Através do exemplo dos Estados Unidos pode-se aprofundar o conhecimento de um dos principais diferenciais das políticas específicas para o ciberespaço: a parceria entre o setor público-privado.

2.3.1 Os Estados Unidos: primeira referência em estratégia de cibersegurança

A Internet teve como berço este país e ele é referência sempre que se fala do crescimento e desenvolvimento do campo ciber nos anos 1980 e do papel da ARPANET[9] no princípio dessa história (BELOW, 2014). De outro lado, a Internet surge nos Estados Unidos sob uma perspectiva de análise mais voltada para as relações internacionais, como um fenômeno tecnológico que corrobora com a afirmação deste país enquanto centro econômico, político e militar no Sistema Internacional, dentro do cenário de hegemonias com o qual depara-se no período pós-Guerra Fria (LUCERO, 2011).

Torna-se, então, relevante fazer uma análise primária do desenvolvimento da estratégia voltada para o ciberespaço justamente a partir do país que acolheu e acompanhou os "primeiros passos" desse novo domínio - sendo o governo norte-americano ator relevante tanto no início do ciberespaço, como ARPANET e, posteriormente, a Internet que conhecemos no Século XX, bem como sendo líder e pioneiro, novamente, no desenvolvimento de estratégias nacionais e internacionais específicas para a temática do ciberespaço. Justifica-se, inclusive, a escolha deste país em específico para a análise, quando levanta-se a ideia de que parece ser uma prática comum a países que ainda não tiveram graves incidentes com ciberataques ou problemas com cibersegurança, basearem-se no histórico e reação de outros países que já tiveram maior contato com o assunto (ACÁCIO; LOPES, 2012) para definir suas políticas de cibersegurança. Os Estados Unidos, então, alcançam o status de primeira referência quando se trata do tema das estratégias de cibersegurança, algo que o país conquistou de maneira natural, conforme visto anteriormente, por seu pioneirismo e iniciativa na área, status esse que era almejado pelo país visando manter sua posição de poder e liderança no Sistema Internacional.

---

[9] A ARPANET (*Advanced Research Projects Agency Network)* foi uma rede de comunicação piloto criada pela ARPA (*Advanced Research Projects Agency*) do *Department of Defense* (DoD) Estados Unidos, desenvolvida ao longo da década de 1960, para comunicação e conexão via redes. Em seu princípio de desenvolvimento, a ARPANET permitia a troca de informações e recursos remotamente entre professores, visto que ligava 4 universidades. Ela expandiu e cresceu muito ao longo das duas décadas seguintes e, em 1983, decidiu-se por usar os protocolos de rede TCP/IP. Neste momento, foi quando começou a generalizar-se o uso do termo "Internet" para as redes que fossem constituídas pelas redes que usam protocolos TCP/IP ou fossem capazes de se comunicar com essas redes (REMOALDO, 1998; CEPIK; CANABARRO; BORNE, 2014).

Desde os tempos “embrionários” da Internet até que chegasse ao formato como a conhecemos hoje, sempre houve participação e envolvimento de pesquisadores, professores, estudantes e funcionários de empresas norte-americanas no processo. Tratava-se de um projeto financiado pelo DoD, mas era, majoritariamente, liderado por atores não estatais. Há, então, desde o princípio, uma grande ligação entre as empresas e o universo ciber, principalmente nos Estados Unidos, tendo este país cerca de 90% da sua infraestrutura crítica[10] privatizada (McCARTHY, 2018), e sendo um ponto em comum entre a esfera pública e a esfera privada o interesse pela segurança dessas estruturas, motivo pelo qual mais procuram trabalhar juntas e encontrar caminhos, de alguma forma, coesos. Este é um dos principais diferenciais das políticas específicas para o ciberespaço: o caráter fundamental da comunicação e parceria entre o setor público-privado, alinhando interesses e fomentando o conhecimento do campo para desenvolver a estratégia do governo de defesa nacional e internacional no ciberespaço.

A parceria público-privada não é exclusivamente utilizada no âmbito da cibersegurança, já tendo sido aplicada como método em outros campos tanto pelos EUA, como pelo Reino Unido (CARR, 2016), tendo sido criada, de acordo com McCarthy (2018), na intenção de se reproduzir a privatização do poder político, característica básica da sociedade capitalista liberal. Também de acordo com o autor, essa pode ser considerada a melhor ferramenta disponível para se enfrentar os desafios da cibersegurança e, desde ao menos a virada do século, já é vista de maneira estratégica pelas duas partes nos Estados Unidos. Segundo Carr “Os EUA são um caso essencial porque foi aqui que as estratégias de segurança cibernética baseadas na parceria público-privada foram desenvolvidas em 2000 sob o governo do presidente Clinton.” (CARR, 2016, p. 44-45, tradução nossa)[11]. Portanto, desde muito cedo a cibersegurança é vista como prioridade nacional aos olhos dos governos norte-americanos e uma das ferramentas vitais identificadas para garantir

---

[10] Segundo o *USA Patriot Act* de 2001, *Public Law* 107-56,“[...] o termo “infraestrutura crítica” significa sistemas e ativos, sejam físicos ou virtuais, tão vitais aos Estados Unidos que a incapacidade ou destruição de tais sistemas e ativos teria um impacto debilitante sobre segurança, segurança econômica nacional, saúde ou segurança pública nacional ou qualquer combinação desses assuntos.” (vol. 115, p. 401, tradução nossa). *“[...] the term “critical infrastructure’’ means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”* (115 STAT. 401).

[11] “*The US is an essential case because it is here that cyber-security strategies based on the public-private partnership were developed in 2000 under President Clinton.”* (CARR, 2016, p. 44-45).

a segurança no ciberespaço veio a ser justamente a parceria público-privada (THOMAS, 2013).

Nas palavras de Lobato e Kenkel, "[...] o uso ilegal do ciberespaço tem sido visto como uma ameaça à segurança nacional" (LOBATO; KENKEL, 2015, p. 23, tradução nossa)[12]. No entanto, como apontado por Kremer e Müller (2014), os atores no ciberespaço, tanto estatais como não-estatais, não têm capacidade e/ou competência para defenderem-se sozinhos ou protegerem sua nação de forma independente, sendo *mister* essa relação de troca e segurança mútua possibilitada pela parceria público-privada. McCarthy (2018) justifica o porquê da parceria público-privada ser, então, o meio escolhido para essa promoção de segurança no ciberespaço: "Parcerias público-privadas apresentam-se como um meio-termo efetivo, permitindo o Estado a se engajar em decisões *ex ante* sobre os resultados da segurança cibernética em cuidadosa conversa com o setor privado." (McCARTHY, 2018, p.7, tradução nossa)[13]. No entanto, uma das maiores dificuldades encontradas por aqueles governos que se propõem a utilizar essa parceria como forma de construção da sua estratégia nacional e internacional de cibersegurança, exemplo aplicável aos Estados Unidos, é que a primazia sobre a definição da estratégia de defesa das infraestruturas críticas está com os operadores ou detentores destas infraestruturas – no caso dos EUA, em sua maioria, trata-se de empresas privadas. O interesse dessas empresas, ainda que seja defender as infraestruturas que detêm, não é desenvolver uma segurança a nível nacional (CARR, 2016). Verifica-se uma dificuldade de engajar as empresas de maneira independente para garantir a segurança coletiva do país. É na ausência de uma mobilização espontânea que o governo norte-americano procura agir e incentivar a parceria público-privada, buscando apresentar vantagens à esfera privada através da colaboração com o governo na construção de uma segurança cibernética comum e benéfica a todos.

Este é um dos principais problemas identificados no desenvolvimento e crescimento da parceria público-privada, há um conflito de interesses entre as partes: o Estado não quer perder sua soberania, delegando a segurança nacional a

---

[12] *"[...] the illegal use of cyberspace is being perceived as a threat to national security."* (LOBATO; KENKEL, 2015, p. 23).

[13] *"PPPs present themselves as an effective middle way, allowing the state to engage in* ***ex ante*** *decisions regarding cybersecurity outcomes in careful consultation with the private sector."* (McCARTHY, 2018, p.7).

empresas que provavelmente não desenvolverão espontaneamente uma estratégia de cibersegurança completa que contemple toda a sociedade *x* as empresas não querem se curvar aos desígnios do Estado, sem ao menos garantir que terão alguma vantagem nesse relacionamento (CARR, 2016). Existe um receio, por parte das empresas, que o governo aja de maneira intervencionista, sobrepondo-se à privacidade e decisões internas de cada um dos representantes do setor privado. A literatura aponta para a solução dessa contenda na trilha da identificação dos interesses compartilhados entre as partes, além da criação de leis que realmente vinculem e obriguem os envolvidos, orientando a relação e delimitando responsabilidades, direitos e deveres cabíveis a cada um. Enxerga-se uma necessidade de compartilhar objetivos dentro da parceria e colaborar mutuamente para que ambas as partes alcancem seus objetivos individuais e principalmente os coletivos, dividindo e complementando as pesquisas, desenvolvimento, capital humano, avanços técnicos e desenvolvimento de política nacional e internacional entre os setores públicos e privados. Além disso, também se aponta para uma mudança da abordagem do governo, empregando uma estrutura de governança adequada partindo, preferencialmente, de um ponto central que corresponda aos interesses da sociedade – o que aumentaria as chances de abarcar tanto os interesses públicos quanto privados. (CARR, 2016; THOMAS 2013).

2.3.2 Antecedentes: primeiras iniciativas de parceria público-privada na cibersegurança no governo norte-americano

A preocupação, interesse e urgência em proteger-se de ameaças advindas do ciberespaço, bem como exigir maior troca de informações entre o setor público e o privado para auxiliar na defesa nacional dos Estados Unidos, aumentou de forma vertiginosa após os atentados do 11 de setembro[14]. No entanto, antes desse marco histórico já se verificava uma movimentação em direção à priorização do tema nas pautas do governo norte-americano. Foram nas administrações de Bush (2001-2009) e Obama (2009-2017) que se identificaram esforços em produzir e sedimentar uma política específica para o ciberespaço, procurando consolidar estratégias de cibersegurança. Já na administração de Clinton (1993-2001), porém, aumentava o

[14] Ataques dirigidos ao World Trade Center e ao Pentágono – em Nova Iorque, NY e Washington, DC –, no dia 11 de setembro de 2001. O grupo pan-islâmico Al-Qaeda é acusado de ter dirigido os ataques (WELLAUSEN, 2002).

reconhecimento da importância do tema, identificando-se a necessidade de construção de uma política de segurança específica a esse escopo (HARKNETT; STEVER, 2011).

Ainda antes desses três presidentes, na década de 1990, durante o mandato de George H. W. Bush (1989-1993), já se percebia uma intensificação nos debates sobre cibersegurança. A origem desse interesse mais agudo surge como resultado da Terceira Revolução Industrial – ou Revolução da Informação[15] (RIBEIRO; RIVERA, 2014). Por isso, durante essa década, ocorre uma migração do processo de politização da cibersegurança – ou introdução do assunto nas agendas e debates políticos - para um processo de securitização propriamente dito, ainda que não fosse consenso entre teóricos da securitização enxergar o ciberespaço como uma ameaça real aos Estados (LOBATO; KENKEL, 2015).

Seguindo esse caminho evolutivo dos processos relativos à Internet e à securitização da cibersegurança, o presidente Clinton transparece uma preocupação maior com a temática, tendo sido criada, em 1996, uma comissão específica para assuntos relativos às infra-estruturas críticas, que já tinham espaço dentro do ciberespaço: *President's Comission for Critical Infrastructure Protection* (PCCIP). No documento de Overview Briefing produzido pela própria PCCIP, fica claro qual o objetivo e razão de Clinton ter assinado a *Executive Order* 13010 que criava a comissão: "Essa Comissão está, portanto, em sua tarefa de quinze meses de avaliação de ameaças físicas e cibernéticas às nossas infraestruturas vitais e desenvolvimento de políticas e estratégias para protegê-las." (ESTADOS UNIDOS, 1997, p.1, tradução nossa)[16]. A missão da Comissão era: identificar o escopo e natureza das ameaças e vulnerabilidades das infraestruturas críticas; determinar que problemas legais e políticos nascem do esforço de proteger infraestruturas críticas; e recomendar uma política nacional abrangente, implementando estratégia para proteger a infraestrutura crítica de ameaças físicas e ciber, garantindo sua operação contínua. Ao longo do documento, utiliza-se o termo "cyber" por 40 vezes em todo o texto, inclusive alertando para os perigos advindos das ciberameaças – menos

---

[15] A Terceira Revolução Industrial, ou Revolução da Informação, é o nome dado ao resultado rápido do avanço de tecnologias no âmbito da informática e telecomunicação, que modificaram as formas de armazenamento, processamento e recuperação da informação (CAVALCANTI, 1995).

[16] *"The commission is therefore well along in its fifteen-month task of assessing physical and cyber threats to our vital infrastructures and developing policies and strategies to protect them."* (ESTADOS UNIDOS, 1997, p.1).

evidentes do que ameaças físicas, mas tão importantes quanto estas –, discutindo a responsabilidade sobre os ataques feitos no ciberespaço que afetam as infraestruturas protegidas, dentre outras pautas de discussão sobre o tema (ESTADOS UNIDOS, 1997).

Além dessa Comissão, também se verifica o crescimento da tratativa do tema de cibersegurança a partir do documento produzido pelo governo norte-americano à época, acerca da estratégia do governo: *A National Security Strategy for a New Century (*1999). Neste documento o termo "*cyber*" é mencionado 11 vezes ao longo do texto, relacionado a outras palavras comentadas a seguir: a) "*cyber-attack*" – ciberataque – informa-se a existência de risco de ataques às infraestruturas nacionais críticas também no ciberespaço, além dos ataques físicos e sabotagens, e que governos e grupos terroristas estão criando ciberataques cada vez mais sofisticados e organizados contra os EUA, para os quais está desenvolvendo-se um sistema de resposta rápido a ataques cibernéticos; b) "*cyber-criminals*" – cibercriminosos – citados juntamente aos *hackers* como indivíduos que não têm dificuldades impostas para agir em função de fronteiras, que são praticamente inexistentes no ciberespaço; c) "*cybercrime*" – cibercrime – comenta que é do interesse do governo norte-americano encorajar o desenvolvimento e pesquisa cooperativa com outros países, focando no combate principalmente do cibercrime, e também reporta a realização de treinamento sobre o assunto para os membros da ASEAN; d) "*cyberspace*" – ciberespaço – "Mais do que qualquer nação, os Estados Unidos são dependentes do ciberespaço" (ESTADOS UNIDOS, 1999, p. 17, tradução nossa)[17]; e) "*cyber*" – ciber – alerta para o fato de o setor privado e o governo federal serem alvos de ataques às infraestruturas críticas tanto via meios tradicionais quanto cibernéticos, bem como comunica a criação de um sistema de proteção às infraestruturas; f) "*cyber-threats*" – ciberameaças – afirma que está sendo criado um sistema para detectar e responder ataques antes que causem danos sérios e comemora-se que é a primeira vez que diversos setores estão compartilhando informações sobre ameaças cibernéticas, vulnerabilidades e ataques em prol da defesa do país; g) "*cyber-security*" – cibersegurança – afirma que crescerá o investimento no treinamento e educação sobre práticas de cibersegurança (ESTADOS UNIDOS, 1999).

---

[17] *"More than any nation, America is dependent on cyberspace."* (ESTADOS UNIDOS, 1999, p. 17)

Percebe-se que a abordagem dada ao ciberespaço e cibersegurança na estratégia exposta no documento ainda era bastante rasa e o assunto, discutido de uma maneira abstrata, configurando-se mais como uma previsão e precaução do que propriamente uma defesa contemporânea. A estrutura do documento situa ameaças cibernéticas mais como uma possibilidade futura do que uma realidade presente. De toda forma, é extremamente relevante perceber a preocupação do governo norte-americano para com o assunto já antes da virada dos anos 2000. E, já nessa época, os Estados Unidos utilizavam-se da parceria público-privada para gerenciar e melhorar o monitoramento e prevenção dos ataques e vulnerabilidades cibernéticas, muito em função da preocupação com a defesa das infraestruturas críticas. A parceria público-privada chegava a ser, segundo Carr (2016), o centro do programa tecnológico do país, já no início dos anos 2000. Ainda que se tenham feito todos esses esforços na produção de um documento de estratégia e movimentação para trazer os temas do ciberespaço e cibersegurança para a agenda primária dos Estados Unidos, fica a percepção de que a questão ainda se encontrava muito no campo das ideias durante a administração Clinton. “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” (RIBEIRO; RIVERA, 2014, p. 147).

3 ANÁLISE COMPARATIVA ENTRE AS AÇÕES DOS GOVERNOS BUSH E OBAMA PARA A PARCERIA PÚBLICO-PRIVADA NA CIBERSEGURANÇA (2001-2017)

Conforme apontado no final do capítulo anterior, por mais que já houvesse um movimento inicial de busca por estabelecer uma estratégia para a cibersegurança, bem como trabalhar com a parceria público-privada também no âmbito do ciberespaço, é apenas a partir de 2001 que é possível observar uma estratégia um pouco mais estruturada, ao menos no papel, nos Estados Unidos. É a partir desse ano que a análise será realizada no presente capítulo, iniciando pela análise do governo Bush (2001-2009) até o governo Obama (2009-2017), tendo por foco documentos referentes à ciberestratégia do país e da relevância e atuação das empresas privadas no desenvolvimento do campo juntamente ao governo federal. Ao final do capítulo, propõe-se uma análise comparativa entre os governos, verificando onde houve evolução e em que questões ainda se percebe falta de desenvolvimento e necessidade de fomentá-lo.

3.1 ESTRATÉGIA DA PARCERIA PÚBLICO-PRIVADA NA CIBERSEGURANÇA DO GOVERNO BUSH (2001-2009)

Para analisar a política estratégica do governo Bush (2001-2009), principalmente no que tange à relevância da parceria público-privada, escolheu-se a revisão de dois documentos fundamentais produzidos ao longo do período referenciado. Quais sejam: *The National Strategy to Secure Cyberspace*, de 2003, e *Federal Plan for Cyber Security and Information Research and Development: Report by the Interagency Working Group on Cyber Security and Information Assurance*, de 2006.

