UNIVERSIDADE ESTADUAL PAULISTA "JULIO DE MESQUITA FILHO"
FACULDADE DE FILOSOFIA E CIÊNCIAS DE MARÍLIA
GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

ANA LUIZA DE CAMPOS BURSSED

AS SEMELHANÇAS E AS DIFERENÇAS NAS ABORDAGENS DAS ADMINISTRAÇÕES OBAMA (2009-2016) E TRUMP (2017-2020) NAS POLÍTICAS DE CIBERSEGURANÇA DOS ESTADOS UNIDOS

MARÍLIA
2021

ANA LUIZA DE CAMPOS BURSSED

AS SEMELHANÇAS E AS DIFERENÇAS NAS ABORDAGENS DAS ADMINISTRAÇÕES OBAMA (2009-2016) E TRUMP (2017-2020) NAS POLÍTICAS DE CIBERSEGURANÇA DOS ESTADOS UNIDOS

Trabalho de Conclusão de Curso apresentado para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Filosofia e Ciências (FFC), Universidade Estadual Paulista (UNESP), campus de Marília.

Orientador: Prof. Dr. Rodrigo Duarte Fernandes dos Passos

MARÍLIA
2021

B972s

Burssed, Ana Luiza de Campos

As semelhanças e as diferenças nas abordagens das administrações Obama (2009-2016) e Trump (2017-2020) nas políticas de cibersegurança dos Estados Unidos / Ana Luiza de Campos Burssed. -- Marília, 2022

Trabalho de conclusão de curso (Bacharelado - Relações Internacionais) - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, Marília

Orientador: Rodrigo Duarte Fernandes dos Passos

1. Relações Internacionais. 2. Cibersegurança. 3. Estados Unidos. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Filosofia e Ciências, Marília. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

ANA LUIZA DE CAMPOS BURSSED

AS SEMELHANÇAS E AS DIFERENÇAS NAS ABORDAGENS DAS ADMINISTRAÇÕES OBAMA (2009-2016) E TRUMP (2017-2020) NAS POLÍTICAS DE CIBERSEGURANÇA DOS ESTADOS UNIDOS

Trabalho de Conclusão de Curso apresentado para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Filosofia e Ciências (FFC), Universidade Estadual Paulista (UNESP), campus de Marília.

BANCA EXAMINADORA

_____

Prof. Dr. Rodrigo Duarte Fernandes dos Passos
Universidade Estadual Paulista "Julio de Mesquita Filho"
Faculdade de Filosofia e Ciências de Marília

_____

Raquel Torrecilha Spiri
Universidade Estadual Paulista "Julio de Mesquita Filho"
Faculdade de Filosofia e Ciências de Marília

_____

Friedrich Maier
Universidade Estadual Paulista "Julio de Mesquita Filho"
Faculdade de Filosofia e Ciências de Marília

Marília, 21 de fevereiro de 2022

AGRADECIMENTOS

Gostaria de agradecer aos meus pais, Rosana e Elcio, e ao meu irmão, André, que me apoiaram durante toda a minha jornada sempre me incentivando a correr atrás dos meus objetivos.

Agradeço as minhas amigas, Giovanna, Juliana, Lívia, Maria Carolina e Tamiris por toda alegria e apoio durante esses anos.

Agradeço ao meu orientador, o Professor Rodrigo Passos pela paciência e toda ajuda prestada, não só para esse trabalho, mas também ao longo de toda minha graduação.

Agradeço, por fim, a Deus por me dar forças para superar todos os obstáculos e colocar todas essas pessoas na minha vida.

RESUMO

O presente trabalho visa mostrar as diferenças e semelhanças entre as abordagens que o governo de Barack Obama (2009-2016) e o de Donald Trump (2017-2020) tiveram em relação a suas políticas cibernéticas. Para isso se utiliza a hipótese de Maier (2019) de que, apesar das diferenças, os dois governos tem o mesmo o propósito, ou seja, manter a condição hegemônica do país. A partir disso, o trabalho aborda os documentos da era Obama, *Cyberspace Policy Review* (2009), a Estratégia Internacional para o Ciberespaço (2011), o Plano Nacional de Ação de Cibersegurança (2016) e a criação do *USCYBERCOM*, além das consequências dos vazamentos feitos por Edward Snowden em 2013 para o governo. Para o governo de Trump são utilizados a Ordem Executiva 13800 e a Estratégia Cibernética Nacional, as ações do presidente para a proteção das redes militares, sua posição em relação à China e sua postura após a interferência russa nas eleições de 2016.

Palavras-chave: cibersegurança; ciberespaço; Estados Unidos da América; política interna; política externa; Barack Obama; Donald Trump.

ABSTRACT

The present work aims to show the differences and similarities between the approaches that the government of Barack Obama (2009-2016) and that of Donald Trump (2017-2020) had regarding their cyber policies. For this, Maier's hypothesis (2019) that, despite these differences, the two governments aim for the same purpose, that is, to maintain the hegemonic condition of the country, is used. In this manner, the work addresses the Obama era's documents Cyberspace Policy Review (2009), the International Strategy for Cyberspace (2011), the National Cybersecurity Action Plan (2016) and the creation of USCYBERCOM in addition to the consequences of the leaks made by Edward Snowden for the administration. For the Trump administration, it is analyzed the Executive Order 13800, the National Cyber Strategy, the president's actions to protect military networks and his position in relation to China in addition to his posture after the Russian interference in the 2016 elections.

Keywords: cyberspace; cybersecurity; United States; foreign policy; domestic policy; Barack Obama; Donald Trump.

LISTA DE TABELAS

Tabela 1 – Estratégia Internacional para o Ciberespaço: Áreas de Investimentos 38

Tabela 2 – Estratégia Cibernética Nacional: Ações do Governo Trump para Ciberespaço 54

LISTA DE SIGLAS

APEC – Cooperação Econômica Ásia-Pacífico

CI – Comunidade de Inteligência

CIA – Agência Nacional de Inteligência

CMSI – Cúpula Mundial sobre a Sociedade da Informação

CNAP – *Cybersecurity National Action Plan*

CNCI - *Comprehensive National Cybersecurity Initiative*

CNE – Exploração da Rede Computacional

CPR – *Cybersecurity Policy Review*

DCCC – Comitê de Campanha Parlamentar Democrata

DHS – Departamento de Segurança Interna dos Estados Unidos

DNC – Comitê Nacional Democrata

DNI – Diretor de Inteligência Nacional

DoD – Departamento de Defesa dos Estados Unidos

EO – Ordem Executiva

FBI – *Federal Bureau of Investigation*

FISA – *Foreign Intelligence Surveilance Act*

FISC – *Foreign Intelligence Surveilance Court*

FMI – Fundo Monetário Internacional

FSB – Serviço de Segurança Federal

GAO – *Government Accountability Office*

GCHG - Central de Comunicações do Governo Britânico

GRU – Departamento Central de Inteligência Russa

ICI-IPC – Comitê de Política Interagências de Infraestrutura de Informação e Comunicação

IRA – Agência de Pesquisa de Internet

NIST – Instituto Nacional de Padrões e Tecnologia

NSA – Agência de Segurança Nacional

NSC – Conselho de Segurança Nacional

ODNI – Gabinete do Diretor Nacional de Inteligência

OMB - Gabinete de Gestão e Orçamento

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

PPD – Diretiva de Decisão Presidencial

SIGINT – Inteligência de sinais

SSO – Operações de Fontes Especiais

TI – Tecnologia da Informação

USCYBERCOM – Comando Cibernético dos Estados Unidos

USSTRATCOM – Comando Estratégico dos Estados Unidos

SUMÁRIO

1. INTRODUÇÃO 10

2. GOVERNO OBAMA (2009-2016) 12

2.1 Cyberspace Policy Review 13

2.2 O Caso Edward Snowden 21

2.3 Principais inovações do Governo 31

3. GOVERNO TRUMP (2017-2020) 44

3.1 Eleições de 2016 44

3.2 Principais ações do Governo 51

4. CONSIDERAÇÕES FINAIS 61

APÊNDICE A - LINHA DO TEMPO GOVERNO OBAMA 64

APÊNDICE B - LINHA DO TEMPO GOVERNO TRUMP 65

REFERÊNCIAS BIBLIOGRÁFICAS 66

1. INTRODUÇÃO

O advento da internet trouxe uma gama de novidades e novos desafios para o mundo. Essa nova tecnologia mudou a forma como as pessoas se relacionam, trabalham e entendem a realidade. Com isso, novas categorias de problemas surgem como: cibercrimes, ciberguerras, questões de privacidade, entre outros.