Em 1997, uma Comissão Presidencial já identificava os riscos cibernéticos em um reporte público. É informado pela *National Strategy to Secure Cyberspace* que em 1998: “[...] invasores executaram uma série sofisticada e bem orquestrada de intrusões cibernéticas nos computadores do Departamento de Defesa, NASA e laboratórios de pesquisa do governo.” (ESTADOS UNIDOS, 2003, p. 50, tradução nossa)[18]. Nos anos 2000, aparece pela primeira vez o problema da cibersegurança

[18] *“[...] attackers carried out a sophisticated, tightly orchestrated series of cyber intrusions into the computers of* DoD*,* NASA*, and government research labs.”* (ESTADOS UNIDOS, 2003, p. 50).

no Plano Nacional. Somente após o atentado do 11 de setembro de 2001, porém, que acontece um crescente real na preocupação da população e do governo norte-americano em relação às ameaças advindas do ciberespaço. A cibersegurança passa, neste momento, a ser vista como prioridade e são liberados fundos maiores para as redes de segurança federais (ESTADOS UNIDOS, 2003).

A estratégia nacional, *National Strategy for Homeland Security* é publicada em 2002, como uma resposta do governo Bush ao incidente do ano de 2001, mas já não se fazia suficiente na apresentação e exposição das perspectivas do futuro especificamente para o ciberespaço e a cibersegurança. No mesmo ano, seguindo a lógica do momento, passa a acontecer um movimento com o fim de consolidar e fortalecer as agências de cibersegurança como parte de departamento da *Homeland Security* (Segurança Nacional). Antes do advento do ciberespaço, os Estados Unidos estavam isolados fisicamente de ameaças e essa realidade é modificada com as peculiaridades das possibilidades de ataques pertencentes ao ciberespaço. Além disso, a economia e a segurança nacional dos Estados Unidos, a partir de 2003, se tornaram totalmente dependentes da tecnologia e infraestrutura da informação (ESTADOS UNIDOS, 2003). Decorrente disso, surge então a necessidade da formulação de uma estratégia própria para as demandas ciber, *The National Strategy to Secure Cyberspace*, publicada no ano seguinte à estratégia nacional de segurança. Além do lançamento da Estratégia para o Ciberespaço, "[...] o presidente Bush solicitou que o Congresso aumentasse os fundos para proteger computadores federais em 64%" (ESTADOS UNIDOS, 2003, p. 9, tradução nossa)[19], em 2003. Em 2006, o governo lança ainda outro documento relevante para a análise da estratégia para o ciberespaço: *Federal Plan for Cyber Security and Information Research and Development: Report by the Interagency Working Group on Cyber Security and Information Assurance*.

3.1.1 *The National Strategy to Secure Cyberspace*

Já na carta de introdução do documento, o presidente George W. Bush expõe um dos principais pontos que explicam a necessidade da formulação de uma estratégia própria para o ciberespaço, uma vez que garantir a segurança no

[19] *"[...] President Bush requested that Congress increase funds to secure federal computers by 64 percent."* (ESTADOS UNIDOS, 2003, p. 9).

ciberespaço é algo de maior complexidade do que se imagina e não depende apenas de ações do Governo Federal. Nas palavras do presidente:

> Proteger o ciberespaço é um desafio estratégico extraordinário e difícil que requer um esforço coordenado e concentrado de toda a sociedade - governo federal, governos estaduais e locais, setor privado e povo americano. [...] A pedra angular da estratégia dos EUA de segurança para o ciberespaço é e continuará sendo a parceria público-privada. (ESTADOS UNIDOS, 2003, tradução nossa)[20].

Com este documento, fica claro também que proteger e garantir a segurança no ciberespaço faz parte de um dos cernes da estratégia de segurança nacional norte-americana e que deve ser tratada como prioridade na agenda governamental e da sociedade como um todo. O foco principal, apresentado no documento, mostra-se ser a ideia de trabalhar para diminuir as vulnerabilidades e também consolidar um programa de pronta-resposta, visto que é bastante difícil antecipar ataques proferidos no ciberespaço, sendo necessário trabalhar em outras áreas que não a reação do próprio ataque. Prevenir-se contra ataques é o caminho indicado, não deixando, simplesmente, para se agir após um ataque – que pode afetar inclusive as unidades de resposta rápida. O documento, então, apresenta um programa diretivo com os seis princípios guias:

I. Esforço Nacional: o Governo sozinho não consegue defender a nação no ciberespaço e precisa da cooperação de cada indivíduo; incentiva e promove a parceria público-privada, com fim de haver uma maior conscientização sobre o uso da Internet e demais ferramentas fundamentais do ciberespaço. O Governo acaba tendo que utilizar tal política por ter seu escopo de ação muito limitado, o que dificulta sua atuação dentro do setor privado;

II. Proteger a liberdade e privacidade dos civis: defesa de que cibersegurança e privacidade pessoal não podem ser objetivos opostos;

III. Regulação e forças do mercado: o governo não se encarregará de criar leis e regulações tão vinculantes e padronizadoras de como agir no ciberespaço, bem como se defender e trabalhar a cibersegurança. A criação de leis poderia ser prejudicial à cibersegurança, deixando-a mais fraca e com arquiteturas mais

---

[20] *"Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people. [...] The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."* (ESTADOS UNIDOS, 2003).

homogêneas, o que facilitaria o ataque a várias destas simultaneamente; a regulação seria conduzida pelo próprio mercado de maneira natural;

IV. Prestação de contas e responsabilidade: “A Estratégia Nacional para Proteger o Ciberespaço está focada na produção de uma infraestrutura de informações mais resiliente e confiável.” (ESTADOS UNIDOS, 2003, p. 15, tradução nossa)[21]. Nessa ideia, o *United States Department of Homeland Security* – DHS acaba sendo o maior responsável pelas ações do Governo para cibersegurança, portanto, também é o órgão referência no assunto, que terá de prestar contas com maior detalhamento e será mais responsabilizado, de parte do Governo;

V. Garantir a flexibilidade: no ambiente ciber, realinhamentos e ajustes são necessários constantemente por causa da rapidez de mudanças das ameaças que circundam o ciberespaço e ameaçam a segurança nacional norte-americana;

VI. Planejamento multi-anual: proteger o ciberespaço é uma tarefa que exige atenção contínua, em função das mudanças recorrententes que acontecem no ambiente, de modo que é necessária uma atualização dos planos de defesa. A Estratégia recomenda que sejam feitos planos multi-anuais para cibersegurança, visto que o presente documento apenas indica as linhas iniciais por onde seguir na proteção no ciberespaço. Sugere que sejam criadas estratégias não apenas por agências e órgãos do Governo, mas que outras organizações ou instituições do setor privado também estabeleçam seus planos multi-anuais e que estes sejam compatíveis com seus objetivos e ameaças enfrentados.

Ao longo de todo o documento verifica-se a exaltação do setor privado como peça-chave na ação em conjunto com o governo. Logo na abertura do texto vemos ser afirmado que, normalmente, o setor privado é melhor equipado e estruturado para responder a uma ameaça advinda do ciberespaço (ESTADOS UNIDOS, 2003). O próprio Governo Federal salienta essa realidade e, na proposta de fortalecer a parceria, coloca como funções do DHS, fundado em novembro de 2002, auxiliar na manutenção da segurança no ciberespaço e prover assistência técnica ao setor privado, também no que tange às necessidades relativas à cibersegurança. O Governo Federal deixa claro no documento que não é possível garantir a cibersegurança sozinho. Argumenta que essa tarefa requer um esforço coordenado e conjunto, guiado por parcerias voluntárias, que delineiam as estratégias de

---

[21] *“The National Strategy to Secure Cyberspace is focused on producing a more resilient and reliable information infrastructure.”* (ESTADOS UNIDOS, 2003, p. 15).

segurança para cada setor específico de acordo com suas demandas, mas com um fim coletivo da segurança nacional no ciberespaço (ESTADOS UNIDOS, 2003). Assim, o Governo Federal aponta que, para que essa parceria seja realmente produtiva e eficaz em seus objetivos, é necessário que haja uma coordenação e comunicação fluída e organizada entre as partes, de modo a não surgirem novos *gaps* de conhecimento e informação entre os setores público e privado.

O documento aponta cinco prioridades nacionais dentro do escopo de segurança no ciberespaço: (i) Sistema Nacional de Resposta de Segurança no Ciberespaço; (ii) Programa de Redução de Vulnerabilidades e Ameaças à Segurança Nacional no Ciberespaço; (iii) Programa de Treinamento e Conscientização sobre Segurança Nacional no Ciberespaço; (iv) Protegendo o Ciberespaço do Governo; e (v) Segurança Nacional e Cooperação Internacional de Segurança no Ciberespaço. Cada uma das prioridades nacionais traz consigo algum ponto no qual a parceria dos setores público-privado tem seu campo de ação e atuação em conjunto.

A primeira prioridade, que trata da questão do desenvolvimento de um sistema de resposta a ameaças, já destaca a necessidade da parceria para a real efetividade do programa a nível nacional. Das oito iniciativas elencadas para se criar esse Sistema Nacional de Respostas, quatro tratam especificamente sobre o setor privado e sua atuação necessária para o bom funcionamento do sistema de resposta rápida a ameaças proposto, quais sejam: a) estabelecer “arquitetura” público-privada – trabalhando conjuntamente, buscando as melhores soluções e ideias para a fundação do sistema; b) encorajar o desenvolvimento do setor privado – sabendo que o setor privado tem capacidades e potencialidades que, por vezes, o setor público não tem, reafirma a necessidade de incentivo ao desenvolvimento independente das empresas e indústrias; c) coordenar processos para participação voluntária da parceria – criar, também, incentivos ao setor privado para que este obtenha vantagem em participar da parceria, sem ser coagido a isto, de forma que todos sejam beneficiados ao colaborar e que a participação na parceria seja algo que ocorre de maneira natural; d) melhorar e fomentar a troca de informações público-privada. Esse último ponto é o principal tratado nesta prioridade; a Estratégia fala muito sobre a importância da troca de informações e conhecimento entre os setores público e privado para melhor desenvolver o sistema de resposta rápido,

pois com mais informações é maior a viabilidade de antecipação de alguns tipos de reações possíveis e recomendáveis, a serem efetuadas contra-ataques cibernéticos.

Conforme a Estratégia afirma “O desenvolvimento bem-sucedido de recursos para análise, indicações e advertências requer um esforço voluntário de compartilhamento de informações público-privadas” (ESTADOS UNIDOS, 2003, p. 24, tradução nossa)[22]. É tarefa do DHS fazer essa ligação ou ponto de contato entre o Governo Federal e os parceiros do setor privado. Nesta tarefa, acaba deparando-se com o desafio de vencer o “medo”, por parte das empresas, de que o governo vá utilizar de maneira má intencionada as informações compartilhadas e de que vantagens competitivas poderiam ser perdidas ao se compartilharem dados e informações sobre vulnerabilidades e descobertas relativas à segurança da informação. O documento propõe essa maior vinculação e compartilhamento de informações entre os setores, porém admite que ainda não existe nenhum modo eficiente para efetuá-lo e colocar em prática essa ideia, sendo objetivo também da estratégia fomentar o desenvolvimento dessa via mais adequada à realidade existente.

Quanto à segunda prioridade, que trata sobre a criação de um programa de redução de vulnerabilidades e ameaças, admite-se que o problema é interno e não é factível que se coloque como meta eliminar todas as vulnerabilidades com este programa. São muitos atores e muitas formas de ataque, o que demanda uma ação conjunta, mais uma vez, unindo o trabalho e disposição do Governo Federal, governos locais e o setor privado na defesa dos Estados Unidos frente a ciberameaças. Com esse programa, pretendeu-se criar leis e mecanismos de identificação e punição rápida aos autores dos ataques. A Estratégia aponta como prioridade nacional a proteção dos DCS/SCADA (*Digital Control Systems/ Supervisory Control and Data Acquisition Systems*), que têm responsabilidade compartilhada pelos setores públicos e privados em prover a defesa desses sistemas. Por fim, mais uma vez o DHS aparece como interlocutor entre os setores, responsável por salvaguardar os esforços das empresas privadas e também coordenar mecanismo de desenvolvimento e compilação de metodologias e pesquisas realizadas na indústria, governo e academia, de modo que esses estudos

---

[22] *“Successfully developing capabilities for analysis, indications, and warnings requires a voluntary public-private information sharing effort.”* (ESTADOS UNIDOS, 2003, p. 24).

não se sobreponham ou se repitam, mas que se complementem e cresçam em harmonia (ESTADOS UNIDOS, 2003).

O documento aborda a terceira prioridade, da criação de um programa de conscientização e treinamento, expondo o problema de que a falta de conhecimento e treinamento específico das pessoas que trabalham na área aumenta as vulnerabilidades dos sistemas. Quem lida com os sistemas precisa ter o conhecimento bem trabalhado e, por isso, é proposta da Estratégia promover apoio ao setor privado para emitir certificações padronizadas para os funcionários da iniciativa privada. Além disso, é de responsabilidade coletiva, novamente, fomentar e participar de programas de educação e apoio à certificação profissional, bem como trabalhar na educação da população em geral, para que a defesa do ciberespaço seja possível em todos os níveis. A quarta prioridade, que trata menos sobre a participação do setor privado e da parceria, pois lida mais com a segurança governamental, discorre sobre a responsabilidade do Governo Federal sobre as infraestruturas críticas. Reforça-se, nesse ponto, que o Governo Federal, ainda que de forma diferente do tradicional, segue tendo autoridade e responsabilidade quanto à segurança também no ciberespaço. Por fim, a quinta prioridade discorre sobre a necessidade de cooperação internacional e cultura global de segurança no mundo ciber. Neste âmbito, os Estados Unidos também devem liderar e guiar os demais países. Há uma ideia de replicar o que se fez/faz estrategicamente internamente, a um nível global, mantendo a atenção e projeto de cibersegurança ativos mesmo em tempos de paz, visto que é iminente o risco de estar sofrendo com espionagem e outras ameaças. Quanto mais países defenderem-se mutuamente, mais vantajoso aos Estados Unidos. Para melhor funcionar a coordenação entre países, menciona-se a utilização de organizações já existentes e para atingir o setor privado de outras nacionalidades pretende-se utilizar o *Transatlantic Business Dialogue*[23].

Da análise do documento, identifica-se que um dos fatores mais reforçados e destacados ao longo do texto é o chamado do Presidente à fomentação de parcerias entre os setores público e privado e como essa cooperação já vem apresentando

---

[23] O *Transatlantic Business Dialogue* (TABD - Diálogo Transatlântico de Negócios) é o conselho executivo do *Trans-Atlantic Business Council* (TABC - Conselho Transatlântico de Negócios). O TABD é o fórum mais alto do TABC e reúne diretores executivos das principais empresas americanas e europeias que trabalham por um mercado transatlântico sem barreiras que contribua para o crescimento, emprego, inovação e sustentabilidade na economia global (TRANS-ATLANTIC BUSINESS COUNCIL, 2019).

efeitos positivos no desenvolvimento de estratégias específicas para cada “parte” do ciberespaço que ocupam, ajudando no aumento da segurança nacional em conjunto. O documento já coloca a parceria público-privada como algo permanente e extremamente necessário para a evolução nas soluções de cibersegurança norte-americanas, visto que a maior parte dos recursos e infraestruturas críticas são controlados por entidades não-governamentais. É possível verificar a grande importância dessa ponte que a parceria público-privada faz, ligando os interesses do governo de salvaguardar a segurança nacional e das empresas privadas em se manterem protegidas frente a ameaças externas no ciberespaço (ESTADOS UNIDOS, 2003). Como previsão para o futuro, em complemento, o documento é finalizado com a seguinte proposição: “No futuro próximo, duas coisas serão verdadeiras: a América dependerá do ciberespaço e o governo federal buscará uma ampla e contínua parceria para desenvolver; implementar e refinar a NSSC[24].” (ESTADOS UNIDOS, 2003, p. 54, tradução nossa)[25]. Com isto, demonstra a consciência quanto à necessidade de preocupar-se com o ciberespaço e a cibersegurança, bem como seus avanços e deixando proposto a ideia de que o Governo gostaria de contar sempre com parcerias para atuar nesse âmbito.

3.1.2 *Federal Plan for Cyber Security and Information Research and Development: Report by the Interagency Working Group on Cyber Security and Information Assurance*

O Plano Federal para Cibersegurança e Pesquisa e Desenvolvimento da Informação foi um documento formulado pelo Conselho Nacional de Ciência e Tecnologia que teve como objetivo ser um primeiro passo para desenvolver a agenda do ciberespaço. Buscou verificar, principalmente, as possibilidades de pesquisa e desenvolvimento no ciberespaço, além de tratar de uma resposta a outros reportes produzidos desde 2002, direcionados ao Governo norte-americano e suas agências e conselhos, referentes ao desenvolvimento e segurança no ciberespaço. O Diretor do Escritório Executivo do Presidente, John H. Marburger, em sua carta de abertura do documento, expõe quais as prioridades e focos do Governo

---

[24] NSSC – *National Secure Strategy for Cyberspace.*

[25] *“For the foreseeable future, two things will be true: America will rely upon cyberspace and the federal government will seek a continuing broad partnership to develop, implement, and refine the National Strategy to Secure Cyberspace.”* (ESTADOS UNIDOS, 2003, p. 54)

norte-americano, no período: “Proteger a infraestrutura de TI da Nação e os setores críticos de infraestrutura para o futuro é uma questão de segurança nacional e patriótica” (ESTADOS UNIDOS, 2006, tradução nossa)[26].