A dependência que o mundo tem da internet cresceu de tal forma que, atualmente, grande parte dos países tem aspectos críticos de sua infraestrutura conectados à internet, redes militares, telecomunicações, energia, finanças, etc.. O ambiente anônimo e sem fronteiras que a internet proporciona deixou essa infraestrutura mais exposta e vulnerável a ataques e vazamentos de informações confidenciais, impactando diretamente na segurança nacional. Essa vulnerabilidade levou os países a criarem planos de segurança nacional para suas redes e sistemas de modo a proteger suas informações de possíveis ataques e, eventualmente, atacarem utilizando esse novo ambiente (HARKNETT; STEVER, 2011).

Esse movimento de securitização das redes criou o campo da cibersegurança, definida pela Agência de Segurança Cibernética e Infraestrutura dos Estados Unidos como "[...] a arte de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso e a garantir a confidencialidade, a integridade e a disponibilidade de informações." (CISA, 2019, tradução nossa). Esse campo visa abordar essas questões de um ponto de vista multidisciplinar e que ajude os países a desenvolver desde tecnologias até protocolos militares para lidar com o problema (MAIER, 2019).

Os Estados Unidos dependem da segurança das redes para o bom funcionamento de suas infraestruturas e tiveram um grande peso na criação de estruturas de defesa cibernética mundial. Desde a presidência de Bill Clinton a cibersegurança passa a ocupar um lugar cada vez mais importante na agenda política do país. Os departamentos de defesa, como o FBI, a CIA e o Departamento de Defesa do país criam divisões internas que lidem com a questão. A partir do governo de George W. Bush o país tem a criação de sua primeira estratégia para lidar com os problemas advindos do ciberespaço, a Estratégia Nacional para Securitizar o Ciberespaço (HARKNETT; STEVER, 2011).

Seguindo o governo de Bush, temos a presidência de Barack Obama que construiu suas políticas de cibersegurança tendo como base a estratégia desenvolvida por Bush. Mesmo trazendo uma nova perspectiva para o tema, Obama dá continuidade a diversas políticas criadas

por seu antecessor. Seu sucessor, Donald Trump, também, dá suas próprias contribuições para a área, porém mantém muitos aspectos de sua política permanecem os mesmos.

A partir dessas considerações, o presente trabalho pretende responder à seguinte questão: quais são as semelhanças e as diferenças entre a abordagem que o governo Obama e o governo Trump tiveram em relação a cibersegurança? Para isso, é utilizada a hipótese, levantada por Maier (2019), de que não há, entre as duas administrações uma mudança no objetivo dos Estados Unidos. Por mais que cada administração tenha utilizado meios diferentes na abordagem da temática, o propósito continua o mesmo, isto é, a perpetuação da condição hegemônica do país.

O trabalho está dividido em duas seções, uma para a administração de Barack Obama e uma para o governo de Donald Trump. Para o governo de Obama analisaremos os documentos *Cyberspace Policy Review*, a Estratégia Internacional para o Ciberespaço, o Plano Nacional de Ação de Cibersegurança e a criação do *USCYBERCOM*. O trabalho abordará, além desses documentos, o caso de Edward Snowden que trouxe à tona o poder cibernético americano. O caso em questão mudou a forma como o mundo protege seus dados e como regula suas políticas de compartilhamento. Para os Estados Unidos, o caso significou uma queda na confiança internacional no país e, especialmente, em Obama e seu discurso de multilateralismo.

Já para o governo Trump será abordado o caso da interferência russa nas eleições presidenciais de 2016 e a resposta que a administração deu ao acontecimento. Analisaremos, também, a Ordem Executiva 13800 e a Estratégia Cibernética Nacional, além das ações do presidente para a proteção das redes militares e sua posição em relação à China. Por fim, será realizada uma breve análise considerando as diferenças e as semelhanças entre as duas abordagens.

2. GOVERNO OBAMA (2009-2016)

George W. Bush deixou o governo dos Estados Unidos em meio à crise econômica de 2008 e com as consequências de duas guerras no Oriente Médio, resultado de sua política pós-11 de setembro. Consequentemente, quando Obama assume a presidência ele herda um cenário de instabilidade tanto no plano nacional quanto internacional. Isso fez com que as políticas adotadas por ele, no plano nacional, fossem pautadas pelo combate à crise e suas consequências e pelo investimento no crescimento do país. Já no plano internacional, o 44º presidente, além de enfrentar as consequências da crise econômica, enfrentou preocupações sobre a queda da hegemonia do país causada, entre outros fatores, pela ascensão da China. Sua atuação nesse sentido, foi de empregar muito mais esforços no campo da cooperação multilateral que seu antecessor para restaurar a capacidade de liderança do país. Mesmo com esses esforços, a atuação de Obama não pode ser vista, apenas, no campo do multilateralismo, houve momentos em que o governo agiu de forma unilateral, o que leva a caracterização de sua atuação como "pendular" (MAIER, 2019).

É possível acrescentar a esse cenário o aumento da dependência mundial da tecnologia e, consequentemente, a preocupação com a segurança das redes. Desde o início, o governo Obama já ressaltou a importância do ciberespaço e da segurança cibernética para o país. Seus objetivos incluíam prevenir ataques cibernéticos às redes governamentais e privadas. Além disso, pontos como a proteção da rede e da privacidade, o investimento na infraestrutura da rede, para torná-la mais complexa e segura, a obtenção de dados sobre ciberataques e a criação de planos de resposta para combater os ataques, foram os guias das políticas empreendidas pelo ex-presidente estadunidense (MAIER, 2019).

Isso posto, neste capítulo analisaremos essas políticas implementadas pelo governo de Barack Obama. O primeiro passo será a análise do documento *Cyberspace Policy Review*, que traz o molde que as políticas futuras deveriam seguir. Será examinado, também, as consequências das informações divulgadas por Edward Snowden na visão e na postura da administração para as políticas de segurança cibernética desenvolvidas após o ocorrido. Por fim, será apresentado as principais políticas e iniciativas de cibersegurança empregadas durante sua administração como, a Estratégia Internacional para o Ciberespaço, o Plano Nacional de Ação de Cibersegurança e o *USCYBERCOM*.

2.1 Cyberspace Policy Review

A primeira medida da administração Obama sobre segurança cibernética foi uma revisão da política do país sobre o tema. O documento, *Cyberspace Policy Review* (CPR), foi elaborado durante 60 dias, com pesquisas que consideraram a posição sobre a temática do setor privado; da academia; dos setores públicos; de parceiros internacionais; de setores da sociedade civil; e das esferas legislativa e executiva. Essa revisão teve como objetivo lançar as bases para uma nova abordagem do tema, propondo 24 medidas de curto, médio e longo prazo para fortalecer a infraestrutura cibernética do país. Foram apontadas diversas sugestões de como preparar o país para lidar com sua dependência cada vez maior do campo cibernético e os riscos a sua segurança e economia decorrentes disso (ESTADOS UNIDOS DA AMÉRICA, 2009).

Os principais pontos que a pesquisa trabalha são: a centralização da coordenação de políticas de cibersegurança; cooperação entre as agências do governo; cooperação público-privada e internacional; educação; e inovação no setor de pesquisa e desenvolvimento. As recomendações que foram apresentadas para cada um desses assuntos, deveriam, em sua maioria, ser organizadas na forma de iniciativas e políticas de cibersegurança. O documento ressalta que,

> A política de segurança cibernética, conforme usada neste documento, inclui estratégia, política e padrões relativos à segurança e às operações no ciberespaço e abrange toda a gama de redução de ameaças, redução de vulnerabilidade, dissuasão, envolvimento internacional, resposta a incidentes, resiliência e políticas e atividades de recuperação , incluindo operações de rede de computadores, garantia de informações, aplicação da lei, diplomacia, militares e missões de inteligência no que se refere à segurança e estabilidade da infraestrutura global de informações e comunicações. O escopo não inclui outras políticas de informação e comunicação não relacionadas à segurança nacional ou à proteção da infraestrutura. (ESTADOS UNIDOS DA AMÉRICA, 2009, p.2, tradução nossa)

Um dos principais pontos a serem trabalhados, de acordo com a pesquisa, é a maior coordenação entre as agências do país. Até o momento de sua publicação, Obama já havia criado o Comitê de Política Interagências de Infraestrutura de Informação e Comunicação (ICI-IPC, na sigla em inglês) composto por membros do Conselho de Segurança Nacional e pelo Conselho de Segurança Interna. O objetivo do comitê era ser o

> [...] principal órgão de coordenação de políticas para questões relacionadas à obtenção de informações globais garantidas, confiáveis, seguras e com capacidade de sobrevivência de infraestrutura de comunicações e informações

> e recursos relacionados. (ESTADOS UNIDOS DA AMÉRICA, 2009, p.7, tradução nossa)

O principal apontamento da pesquisa sobre essa questão, é que a cibersegurança é tratada por muitos departamentos governamentais dentro dos Estados Unidos. Em decorrência disso, nenhuma dessas divisões era unicamente responsável por coordenar atividades e políticas sobre o tema, mesmo com grande parte dos esforços serem feitos pelo Departamento de Segurança Interna (DHS, em inglês). Somado a isso, também, há o problema de que as mesmas agências que lidam com a segurança cibernética lidam, também, com outras questões de segurança, não dando ao tema a devida atenção (ESTADOS..., 2009; HARKNETT e STEVER, 2009).

Outro ponto a ser levado em consideração, é que, diferentes agências trabalham com o problema sob perspectivas diferentes. Com isso, foi proposto a centralização dos esforços na Casa Branca juntamente com uma maior cooperação entre o governo federal e os governos estaduais e locais para corrigir esses problemas e dar ao tema a devida atenção. É importante ressaltar que essas diferentes abordagens são resultado da forma que cada agência atende suas demandas e é importante que o governo leve isso em consideração ao concentrar os esforços. Sendo assim, o objetivo da centralização do tema é diminuir a burocracia e o tempo de resposta em casos de incidente, uma vez que haveria um responsável que se reportaria diretamente ao presidente. (ESTADOS..., 2009; HARKNETT e STEVER, 2009).

Para resolver o problema da falta de centralização, o documento propôs a criação de um cargo de Coordenador de Cibersegurança, que presidiria o ICI-IPC. Esse “Czar” da Cibersegurança, como foi apelidado pela mídia, participaria de discussões em diversos temas pertinentes, apresentando considerações sob a perspectiva da segurança cibernética e buscando harmonizar e coordenar políticas sobre o assunto. Com isso em mente, a primeira obrigação desse oficial seria preparar uma estratégia nacional de proteção da infraestrutura de comunicações e informações. Para tal, o oficial deveria levar em conta os sucessos e as falhas da *Comprehensive National Cybersecurity Initiative* (CNCI), criada no governo de Bush (ESTADOS..., 2009; HARKNETT e STEVER, 2009).

O cargo foi criado pela administração Obama sete meses após a publicação da pesquisa. Isso fez com que a responsabilidade de coordenar os esforços no assunto passassem do Departamento de Segurança Interna, e outras instituições, para a Casa Branca. O DHS administrava a maioria das políticas de segurança cibernética do país, trabalhando com a

cibersegurança como uma dimensão da segurança nacional que afetava outras estruturas. A alteração da coordenadoria do tema para a Casa Branca não mudou a forma como ele é tratado; porém, agora, há uma maior visibilidade e uma maior facilidade da cooperação interagências (HARKNETT e STEVER, 2009).

A cooperação interagências, por sua vez, apresenta outros problemas internos além da falta de centralização. O excesso de burocracia em relação ao compartilhamento de informações é um grande dificultador da criação de uma política conjunta. Os diferentes departamentos têm diferentes políticas sobre o assunto e é necessária uma autorização para se ter acesso a essas informações. Para essa questão, a pesquisa recomenda que sejam criadas políticas que facilitem o compartilhamento de informações sobre o assunto, sempre levando em conta a proteção à privacidade, das liberdades civis e dos dados sensíveis que cada agência é responsável. Junto com essas políticas o documento aponta a necessidade da criação de definições mais claras no escopo em que cada agência deve trabalhar, no âmbito da cibersegurança, para que políticas conjuntas possam ser mais facilmente criadas (ESTADOS UNIDOS DA AMÉRICA, 2009).

Em relação a cooperação entre as esferas pública e privada, o documento aconselha que essas parcerias sejam mais bem estudadas e expandidas A importância do setor privado na cibersegurança pode ser explicada pela privatização de infraestruturas críticas do país, que levam a dependência entre as esferas. A publicação, então, aponta a importância da indústria na elaboração, operação e desenvolvimento da infraestrutura cibernética do país. A partir disso, faz-se necessário que a preocupação com a segurança seja compartilhada entre as esferas e, consequentemente, que as medidas para fortalecer e desenvolver o campo também sejam divididas entre elas (CARR, 2016; ESTADOS..., 2009).

Essas parcerias não foram uma novidade do documento e já eram encorajadas desde a administração de Bill Clinton com a Diretiva de Decisão Presidencial 63 (GREENWALD, E. 2010). A mudança proposta com Obama foi a ampliação dessas parcerias e uma melhor definição das funções de cada uma das esferas, já que foi apontado que a falta de definições claras do papel de cada um desestimula a participação do setor privado. Nesse sentido, a contribuição da indústria seria o compartilhamento de dados que possam ajudar na proteção da infraestrutura cibernética e o desenvolvimento de mais tecnologias que assegurem a segurança dos usuários. Além disso, seria responsável por ajudar na criação de um padrão para casos em que se deve reportar vazamento de dados e outros incidentes do tipo que não viole a privacidade dos usuários. Já o governo contribuiria com a criação de leis que incentivassem esse tipo de

comportamento por parte do setor privado e que regulassem o compartilhamento de informações (ESTADOS UNIDOS DA AMÉRICA, 2009).

As preocupações levantadas pela indústria em relação à cooperação com o governo são no campo econômico, principalmente no que diz respeito à privacidade. As empresas relataram serem relutantes em notificar incidentes cibernéticos por medo de sofrer com perdas econômicas e com ações reguladoras por parte do governo. Para que isso seja resolvido, o CPR orientou o governo a criar mecanismos e estruturas que garantam a integridade da privacidade de cada empresa que colaborar com o governo. Outra sugestão foi a criação de leis que notifiquem tanto a sociedade civil quanto o governo sobre o vazamento de dados. Seja qual das medidas for adotada, o documento ressalta que é preciso garantir a privacidade dos dados junto com a possibilidade de se estudar e desenvolver mais soluções para os problemas de cibersegurança (ESTADOS UNIDOS DA AMÉRICA, 2009).