O documento está organizado de maneira a apresentar a estratégia para o ciberespaço de pesquisa e desenvolvimento através de conclusões e recomendações. A sua justificativa e proposta são apresentadas com clareza na seguinte passagem:

> É necessária uma pesquisa e desenvolvimento estratégico entre agências para fortalecer a cibersegurança e a garantia de informações da infraestrutura de TI da Nação. O planejamento e a realização de tal pesquisa e desenvolvimento exigirão atividades federais concertadas em várias frentes como também em colaboração com o setor privado. As especificidades da estratégia proposta neste Plano estão articuladas em um conjunto de descobertas e recomendações. (ESTADOS UNIDOS, 2006, p. xi, tradução nossa)[27]

Dentre as 10 conclusões e recomendações apresentadas no documento, duas são importantes e destacáveis para a análise do relacionamento do Governo com as empresas e instituições privadas também no escopo de pesquisa e desenvolvimento para cibersegurança no ciberespaço. O primeiro ponto é também o primeiro apresentado no documento: direcionar investimento federais para Pesquisa e Desenvolvimento para necessidades estratégicas de cibersegurança e garantia de informações. Neste ponto, reforça-se a ideia de que o Governo deve trabalhar conjuntamente com o setor privado em Pesquisa e Desenvolvimento de ideias para o ciberespaço, direcionando fundos para as áreas de pesquisa nas quais o setor privado está engajado e alcançando novas descobertas, principalmente no que tange a melhoria na defesa e detecção de vulnerabilidades internas no ciberespaço. O outro ponto que é relevante à relação do setor público com o setor privado é o nono do documento, que afirma ser necessário “Instituir uma maior coordenação eficaz com o setor privado” (ESTADOS UNIDOS, 2006, p. xii, tradução nossa)[28]. A ideia principal - e uma das maiores preocupações do Governo quando se analisa o

---

[26] *“Safeguarding the Nation’s IT infrastructure and critical infrastructure sectors for the future is a matter of national and homeland security.”* (ESTADOS UNIDOS, 2006).

[27] “*Strategic interagency R&D is needed to strengthen the cyber security and information assurance of the Nation’s IT infrastructure. Planning and conducting such R&D will require concerted Federal activities on several fronts as well as collaboration with the private sector. The specifics of the strategy proposed in this Plan are articulated in a set of findings and recommendations.”* (ESTADOS UNIDOS, 2006, p. xi).

[28] *“Institute more effective coordination with the private sector” (ESTADOS UNIDOS, 2006, p. xii).*

todo do documento, observando-se a relevância de tal ponto - dessa recomendação é fomentar uma melhoria na comunicação entre o Governo e o setor privado. Há uma lacuna na troca de informação entre os setores e até intra-agências governamentais, onde a interlocução por vezes é prejudicada e identifica-se uma sobreposição de pesquisas e duplicidades, ao invés de haver um esforço conjunto e complementar entre os setores e agências (ESTADOS UNIDOS, 2006).

Esse documento, de maneira geral, se foca prioritariamente nas ações que devem ser tomadas a nível interagencial, dentro do próprio Governo norte-americano. Destaca os fatores mais onerosos aos que buscam se defender no ciberespaço: a existência de diversos agentes, de diferentes naturezas, que podem realizar ataques que afetem os Estados Unidos – *hackers*, crime organizado, *insiders*, terroristas e Estados-nações; e também a dificuldade de se antecipar ameaças, bem como o alto custo que se tem para detectar e corrigir vulnerabilidades, ao passo que para realizar um ataque não se tem que dispender muito capital e não se precisa ter nenhuma sofisticação diferenciada. Além disso ressalta que "Um atacante precisa encontrar apenas uma vulnerabilidade; o defensor precisa tentar eliminar todas as vulnerabilidades." (ESTADOS UNIDOS, 2006, p. 6, tradução nossa)[29], o que torna a "corrida" atacante x atacado assimétrica. Destaca-se aí a necessidade e relevância da parceria público-privada, cooperação que, na teoria, possibilita obter-se vantagens para a construção de uma cibersegurança sólida a nível nacional.

Ao reunir os conhecimentos e informações sobre cibersegurança de diversos setores em uma troca constante de dados e pesquisa, é possível alcançar uma maior proteção, mais completa e abrangente, a todos os norte-americanos.

Quanto aos tópicos apresentados como preocupações imediatas ao Plano, são apresentados os PCSs Industriais[30], que são muito visados para ataques por

---

29 *"An attacker needs to find only one vulnerability; the defender must try to eliminate all vulnerabilities"* (ESTADOS UNIDOS, 2006, p. 6).

30 *Industrial Process Control Systems*, ou Sistemas de controle de processos industriais, são assim definidos: "Os sistemas de controle de processo industrial (PCSs) desempenham funções de monitoramento e controle em diversas infraestruturas críticas, como geração, transmissão e distribuição de energia elétrica; transporte de petróleo e gás; e bombeamento, purificação e suprimento de água. Alguns desses sistemas, como os *Supervisory Control and Data Acquisition* - Sistemas de Controle de Supervisão e Aquisição de Dados (SCADA - SCSAD), geralmente abrangem grandes áreas geográficas e contam com uma variedade de sistemas de comunicação, aumentando a dificuldade de torná-los seguros." (ESTADOS UNIDOS, 2006, p. 53, tradução nossa). *"Industrial process control systems (*PCS*s) perform monitoring and control functions in such diverse critical infrastructures as electrical power generation, transmission, and distribution;*

englobarem infraestruturas críticas dos Estados Unidos. Além disso, se tornam alvos mais vulneráveis, além de despertarem interesse pela sua importância, por adotarem sistemas e programas comuns do seu setor de atuação, sem muita variação. Se uma vulnerabilidade for encontrada em um alvo, diversos outros do setor podem vir a ser atacados da mesma forma com resultado positivo para aquele de onde se origina a ameaça. Outro risco que é apontado no documento, para os PCSs, é a popularização do uso de Wireless também nesses sistemas, prática que deixa as redes internas mais desprotegidas e vulneráveis. O outro setor, ainda, apresentado como de preocupação imediata também tem ligação com o setor privado: o Setor Bancário e Financeiro. É apontado no documento que, cada vez mais, a economia dos Estados Unidos é visada como alvo-chave de ataques ciberdirigidos. Mesmo em 2006, já havia uma grande utilização de armazenamentos em base de dados localizadas em computadores, de modo que "[...] cibersegurança e garantia da informação são um valor essencial e um elemento vital do modelo de negócios do setor financeiro." (ESTADOS UNIDOS, 2006, p. 11, tradução nossa)[31].

Embora aponte para essas prioridades mais ligadas ao setor privado, o documento em sua maior parte discorre sobre as prioridades interagências do Governo norte-americano, salientando também como essas prioridades podem ser diferentes das que cada órgão individualmente, analisando os escopos sozinho, terá. Dessa forma, entende-se o porquê de se ter investimentos diversos em cada uma dessas áreas, não seguindo um padrão, necessariamente. No entanto, são apontadas no documento prioridades técnicas interagência que também são prioridades nos investimentos do Governo, são elas: autenticação, autorização e gestão de confiança; controle de acesso e gestão de privilégio; proteção de ataque, prevenção e preempção; segurança wi-fi; e teste de software e ferramentas de avaliação. Fica claro que existem áreas e focos de pesquisa e desenvolvimento que não foram apresentados como prioridades dos fundos do Governo, mas que estão nas prioridades técnicas dele, pois mesmo não havendo investimento direto nos tópicos, espera-se que outros setores invistam em melhorias e desenvolvimento de

---

*oil and gas transport; and water pumping, purification, and supply. Some of these systems, such as Supervisory Control and Data Acquisition (*SCADA*) systems, typically span large geographic areas and rely on a variety of communication systems, compounding the difficulty of making them secure."* (ESTADOS UNIDOS, 2006, p. 53).

31 *"[...] cyber security and information assurance is a core value and a vital element of the financial industry's business model."* (ESTADOS UNIDOS, 2006, p. 11).

ferramentas e áreas da cibersegurança (ESTADOS UNIDOS, 2006). É neste espectro que verificamos uma forte “dependência” do Estado norte-americano em relação aos movimentos do setor privado, pois colocam a confiança de que haverá investimento e desenvolvimento próprio neste espaço e que existem tópicos que podem ser retirados de sua relação de prioridades de aplicações, por estarem salvaguardados pelo setor privado. Além disso, paira no imaginário do setor público uma ideia de que o setor privado tem maior capacidade de Pesquisa e Desenvolvimento, estando à frente do setor público, tendo um foco de interesse mais direcionado e tendo maior efetividade nos seus empreendimentos de evolução em áreas da cibersegurança.

3.1.3 Balanço da estratégia para o ciberespaço do Governo Bush, sobre o espectro da parceria público-privada

Em primeiro lugar, há de se recordar o contexto em que o Governo Bush se encontrava ao lançar suas estratégias e políticas no início do novo milênio. Os dois pilares fundamentais nos quais estavam baseados os Estados Unidos, em 2003, eram a importação do conceito da Guerra Fria de “dissuasão” para resolver problemas e a confiança para processos de desenvolvimento da política (HARKNETT; STEVER, 2011). Há duas reflexões importantes a se fazer diante dessa afirmativa. Por um lado, o Governo norte-americano estava focado em defender-se contra novos ataques terroristas e, para tanto, tentando antecipar todo tipo de ataque - inclusive via ciberespaço. Sendo assim, seu interesse primordial não era necessariamente formular estruturadamente uma parceria público-privada para o desenvolvimento do ciberespaço, essa parceria iria se desenvolver e ser muito útil. Por outro lado, era necessário apoio público para conseguir sustentar suas políticas a nível nacional. Para que a estratégia nacional funcionasse, era *mister* a parceria com o setor privado, dando um caráter único de adaptação da estratégia central para cada ambiente e setor industrial do país. A Doutrina Bush trazia como pauta corrente o terrorismo, guerra ao terror e o incidente do 11 de setembro (RIBEIRO; RIVERA, 2014), estando todos esses fatores interligados com o medo da infraestrutura crítica do país correr perigo, principalmente sendo exposta por vias cibernéticas e não físicas. Neste contexto, foi aprovado o *Patriot Act*, em 26 de outubro de 2001, lei que “[...] expande os poderes de vigilância e investigação da

polícia e representa uma das ameaças mais significativas às liberdades civis, à privacidade e às tradições democráticas da história dos EUA." (ELETRONIC FRONTIER FOUNDATION – EFF, 2019, tradução nossa)[32]. Esta também é uma das principais leis, senão a fundamental, para se estudar e analisar a doutrina de segurança do Governo Bush. Ela aumentou as penalidades contra crimes de ciberterrorismo, instituindo uma responsabilização de acordo com o dano econômico causado pelo ataque, bem como autorizou uma verba de U$50 milhões para criação e suporte de uma rede regional forense de computadores (RIBEIRO; RIVERA, 2014). Por mais que o *Patriot Act* seja visto como potencial ameaça à privacidade e liberdade dos norte-americanos, no próprio texto da lei existe uma demonstração de interesse e necessidade do Governo em manter contato e parceria com o setor privado para conseguir levar ao cabo esse ideal de proteção e defesa. Na seção 1013 do *Patriot Act*, expõe-se sem reservas a necessidade do Governo de utilizar a *expertise* do setor privado e seus recursos para a pesquisa, preparação e resposta governamental (ESTADOS UNIDOS, 2001), ou seja, demonstra interesse em compartilhamento de informação e conhecimento entre os setores, de forma a auxiliar na proteção e garantia de segurança do país. Já na seção 1016, também é reforçada a ideia de que os negócios privados, o governo e os aparatos da segurança nacional estão cada vez mais interligados e interdependentes em uma rede de infraestruturas críticas. Desta forma, todas as ações necessárias para que a política reportada no *Patriot Act* tenha sucesso devem ser realizadas em parceria público-privada envolvendo organizações corporativas e não-governamentais (ESTADOS UNIDOS, 2001).

Entendendo o contexto no qual a Estratégia para o Ciberespaço se apresenta como primeiro passo em direção a uma consolidação e afirmação da relevância do ciberespaço para o futuro do país, é necessário reconhecer o pioneirismo do esforço empreendido pelo Governo Bush. Neste mandato, observa-se a procura em estruturar uma estratégia específica para a cibersegurança no ciberespaço, visto que ainda que já tivesse acontecido movimentação por parte dos presidentes anteriores, nenhum chegou ao passo de formular, de fato, uma estratégia para a cibersegurança norte-americana. No entanto, à época, tinha-se criado muitas

[32] *"[...] expands law enforcement's surveillance and investigative powers and represents one of the most significant threats to civil liberties, privacy, and democratic traditions in US history."* (ELETRONIC FRONTIER FOUNDATION – EFF, 2019).

expectativas em relação ao que poderia ser determinado a partir da estratégia emitida pelo governo norte-americano e, por isso, existem diversas críticas e comentários formulados a respeito, principalmente em relação à Estratégia Nacional. Uma das principais refere-se à realidade de que a Estratégia foca menos em propor regulamentos e detendo-se mais em recomendações, o que não necessariamente levaria a uma construção efetiva de uma estratégia palpável. Surgem, logo após a publicação da Estratégia, críticas quanto a ausência de firmeza do governo em dar passos mais concretos em direção à formação de ferramentas e aplicações para fomentar a cibersegurança do espaço norte-americano. De acordo com Zimmer (2004), ao ler-se a Estratégia percebe-se que não se tinha em vista, por parte do Governo, uma transformação da arquitetura da Internet em um ambiente mais regulado - o que era esperado - sendo pequena a perspectiva de haver o aumento e desenvolvimento esperado da segurança nacional, a partir da cibersegurança (ZIMMER, 2004). No entanto, é possível verificar que, ainda antes da Estratégia para o Ciberespaço de 2003 ser lançada, o governo já havia aprovado o *Sarbanes-Oxley Act (*SOX*)* em 2002, lei que exige que as empresas tenham sistemas de controle interno sólidos, emitindo relatórios de sistemas financeiros confiáveis e, de acordo com Gordon et al (2015, p. 12, tradução nossa)[33]: “Em um ambiente moderno de sistema de informações baseado em computador, as empresas não podem produzir resultados confiáveis de relatórios financeiros sem ter sistemas de computador seguros.” Portanto, a proposição dessa lei acaba criando uma obrigatoriedade por parte do setor privado de manter seus sistemas seguros e investir em cibersegurança, criando, de certa forma, uma maneira de regulação por parte do governo.

Um ponto importante e diferenciado para a época em que a Estratégia foi lançada é que o Governo, indo contra as expectativas, afirma desde 2003 a necessidade de cooperação para fazer a Internet se tornar um ambiente seguro, não sendo algo que dependa apenas da ação do governo, o que é um caráter de inovação que a Estratégia traz consigo. O Governo clama pelo trabalho conjunto, mostrando que a responsabilidade por assegurar a cibersegurança é compartilhada com todos os usuários da Internet, em contraponto ao pensamento corrente da época, de que tudo ficaria nas mãos do Governo (ZIMMER, 2004). A Estratégia dá

[33] *“In a modern computer-based information system environment, firms cannot produce reliable financial reports results without having secure computer systems.”* (GORDON et al, 2015, p. 12)

uma tônica muito forte para a parceria e cooperação entre indústria e governo, ao invés de seguir por uma linha que apontasse a regulação como única solução possível para o problema de segurança na Internet. Lemos (2003) complementa, inclusive, que esse caminho escolhido pelo Governo se alinhava com o que os especialistas afirmavam à época: que a regulação aumentaria os custos sem garantir que traria realmente maior proteção ao ciberespaço. Membros do setor privado também emitiram suas opiniões sobre a Estratégia e o significado dessa ação para se alcançar níveis maiores de segurança no ciberespaço:

> 'Nós temos uma estratégia presidencial e isso é bom, mas é apenas um primeiro passo', disse Dan Burton, vice-presidente de assuntos governamentais da empresa de segurança Entrust. 'Se nós olharmos para o relatório, ele é bastante forte quanto à ação do governo. É bastante forte no gerenciamento da Internet e em como a indústria e o governo podem trabalhar juntos para proteger a Internet. Mas é praticamente silencioso sobre como o setor privado pode melhorar a governança de seus próprios sistemas de TI.' (LEMOS, 2003, tradução nossa)[34].

Dessa forma, verifica-se que a Estratégia oferece uma certa esperança para o setor privado de que o Governo busca formas de trabalhar e fomentar a segurança no ciberespaço em parceria com a indústria, porém em seguida percebe-se que o documento traz ideias bastante abstratas e não planos de ação efetivos e factíveis. A falta de proteção e auxílio específico para o setor privado pode colocar em risco o país inteiro, mesmo que o Governo esteja aparentemente seguro e preocupando-se com esses tópicos. Se os sistemas do setor privado não estiverem seguros, é difícil afirmar que haverá, de fato, segurança (LEMOS, 2003).

Em 2003, o Governo se empenhou, além de lançar a Estratégia para o Ciberespaço, em dedicar parte relevante do orçamento para implementar esforços para cibersegurança, como a projeção de aumento de mais de U$50 milhões no orçamento do *National Infrastructure Protection Center* – chegando a U$125 milhões. Além disso, prometeram dedicar U$30 milhões para a *Cyberspace Warning Intelligence Network*; U$20 milhões para o *National Infrastructure Simulation and Analysis Center (*NISAC*)* do Departamento de Energia e U$11 milhões para

---

[34] *"We have a presidential strategy, and that's good, but it's only a first step," said Dan Burton, vice president of government affairs for security firm Entrust. "If you look at the report, it is fairly strong as to government action. It is fairly strong in Internet management and how industry and government can work together to secure the Internet. But it's virtually silent on how the industry can improve the governance of their own IT systems."* (LEMOS, 2003)

Cybercorps Scholarships, organizadas pela *National Science Foundation* e OMB, para estudantes da universidade serem capacitados para trabalhar como profissionais de segurança no governo (TURPEN et al, 2002). Vê-se, portanto, que ainda que o Governo Bush seja considerado mais teórico no que tange aos esforços para combater a insegurança no ciberespaço, existe um movimento de maior investimento em defesa e desenvolvimento de tecnologia no ciberespaço por parte do Governo, mostrando que o campo vinha nesse crescente de relevância e preocupação para todos os setores da sociedade. Também no ano de 2003 é perceptível o crescimento dos *Information Sharing and Analysis Centers (*ISACs*)*, muito por causa da ajuda voluntária do setor privado (THOMAS, 2013), apresentando de maneira marcante a forma como a parceria público-privada sói acontecer no período do Governo Bush – algo mais voluntário e menos estruturado/normatizado. A relação entre as esferas público e privada em relação ao ciberespaço acabam se desenvolvendo de acordo com a necessidade, mais do que através de um plano concreto.