Enquanto a parceria público-privada é elemento fundamental no desenvolvimento de políticas e estudos sobre segurança cibernética, alguns autores levantam algumas ressalvas acerca do tema. Madaline Carr (2016) levanta o ponto de que os interesses do governo e do setor privado são diferentes. Enquanto o primeiro se preocupa com a segurança da infraestrutura e a proteção de dados, o segundo, se preocupa com sua reputação e as possíveis consequências financeiras. Carr argumenta que a esfera privada faz esforços para proteger dados essenciais até o ponto que é lucrativo, pois diferentemente do governo seus planos de segurança da rede são baseados em modelos de negócios que levam em consideração a posição de acionistas e do próprio mercado. Essa visão entra em conflito com a função do governo de garantir a segurança de todos. Como resultado, o setor privado mostra certa resistência em assumir responsabilidade por toda infraestrutura do país. Segundo ela,

> O setor privado levanta duas objeções principais ao papel que o governo percebe para ele nas estratégias de segurança cibernética. Em primeiro lugar, argumenta que o custo de garantir a segurança cibernética a um nível de segurança nacional seria significativo; em segundo lugar, argumenta que a natureza litigiosa da sociedade (especialmente nos Estados Unidos) significa que a indústria seria muito resistente em aceitar a responsabilidade pela segurança de seus produtos ou sistemas. (CARR, 2016, p. 56, tradução nossa)

Harknett e Stever (2009) seguindo a mesma linha argumentativa dizem que, embora haja estímulos internos e externos para as empresas investirem na segurança e prevenirem vazamentos e ataques, muitas vezes, as vantagens para o cliente são priorizadas sobre sua proteção, o que não está de acordo com as prioridades do governo. Os autores chamam atenção

para o fato de que enquanto a prática das empresas for apenas orientada para lucro a segurança não será aperfeiçoada. A solução proposta por eles para essa questão é a junção dos esforços da indústria com a criação de uma regulamentação governamental que defina melhores padrões de segurança para deixar a parceria benéfica para todos.

Embora não aborde diretamente esses temas, o CPR (2009), apontou algumas possíveis soluções para garantir uma melhora qualitativa nas parcerias. O *Cyberspace Policy Review* ressaltou diversas vezes a necessidade de transparência e a responsabilidade não só nas parcerias com o setor privado, mas entre as relações dentro do próprio governo e com outros Estados. Para isso, o documento sugeriu a criação de diversas políticas para garantir a privacidade das empresas e a regulamentação dos dados obtidos pela parceria. Outra sugestão foi a

> Criação de uma organização não governamental sem fins lucrativos para servir como um host terceirizado confiável, onde as informações do governo e do setor privado podem ser compartilhadas para aumentar a segurança de redes críticas do governo e do setor privado. Tal organização poderia alavancar serviços comerciais sem interromper o crescente mercado de serviços de segurança. (ESTADOS UNIDOS DA AMÉRICA, 2009, p. 26, tradução nossa)

No tocante à relação entre governos e outros atores internacionais, foi proposto a criação de uma estratégia que possibilitasse a criação de normas e parcerias, as quais não eram limitadas a governos, incluindo, também, empresas estrangeiras. Essa estratégia deveria ter o objetivo de moldar o ambiente internacional trazendo normas no campo do combate a cibercrimes, da proteção e privacidade de dados e da infraestrutura de comunicação e informação (ESTADOS UNIDOS DA AMÉRICA, 2009).

O documento colocou a cargo do Coordenador de Cibersegurança o papel de trabalhar com outras agências para o desenvolvimento de políticas conjuntas. O objetivo, dessa forma, deve ser estabelecer parcerias bilaterais e multilaterais que ajudem na formação de uma política conjunta, que estejam de acordo com os interesses do país e que ajudem na proteção de sua economia e privacidade (ESTADOS UNIDOS DA AMÉRICA, 2009).

Outra recomendação é que deve ser preparado uma estratégia para lidar com as agências internacionais, como as Nações Unidas (ONU), a OTAN (Organização do Tratado do Atlântico Norte), o G8, o Conselho Europeu, a Colaboração Econômica Ásia-Pacífico (APEC), entre outras organizações que o país faz parte. O documento aponta a importância de o país estar preparado para discutir e elaborar políticas dentro dessas organizações, devendo, inclusive,

auxiliar instituições como o Banco Mundial e o Fundo Monetário Internacional (FMI) a desenvolver políticas de cibersegurança. Ademais, devem ser criados acordos que regulamentem o compartilhamento de dados e protejam os produtos de empresas com cadeias produtivas divididas entre vários países (ESTADOS UNIDOS DA AMÉRICA, 2009).

A inovação que o documento traz na área das parcerias internacionais é a questão do armazenamento na "nuvem" como um desafio a ser encarado em termos de desenvolvimento de políticas.

> A movimentação de dados através das fronteiras jurisdicionais apresenta desafios para a aplicação da lei, a proteção da privacidade e das liberdades civis conforme definido por diferentes países e decisões de responsabilidade no caso de violação de dados ou rede (ESTADOS UNIDOS DA AMÉRICA, 2009, p.32, tradução nossa).

Para melhor regulamentar a falta de fronteiras da internet e os problemas decorrentes disso é necessário que o país dialogue com outros países e com instituições internacionais para a formação de acordos. Esses acordos devem conter questões relacionadas a ciberataques, defesa, dissuasão, jurisdição territorial e como investigar e julgar os cibercrimes.

O assunto da cooperação internacional permaneceu durante todo o governo de Obama em consonância com a sua política de multilateralismo. Em 2011, a administração lançou uma estratégia para as políticas cibernéticas internacionais, intitulada *International Strategy for Cyberspace*, que será discutida posteriormente nesse trabalho.

No ramo da educação, a principal proposição foi o investimento em campanhas de conscientização sobre o tema. O documento ressalta a importância da criação de campanhas que abordem formas de uso seguro e consciente da internet. Essa conscientização, no entanto, não é restrita às escolas e às universidades; o governo deve trabalhar junto com os demais setores da sociedade para garantir que toda a população possa ser atingida (ESTADOS UNIDOS DA AMÉRICA, 2009).

Envolvendo especificamente a educação de crianças e jovens, o documento destacou a importância da criação de um programa para o Ensino Básico, que inclua a cibersegurança nos currículos escolares, ensinando questões como ética, privacidade e proteção no meio cibernético. A pesquisa sugere, além disso, a criação de bolsas de estudo e investimentos que fortaleçam programas de educação já existentes como o *National Science Force* e diversas outras que tenham o mesmo objetivo (ESTADOS UNIDOS DA AMÉRICA, 2009).

O CPR destaca, ainda, a necessidade do investimento na área de Ciências Exatas, a expansão dos cursos sobre o assunto em Universidades e a abertura de oportunidades de trabalho dentro do próprio governo federal. O objetivo desse investimento é a criação de uma mão-de-obra especializada que esteja pronta para trabalhar nesse ramo e que já tenha, no próprio país, oportunidades de emprego. Com isso, o país consegue formar e reter a mão-de-obra que trabalhe tanto no setor privado quanto diretamente com o governo. Apenas investindo na educação e em futuros empregos é possível que os Estados Unidos mantenham sua vantagem competitiva no futuro. A importância desse investimento é tão grande que é comparado com a corrida espacial durante a Guerra Fria (ESTADOS UNIDOS DA AMÉRICA, 2009).

Para colaborar nessa questão a administração estabelece em 2014 a Iniciativa Nacional para Educação em Segurança Cibernética (NICE). A iniciativa se trata de uma parceria entre o setor público, privado e a academia e promove treinamentos e formação da força de trabalho capacitada em segurança cibernética além de colaborar para a inovação no setor (NEWHOUSE *et al.*, 2017).

Juntamente com o investimento em educação, o documento aponta o investimento e a criação de uma estratégia de Pesquisa e Desenvolvimento (P&D) como indispensável para a elaboração de novas tecnologias que possam contribuir para o aperfeiçoamento da infraestrutura e segurança no país. Esse investimento deve ser feito dentro do próprio governo, junto à academia e no setor privado (ESTADOS UNIDOS DA AMÉRICA, 2009).

O desenvolvimento do setor foi melhor especificado dois anos após a publicação do documento. O trabalho, intitulado *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* (2011), teve o objetivo de coordenar os trabalhos de P&D nos Estados Unidos e investir em medidas que possam combater ciberataques atuais e que estejam prontas para enfrentar desafios futuros. A estratégia definiu quatro pontos centrais: criação de inovações disruptivas, criação uma base científica de conhecimentos sobre cibersegurança, cooperação com o setor privado e outros países para desenvolver pesquisas e, por fim, implementação mais rápida das tecnologias desenvolvidas (NATIONAL SCIENCE AND TECHNOLOGY COUNSIL, 2011; Vagoun e Strawn, 2015).

Apesar de se apresentar como algo novo, o *Cyberspace Policy Review*, é baseado em políticas já existentes de outras administrações. Em particular, a *Comprehensive National Cybersecurity Initiative*, lançada no final do governo de Bush, em 2008 (MAIER, 2019). Outro documento que também serviu de base foi a Diretiva de Decisão Presidencial 63 (PDD-63)

lançada pelo governo de Bill Clinton em 1998. Esse documento já previa a criação de um aparato que protegesse a infraestrutura do país tanto de ataques físicos quanto cibernéticos. Algumas medidas pautadas na revisão de Obama já se encontravam no PDD 63, como o estabelecimento de parcerias público-privadas, estímulo à educação cibernética na sociedade, cooperação internacional no campo da cibersegurança etc. (GREENWALD, E. 2010).

Mesmo tendo esses documentos como base, a abordagem que Obama trouxe para o tema foi diferente. Enquanto as administrações anteriores focaram no problema da cibersegurança pensando, principalmente, em computadores e sistemas, o governo de Obama tratou o tema de maneira mais holística. Suas principais contribuições foram o aumento do escopo do tema no país, tornando-o questão central na segurança interna e externa do país. O ex-presidente, ainda, foi bem-sucedido em criar o cargo de Coordenador de Cibersegurança na Casa Branca, centralizando os esforços para desenvolver e resolver questões relacionadas à segurança cibernética (JENSEN, 2011; LILLI, 2020).

O governo demorou para iniciar a aplicação das medidas. Em outubro de 2010 o Escritório de Responsabilidade Governamental (GAO, na sigla em inglês) publicou um relatório intitulado "*Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*". No relatório a organização criticou a demora na implementação das políticas sugeridas pelo CPR. Até o mês de sua publicação o documento relata que das 24 medidas apenas duas medidas foram completamente implementadas e outras 22 foram apenas parcialmente executadas. As principais críticas feitas, em vista disso, foram a falta de determinação de funções e responsabilidades para as agências do governo conseguirem realizar as recomendações. Ambos os problemas têm como causa a demora para o apontamento do Coordenador de Cibersegurança na Casa Branca (GAO, 2010).

Esse foi o quarto documento pedindo pela aceleração da aplicação das medidas mencionadas no CPR. Assim como os outros três documentos, a agência recomendou que responsabilidades fossem atribuídas para cada um dos pontos que falta e que fossem implementadas metas que demonstrassem o progresso do governo na implantação das mudanças recomendadas (GAO, 2010).

Assim, o *Cyberspace Policy Review* abordou as principais medidas a serem tomadas pelo governo no campo da cibersegurança. O documento abordou, principalmente, a questão das relações do governo com suas repartições, com empresas privadas e com outros governos e entidades internacionais. Nas relações interagências a principal contribuição do documento

foi a urgência que deu a centralização das políticas de segurança cibernética na Casa Branca, o que culminou na criação do cargo de Coordenador de Cibersegurança pelo presidente Obama. Outro ponto levantado foi a importância da colaboração com empresas privadas para a construção das políticas nesse ramo da segurança e a criação de tecnologias cada vez mais seguras. As parcerias público-privadas, apesar de essenciais para a construção da política cibernética, apresentam algumas críticas principalmente em relação ao papel de cada uma das partes e em relação à questão de como se garantir a privacidade. O documento, ainda, recomendou que fosse colocado a cargo do Coordenador de Cibersegurança o relacionamento com outros países e organizações como a OTAN e a ONU e destacou a importância da presença estadunidense nas discussões sobre o tema nos demais fóruns internacionais. Ademais, o documento apresenta medidas para serem implementadas junto à sociedade civil, principalmente no campo da educação básica, da formação de futuros profissionais da área e das pesquisas acadêmicas.

No tópico seguinte será discutido as revelações de Edward Snowden em relação ao desenvolvimento das parcerias entre o Estado e empresas privadas, o que culminou na vigilância e espionagem em massa tanto nacional quanto internacional.

2.2 O Caso Edward Snowden

Obama começou seu governo advogando pela proteção da privacidade, liberdades individuais e do multilateralismo, buscando situar-se longe do unilateralismo de Bush. O caso de Snowden, no entanto, trouxe à tona que, na realidade, as coisas não aconteceram assim. O 44º presidente dos Estados Unidos manteve diversas características do governo de seu antecessor. Os vazamentos feitos por Edward Snowden mostraram como a administração continuou com a retórica da Guerra ao Terror para utilizar e ampliar os meios de vigilância em massa do país (GREENWALD, G. 2014).

A vigilância em massa não foi exclusividade do governo Obama. Desde a Guerra Fria o país desenvolvia tecnologias que possibilitavam a espionagem de cidadãos americanos. Essas tecnologias, de maneira geral, eram focadas, principalmente, na obtenção de informações de estrangeiros. Ainda assim, escândalos envolvendo as agências de inteligência dos Estados Unidos espionando seus próprios cidadãos não são uma novidade do mundo pós-11 de setembro. Em 1970, por exemplo, investigações já apontavam que o FBI praticava a vigilância

em massa. Era estimado que meio milhão de cidadãos estadunidenses espionados com a justificativa de serem considerados “subversivos”, entre eles figuras como Martin Luther King e Malcolm X. A diferença trazida em 2001 é o uso da internet para a coleta de dados, que possibilitou que o país criasse um aparato global de vigilância em massa. Somado a isso, há o medo que os ataques de 2001 trouxeram as pessoas, que justificou a flexibilização das leis de privacidade do país e a própria vigilância (GREENWALD, G. 2014).

As denúncias feitas por Snowden, mencionaram a violação da privacidade feita pela Comunidade de Inteligência (CI) dos Estados Unidos. A Comunidade é administrada pelo Gabinete do Diretor Nacional de Inteligência (ODNI) e tem o objetivo de coletar e armazenar todo tipo de inteligência. A CI é formada por dezesseis agências:

> Central Intelligence Agency (CIA); Defense Intelligence Agency (DIA); Federal Bureau of Investigation (FBI); National Geospatial-Intelligence Agency (NGA); National Reconnaissance Office (NRO); National Security Agency (NSA); Department of Energy (DOE); Department of Homeland Security (DHS); Department of State (DOS); Department of Treasury (OIA); US Air Force Intelligence; Drug Enforcement Administration (DEA); US Army Intelligence (G-2); US Coast Guard Intelligence; US Marine Corps; Office of Naval Intelligence (ONI) (SQUADRANS, 2017, p. 26).