A parceria se desenvolve desta forma no período por dois motivos aparentes: o primeiro é, como já visto, a prioridade do Governo em uma defesa mais ampla e abrangente, efetuada de maneira menos coordenada do que seria demandada para uma formação de parceria regularmente; e o segundo são as limitações – em questão de autoridade – que Governo norte-americano tinha em algumas situações, por causa de seu sistema de governo, o que acaba fazendo com que as organizações tenham que tomar a liderança na cibersegurança. Neste caso, falta ao Governo a autoridade plena – que poderia impor regulações e normas vinculantes para a cibersegurança –, mas também a *expertise* para agir na administração do setor privado nas questões de cibersegurança. O principal problema para o Governo é que muitos dos setores em posse do setor privado ainda são centrais à segurança nacional (CARR, 2016). Visto que o Governo está empreendendo esse movimento de buscar garantir de maneira mais efetiva a segurança e cibersegurança do país, torna-se assim extremamente necessário esse contato direto e preocupação legítima com o setor privado, buscando estreitar laços e obter cada vez mais troca de informação entre os setores.

Dessa forma, é possível verificar que ainda que existisse um movimento de maior preocupação e colocação do ciberespaço como tema central na política nacional e externa nos Estados Unidos, a parceria público-privada de

cibersegurança acabou sendo prejudicada ao não receber tanta atenção por parte do Governo. Este reconhecia a necessidade da parceria, porém não dispendeu tantos incentivos ou investimentos, deixando que a cooperação transcorresse de forma mais espontânea e de acordo com as necessidades apresentadas. A parceria é abordada nos documentos como de extrema relevância e é necessária para a evolução do Governo Bush no desenvolvimento de estratégias para a cibersegurança. No entanto, em função do contexto no qual a colaboração acontece, a importância e planejamento da parceria se dá mais no campo teórico do que efetivamente com políticas e ações que deem retorno à sociedade. Uma ação por parte do Governo que cria perspectivas de fomentação da parceria público-privada de maneira mais incisiva se dá quando os Estados Unidos lançam a *Comprehensive National Cybersecurity Initiative* – CNCI), quase no final do mandato de Bush, em 2008. Nesse documento tem-se uma nova premissa, de que o Governo Federal deve liderar as tecnologias de cibersegurança, repassando para os parceiros de acordo com suas necessidades essas tecnologias e possibilidades de avanços e desenvolvimento (HARKNETT; STEVER, 2011). O Governo norte-americano se posiciona, assim, como líder diante dos desafios do ciberespaço, garantindo, de certa forma, apoio aos que necessitarem internamente, incluindo o setor privado. A CNCI “estabelece a política, estratégia e diretrizes de defesa para proteger os sistemas de rede e servidores federais” (RIBEIRO; RIVERA, 2014, p. 143), buscando antecipar ameaças e vulnerabilidades, sempre sinalizando a importância de se ter apoio do setor privado – que normalmente já tem tecnologias mais inovadoras desenvolvidas, nesse empreendimento. A CNCI, em seguida, será revisada pelo Governo Obama, conforme veremos, adaptando-se às realidades do novo contexto e novo mandato em que este governo ocorre.

3.2 ESTRATÉGIA DA PARCERIA PÚBLICO-PRIVADA NA CIBERSEGURANÇA DO GOVERNO DO GOVERNO OBAMA (2009-2017)

Com o fim do mandato de Bush, Barack Obama é eleito presidente dos Estados Unidos nas eleições de 2008 e seu mandato tem início em janeiro de 2009. Obama inicia suas ações relativas à preocupação com o ciberespaço logo nos primeiros meses de seu Governo, quando solicita uma revisão da iniciativa originalmente lançada pelo Governo Bush em 2008, *The Comprehensive National*

Cybersecurity Initiative (CNCI). Nesta, indo mais além, “O Presidente dirigiu uma revisão abrangente, de 60 dias, para avaliar as políticas e estruturas dos EUA para segurança cibernética.” (ESTADOS UNIDOS, 2009a, tradução nossa)[35]. O objetivo dessa revisão era analisar e realinhar alguns pontos da CNCI para que a mesma obtivesse resultados positivos, sendo integrada adequadamente, alocando e coordenando de maneira orgânica seus fundos e ações, conjuntamente com o Congresso e o setor privado (ROLLINS; HENNING, 2009). Desde o início de seu mandato, Obama empreendeu um esforço em identificar problemas e boas práticas relacionadas à cibersegurança do país. Mostrando ter interesse em ser pró-ativo quanto à questão, buscou não permitir que as estratégias de defesa para o ciberespaço ficassem defasadas, expondo a um risco ainda maior toda a população norte-americana. Essa revisão da CNCI e iniciativa de adaptação e melhoria das ferramentas utilizadas para garantir a cibersegurança norte-americana também levou o governo Obama a recomendar “[...] uma avaliação das barreiras que continuavam a impedir a evolução da PPP[36] na segurança cibernética.” (THOMAS, 2013, p.13, tradução nossa)[37].

É percebendo esse movimento de interesse em mudança e aprimoramento nas táticas e estratégias de cibersegurança por parte do Governo Obama que se mostra relevante a análise de alguns documentos em específico bem como dos resultados obtidos pelos esforços do setor público em organizar e melhor gerir o meio cibernético norte-americano. Este esforço se deu, principalmente, em relacionar e envolver o setor privado nesse desenvolvimento de tecnologia e inovação. Nas subseções seguintes apresenta-se os principais pontos de dois documentos relevantes do período, emitidos pelo Governo Obama, relativos à cibersegurança e abordando a questão da parceria público-privada: *Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) e *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011). A partir dos principais pontos desses documentos, foi possível, juntamente com o cruzamento com demais dados e informações obtidas no estudo, encaminhar uma análise referente ao possível

---

35 *“The President directed a 60-day, comprehensive, ‘clean-slate’ review to assess U.S. policies and structures for cybersecurity.”* (ESTADOS UNIDOS, 2009a).

36 *Public Private Partnership*. Parceria público-privada.

37 *“[…] an evaluation of barriers that continued to impede the evolution of cybersecurity PPP.”* (THOMAS, 2013, p.13).

desenvolvimento da estratégia de cibersegurança, focando no crescimento e aprimoramento da parceria público-privada, ocorrido no período do Governo Obama.

3.2.1 *Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*

Este documento foi montado a partir da necessidade identificada pelo Governo Obama de identificar o que precisava ser alterado ou melhorado na forma como lidava-se com a cibersegurança nos Estados Unidos, a partir de reportes externos ao governo. É uma demonstração muito clara de que, durante o período do mandato de Obama, esta teria um lugar de destaque e seria tratada como prioridade, identificado como necessário o bom andamento do desenvolvimento da cibersegurança nacional para que as demais áreas de segurança também fossem eficazes e tivessem resultado positivo para a nação como um todo. O documento, então, é o resultado da análise de 60 dias feita pelas agências do governo, para buscar construir uma política e uma estrutura adequadas ao ciberespaço e à cibersegurança.

A primeira conclusão que o documento aponta é que a cibersegurança se encontra descentralizada em várias agências do governo, sem que nenhuma delas tenha autoridade o suficiente para tomar decisões sozinha ou, ainda, coordenar as outras áreas. Percebe-se, então a necessidade de uma estrutura abrangente para alinhar o governo, suas agências e também o setor privado e demais aliados na busca por uma Internet mais segura. O documento se fixa em três ideias principais: a liderança do governo, como autoridade que deve ajudar a gerenciar todas as áreas da cibersegurança; a educação e programas de conscientização de todos os níveis da população quanto a riscos e necessidade de cibersegurança para segurança nacional dos Estados Unidos; e a parceria público-privada, como meio de compartilhamento de informação e desenvolvimento na área ciber, buscando inovações no mundo digital e procurando garantir cada vez mais a segurança do país e seu povo (ESTADOS UNIDOS, 2009a).

Esse relatório traz à tona a importância da parceria com o setor privado, afirmando constantemente que o Governo Federal deveria se dedicar mais a essa cooperação, buscando delimitar conjuntamente com os parceiros os direitos, áreas de atuação e responsabilidades de cada parte envolvida, dando espaço para novas

parcerias e otimizando as já existentes. É reforçada a ideia de que a comunicação e troca de informações relativas a infraestruturas articuladas pelo governo com a academia e o setor privado devem ser melhoradas e desenvolvidas, pois uma das maiores dificuldades e impeditivos da evolução da parceria é o *déficit* de comunicação que existe entre as áreas. Essa convicção é visível no oitavo ponto – de dez levantados – no Plano de Ação de Curto Prazo:

> Preparar um plano de resposta de incidentes de cibersegurança; iniciar um diálogo para aprimorar parcerias público-privadas, visando à racionalização, alinhamento e fornecimento de recursos para otimizar sua contribuição e engajamento. (ESTADOS UNIDOS, 2009a, p. vi, tradução nossa)[38].

A necessidade de maior coordenação e integração no desenvolvimento da política para cibersegurança é apresentada e, a partir disso, 6 pontos são levantados no documento como principais para aprimorar a cibersegurança norte-americana. O primeiro deles é tratar a cibersegurança como prioridade nacional, sendo a liderança do Governo entendida como algo fundamental, com fim de formular uma política de cibersegurança coerente e unificada. Neste ponto também são contempladas as parcerias, com o Congresso – por leis adequadas – e com a indústria – para entender os impactos das leis e políticas nas operações de cada setor. O segundo ponto trata sobre a necessidade de construção de capacidade para uma nação digital, apresentando como o principal desafio enfrentado nesta tarefa: manter um ambiente que promova inovação, interconectividade aberta, prosperidade econômica, livre mercado e liberdade, garantindo também a segurança pública, liberdades civis e privacidade. É nesse ponto que se destaca a necessidade de programas de educação para o uso do ciberespaço como responsabilidade individual de cada usuário, além do incentivo ao desenvolvimento de novas tecnologias e ferramentas a serem usadas no ciberespaço e na cibersegurança. Também sugere o compartilhamento, treinamento e "rotação" entre agentes do governo com funcionários do ciberespaço, com a finalidade de trocar experiências, fazer "*cross-fertilization*"[39] e *network* (ESTADOS UNIDOS, 2009a).

---

[38] *"Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement"* (ESTADOS UNIDOS, 2009a, p. vi).

[39] "Intercâmbio ou interação (como entre ideias, culturas ou categorias diferentes), especialmente de natureza ampliada ou produtiva." (CROSS-FERTILIZATION, 2019).

O terceiro ponto é o mais relevante para o presente trabalho, pois trata do compartilhamento da responsabilidade pela cibersegurança. A primeira iniciativa necessária para melhorar essa delegação de responsabilidade incide em melhorar a parceria entre o governo e o setor privado, procurando saber onde as leis podem ajudar ou prejudicar as empresas parceiras. Além disso, um ponto relevante levantado no documento é a necessidade de se dar uma razão para o setor privado que justifique a integração de sistemas de informação e comunicação de segurança, pois naturalmente não parece ser vantajoso para as empresas, dificultando que aconteça um movimento espontâneo das mesmas em busca da parceria com o setor público. Cabe, então, ao governo procurar demonstrar que a parceria é interessante para mitigar os riscos individuais e coletivos, mostrando valor e promovendo um ambiente que facilite e encoraje a parceria e compartilhamento de informações entre setores. É reportado no documento que é tarefa do Governo empenhar-se na busca por identificar um modelo já utilizado nas parcerias que se mostre o mais adequado e efetivo – ou, observando todos os existentes, adaptá-los de forma a chegar no melhor ponto ótimo da relação –, pois o que temos hoje é uma variedade de parcerias, sem padrão algum de funcionamento e nenhum asseguramento dos direitos e deveres envolvidos (ESTADOS UNIDOS, 2009a). Esse trabalho de revisão de modelos de parceria utilizados é preciso por terem-se identificado diversos problemas nas parcerias existentes, tais quais delineamento de papéis e responsabilidades, desigualdade de capacidade entre grupos e uma proliferação muito grande de planos e recomendações quanto ao assunto, sem haver uma ordem ou padrão para os mesmos. Verifica-se a simultaneidade de esforços muito semelhantes e duplicados, que não dialogam entre si para utilizar ferramentas já desenvolvidas. Por essa razão, o documento afirma que deveriam definir-se claramente a natureza de cada uma das relações, os papéis dos agentes e as responsabilidades que cada um terá, bem como expor as expectativas e objetivos de cada parte, de forma a haver uma ciência coletiva dos papéis individuais na parceria (ESTADOS UNIDOS, 2009a). Dentre as atividades de cada grupo, o Governo se vê responsável por avaliar a potencial existência de barreiras impeditivas à evolução da parceria público-privada, como leis federais e regulações que podem afastar o setor privado da cooperação.

> Como parte da parceria, o governo deve trabalhar de forma criativa e colaborativa com o setor privado para identificar soluções personalizadas que levem em conta a necessidade de trocar informações e proteger interesses públicos e privados e adotar uma abordagem integrada à segurança nacional e econômica. (ESTADOS UNIDOS, 2009a, p. 19, tradução nossa)[40].

É crucial para o bom desenvolvimento dessas parcerias o cuidado dos agentes do governo em procurar identificar quais os pontos que desmotivam o setor privado a participar da parceria. Toma-se por exemplo: entende-se que as empresas se sentiriam mais confortáveis em compartilhar suas informações caso a cooperação não exigisse o envio de dados de propriedade particulares para o seu funcionamento. Além disso, também é levantada a importância de, a partir da parceria público-privada, construir cooperações com o setor privado também no ambiente internacional, aproveitando oportunidades associadas às infraestruturas de comunicação e informação, que são tão relevantes para o desenvolvimento de negócios, serviços governamentais e militares norte-americanos (ESTADOS UNIDOS, 2009a).

O quarto ponto trata da obrigação de serem criadas respostas a incidentes e compartilhamento de informações no ambiente do ciberespaço, tanto intra-agências do governo quanto em relação aos demais parceiros e aliados, havendo uma coordenação das as ações que visam combater ameaças no ciberespaço. De acordo com o documento, apenas o governo teria autoridade o suficiente para sistematizar essas ações, sendo tarefa do governo, também, mapear as ameaças e possíveis reações existentes, de maneira a divulgar esse mapa e orientar os demais em busca de criar uma coesão. Uma vez que o governo teria essa característica de liderança e autoridade, seria de sua incumbência, também, desenvolver processos que ligassem o setor privado e público para dar assistência na prevenção, detecção e resposta a incidentes no ciberespaço, sendo o compartilhamento de informação – com clareza e prestação de contas – a chave para o bom funcionamento dessa iniciativa, defendendo o que realmente é fundamental para a segurança norte-americana: as infraestruturas críticas (ESTADOS UNIDOS, 2009a). O penúltimo ponto trata sobre a primordialidade de se encorajar a inovação, visto que quando o relatório foi

---

[40] *"As part of the partnership, government should work creatively and collaboratively with the private sector to identify tailored solutions that take into account both the need to exchange information and protect public and private interests and take an integrated approach to national and economic security.."* (ESTADOS UNIDOS, 2009a, p. 19).

elaborado não havia uma linha guia que orientasse as tomadas de decisões para seguimento em uma área ou outra de tecnologia e desenvolvimento, não havendo uma coordenação salutar na busca por conhecimento e avanços tecnológicos. O documento urge pela definição de padrões e criação de incentivos à pesquisa e desenvolvimento. Por fim, o último ponto expõe os planos de ação de curto e médio prazo, consolidando as ideias expostas ao longo do documento em um grupo de ideias focais, divididas pelo tempo a serem implementadas. O ponto referente à parceria público-privada do plano de ação de curto prazo já foi citado no início deste subcapítulo[41]. Na lista de médio prazo, identifica-se duas ideias que abordam o tema da parceria público-privada, apresentadas a seguir: o ponto 7, que propunha "Desenvolver um processo entre o governo e o setor privado para dar assistência na prevenção, detecção e resposta aos ciberincidentes." (ESTADOS UNIDOS, 2009a, p. 38, tradução nossa)[42]; e o 11, que visa "Encorajar a colaboração entre acadêmicos e laboratórios industriais para desenvolver '*migration paths*' e incentivos para rápida adoção de pesquisa e inovação no desenvolvimento de tecnologia." (ESTADOS UNIDOS, 2009a, p. 38, tradução nossa)[43].

O objetivo final do documento, então, é consolidar infraestruturas de comunicação e informação confiáveis e resilientes, construídas por meio de uma parceria público-privada nacional e também por um plano de ação, de curto e longo prazo, coerentes entre si e não sobrepujantes (ESTADOS UNIDOS, 2009a). O relatório, no seu todo, apresenta a urgência de se criar e manter uma política mais balanceada e integrada para o ciberespaço, abrangendo todos os atores envolvidos, de modo a não excluir ou deixar em desvantagem nenhum deles. É necessário, por fim, que o governo desenvolva proposições de valor compreensíveis juntamente com a indústria, de modo a proteger as infraestruturas críticas encontradas no meio digital – e quase todas pertencentes ao setor privado. O ponto mais tocado e reforçado no documento é, então, a necessidade de um ambiente colaborativo e da construção de trabalho conjunto, respeitando as particularidades e objetivos de cada um dos parceiros.

---

41 Ver p. 51.

42 *"Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents."* (ESTADOS UNIDOS, 2009a, p. 38).

43 *"Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations."* (ESTADOS UNIDOS, 2009a, p. 38).

3.2.2 *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*

A Estratégia Internacional para o ciberespaço produzida pelo Governo Obama deixa claro desde seu princípio que não pretende ser um reporte com visões e sugestões para o futuro, mas sim uma agenda a ser realizada no presente. Em sua introdução reforça que ações executadas na Internet têm consequências reais no mundo físico e que existe uma alta dependência da Internet no mundo todo, sendo, por isso, necessário fazê-la um lugar seguro. Os Estados Unidos surgem nesse contexto como um líder que pretende ensinar e auxiliar as demais nações através do exemplo. Em sua carta de apresentação, logo na abertura da Estratégia, o presidente Barack Obama afirma que

> O mundo digital não é mais uma fronteira sem lei, nem a província de uma pequena elite. É um lugar onde as normas de conduta responsável, justa e pacífica entre estados e povos começaram a se firmar. É um dos melhores exemplos de organização comunitária, pois a sociedade civil, a academia, o setor privado e os governos trabalham em conjunto democraticamente para garantir sua gestão eficaz. (ESTADOS UNIDOS, 2011, tradução nossa)[44].