Essas agências de inteligência ganharam maior relevância durante a Guerra Fria, apesar de já existirem e já realizarem trabalhos de coleta de informação. O Ato de Segurança Nacional em 1947 promulgado pelo presidente Harry Truman lançou as bases para a criação de agências como a Agência Central de Inteligência (CIA) e o Conselho de Segurança Nacional (NSC). No entanto, foi com a criação da Agência de Segurança Nacional (NSA), em 1952, e o *Foreign Intelligence Surveillance Act* (FISA), de 1978, que o sistema de inteligência norte-americano foi se moldando como ele é hoje (SQUADRANS, 2017).

A NSA surge do braço militar da agência *Cable e Telegraph Section*, chamado Câmera Negra, criado na Primeira Guerra Mundial. O objetivo dessa agência era interceptar comunicações entre estrangeiros e reportar ao Departamento de Estado. As reformas feitas nas agências de inteligência do país após Pearl Harbor e com a Guerra Fria culminaram na criação da NSA, em 1952. Seu documento de criação deu-lhe poderes de organizar, controlar e coletar as comunicações da inteligência norte-americana conduzidas contra governos estrangeiros. O impacto de sua criação foi tal que em 1961 já havia se tornado a principal agência de inteligência do país (SQUADRANS, 2017).

O primeiro escândalo de participação da agência em serviços de espionagem foi em 1975 com o caso Watergate. Investigações feitas pelo Congresso dos Estados Unidos revelaram que há 20 anos a NSA vinha espionando as comunicações internacionais. Como resultado, diversos dispositivos voltados para a regulamentação das atividades de espionagem da Comunidade de Inteligência do país, entre essas legislações foi criado o FISA (SQUADRANS, 2017).

O FISA (*Foreign Intelligence Surveilance Act*), criado em 1978, foi o documento que criou o arcabouço legal que legitimou, auxiliou e regulamentou a atividade de coleta de dados eletrônicos tanto da NSA quanto dos demais serviços de inteligência do país. O documento autorizou a vigilância da comunicação de terceiros que passasse por território americano. Essas operações seriam autorizadas por meio da aprovação da Corte FISA (FISC) ou pela autorização emergencial do Procurador-Geral. O mandado de aprovação era obtido desde que fossem definidos os alvos, os motivos e os procedimentos que seriam usados na investigação. A principal função da Corte era assegurar as liberdades individuais dos cidadãos do país conforme previsto pela Constituição. (ESTADOS UNIDOS DA AMÉRICA, 1978 apud. SQUADRANS, 2017).

A principal crítica feita ao FISA e ao FISC é seu papel subserviente. Conforme apresentado por Greenwald (2014), desde sua criação em 1978 até 2002 não houve nenhum pedido de investigação negado entre milhares de aprovados. Já no período de 2002 a 2012, apenas 11 pedidos foram negados entre mais de 20 mil aprovados. Segundo o autor,

> [...] o tribunal da FISA foi criado não para manter um controle genuíno sobre o poder do governo, mas como uma medida ornamental, para proporcionar apenas uma aparência de reforma que aplacasse a ira da população quanto aos abusos de vigilância denunciados nos anos 1970 (GREENWALD, G. 2014, p.111).

Essa inutilidade da Corte do FISA em, realmente, advogar contra os abusos da Comunidade de Inteligência fizeram com que agências como a NSA pudessem crescer e aumentar seu poder de vigilância desenfreadamente, isto é, sem nenhuma restrição legal que realmente impusesse limites (GREENWALD, G. 2014).

Após o 11 de setembro, o Ato Patriota flexibiliza as leis de coleta de informações e aumenta o investimento do país na área de inteligência. Entre algumas mudanças implementadas, o Ato Patriota mudou o documento do FISA permitindo que o governo coletasse dados em território estrangeiro sem propósito específico. Segundo Squadrans (2017,

p.44), a mudança implicava que a “a inteligência poderia ser empregada para outros fins não previstos e seu emprego poderia não se restringir ao âmbito externo”.

Para a NSA, o 11 setembro significou o ampliamento do escopo das atividades. A principal mudança é que a agência passa a espionar, também, cidadãos estadunidenses. Em 2006, duas investigações mostraram o envolvimento da NSA em vigilância em massa dentro do território norte-americano. Em maio de 2006 foi noticiado o envolvimento da agência com a companhia telefônica AT&T para obter e armazenar dados sobre a navegação na internet de seus clientes. Já em novembro do mesmo ano, outra investigação envolvendo a NSA e as companhias telefônicas do país descobriu que a agência estava coletando dados de chamadas telefônicas de milhões de cidadãos (SQUADRANS, 2017).

O Ato Patriota e outros mecanismos criados após os atentados de 2001, dessa forma, aumentaram as leis de inteligência do país fortalecendo o poder de vigilância em massa dos Estados Unidos. As flexibilizações e concessões à Comunidade de Inteligência feitas a partir de 2001 tornaram possível a ação desenfreada do país em relação à coleta de dados. A violação das liberdades individuais e privacidade dos cidadãos foi justificada pela doutrina de Guerra ao Terror. Essa ação desmedida por parte do governo levou, em 2013, à divulgação de Snowden.

A maior parte da carreira de Edward Snowden foi feita durante a administração Bush, ele trabalhou principalmente junto à CIA e à NSA. Em sua entrevista com Greenwald ele declara que em 2009 já pensava delatar as práticas abusivas do governo; porém as promessas realizadas por Obama durante sua campanha o fizeram acreditar que medidas seriam criadas para regular as atividades de inteligência. Todavia, contrário ao que foi prometido, Obama continuou e expandiu as práticas de vigilância em massa (GREENWALD, G. 2014).

Nos primeiros anos do governo Obama uma série de medidas foram adotadas para continuar com a captação de dados. Obama, assinou um documento estendendo a validade do Ato Patriota por mais 5 anos. Em 2012, o Congresso do país estendeu para 2017 a validade das emendas no FISA feitas em 2008, as quais autorizaram a coleta de dados das companhias telefônicas do país. Além de estender seu prazo, foi acrescentado ainda a possibilidade das agências da CI supervisionarem as comunicações dos cidadãos do país apenas com uma aprovação da Corte FISA, isto é, sem mandato (SQUADRANS, 2017).

Snowden chegou a divulgar cerca de 50.000 arquivos contendo memorandos e documentos internos e entre a agência e serviços de inteligência de outros países. Os arquivos mostravam o volume de coleta de dados e as operações conduzidas no mundo inteiro e os

programas utilizados para essa captação, entre eles os mais mencionados foram o PRISM e o FAIRVIEW. Além disso, os documentos revelaram que, ao contrário do que foi dito ao Congresso, a NSA podia quantificar e armazenar os dados daqueles que ela investigava. Esse trabalho era feito pelo programa *BOUNDLESS INFORMANT* e conforme os documentos, esse programa era capaz de coletar bilhões de dados diariamente, que iam de e-mails a chamadas telefônicas (GREENWALD, G. 2014; SQUADRANS, 2017).

O FAIRVIEW tratava da parceria da NSA com empresas privadas; esse foi um de quatro programas desenvolvidos para a captação de dados em parceria com o setor privado. Programas desse tipo eram administrados por uma divisão secreta da agência chamada Operações de Fontes Especiais (SSO). O programa é responsável pela interceptação e repasse das informações obtidas por empresas de telecomunicações. Segundo descreve Greenwald (2014, p. 84),

> a NSA explora o acesso de determinadas empresas de telecomunicações a sistemas internacionais depois de elas terem firmado contratos com companhias semelhantes no exterior para criação, suporte e melhoria de suas redes. Em seguida, as empresas norte-americanas redirecionam os dados de comunicação do país-alvo para repositórios da NSA.