O presidente reforça, desde o início, a importância dessa inter-relação e cooperação entre as mais diversas áreas, para fazer do ciberespaço um ambiente de desenvolvimento e prosperidade. Além disso, o texto apresentado na Estratégia salienta diversas vezes a necessidade de se manter o livre fluxo de informações para que o ciberespaço possa ter valor e ser um ambiente agradável aos seus usuários. No entanto, é registrado o desafio de manter as liberdades fundamentais e também garantir a segurança do país no ciberespaço, situações que parecem ser conflitivas, pelo fato de questões da segurança afetarem possivelmente a privacidade. O Governo norte-americano, entretanto, afirma ser factível buscar ambos objetivos e se coloca como meta fazê-lo (ESTADOS UNIDOS, 2011). Uma das ferramentas que se pretendem a utilizar é a alta comunicação e troca de informação, que permitiria ter os princípios de liberdade, privacidade e livre fluxo de informações e, em paralelo, também conseguir monitorar o mau uso da Internet.

---

[44] *"The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just, and peaceful conduct among states and peoples have begun to take hold. It is one of the finest examples of a community self-organizing, as civil society, academia, the private sector, and governments work together democratically to ensure its effective management."* (ESTADOS UNIDOS, 2011).

Ao projetar um futuro, na Estratégia, o Governo Obama afirma que indivíduos e negócios terão fácil e rápido acesso a ferramentas para garantir e gerenciar sua presença online. Nessa perspectiva, as empresas do setor privado também teriam responsabilidade pela limpeza de sua rede, sabendo como fazê-lo e protegendo seus investimentos (ESTADOS UNIDOS, 2011). A argumentação do documento é que os Estados Unidos já estão trabalhando por esse futuro, mas que isso não se alcançará num empreendimento solo, dando alta relevância para as parcerias e cooperações - nacionais e internacionais. A Estratégia traz interesses nacionais dessa projeção de futuro, no entanto, o Governo alega que muitos dos seus objetivos são também objetivos compartilhados internacionalmente. A colaboração internacional propiciará a sedimentação de uma infraestrutura de informação e comunicação que apoia o comércio e os negócios internacionais de maneira aberta, interoperável, segura e confiável. Dessa projeção é concluída a necessidade de estabelecerem-se, também, normas de comportamento responsável para a parceria (ESTADOS UNIDOS, 2011).

Ao longo de todo documento, “companhias” e “empresas” são citadas como agentes promotores de pesquisa e desenvolvimento, mostrando a visão do Governo de que o setor privado é fonte de inovação e tecnologias diferenciadas para o ciberespaço. A partir dessa ideia, levanta-se a proposição de que a Estratégia só será eficaz se se agir em diversas frentes, com responsabilidades compartilhadas, havendo uma colaboração e troca de informações e métodos de desenvolvimento, principalmente no quesito de resposta a incidentes, entre o Governo, setor privado e comunidade internacional (ESTADOS UNIDOS, 2011). No entanto, esse compartilhamento de informações, diferentemente dos outros documentos analisados no presente trabalho, é incentivado a ser uma tarefa pertinente a todos os países e atores/setores interessados em diminuir vulnerabilidades, construindo um consenso de comportamento adequado no ciberespaço, capaz de abranger tanto países quanto setores e indivíduos.

Os Estados Unidos têm o objetivo de promover três pontos através dessa Estratégia e plano de ação para o presente/projeção para o futuro: diplomacia, defesa e desenvolvimento. A ideia é que, a partir da promoção desses tópicos, se aumente a segurança, prosperidade e abertura no ciberespaço, crescendo neste ambiente um sentimento de responsabilidade coletiva, de cooperação. A diplomacia foca em fortalecer as parcerias, sejam ela bilaterais, multilaterais, com organizações

ou em colaboração com o setor privado. Neste contexto, a diplomacia pretende abarcar toda a comunidade da Internet e fomentar esse contato e colaboração com o setor privado, sociedade civil, academia e governos. Ainda assim, o documento enfatiza que "Esses esforços serão apoiados por uma colaboração significativa com o setor privado em casa e no exterior." (ESTADOS UNIDOS, 2011, p. 11, tradução nossa)[45]. Mais uma vez, a preocupação corrente para ambos governos analisados neste trabalho de cooperação com os detentores e operadores das infraestruturas críticas é apresentada. Neste mandato, se dá com o Governo afirmando dar especial atenção para essa parceria, procurando aumentar os mecanismos de engajamento com seus parceiros industriais. A defesa tem um foco maior em dissuasão, principalmente externa, garantindo a resiliência das redes e sistemas de informação, o que necessita de esforço e colaboração do Governo, setor privado e indivíduos. É interessante verificar que nesta parte da Estratégia o Governo reconhece que já é possível verificar a eficácia das ações de conscientização, de melhora do tempo de resposta a incidentes e também do compartilhamento de informações, sendo resultado das ações conjuntas do Governo com o setor privado. Ao mesmo tempo que veem os efeitos das ações, o Governo segue querendo manter essa parceria e fazê-la crescer cada vez mais, como é possível verificar: "[...] buscamos continuamente novas formas de fortalecer nossa parceria com o setor privado para aumentar a segurança dos sistemas nos quais ambos confiamos" (ESTADOS UNIDOS, 2011, p. 13, tradução nossa)[46].

Como é o foco do presente trabalho analisar a relação do Governo com o setor privado ao tratar de temas como ciberespaço e cibersegurança, vale destacar que o Governo Obama evidencia muito a parceria com o setor privado na Estratégia Internacional para o Ciberespaço. Recomendando, inclusive, para os demais países que desejarem se espelhar no exemplo norte-americano, que fomentem e busquem alcançar uma parceria e cooperação com o setor privado presente e ativo em sua nação, identifica que boa parte da eficácia do desenvolvimento norte-americano na área se deu por causa do bom relacionamento e esforço em compartilhar informações e dados com quem detinha um conhecimento mais desenvolvido que o

---

[45] *"This efforts will be suported by meaningful colaboration with the private sector at home and abroad."* (ESTADOS UNIDOS, 2011, p. 11).

[46] *"[...] we continually seek new ways to strengthen our partnership with the private sector to enhance the security of the systems on which we both rely."* (ESTADOS UNIDOS, 2011, p. 13).

Estado, o setor privado (ESTADOS UNIDOS, 2011). Além disso, os Estados Unidos, incentivam uma construção de capacidade técnica a nível mundial, que precisa de investimento do setor privado e do trabalho conjunto dos Estados Unidos com governos e empresas globais. Essa cooperação se dá principalmente àqueles países que não fazem restrições de acesso na Internet, que buscam garantir o fluxo livre de informações – uma das prioridades políticas do Governo Obama – e promovem redes interoperáveis a nível mundial.

Como tópicos finais da Estratégia, o Governo expõe 7 áreas interdependentes de atividades, que necessitam de colaboração do Governo com parceiros internacionais e o setor privado. A primeira é a Economia, onde o Governo busca promover um mercado aberto e incentiva a inovação, protegendo a propriedade intelectual, além de buscar desenvolver um padrão para cibersegurança baseada em consenso, envolvendo tanto o setor público como o privado no estabelecimento desse padrão. A segunda área é a Proteção das Redes Locais, procurando alcançar a garantia dessa proteção através de cooperação com organizações internacionais, relacionando-se com outros países através delas. Além disso, responsabiliza as agências e o setor privado, em coordenação, como atores que devem buscar garantir a proteção de invasões não autorizadas que podem afetar a integridade da economia e segurança nacional. Nesse ponto, o compartilhamento de informações e ameaças que afetam a todos, não só a nível nacional, mas internacional, também é bastante importante e destacado. A terceira área é de Aplicação da Lei, que trata sobre o desenvolvimento internacional coletivo de leis e o incentivo norte-americano de adesão à Convenção de Budapeste[47]. A quarta área é a Militar, que busca preparar-se para os desafios do século XXI através de cooperação e alianças militares com outros países que compartilham interesses e objetivos semelhantes

[47] A Convenção de Budapeste foi resultado de um "[...] esforço da União Europeia para constituição de um instrumento jurídico hábil a combater o cibercrime tem como precursores os trabalhos desenvolvidos pela OCDE e pelo G8, e também, de outros estudos viabilizados pelas Nações Unidas e pelo Conselho da Europa. A Convenção de Budapeste resultou assim, como fruto destes estudos e recomendações que se fizeram prementes, principalmente a partir da construção do ideal de cooperação em matéria penal que já amadurecido neste espaço comunitário." (MORAIS NETO, 2009, p. 120-121). Em um primeiro momento, a Convenção tinha foco em atender as demandas europeias por regulamentação da Internet, no entanto "Desde sua adoção em 23 de novembro de 2001, em Budapeste, Hungria, um total de 46 Estados já assinaram a Convenção sobre Cibercrime (Convenção de Budapeste), sendo que deste total, até 16 de abril de 2009, 28 nações já a ratificaram, incluindo países que não integram a União Europeia: Canadá, Costa Rica, República Dominicana, Japão, México, Filipinas África do Sul e com destaque os Estados Unidos, berço da internet (a Convenção foi ratificada em 2006 e entrou em vigor em 1 de janeiro de 2007)." (MORAIS NETO, 2009, p. 123).

aos Estados Unidos. A quinta área é a Governança da Internet, que tem como prioridade preservar e aumentar o acesso a uma Internet global (ESTADOS UNIDOS, 2011), mantendo o ambiente descentralizado, cooperativo e dividido em camadas – cada qual com suas demandas e prioridades. A sexta área é o Desenvolvimento Internacional, onde o Governo norte-americano se propõe a ajudar outros países a aprender da experiência dos Estados Unidos e desenvolverem suas próprias estratégias e políticas para o ciberespaço. Nesta área, mais uma vez, destaca-se a importância da parceria público-privada para bom desenvolvimento da cibersegurança por parte dos Estados. A sétima área é a Liberdade na Internet, que visa apoiar as liberdades fundamentais e privacidade também no âmbito do ciberespaço.

Por fim, o documento é encerrado trazendo a memória de que a quase 40 anos, no momento em que se escreve o presente trabalho, " [...] poucos entenderam que algo chamado Internet levaria a uma revolução em como trabalhamos e vivemos" (ESTADOS UNIDOS, 2011, p. 25, tradução nossa)[48]. No entanto, 30 anos depois, a Estratégia de 2011 para Ciber Segurança Internacional dos Estados Unidos surge como uma necessidade de projeção para o futuro do desenvolvimento a nação e também como um projeto/plano de ação para os departamentos e agências norte-americanas inseridos na realidade do país. A Estratégia é apresentada como um documento a ser utilizado no dia-a-dia, um *roadmap* para organizar a ação de cada um dos agentes envolvidos e preocupados com a cibersegurança dos Estados Unidos. Por fim, a Estratégia "É uma chamada para o setor privado, a sociedade civil e os usuários finais a reforçarem os esforços por meio de parcerias, conscientização e ação." (ESTADOS UNIDOS, 2011, p. 25, tradução nossa)[49], em conjunto com o Governo norte-americano e buscando sempre reforçar e garantir a segurança nacional no âmbito do ciberespaço, sem advogar contra a privacidade e liberdades fundamentais, princípio básico do Governo dos Estados Unidos.

---

[48] *"[...] few understood that something called the Internet would lead to a revolution in how we work and live."* (ESTADOS UNIDOS, 2011, p. 25).

[49] *"It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action."* (ESTADOS UNIDOS, 2011, p. 25).

3.2.3 Balanço da estratégia para o ciberespaço do Governo Obama, sobre o espectro da parceria público-privada

Ao analisar os documentos do Governo Obama, que visavam construir e sedimentar uma estratégia para o ciberespaço e cibersegurança norte-americana, percebe-se que o Governo em questão é aquele que apresenta ações e proposições mais práticas em comparação com os anteriores. É necessário considerar que o Governo Obama se beneficia da própria evolução que o ciberespaço e a Internet obtiveram ao longo dos anos - modernizações e novas tecnologias facilitam a tomada de decisão e a comunicação -, mas ainda assim a decisão de se envolver diretamente na busca por garantia de segurança neste ambiente é destacável dentre as diversas ações tomadas pelo gabinete presidencial e agências ligadas ao presidente ao longo do mandato de Obama. De acordo com o *National Preparedness Report* de 2012, houve um aumento de 650% no número de reportes de ciberataques nos Estados Unidos comparando os anos de 2006 e 2010 e quando analisamos os anos de 2006 e 2014 esse número aumenta ainda mais, chegando a 1121% mais ciberataques reportados nos Estados Unidos. Isto explica o crescimento do interesse por parte do Governo norte-americano em segurança das infraestruturas críticas, principalmente as alocadas em ambiente virtual (JENTLESON, 2014; PANG; TANRIVERDI, 2017). No entanto, antes mesmo de se deparar com esses números, logo no seu quarto mês como presidente dos Estados Unidos, Barack Obama fez um discurso intitulado "*Remarks by the President on Securing Our Nation's Cyber Infrastructure*", demonstrando a preocupação que seu Governo viria a ter durante todo o seu mandato. Neste discurso, Obama já salientava também a importância que o setor privado teria para desenvolver métodos e programas de cibersegurança eficazes e satisfatórios: "trabalharemos com todos os principais atores – incluindo governos estaduais e locais e o setor privado – para garantir uma resposta organizada e unificada a futuros incidentes cibernéticos." (ESTADOS UNIDOS, 2009b, tradução nossa[50]; LOBATO; KENKEL, 2015).

Além de lidar desde o princípio com as questões do ciberespaço e, simultaneamente, se deparar com o crescimento dos riscos e ameaças neste ambiente que os norte-americanos corriam, a Doutrina de Obama teve que se

---

[50] *"[…] we will work with all the key players -- including state and local governments and the private sector -- to ensure an organized and unified response to future cyber incidents."* (ESTADOS UNIDOS, 2009b).

ocupar com outras demandas e preocupações totalmente novas que ficavam cada vez mais em evidência durante o período do início do mandato de Obama, quais sejam: aquecimento global; guerra cibernética; endividamento nacional e terrorismo doméstico (RIBEIRO; RIVERA, 2014). Para enfrentar esses novos desafios, com dinâmicas diferenciadas, o Governo Obama inova na forma de ação e promove uma ruptura com a abordagem de intervenções militares unilaterais, abrindo espaço para a coparticipação de diversas áreas e setores da sociedade nas ações do Governo. As ações deixavam de ser puramente independentes por parte do Governo, que inclusive procurava a participação e envolvimento de outras áreas, principalmente do setor privado.

Conforme verificado anteriormente, a ação do Governo Obama de empreender uma revisão de 60 dias para verificar a efetividade da CNCI através da *Cyber Space Review: Assuring a Trusted and Resilient Information Communications Infrastructure* se configurou como o norteador do planejamento do Governo norte-americano neste período. Esse reporte e revisão acarretaram no desenvolvimento da *Executive Order 13636* e também em modificações da CNCI. Ambos documentos merecem destaque, pois a partir deles é que são lançadas novas diretrizes do Governo para trabalhar com os elementos-chave da cibersegurança: os governos estaduais e locais e principalmente o setor privado, de forma a garantir uma resposta organizada e unificada a incidentes, e também uma campanha para a conscientização em relação à segurança cibernética (RIBEIRO; RIVERA, 2014).

A revisão da *Comprehensive National Cybersecurity Initiative* (CNCI), publicada em 2009 pelo Governo Obama, aponta a cibersegurança como o maior desafio econômico e de segurança nacional dos Estados Unidos, mostrando a importância do tema para o Governo. Em maio de 2009, o presidente Obama aceitou as recomendações do *Cyberspace Policy Review*, orientando-se em direção ao fortalecimento da parceria público-privada para desenvolver e alcançar tecnologias que levem à segurança e prosperidade do país, sem afetar a privacidade dos cidadãos - tópico bastante importante para o Governo e reforçado diversas vezes ao longo dos documentos emitidos durante o mandato de Obama. Os três objetivos principais do CNCI foram definidos como: estabelecer uma defesa com linha de frente contra ameaças imediatas - através da parceria público-privada -, defender-se contra o espectro total de ameaças e, por fim, fortalecer o futuro ambiente da cibersegurança (ESTADOS UNIDOS, 2010b). A partir desses objetivos, o Governo

norte-americano estabelece 12 iniciativas que ajudam a promover a proteção do ciberespaço dos Estados Unidos. Estas, porém, só se alcançariam, de acordo com Ribeiro e Rivera, com “certo fortalecimento de certas capacidades fundamentais e estratégicas dentro do governo” (RIBEIRO; RIVERA, 2014, p. 144). Também na revisão feita para a nova e reformulada CNCI, o presidente Obama recomendou uma avaliação das barreiras que continuavam a impedir a evolução da parceria público-privada, identificada como fundamental para trabalhar em direção a uma garantia de cibersegurança para os cidadãos norte-americanos (THOMAS, 2013). Além disso, de acordo com Harknett e Stever (2011), o Governo Obama trouxe um novo *approach* para a implementação da CNCI – abrangente e racional –, colocando como ator central o Congresso e, assim, contrariando o tratamento dado para esse ator nas estratégias advindas do Governo Bush.

Quatro anos depois, é lançada a *Executive Order* 13636, sobre a qual é importante frisar o foco dado à necessidade de se aumentar a cibersegurança das infraestruturas críticas. Através dela buscou-se proteger, incentivar o desenvolvimento e manter a confidencialidade e privacidade própria às infraestruturas críticas, através de parcerias com os detentores e operadores dessas infraestruturas, de modo a aumentar o compartilhamento de informações e colaboração no desenvolvimento e implementação de padrões de ação baseados em riscos (ESTADOS UNIDOS, 2013). O documento decretou uma produção de relatórios de ciberameaças que permita identificar uma entidade específica ameaçadora e também lançou um programa voluntário de compartilhamento de informação, que tinha como ideia principal o intercâmbio de funcionários do setor privado no serviço Federal para auxiliar com melhorias nos programas de compartilhamento de informações do Governo com a indústria. Além disso, lançam também *The Cybersecurity Framework*, que procura entregar uma estratégia de abordagem flexível, repetível e baseada em performance, que ajude os detentores e operadores das infraestruturas críticas a encontrarem padrões em seu desenvolvimento e enfrentamento de desafios. Estabelecem também um programa voluntário de adesão a esse *Framework*, que ainda que seja espontâneo deve receber apoio e incentivo do Secretário do Governo para fomentar e promover a participação. Mais uma vez, é lançado um documento que motiva o compartilhamento de informações e respostas a ameaças, principalmente preocupando-se com as infraestruturas críticas, o que coloca o Governo em contato

com o setor privado de modo a formarem uma parceria para garantir a segurança no ciberespaço tanto individual de cada setor, como coletivamente de toda a nação.

O Governo Obama também altera o sistema de coordenação das questões cibernéticas, trazendo para mais perto da Casa Branca o gerenciamento das ações e possibilitando que o DHS se dedique mais ao desenvolvimento de estratégias para as áreas críticas (HARKNETT; STEVER, 2011). Dessa ação surge uma oportunidade de criar uma infraestrutura mais institucional para avançar nas políticas de cibersegurança, ratificando a importância que esse tema tem para o Governo. Outra questão que é reforçada diversas vezes ao longo dos documentos analisados, e também se faz visível nas ações práticas do Governo, é a intenção de fortalecer as parcerias de um modo geral, com diversos setores e atores do ciberespaço, mas em especial com o setor privado (THOMAS, 2013). Ambos os setores vão se adequando e buscando melhorias internamente para melhor aproveitar o que a parceria tem a oferecer. Thomas destaca esse movimento ao dizer que

> Como a Casa Branca e as agências federais reforçaram seu foco e estratégia em relação à segurança cibernética, o setor privado também passou por mudanças organizacionais, tornando-o mais adequado à participação em PPPs de segurança cibernética. (THOMAS, 2013, p. 14, tradução nossa)[51].

É possível verificar que o interesse do Governo em fortalecer a parceria e aumentar o fluxo de compartilhamento de informações entre empresas privadas e o setor público também é reflexo do desejo do Governo de se fazer mais presente no ambiente cibernético nacional, exercendo sua liderança nesse espaço também. Além da *Executive Order 13636* e a retificação da CNCI, o Governo Obama demonstra, ainda, seu interesse em fortalecer a cooperação e aproximar-se do setor privado através do *National Institute for Standards and Technology*[52] (NIST), que

---

[51] *"As the White House and federal agencies have strengthened their focus and strategy relating to cybersecurity, the private sector has also undergone organizational changes making it better suited to participation in cybersecurity PPPs."* (THOMAS, 2013, p. 14)

[52] "O Instituto Nacional de Padrões e Tecnologia (NIST) foi fundado em 1901 e agora faz parte do Departamento de Comércio dos EUA. O NIST é um dos mais antigos laboratórios de ciências físicas do país. O Congresso estabeleceu a agência para remover um grande desafio à competitividade industrial dos EUA na época – uma infra-estrutura de medição de segunda categoria que ficou para trás das capacidades do Reino Unido, Alemanha e outros rivais econômicos." (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, 2019a, tradução nossa). "The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged

passa a trabalhar também com cibersegurança e tem como meta identificar padrões de segurança dentro das indústrias, com fim de identificar um quadro geral de boas práticas e métodos eficazes de implementar cibersegurança. O Governo reconhece que as empresas estão avançadas em relação ao setor público no quesito desenvolver e manter uma estrutura cibernética – e de segurança – sólida, e procura esse contato com o setor privado voluntariamente para, através da parceria, aprender e aumentar sua capacidade de gerenciar a cibersegurança nacional. Além disso, o movimento do Governo em direção a um fomento da parceria dá-se por ficar claro que a quantidade de empresas detentoras e operadoras das infraestruturas críticas e do setor de comunicação serem pertencentes ao setor privado só aumentou com o passar dos anos. Sendo assim a parceria com esse setor uma das únicas opções para a administração dos Estados Unidos manter-se em contato e, de certa forma, influenciando as práticas desses setores que são tão relevantes para manter a segurança do país inteiro (RIBEIRO; RIVERA, 2014).

Em 2014, o NIST, recebendo ajuda do setor privado, lança o documento *Framework for Improving Critical Infrastructure Cybersecurity*, baseado na *Executive Order 13636*, consolidando a estratégia unificada para a cibersegurança nacional e trazendo a cooperação governo-empresa como carro chefe dessa ação. O documento é formulado de maneira a compreender uma linguagem comum entre os setores, tendo por motivações e objetivos principais gerenciar os riscos de maneira eficaz na manutenção da cibersegurança, sem adicionar novas exigências regulatórias às empresas – o que muitas vezes dificultava o desenvolvimento interno das empresas bem como da parceria (NIST, 2014; RIBEIRO; RIVERA, 2014).

No entanto, ainda que o Governo Obama realizasse um esforço ímpar para abranger mais campos dentro do ciberespaço e buscasse se atualizar nas tecnologias, visando apoio do setor privado nesse empreendimento, foram registradas algumas críticas à conduta do Governo, marcadamente durante o mandato de Obama. Harknett e Stever (2011) argumentam criticamente em relação às ações do Governo Obama ainda no terceiro ano de mandato, afirmando que

---

behind the capabilities of the United Kingdom, Germany, and other economic rivals.” . (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, 2019a). O NIST tem atuação em diversas áreas e frentes, a parte que lida com cibersegurança, implementa segurança cibernética e privacidade práticas por meio de divulgação e aplicação de padrões e melhores práticas, de forma que os Estados Unidos adotem recursos adequados e eficazes de cibersegurança. (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, 2019b).

Obama havia prometido uma “cara” nova para sua ciberpolítica, com a proposição de um novo pensamento estratégico, mas o que vinha entregando era apenas uma continuação sem grandes mudanças, apenas um “crescente linear” do que o Governo Bush já vinha realizando neste campo. Em 2014, Ribeiro e Rivera (2014) apontam que o Governo Obama se propõe a desenvolver uma força de trabalho especializada em cibersegurança forjando também nessa proposta a parceria do setor público com o setor privado e com os acadêmicos. Porém, no ano seguinte observa-se Schneier (2015), tecendo não uma crítica diretamente ao modo de agir do Governo mas, em seu livro *Data and Goliath*, expondo que o Governo e seus gestores, agências e departamentos “[...] devem trabalhar com as comunidades acadêmicas e empresariais para garantir que quaisquer vulnerabilidades inseridas por partes mais hostis sejam descobertas, reveladas e desativadas.” (SCHNEIER, 2015, p. 183, tradução nossa)[53]. Essa recomendação mostra que, ainda que o Governo Obama estivesse dirigindo esforços em lançar documentos e ações para maior engajamento, compartilhamento de informações, evolução do ciberespaço e fomento da parceria público-privada, no mínimo, as ações não estavam surtindo efeito até o momento, o que deixou os especialistas no assunto preocupados. Por fim, Gordon et al (2015) também elogiam o fato do presidente Obama ter reconhecido a importância da cibersegurança para garantir a segurança nacional. Apontam que esse reconhecimento é um primeiro passo necessário para resolver os desafios de riscos de cibersegurança e incidentes, porém, ainda é apenas um primeiro passo num longo caminho. Os próximos passos envolveriam identificar as soluções para esses desafios e obstáculos, que têm como exemplo citado pelos autores a tendência das empresas do setor privado a investirem muito pouco – principalmente quando comparado com o quanto deveriam gastar – em cibersegurança (GORDON et al, 2015). Vê-se, assim, que ainda em 2015 o Governo norte-americano não tinha consolidado o suficiente uma parceria público-privada de modo que esse tipo de desafio ainda seria um dos mais representativos dentre a lista de problemas a serem resolvidos envolvendo o ciberespaço.

Quanto ao investimento despendido em cibersegurança e para que o recurso foi destinado dentro do escopo de cibersegurança, sabe-se que em 2011 cerca de

---

[53] *“[...] should work with the academic and business communities to ensure that any vulnerabilities inserted by more hostile parties are discovered, revealed, and disabled.”* (SCHNEIER, 2015, p. 183).

US$ 245 milhões foram dispostos para combate de ameaças envolvendo o terrorismo e para aumentar a Segurança Nacional. A cibersegurança foi incluída dentro dessa divisão, repartindo o fundo com a área de contraterrorismo, contrainteligência e outras ameaças contra a Segurança Nacional. A cibersegurança também recebeu investimento advindo da quota de capital destinada para proteção de redes de informações críticas. O orçamento, nesse caso, era ainda maior, reservando US$364 milhões para apoiar as operações da Divisão Nacional de Ciber Segurança, que tem função de proteger os sistemas Federais e também empreender esforços indicados na CNCI, focando principalmente na proteção das redes de informação frente a ameaças de ataques (ESTADOS UNIDOS, 2010a). O cibercrime, no entanto, continuou a evoluir e a aumentar o prejuízo deixado após os ataques, também em despesas monetárias para os afetados. Em 2015, o cibercrime custou cerca de US$500 bilhões, a nível global e esse número não apresentava tendência de baixar. A preocupação norte-americana cresce ainda mais por ter responsabilidade em mitigar esses ataques, visto que o setor de cibersegurança global é formado por 40% de empresas norte-americanas. Sendo assim, gera-se um interesse em atacar os Estados Unidos, mas também existe uma expectativa global de que as empresas norte-americanas desenvolvam tecnologias e métodos que capacitem os indivíduos, empresas e governos a se defenderem no ciberespaço. Na tentativa de contribuir com as empresas norte-americanas focadas em cibersegurança, para fomentar a parceria público-privada e cumprir seu dever como provedor de soluções e educador quanto às ameaças do ciberespaço, o Governo Obama começou a trabalhar em aumentar a cibersegurança para infraestruturas críticas e importantes tecnologias, cunhando-se como o maior investidor e financiador de cibersegurança no país, em 2017, com orçamento de US$19 bilhões para este ano (AUSTRALIA, 2019).

> Em particular, esse financiamento apoiará o Plano de Ação Nacional de Cibersegurança, que realiza ações de curto prazo e implementa uma estratégia de longo prazo para aumentar a conscientização e proteção da cibersegurança, proteger a privacidade, manter a segurança pública, bem como a segurança econômica e nacional, e capacitar os americanos a assumir um melhor controle de sua segurança digital. [...] Conforme descrito acima, o Orçamento fornece US $ 19 bilhões em recursos para segurança cibernética. Isso inclui a criação de um novo fundo rotativo de US $ 3,1 bilhões, o *Information Technology Modernization Fund* (Fundo de Modernização da Tecnologia da Informação - ITMF), para aposentar os sistemas de TI antiquados do Governo e fazer a transição para sistemas modernos de TI mais seguros e eficientes, financiamento para otimizar a

> governança e proteger as redes federais e investimentos fortalecer a força de trabalho em segurança cibernética e a educação em segurança cibernética em toda a sociedade. (ESTADOS UNIDOS, 2009b, tradução nossa)[54]

3.3 RELAÇÕES IDENTIFICADAS E PERSPECTIVAS FUTURAS

Ao analisar os documentos emitidos pelo governo norte-americano apresentados neste trabalho a partir da metodologia apresentado por Souza Júnior e Streit (2017), baseados em Godoy (1995), e visando-se fazer uma comparação preliminar, é possível chegar à conclusão que o Governo Bush se dedicou mais em fortalecer a parceria público-privada nas questões envolvendo o ciberespaço em relação ao Governo Obama. Porém, quando analisado mais profundamente o conteúdo apresentado por cada um dos documentos, bem como os contextos de cada um dos mandatos dos dois presidentes, percebe-se que houve um indício maior de interesse apresentado por parte do Governo liderado por Barack Obama. A conclusão que se chega numericamente, vantajosa para o Governo Bush, se dá pela análise da quantidade de menções a determinados temas ou palavras. Para fazer essa análise, procuramos identificar a quantidade de vezes que os termos "*private sector*" e "*public-private*" foram citados em cada um dos documentos analisados. Essas expressões não precisavam estar diretamente relacionadas - como termos - a palavras como "cibersegurança", "ciberespaço" ou "ciberdefesa", pois os documentos analisados já trabalhavam nesse escopo específico, sendo válido registrarmos a menção isolada aos termos selecionados.

Comparativamente, conforme podemos verificar pelos dados apresentados na Tabela 1, o Governo Bush busca, em meio a sua preocupação em garantir a cibersegurança, combater o ciberterrorismo e diminuir as ameaças existentes no ciberespaço para os norte-americanos, mencionando o setor privado 135 vezes ao longo dos documentos, enquanto o Governo Obama menciona apenas 88 vezes. No

---

[54] *"In particular, this funding will support the Cybersecurity National Action Plan, which takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. [...] As outlined above, the Budget provides $19 billion in resources for cybersecurity. This includes the creation of a new $3.1 billion revolving fund, the Information Technology Modernization Fund (*ITMF*), to retire the Government's antiquated IT systems and transition to more secure and efficient modern IT systems, funding to streamline governance and secure Federal networks, and investments to strengthen the cybersecurity workforce and cybersecurity education across society."* (ESTADOS UNIDOS, 2009b)

entanto, cabe destacar que um dos documentos analisados no estudo, referentes ao Governo Obama, trata de uma Estratégia Internacional e que o fato do setor privado ser citado 20 vezes ao longo do documento – ainda que seja o menor número apresentado na análise – já é um número relevante por se tratar de um documento voltado a mostrar a posição do país em relação aos demais Estados. Neste caso, as 20 menções ao setor privado, se mostram destacáveis por fazerem parte da Estratégia Internacional do país, recebendo um destaque ímpar à necessidade da ação conjunta ao setor privado.

Tabela 1 - Quantidade de vezes que o termo "*private sector*" é citado nos documentos selecionados do Governo norte-americano, entre 2003 e 2011

Título do Documento	Ano	Presidente	Número de menções a "*private sector*"
The National Strategy to Secure Cyberspace	2003	George W. Bush	82
Federal Plan for Cyber Security and Information Research and Development	2006	George W. Bush	53
Cyber Police Review: Assuring a Trusted and Resilient Information and Communication Infrastructure	2009	Barack Obama	68
International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World.	2011	Barack Obama	20

Fonte: Dados da Pesquisa (2019).

Também se mostrou fundamental observar a utilização do termo "*public-private*" nos documentos, expressão que é apresentada principalmente atrelada ao significado da parceria em si entre os dois setores mencionados no termo. Novamente, o Governo Bush possui uma maior quantidade de menções no comparativo total entre os dois presidentes, conforme é possível verificar na Tabela 2, obtendo-se a proporção de 29 x 16 menções à parceria público-privada, diretamente. Numericamente, ainda buscou-se verificar qual governo teria mencionado mais vezes as empresas e indústrias em seus documentos, supondo-se que, talvez, a discrepância entre as menções se desse por causa da escolha do termo. No entanto, a investigação apresentou um resultado que corrobora com os dados identificados anteriormente. Quando feita a contagem das aparições dos termos "*enterprise*" e "*industry*" a diferença fica ainda maior: Governo Bush conta com 191 menções contra 60 nos documentos analisados emitidos pelo Governo Obama.

Tabela 2 - Quantidade de vezes que o termo "*public-private*" é citado nos documentos selecionados do Governo norte-americano, entre 2003 e 2011

Título do Documento	Ano	Presidente	Número de menções a "*public-private*"
The National Strategy to Secure Cyberspace	2003	George W. Bush	28
Federal Plan for Cyber Security and Information Research and Development	2006	George W. Bush	1
Cyber Police Review: Assuring a Trusted and Resilient Information and Communication Infrastructure	2009	Barack Obama	14
International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World.	2011	Barack Obama	2

Fonte: Dados da Pesquisa (2019).

No entanto, é possível analisar a partir do conteúdo, que engloba as menções nos documentos e preocupações demonstradas pelo Governo Obama, que as questões apresentadas sobre a parceria público privada entre 2009 e 2017 se estabelecem de uma forma mais palpável e mais propensa a ações, enquanto o que o Governo Bush expõe sobre a parceria, é exposto de modo mais abstrato e tem um sentido de chamamento para a parceria, sem grande planejamento. Especialistas defendem que essa postura identificada na conduta do Governo Bush – de intencionar destacar a parceria público-privada, pois era relevante, mas sem necessariamente expor nos documentos os meios para isso –, é compreensível, visto que a parceria nasce mais de uma urgência frente aos desafios e ameaças apresentados no ciberespaço. Desde este surgimento, não para de se desenvolver e expandir até hoje, exigindo respostas sempre novas e mais tecnológicas aos ataques desferidos contra os norte-americanos. Ao invés de partir de um planejamento e análise sistemática das necessidades dos desafios enfrentados na cibersegurança, a parceria é forjada sobre a pressão de responder o mais rápido possível aos problemas apresentados no momento (THOMAS, 2013).

É possível analisar também a questão de que, em cerca de 16 anos, a realidade do ciberespaço mudou grandiosamente, transformando-se em palco central do sistema internacional e parte vital do cotidiano da grande maioria dos indivíduos, empresas e governos. Dessa forma, é natural identificar-se que as estratégias do Estado pioneiro nas ações para essa área se encontrem mais

trabalhadas e desenvolvidas no governo mais recente revisado neste trabalho. A evolução, nesse caso, é lógica e a necessidade do crescimento da parceria público-privada nesse contexto também se apresenta, seguindo a mesma linha de raciocínio. A tendência é que cada vez mais as infraestruturas críticas norte-americanas concentrem-se em poder do setor privado de maneira completa, sendo preciso o estreitamento de laços entre Governo-empresas. O fomento da parceria apresenta crescimento de um governo para outro, porém a principal crítica de Harknett e Stever (2011) em relação aos governos é que, em primeiro lugar, Obama prometeu reverter a situação que encontrou quando assumiu a presidência, saindo do campo teórico e investindo mais diretamente na parceria, mas o que aconteceu foi a continuidade do que Bush vinha fazendo nos anos anteriores. Esta abordagem não era necessariamente ruim, porém não trazia grandes avanços a nível mais estratégico e de planos de ação, como se esperava. Em segundo lugar, os autores trazem uma crítica muito comum aos pesquisadores da área: ambos governos não tomaram grandes decisões práticas, no final das contas, porque acreditavam que a parceria deveria se desenvolver de forma voluntária, visto que era do interesse coletivo a segurança cibernética do país. Essa prerrogativa é falha na questão de que não necessariamente os objetivos e interesses das empresas privadas seriam os mesmos dos respectivos governos.