Os documentos destacaram a importância do programa como um dos maiores fornecedores de metadados para agência. Cerca de 75% dos dados obtidos pelo programa vinham de uma única prestadora de serviços, que não foi revelada nos documentos; porém o envolvimento da NSA com as empresas Verizon e AT&T foi confirmado posteriormente (GREENWALD, G. 2014; SQUADRANS, 2017).

O PRISM, por sua vez, foi o programa mais mencionado e o mais importante em termos de interceptação de dados. O programa foi criado em 2007, porém só se tornou conhecido com as revelações de Snowden. Com o programa a NSA tinha acesso às redes das maiores empresas de internet do mundo – Apple, Facebook, Google, Microsoft, Yahoo, entre outras. O principal atributo do programa é que um agente podia solicitar uma informação ao sistema e receber todas as informações da empresa sem participação de nenhum de seus funcionários. As empresas citadas negaram ter dado o acesso ilimitado à NSA para coletar os dados, afirmando que a agência tinha acesso apenas àquilo que o mandato do FISA previa (GREENWALD, G. 2014; SQUADRANS 2017).

Além do PRISM e do FAIRVIEW é importante destacar mais um programa usado para a interceptação de dados, o *Quantium Insert* ou método de Exploração da Rede Computacional

(CNE). O programa consiste na inserção de *malwares* em computadores específicos para a espionagem de seus usuários. O CNE é fiscalizado pela unidade de *hacking* da NSA e a partir dele a agência tem acesso a tudo o que a pessoa faz no computador. De acordo com o que foi divulgado, cerca de 50.000 computadores foram "infectados" com esse *malware*.

Para além do trabalho da agência com empresas de internet e telecomunicações, a NSA também trabalha com governos para a obtenção de inteligência. Greenwald (2014, p. 102) define essas parcerias em três categorias:

> A primeira delas é com o grupo dos Cinco Olhos: os Estados Unidos espionam junto com esses países, mas raramente os espionam, a menos que solicitados pelas autoridades dos próprios países parceiros. O segundo grupo é formado por países com os quais a NSA trabalha em projetos de vigilância específicos ao mesmo tempo que os espiona de forma ampla. O terceiro é formado por países que os Estados Unidos espionam de forma rotineira, mas com os quais quase nunca coopera.

Grande parte dos documentos divulgados era parte da colaboração entre as agências do grupo *Five Eyes*. A colaboração entre as inteligências dos Estados Unidos, Grã-Bretanha, Canadá, Austrália, Nova Zelândia formou um sistema de espionagem internacional que possibilitou que a NSA aumentasse a capacidade de vigilância.

> Os países-membros dos Cinco Olhos compartilham a maioria de suas atividades de vigilância e se reúnem todo ano em uma conferência de Desenvolvimento de Sinais durante a qual se gabam de sua expansão e dos sucessos do ano anterior (GREENWALD, G. 2014, p. 102).

A NSA desenvolveu um relacionamento estreito com cada uma das agências do grupo; porém a principal colaboradora foi a Grã-Bretanha. A relação era tal que a agência britânica, Central de Comunicações do Governo Britânico (GCHG), recebia 100 milhões de libras da NSA como forma de incentivo para que apoiasse as ações da agência americana e garantisse o seu acesso aos programas de inteligência britânicos. A GCHQ foi extremamente importante para a obtenção de dados no exterior. Sua principal colaboração foi desenvolver as tecnologias que possibilitaram a obtenção de informações com todo tipo de dados *online* provenientes de cabos submarinos (GREENWALD, G. 2014).

A principal justificativa para a ampliação do aparato de vigilância dos Estados Unidos, tanto nacional quanto internacionalmente, foi o combate ao terrorismo. Contudo, apesar de a NSA ter negado diversas vezes, os documentos vazados em 2013 apresentavam indícios de espionagem econômica e diplomática. Para o caso de espionagem econômica destaca-se a interceptação das comunicações da empresa petrolífera brasileira Petrobras e do Ministério de

Minas e Energia, também do Brasil. Essa forma de vigilância serviu para a agência atender os interesses de outros órgãos dentro do governo federal estadunidense, em especial com os departamentos de Agricultura, Tesouro e Comércio, os quais se beneficiariam com esse tipo de informação (GREENWALD, G. 2014).

Em relação à espionagem diplomática, os principais casos divulgados foram o monitoramento da ex-presidente brasileira, Dilma Rousseff e da chanceler alemã Angela Merkel. O monitoramento é feito de modo a obter vantagens diplomáticas em negociações e, no caso brasileiro, monitorar o clima do país em relação a sua proximidade com os Estados Unidos. Além de chefes de Estado, a NSA incluiu na sua lista a vigilância de organizações internacionais como a ONU. Os documentos revelaram que o próprio secretário-geral da organização foi fonte de espionagem. Além desse caso, frequentemente, Estados-membros eram vigiados para se levantar as melhores estratégias de negociação que deveriam ser usadas pelos norte-americanos (GREENWALD, G. 2014).

As informações de espionagem diplomática e econômica tornaram inválida a justificativa do monitoramento em massa para combater atos terroristas. A maior parte dos dados divulgados por Snowden não tem relação com o combate ao terrorismo, a espionagem da Petrobras, por exemplo. Em uma reportagem do *The Washington Post* de 2013, o Departamento de Justiça não menciona sequer uma vez em que a coleta em massa de dados tenha impedido de fato algum atentado. Especialistas também dizem que a coleta em massa não é eficiente na prevenção e impedimento a atentado. O grande número de dados obtidos – mais de 1 bilhão por dia – tende mais a atrapalhar do que a ajudar. As buscas por pessoas e grupos ligados a esse tipo de atividades mostraram ter muito mais sucesso quando conduzidas de maneira direcionada (GREENWALD, G. 2014).

Uma vez que o pretexto de combate a atentados cai por terra, a alternativa que surge é a criação de um sistema global de vigilância em massa. Esse monitoramento é possibilitado pela internet e representa sérios perigos à privacidade e à liberdade individual. A internet se desenvolveu de tal modo que hoje o mundo se tornou extremamente dependente dela. A coleta de metadados pode revelar quase tudo sobre uma pessoa. Seu uso indevido pode inclusive atentar contra a própria democracia, pois pode expor aqueles que são contra determinado regime e possibilitar que o governo constranja a oposição e críticos. Esse sistema de coleta em massa de dados vai contra os próprios princípios fundadores da internet (GREENWALD, G. 2014).

A internet surgiu como forma de democratização do acesso à informação e da possibilidade de debates entre pessoas de grupos diferentes. A existência de programas como PRISM, e outros conduzidos pela NSA, inibe a liberdade associada ao ambiente online e facilita a coerção indireta da população. Greenwald (2014) explica a vontade das potências ocidentais em desenvolver esse modelo de vigilância a partir das crises econômicas que esses países passam. Segundo ele,

> Face a perturbações sociais, as autoridades em geral têm duas alternativas: aplacar a população com concessões simbólicas ou fortalecer seu controle de modo a minimizar os possíveis danos aos seus interesses. As elites ocidentais parecem preferir a segunda alternativa – fortalecer o próprio poder –, talvez o único curso de ação viável para proteger sua posição (GREENWALD, G. 2014, p. 175-176).

Com o fortalecimento de seus próprios poderes, representados na criação do aparato de monitoramento em massa, além de constranger movimentos contrários a seus interesses é possível moldar o pensamento do povo, que tem receio de divulgar suas opiniões (GREENWALD, G. 2014).

A descoberta do mundo sobre o poder dos Estados Unidos em termos de vigilância cibernética causou um clima de desconfiança geral. Para contornar o problema, em 2014, um ano após as revelações de Edward Snowden, Obama lançou a Diretiva de Política Presidencial número 28 (PPD-28), a qual tratava dos meios de obtenção de inteligência por sinais. Inteligência de sinais (SIGINT) "se refere a informações coletadas através da interceptação de sinais de comunicação em território terrestre – navios, aviões, bases militares – e por satélites." (SQUADRANS, 2017, p.26).