Verifica-se uma falta de ação e engajamento por parte do Congresso e de agências do governo especializadas, ao longo de todo o período, em formar uma estrutura de governança mais adequada, mas o pior problema identificado em toda a análise foi a falta de acordo e consenso entre as partes envolvidas na parceria. Não foi possível localizar uma delimitação bem distribuída quanto aos deveres e direitos envolvidos na parceria, não havendo um norte-comum alinhado (THOMAS, 2013; CARR, 2016; HARKNETT; STEVER, 2011). Observa-se uma falta de garantias e incentivos para o setor privado perceber que a parceria poderia ser benéfica para ele também e, assim, buscar fomentá-la em conjunto com as ações que o governo empreendia. Carr (2016) critica severamente o Governo Obama, principalmente, pois quase ao final do mandato do presidente, estando em seu sexto ano à frente dos Estados Unidos, ainda não haviam sido resolvidos problemas identificados desde o Governo de Bill Clinton. Quinze anos depois, ainda não se tinham explicitado os parâmetros, extensão e natureza da relação/parceria entre o setor privado e o setor público. O autor argumenta, também, que parte dessa

incongruência na relação vinha do fato de haver conflito de interesses e o setor privado sentir que havia uma hierarquia na parceria - o que faria com que perdesse sentido inclusive chamá-la de “parceria”. Carr (2016) sugere que se passe a utilizar o termo “relação” neste contexto, pois se adequaria melhor à realidade. Além disso, as empresas não se motivam tanto a se engajar na parceria por sofrerem muita regulação de suas ações por parte do governo (CARR, 2016), o que, supostamente, limita seus horizontes e, deste modo, faz com que se afastem da parceria por medo de não conseguirem se desenvolver da maneira como planejavam.

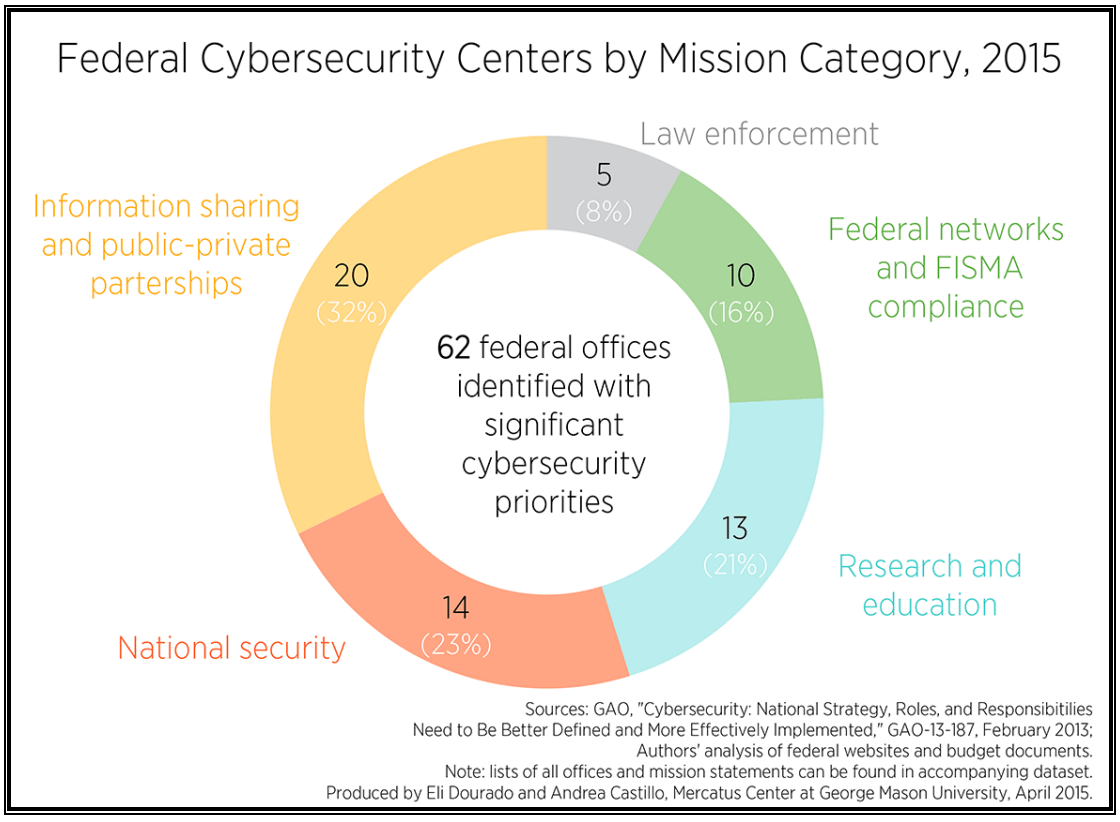
Gordon et al (2015), compartilham do argumento de Carr (2016) indicando a falta de um ponto de ligação, um propósito em comum, entre o setor público e privado, visto que estes ainda não identificam como ameaça os mesmos perigos que o governo constata. Além disso, não é do interesse das empresas privadas se responsabilizar pela Segurança Nacional sem terem a garantia de que seus interesses serão alcançados ou que receberam alguma recompensa em troca. O custo de investimento em ferramentas de proteção e segurança no ciberespaço, para o setor privado, por vezes não compensa e por isso se identifica um baixo nível de investimento em atividades de cibersegurança por parte desse setor. No entanto, Gordon et al (2015) defendem que os governos norte-americanos – mas principalmente o Governo em vigor quando da publicação do seu trabalho – já tomaram e estão tomando diversas ações que alcançaram ou têm grande potencial de alcançarem bons resultados. Tais ações aumentam a visão de valor na parceria e na cibersegurança, abrindo o horizonte das empresas ao investimento nessa área crítica para a segurança dos Estados Unidos.

Outra evolução identificada no Governo Obama, em relação ao Governo Bush, foi a importância dada à transparência, visível na reformulação do CNCI, visto que no governo anterior suas iniciativas eram mantidas como confidenciais. Neste mandato, entretanto, passam a ser de conhecimento público, para que, assim, os atores envolvidos e interessados possam fazer o papel de fiscalizadores do Estado, engajando as diversas camadas da sociedade na busca por maior segurança no ciberespaço. Além disso, a estratégia do Governo Obama, conforme era seu plano, passa a ser mais ampla, abrangente e atualizada, mostrando-se mais coerente com a realidade apresentada (RIBEIRO; RIVERA, 2014). Uma ação coordenada pelo Governo Obama, destacável por seus efeitos positivos para melhoria e crescimento da parceria público-privada, foi inserir o NIST como parceiro no empreendimento por

sedimentar um modelo de cibersegurança que englobe as realidades do governo e do setor privado. Souza Júnior e Streit (2017) elogiam o fato de que, a partir da inserção do NIST nos assuntos de cibersegurança, passou-se a se considerar os riscos presentes no ciberespaço na gestão de riscos do negócio, dando um passo a frente para a melhor estruturação da área como um todo e também na parceria público-privada, visto que o modelo abrange ambos setores.

Ainda assim, duas críticas relevantes são feitas ao Governo Obama, ao finalizar a análise da evolução da parceria público-privada no âmbito da cibersegurança. A primeira delas fala sobre o inchaço existente de centros, agências e departamentos de uma maneira geral, para lidar com o ciberespaço e cibersegurança norte-americana, e especialmente na questão do fomento e desenvolvimento de melhor compartilhamento de informação do setor público com o setor privado. De acordo com a pesquisa feita por Dourado e O'Sullivan (2015), os escritórios federais ocupados com a questão do compartilhamento de informações governo-empresa equivaliam, em 2015, a 32% do total de 62 escritórios com prioridades voltadas à cibersegurança, conforme podemos ver na Figura 1.

Figura 1 – Gráfico dos Centros de Cibersegurança Federais Norte-Americanos por categoria de missão em 2015



Fonte: DOURADO; O'SULLIVAN, 2015.

De um lado, o aumento das agências e escritórios envolvidos com o ciberespaço, bem como as *Executive Orders* que incentivam um maior envolvimento do setor privado no tema e a criação de um órgão para coordenar o compartilhamento de informações, o *Cyber Threat Intelligence Integration Center* (CTIIC - Centro de Integração de Inteligência de Ameaça Ciber) é bom pois acaba resultando no incentivo que falta para o setor privado se engajar na parceria. No entanto, esse inchaço nos órgãos do governo para lidar com o tema também tem seu viés negativo, pois descentralizam a maioria das ações e, ao invés de aumentar o compartilhamento de informações, as áreas ficam mais separadas e distantes. Existe, assim, grande possibilidade de se estar fazendo trabalho redobrado ou sendo necessário um auxílio que outro escritório ou agência poderia oferecer, mas não se tem conhecimento da capacidade dos demais, por cada um ser independente, respondendo nem sempre para o mesmo líder final.

A outra crítica, é menos uma acusação e mais uma recomendação, feita por Gordon et al (2015), de que o Governo Obama, à época – mas de uma maneira geral, qualquer governo de qualquer país deveria acatar a ideia –, deveria desenvolver uma base de dados nacional que monitorasse os investimentos em cibersegurança feitos pelo setor privado. Esse monitoramento já serviria como incentivo para as empresas se motivarem a investir mais em atividades relativas a cibersegurança e boas práticas no ciberespaço (GORDON et al, 2015).

Por fim, ainda que se tenham diversas visões sobre o desenvolvimento e a eficácia da parceria público-privada, Kremer e Müller (2014) defendem que a cooperação foi e continua sendo necessária. A parceria público-privada é vital para ambos os setores, que não teriam capacidade nem competência suficiente para vencer sozinhos as ameaças presentes no ciberespaço, que cada dia ficam mais complexas e onerosas de combater. Verificamos, por isso, uma evolução quanto a atenção dada ao assunto por parte do governo norte-americano ao longo das duas primeiras décadas do século XXI – e inclusive antes da virada do século –, pois abrir mão de manter a parceria seria como desinteressar-se em defender uma parte de seu território, colocando essa visão em um nível de ciberespaço. Essa evolução tende a manter-se, fortificando cada vez mais os laços entre os setores, no mandato corrente de Trump – governo que sucede o de Obama e ainda está em vigência – e nos governos subsequentes.

4 CONCLUSÃO

A partir dos dados e análises realizados neste trabalho, verificou-se a contínua evolução do ciberespaço como ambiente de ampla comunicação e desenvolvimento de novas tecnologias, bem como a necessidade da academia em atualizar-se, dedicando-se mais ao estudo e aprofundamento das relações que ocorrem a nível internacional neste espaço. A investigação mostrou que existe um movimento de tentativa de enquadramento da realidade do ciberespaço e das necessidades de cibersegurança às teorias clássicas e tradicionais das Relações Internacionais. Estas correntes teóricas, porém, não conseguem abarcar todas as peculiaridades e situações diferenciadas do ciberespaço além de não suprirem as demandas únicas que surgem neste ambiente – como a interação entre atores de diferentes níveis, a ausência de fronteiras, a identificação e responsabilização dos ataques proferidos neste ambiente, etc. Também observou-se as tentativas de Kremer e Müller (2014) em formularem um arcabouço teórico específico para a área de estudo, mas o trabalho dos autores ainda sofre com a presença de algumas lacunas e incoerências que não foram solucionadas, até o momento, por aqueles que se dedicam em empreender pesquisas no campo.

Ao aprofundar-se no recorte mais específico, objeto central da pesquisa à qual dedicou-se esse trabalho, da formação de estratégia para o ciberespaço e a relevância da parceria público-privada, identificou-se e comprovou-se o pioneirismo e liderança do governo dos Estados Unidos no tema desde o advento da Internet no século XX até os dias atuais (HARKNETT; STEVER, 2011; RIBEIRO; RIVERA, 2014; CARR, 2016). Além disso, validou-se a relevância de estudar a parceria público-privada dentro do espectro do ciberespaço, ao identificar-se que a parceria entre esses dois setores se mostra fundamental na construção da estratégia de cibersegurança dos Estados Unidos. Esta conclusão é possível a partir do reconhecimento de que a maioria das infraestruturas críticas do país se encontram em poder de representantes do setor privado, criando um laço de interesses comuns em garantir a segurança, também no ciberespaço, desses recursos fundamentais à nação (ESTADOS UNIDOS, 2003).

A análise quantitativa dos documentos e posicionamentos dos Governo Bush (2001-2009) e Governo Obama (2009-2017) quanto a parceria público-privada nas suas estratégias para a cibersegurança apresentou um resultado diferente dos

esperados inicialmente. Identificou-se que os termos *public-private* e *private-sector* são citados mais vezes nos documentos referentes às estratégias e planos para a cibersegurança emitidos pelo Governo Bush do que do Governo Obama. Esperava-se que, num crescente de amadurecimento da parceria e identificação mais consciente e organizada da indispensabilidade do contato e trabalho conjunto dos setores, o número de menções em documentos relativos ao tema crescesse ao longo do período analisado, mas esta não é a realidade verificada. No entanto, ao empreender-se a análise de conteúdo dos textos governamentais, é possível perceber que acontece, de fato, uma evolução na parceria, sendo esta mais valorizada com o passar dos anos e, também, um pouco mais organizada por parte do governo. Ainda que se tenha a impressão de que essas informações são incoerentes, a análise do contexto na qual os governos estão inseridos ajuda a entender o porquê do Governo Bush mencionar mais vezes a parceria público-privada do que o Governo Obama.

O Governo Bush tinha um interesse principal em sua estratégia e doutrina: a contenção e combate ao terrorismo. Na intenção de garantir a segurança das infraestruturas críticas e, por conseguinte, da Segurança Nacional do país frente à essa ameaça que também lidera ações via Internet – o ciberterrorismo –, o Governo Bush lança mão de todas as cartas que tinha disponíveis no momento para defender o país. Dessa forma, emprega um grande esforço em mostrar o valor da parceria com o setor privado, que – em teoria – não necessitaria de tanto investimento direto do governo para desenvolver tecnologias e trabalhar em garantir a cibersegurança de suas empresas. Esta é a estratégia utilizada pelo governo para incentivar o setor privado a se envolver na cibersegurança do país de forma mais pró-ativa e independente. No entanto, percebe-se que a parceria não se desenvolve, ao longo do período analisado, da maneira como o Governo Bush esperava. Houve envolvimento por parte do setor privado na parceria, porém, sem altas somas de investimento direto por parte do governo, as empresas privadas não se aprofundaram tanto na relação, vendo a mesma como acessória na sua formulação de política interna de cibersegurança. A falta de alinhamento de interesses e objetivos entre os setores para a parceria dificultou o desenvolvimento da mesma, visto que nem sempre os participantes se identificavam entre si e nem delimitavam um norte comum, o que acabava por causar um desinteresse das partes em consolidar uma parceria forte para alcançar a cibersegurança da nação.

De outro lado, o Governo Obama se mostrou, desde o princípio, mais interessado em ser transparente e agir em conjunto com seus potenciais parceiros, buscando alinhar as expectativas e objetivos das parcerias nas quais o governo tomava parte. Demonstrou essa decisão, logo no início do mandato, com a revisão da CNCI, consultando diversos níveis da sociedade, reforçando a atenção que o Governo pretendia dar às demandas dos indivíduos, empresas e organizações que atuam no país para o ciberespaço e cibersegurança. Quanto à parceria público-privada, percebeu-se uma maior dedicação e interesse do Governo Obama que, na expectativa de criar um laço forte entre os setores, deu destaque para a parceria e utilizando-a inclusive como exemplo no documento da sua estratégia de cibersegurança internacional. No entanto, verifica-se que o Governo Obama acabou por manter uma continuidade em relação a Bush. Houve, de fato, um crescimento e melhoria na parceria, porém sem que grandes mudanças ocorressem na maneira de gerir e pensar a parceria. Faltou ao Governo Obama ser mais inovador e diferenciado na busca de formalização e estabelecimento de objetivos comuns para assim fortalecer a mobilização do setor privado. Um fator que explica essa ausência de prioridade dedicada à parceria público-privada no âmbito da cibersegurança ao longo do Governo Obama foi a mudança das pautas urgentes enfrentadas pelo governo. A ameaça do ciberterrorismo continuava a pairar sobre o país e a preocupação em garantir a segurança das infraestruturas críticas tem caráter permanente na agenda norte-americana, no entanto surgiram novas pautas referentes ao ciberespaço, como transparência e privacidade, o que levou o governo a dedicar-se mais às relações diretas com os indivíduos, focando em aumentar a confiança dos mesmos no Estado. Porém, essa escolha acabou por deixar as empresas privadas – e a própria parceria público-privada – em um segundo plano nas prioridades do governo, sendo levada de uma forma mais voluntária e menos organizada do que seria esperado.

Verificou-se ao final das análises que a principal lacuna no desenvolvimento da parceria público-privada nos Estados Unidos deve-se em grande parte à pouca liderança empreendida pelos governos na organização e fomento da parceria. Esta realidade é preocupante, uma vez que o governo é o maior interessado na cooperação, que deveria ser prioridade de todos os mandatos norte-americanos do século XX. Ao fim da análise, chega-se à conclusão de que, para que a parceria se desenvolvesse a ponto de suprir todas as deficiências encontradas na comunicação

e compartilhamento de tecnologias entre os setores público e privado, seria necessária uma ruptura com a estratégia adotada pelo Governo Bush. Apesar de prometer essa mudança, o Governo Obama não a empreendeu por completo, como foi comentado anteriormente. Neste trabalho, a análise não pretendia abarcar os avanços da parceria no Governo Trump (2017-atual) pela falta do devido distanciamento temporal necessário para aprofundar esse tipo de análise. Ainda assim, o recorte adotado neste trabalho se mostrou próximo, fato observado ao deparar-se com uma certa limitação de acesso a dados mais completos e consolidados sobre algumas ações do Governo Obama, encerrado há quase 3 anos.

Assim sendo, fica patente a necessidade de continuidade dos estudos sobre as estratégias de cibersegurança, de maneira a aprofundar as análises, a formulação e o entendimento de conceitos pertinentes à realidade única do ciberespaço. Através deste aprofundamento poder-se-á alcançar o estabelecimento de uma teoria de Relações Internacionais própria para o ciberespaço, adequada às suas realidades, peculiaridades e desafios. A construção deste conhecimento beneficiará não só a academia, mas também os Estados, empresas, organizações e indivíduos envolvidos no ciberespaço, propiciando que, dominando em profundidade o funcionamento e características de seu campo de atuação, possam gerir e administrar de forma mais assertiva neste ambiente suas ações, que englobam diferentes níveis de atores e complexas relações.

REFERÊNCIAS

ACÁCIO, Igor D. P.; LOPES, Gills. Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço? In: **ENCONTRO ANUAL DA ANPOCS**, 36., 2012, Águas de Lindóia. Anais eletrônicos. Caxambu: ANPOCS, 2012. Disponível em: https://anpocs.com/index.php/encontros/papers/36-encontro-anual-da-anpocs/gt-2/gt28-2/8169-seguranca-internacional-no-seculo-xxi-o-que-as-teorias-de-relacoes-internacionais-tem-a-falar-sobre-o-ciberespaco/file. Acesso em: 3 abr. 2019.

AUSTRALIA, *Australian Trade and Investment Commission* – AUSTRADE. ***Cyber security to the United States****: Trends and opportunities*. Sidney, 2019. Disponível em: https://www.austrade.gov.au/australian/export/export-markets/countries/united-states-of-america/industries/cyber-security-to-the-united-states. Acesso em: 17 out. 2019.

BARDIN, Laurence. **Análise de Conteúdo.** Lisboa: Edições 70, 1977. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4295794/mod_resource/content/1/BARDlN%2C%20L.%20%281977%29.%20An%C3%A1lise%20de%20conte%C3%BAdo.%20Lisboa_%20edi%C3%A7%C3%B5es%2C%2070%2C%20225..pdf. Acesso em 15 maio 2019.

BELOW, Katharina C. *The Utility of Timeless Thoughts: Hannah Arendt's Conceptions of Power and Violence in the Age of Cyberization*. In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). ***Cyberspace and International Relations:*** *Theory, Prospects and Challenges*. Londres: Springer, 2014. Cap. 6. p. 95-114.

BRYANT, William D. ***International conflict and cyberspace superiority:*** *theory and practice*. London ; New York: Routledge, Taylor & Francis Group, 2016.

CARR, Madeline*. Public-private partnerships in national cyber-security strategies.* ***International Affairs***, [s.l.], v. 92, n. 1, p. 43-62. Oxford: Oxford University Press (OUP), jan. 2016. http://dx.doi.org/10.1111/1468-2346.12504. Disponível em: https://academic.oup.com/ia/article/92/1/43/2199930 Acesso em: 20 abr. 2019.

CAVALCANTI, Elmano P. Revolução Tecnológica: algumas reflexões. **Caderno de Pesquisas em Administração**, São Paulo: V.1, no. 1, 2º. Sem 1995. Disponível em: http://www.ancibe.com.br/artigos%20de%20si/artigo%20-%20Revolu%C3%A7%C3%A3o%20da%20informa%C3%A7%C3%A3o%20-%20algumas%20reflex%C3%B5es.pdf. Acesso em: 15 out. 2019.

CEPIK, M. A. C.; CANABARRO, D. R.; BORNE, T. A Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica. In: SOUZA, A. M.; NASSER, R. M.; MORAES, R. F. (Org.). **Do 11 de Setembro de 2001 à Guerra ao Terror**: reflexões sobre o terrorismo no século XXI. 1ed. Brasília DF: IPEA, 2014, cap. 7, p. 161-186. Disponível em: http://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/livro_11%20de%20setembro_web.pdf. Acesso em: 17 set. 2019.

CHOO, Kim-kwang R*. The cyber threat landscape: challenges and future research directions*. ***Computers & Security***, v. 30, n. 8, p.719-731, nov. 2011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404811001040. Acesso em: 29 mar. 2019.

CROSS-FERTILIZATION. ***Merriam-Webster on line Dictionary*** 2019. Disponível em: https://www.merriam-webster.com/dictionary/cross-fertilization. Acesso em: 21 out. 2019.

DOURADO, Eli; O'SULLIVAN, Andrea. *Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination*. **Mercatus Center at George Mason University**. Arlington-VA: Mercatus Center, 2015. Disponível em: https://www.mercatus.org/publications/technology-and-innovation/dozens-federal-cybersecurity-offices-duplicate-efforts-poor. Acesso em: 16 out. 2019.

ELETRONIC FRONTIER FOUNDATION – EFF. ***PATRIOT Act.*** [2002?] data provável. Disponível em: https://www.eff.org/pt-br/issues/patriot-act. Acesso: 16 out. 2019.

ESCRIVÁ DE BALAGUER, Josemaría. **Caminho**. São Paulo: Quadrante, 2016.

ESTADOS UNIDOS DA AMÉRICA. *Cyber Security and Information Assurance Intergagency Working Group; Networking and Information Technology Research and Development Subcommittee.* ***Federal Plan for Cyber Security and Information Research and Development:*** *Report by the Interagency Working Group on Cyber Security and Information Assurance*. Washington DC, 2006. Disponível em: https://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf. Acesso em: 20 maio. 2019.

ESTADOS UNIDOS DA AMÉRICA. ***Cyberspace Policy Review****: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington DC, Maio 2009a. Disponível em: https://fas.org/irp/eprint/cyber-review.pdf. Acesso em: 25 abr. 2019.

ESTADOS UNIDOS DA AMÉRICA. *Office of Homeland Security.* ***National Strategy for Homeland Security***. 2002. Disponível em: https://www.dhs.gov/sites/default/files/publications/ nat-strat-hls-2002.pdf. Acesso em: 09 abr. 2019.

ESTADOS UNIDOS DA AMÉRICA. *Office of Management and Budget.* ***Budget of the US Government, Fiscal Year 2011***. Washington DC: U.S. Government Printing Office, 2010a. Disponível em: https://www.govinfo.gov/content/pkg/BUDGET-2011-BUD/pdf/BUDGET-2011-BUD.pdf. Acesso em: 16 out. 2019.

ESTADOS UNIDOS DA AMÉRICA. *Office of Management and Budget.* ***The President's Budget for Fiscal Year 2017.*** Washigton DC, Fev. 2016. Disponível em: https://obamawhitehouse.archives.gov/omb/budget. Acesso em:16 out. 2019.

ESTADOS UNIDOS DA AMÉRICA. *President's Comission on Critical Infrastructure Protection (*PCCIP*).* ***Overview Briefing***. Washington DC, Jun. 1997. Disponível em: https://www.hsdl.org/?view&did=487492. Acesso em: 16 out. 2019.

ESTADOS UNIDOS DA AMÉRICA. ***Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism****. Patriot Act, Public Law 107-56*. 26. out. 2001. Disponível em: https://www.sec.gov/about/ offices/ocie/aml/patriotact2001.pdf. Acesso em: 8 out. 2019.

ESTADOS UNIDOS DA AMÉRICA. *US Department of Homeland Security.* ***National Preparedness Report.*** Washington DC, 30. Mar. 2012. Disponível em: https://www.fema.gov/ media-library-data/ 20130726-1833-25045-2705/national _preparedness_report _20120330_v2_1.pdf. Acesso em: 15 out. 2019.

ESTADOS UNIDOS DA AMÉRICA*. White House Office****. Executive Order - Improving critical infrastructure cybersecurity***. Washington DC, 12 fev. 2013. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/ executive-order-improving-critical-infrastructure-cybersecurity. Acesso em: 20 maio 2019.

ESTADOS UNIDOS DA AMÉRICA. *White House Office.* ***International Strategy for Cyberspace****: Prosperity, Security, and Openness in a Networked World*. Washington DC, maio 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/ files/rss_viewer/ international_strategy_for_cyberspace.pdf. Acesso em: 20 maio 2019.

ESTADOS UNIDOS DA AMÉRICA*. White House Office.* ***National Security Strategy for a New Century.*** Washington DC, dez. 1999. Disponível em: https://www.hsdl.org/ ?abstract& did=487539. Acesso em: 7 set. 2019.

ESTADOS UNIDOS DA AMÉRICA. *White House Office.* ***Remarks by the President on Securing Our Nation's Cyber Infrastructure*****.** Washington DC, 29 maio 2009b. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure. Acesso em: 10 jun. 2019.

ESTADOS UNIDOS DA AMÉRICA. *White House Office.* ***The Comprehensive National Cybersecurity Initiative (*****CNCI*****)****.* Washington DC: 2. mar. 2010b https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf. Acesso em: 10 jun. 2019.

ESTADOS UNIDOS DA AMÉRICA*. White House Office.* ***The National Strategy to Secure Cyberspace****.* Washington DC, fev. 2003. Disponível em: https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf. Acesso em: 6 abr. 2019.

GODOY, Arilda S. Pesquisa qualitativa: tipos fundamentais. **RAE - Revista de Administração de Empresas**, [S.l.], v. 35, n. 3, p. 20-29, maio 1995. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rae/article/view/38200/36944. Acesso em: 06 abr. 2019.

GORDON, Lawrence A. et al. *Increasing Cybersecurity Investments in Private Sector Firms.* ***Journal of Cybersecurity***, 2015, v. 1, n° 1. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032551. Acesso em: 15 out. 2019.

HANSEN, Lene; NISSENBAUM, Helen. *Digital Disaster, Cyber Security and the Copenhagen School.* ***International Studies Quarterly***, v. 53, n. 4, p. 1155-1175. Oxford: Oxford University Press, 2009. Disponível em: https://doi.org/10.1111/j.1468-2478.2009.00573.x. Acesso em: 20 mar. 2019.

HARKNETT, Richard J.; STEVER, James A. *The New Policy World of Cybersecurity.* ***Public Administration Review***, [s.l.], v. 71, n. 3, p. 455-460, maio 2011. Disponível em: http://dx.doi.org/10.1111/j.1540-6210.2011.02366.x. Acesso em: 20 abr. 2019.

JENTLESON, Bruce W. ***American Foreign Policy****: The Dynamics of Choice in the 21st Century.* 5. ed. Nova Iorque: Norton & Company, 2014.

KREMER, Jan-Frederik; MÜLLER, Benedikt. *SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World*. In: KREMER, Jan-frederik; MÜLLER, Benedikt (Ed.). ***Cyberspace and International Relations:*** *Theory, Prospects and Challenges.* Londres: Springer, 2014. Cap. 3. p. 41-58.

KUEHL, Daniel T. *From Cyberspace to Cyberpower: Defining the Problem*. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. ***Cyberpower and National Security****.* Washington DC: National Defense University Press (NDUP), 2009. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210. Acesso em: 20 ago. 2019.

LEMOS, Robert. ***Bush unveils final cybersecurity plan***. 2003. Disponível em: https://www.cnet.com/news/bush-unveils-final-cybersecurity-plan/. Acesso em: 16 out. 2019.

LEWIS, James A. ***Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.*** Washington, D.C: *Center For Strategic & International Studies*, 2002. 12 p. Disponível em: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf. Acesso em: 30 mar. 2019.

LOBATO, Luísa C.; KENKEL, Kai M. *Discourses of cyberspace securitization in Brazil and in the United States*. **Revista Brasileira de Política Internacional**, Brasília, v. 58, n. 2, p. 23-43, dez. 2015. Disponível em: http://www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf. Acesso em: 06 abr. 2019.

LUCERO, Everton. **Governança da Internet**: aspectos da formação de um regime global e oportunidade para ação diplomática. Brasília: Fundação Alexandre Gusmão (FUNAG), 2011. 236 p. Disponível em: http://funag.gov.br/biblioteca/download/822-Governanca_da_Internet.pdf. Acesso em: 20 set. 2019.

MAIS DA METADE da população mundial usa internet, aponta ONU: Até o final de 2018, 51,2% da população mundial estará usando a internet. **G1,** 07 dez. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2018/12/07/mais-da-metade-da-populacao-mundial-usa-internet-aponta-onu.ghtml. Acesso em: 15 ago. 2019.

McCARTHY, Daniel R. *Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order.* ***Politics And Governance***, Lisbon, v. 6, n. 2, p.5-12, 11 jun. 2018. Cogitatio. Disponível em: https://www.cogitatiopress.com/politicsandgovernance/article/view/1335. Acesso em: 19 abr. 2019.

MORAIS NETO, Arnaldo S. **Cibercrime e cooperação penal internacional:** um enfoque à luz da Convenção de Budapeste. 2009. Dissertação (Mestrado) – Programa de Pós-Graduação em Ciências Jurídicas, Universidade Federal da Paraíba UFPB/PPCJ, João Pessoa, 2009. Disponível em: http://www.egov.ufsc.br/ portal/ conteudo/cibercrime-e-coopera%C3%A7%C3%A3o-penal-internacional-um-enfoque-%C3%A0-luz-da-conven%C3%A7%C3%A3o-de-budapeste. Acesso em 25 out.2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. ***Framework for Improving Critical Infrastructure Cybersecurity***. Gaithersburg MD: 12 fev. 2014. Disponível em: https://www.nist.gov/sites/default/files/documents/ cyberframework/cybersecurity-framework-021214.pdf. Acesso em: 20 out. 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. ***About NIST***. 2019a. Disponível em: https://www.nist.gov/about-nist. Acesso em: 20 out. 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. ***Cibersecurity***. 2019b. Disponível em: https://www.nist.gov/topics/cybersecurity. Acesso em: 20 out. 2019.

NYE, Joseph S. Jr., ***Cyberpower***. Cambridge: Harvard Kennedy School, maio 2010. Disponível em: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. Acesso em: 2 abr. 2019.

NYE, Joseph S. Jr., ***The future of power***. 1. ed. New York: PublicAffairs, 2011.

O'CONNELL, Mary E. *Cyber Security without Cyber War.* ***Journal Of Conflict And Security Law***, Oxford, v. 17, n. 2, p.187-209, 1 jul. 2012. Oxford University Press (OUP). Disponível em: https://www.law.upenn.edu/live/files/3474-oconnell-m-cyber-security-without-cyber-war-2012. Acesso em: 22 mar. 2019.

PANG, Min-Seok; TANRIVERDI, Hüseyin*.* ***Security Breaches in the U.S. Federal Government.*** 7 Mar. 2017. Fox School of Business Research Paper No. 17-017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933577. Acesso em: 20 out. 2019.

PORTELA, Lucas S. Agenda de Pesquisa sobre o Espaço Cibernético nas Relações Internacionais. **Revista Brasileira de Estudos de Defesa**, v. 3, n. 1, p.91-113, jun. 2016. Disponível em: https://rbed.abedef.org/rbed/article/viewFile/62071/37922. Acesso em: 03 jun. 2019.

REMOALDO, Pedro. **A história da Internet**. Porto: Abr. 1998. FEUP. Disponível em: https://paginas.fe.up.pt/~mgi97018/historia.html. Acesso em: 6 set. 2019.

RIBEIRO, Vinicius G.; RIVERA, César G. A inserção da segurança cibernética na agenda de segurança dos EUA no Século XXI. **Século XXI:** Revista de Relações Internacionais - ESPM/Sul, Porto Alegre, v. 5, n. 2, p.135-150, Jul-Dez 2014. Disponível em: http://seculoxxi.espm.br/index.php/xxi/article/view/79/81. Acesso em: 20 mar. 2019.

ROLLINS, John; HENNING, Anna C*. The Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.* ***Congressional Research Service***. Washington DC, 10 mar. 2009. Disponível em: https://fas.org/sgp/crs/natsec/R40427.pdf. Acesso em: 21 out. 2019.

SCHNEIER, Bruce. *Solutions for Government*. In: _____. ***DATA AND GOLIATH*****.** Nova Iorque: W. W. Norton & Company, 2015. Cap. 13. p. 167-189.

SHELDON, John B. *The rise of cyberpower*. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. ***Strategy in the Contemporary World****: An Introduction to Strategic Studies*. Oxford: Oxford University Press Print Publication, 2015. Disponível em: https://www.oxfordpoliticstrove.com/view/10.1093/hepl/9780198708919.001.0001/hepl-9780198708919-chapter-16. Acesso em: 7 ago. 2019.

SOUZA JUNIOR, Alcyon F.; STREIT, Rosalvo E. Segurança cibernética: política brasileira e a experiência internacional. **Revista do Serviço Público**, Brasília, v. 68, n. 1, p.107-130, mar. 2017. Disponível em: http://repositorio.enap.gov.br/bitstream/1/2952/1/RSP%20V.68%20N.1_artigo%20de%20107-130.pdf. Acesso em: 20 abr. 2019.

THOMAS, Rachel N. ***Securing Cyberspace Through Public-Private Partnership:*** *a comparative analysis of partnership models*. [s.l]: Center For Strategic & International Studies - CSIS, ago. 2013. 63 p. Disponível em: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130819_tech_summary.pdf. Acesso em: 19 abr. 2019.

TRANS-ATLANTIC BUSINESS COUNCIL – TABC. ***About TABD***. 2019 . Disponível em: http://transatlanticbusiness.org/tabd/. Acesso em: 15 out. 2019.

TURPEN, Elizabeth et al. ***Following the money:*** *the Bush administration FY03 budget request and current funding for selected Defense, State, and Energy Department Programs.* Report. Washington DC: Stimson Center, 24 abr. 2002. Disponível em: https://www.files.ethz.ch/isn/ 31134/FollowingtheMoney.pdf. Acesso em: 15 out. 2019.

WALTZ, Kenneth N. **Teoria das Relações Internacionais**. Lisboa: Gradiva, 2002.

WELLAUSEN, Saly S. Terrorismo e os atentados de 11 de setembro. **Tempo Social**, Rev. Sociol. USP, S. Paulo, 14(2), p. 83-112, outubro de 2002. Disponível em: http://www.scielo.br/pdf/ts/v14n2/v14n2a05.pdf. Acesso em: 15 out. 2019.

ZIMMER, Michael T. *The tensions of securing cyberspace: the Internet, state power & the National Strategy to Secure Cyberspace*. In: **First Monday**, vol. 9, no. 3, 1 mar. 2004. Disponível em: https://journals.uic.edu/ojs/index.php/fm/article/view/1125/1045. Acesso em: 15 out. 2019.