O papel do documento, assim, foi articular "[...] princípios para orientar por que, se, quando e como os Estados Unidos conduzem atividades de inteligência de sinais para fins autorizados de inteligência estrangeira e contraespionagem." (THE WHITE HOUSE, 2014, tradução nossa). Além disso, ao obter alguma forma de inteligência por sinais as agências da CI deviam considerar

> [...] que todas as pessoas devem ser tratadas com dignidade e respeito, independentemente de sua nacionalidade ou onde quer que residam, e que todas as pessoas têm legítimos interesses de privacidade no tratamento de suas informações pessoais (THE WHITE HOUSE, 2014, tradução nossa).

São definidos quatro princípios para os quais as operações de obtenção de inteligência são autorizadas:

> (a) A coleta de informações de sinais deve ser autorizada por estatuto ou Ordem Executiva, proclamação ou outra diretiva presidencial, e realizada de acordo com a Constituição e estatutos aplicáveis, Ordens Executivas, proclamações e diretivas Presidenciais. (b) A privacidade e as liberdades civis devem ser considerações integrais no planejamento das atividades de inteligência de sinais dos EUA. Os Estados Unidos não coletarão informações de sinais com o objetivo de suprimir ou opor-se a críticas ou dissidências, ou para prejudicar pessoas com base em sua etnia, raça, gênero, orientação sexual ou religião. A inteligência de sinais deve ser coletada exclusivamente onde houver uma inteligência estrangeira ou propósito de contraespionagem para apoiar missões nacionais e departamentais e não para quaisquer outros fins. (c) A coleta de informações comerciais privadas estrangeiras ou segredos comerciais é autorizada apenas para proteger a segurança nacional dos Estados Unidos ou de seus parceiros e aliados. Não é uma inteligência estrangeira autorizada ou propósito de contraespionagem coletar tais informações para proporcionar uma vantagem competitiva às empresas dos EUA e aos setores de negócios dos EUA comercialmente. (d) As atividades de inteligência de sinais devem ser tão adaptadas quanto possível. Ao determinar se devem coletar inteligência de sinais, os Estados Unidos devem considerar a disponibilidade de outras informações, inclusive de fontes diplomáticas e públicas. Essas alternativas adequadas e viáveis para a inteligência de sinais devem ser priorizadas (THE WHITE HOUSE, 2014).

Respondendo à principal queixa feita a vigilância em massa, a diretiva também prevê a imposição de limites à coleção de dados em grande volume. É proposto que o Diretor de Inteligência Nacional (DNI) elabore uma lista em que preveja os casos em que a captação de dados em massa seja autorizada. Essa lista deve ser revisada uma vez por ano e deve estar disponível ao público (GREENWALD, G. 2014).

Apesar de destacar a necessidade de se manter a privacidade e a necessidade impor limites na coleção de em massa, o documento ressalta a importância que a coleta de dados tem para a proteção do país. Proteção essa que pode entrar em risco com a divulgação indevida para o público de informações sobre as atividades performadas pelas agências. As consequências de divulgações mencionadas são, as parcerias com outros países, os interesses comerciais do país, a credibilidade internacional e a proteção das fontes e os métodos de obtenção de inteligência (THE WHITE HOUSE, 2014). Ainda que a Diretiva Presidencial apresente algumas medidas a serem tomadas para a vigilância feita pelos Estados Unidos na internet, o documento é vago e não apresenta mecanismos concretos de resolução dos problemas.

Peter Margulies (2017) define a Diretiva como uma lei branda feita pelo governo Obama. Para ele, a dificuldade de conseguir com que o Congresso aprovasse um pacote de leis sobre o tema levou o presidente a emitir o documento. O autor divide as medidas tomadas pelo governo Obama após as revelações de Snowden em dois campos: as leis brandas (*soft laws*) e

a discrição das agências. As leis brandas são definidas como a celebração de políticas e acordos não vinculativos, ou seja, sem muita especificidade de normas e elementos de fiscalização. Já a discrição das agências é a ação unilateral por parte das agências federais.

As *soft laws* são bastante úteis no campo internacional, pois facilitam a celebração de acordos que não precisam ser formalmente ratificados. Essa prática "articula as melhores práticas que refletem o consenso entre múltiplas partes" (MARGULIES, 2017, p. 467, tradução nossa). Outra vantagem é a maior flexibilidade que dá aos acordos, permitindo que as partes envolvidas possam mudar as normas sem toda a burocracia de leis formais.

As principais desvantagens desse tipo de norma é justamente a falta de mecanismos que assegurem que as partes cumprirão o que foi dito e a falta de uma definição clara das responsabilidades de cada parte. A abordagem da administração de Obama sobre a cibersegurança foi feita, em grande parte, com a utilização de leis brandas. O governo mais de uma vez teve dificuldade em fazer com que o Congresso entrasse em consenso sobre a aprovação de leis sobre o tema, o que fez com que o governo adotasse *soft laws* para a maioria de suas políticas. A cooperação das agências federais com outras entidades, por exemplo, foi encorajada, mas não foi feito uma definição precisa da função de cada parceiro, como foi recomendado no CPR. Ademais, não foram criados mecanismos de regulação tanto nas agências federais quanto nas empresas privadas, resultando na coleta desenfreada de todo tipo de informação, como divulgado por Snowden (MARGULIES, 2017).

Ao contrário da abordagem multilateral das *soft laws*, o modelo de discrição das agências, por sua vez, trata da ação unilateral das agências do governo, isto é, elas agem fora de protocolos estabelecidos. Esse modelo tem menos participação de outros setores da sociedade nas decisões da agência. A principal vantagem da discrição das agências é a contribuição que pode dar em relação à cibersegurança e à privacidade. Esse modelo possibilita a criação e implantação de novas tecnologias e modelos que não precisam esperar a aprovação do Congresso ou outras entidades. Porém com as revelações de Snowden a desconfiança nesse modelo aumentou, uma vez que a própria ação unilateral da Comunidade de Inteligência permitiu a criação do sistema de monitoramento em massa (MARGULIES, 2017).

A vigilância em massa divulgada contribuiu para a falta de confiança no governo Obama, o que, no que lhe concerne, atrapalhou a implantação de medidas de transparência posteriormente. A adoção de leis brandas para restaurar a confiança internacional foi fundamental para que o governo começasse a trabalhar para reconquistar essa confiança interna

e externamente. Contudo, a falta de mecanismos concretos pode apresentar problemas por não impor limites reais às agências de inteligência. Por fim, o debate trazido pelas revelações de Snowden obrigou o presidente a dar um passo atrás na sua criação de uma visão holística da cibersegurança e rever os problemas que não foram abordados de maneira precisa, como a privacidade e os limites do desenvolvimento de tecnologias de espionagem. Snowden revelou também outra agenda da construção da cibersegurança e vigilância no país que precisa ser constantemente monitorada pela sociedade civil para que excessos sejam evitados.

Snowden, dessa forma, abriu um debate sobre cibersegurança no país destacando os limites que devem ser criados para que tanto empresas quanto o próprio governo possam respeitar a privacidade no mundo online. Apesar das parcerias entre os setores serem fundamentais deve haver limites mais rígidos para evitar a vigilância em massa. A falta de legislações que regulamentassem de forma concreta as parcerias entre o governo e a indústria possibilitou o desenvolvimento desenfreado dos programas de captação de informações das agências de inteligência do país com a participação das empresas nacionais de telecomunicações e as maiores empresas de comunicações do mundo. A principal justificativa do governo após as revelações foi a questão da segurança nacional, porém os documentos mostram como o país utilizou os recursos para promover a espionagem econômica e diplomática. Como resposta a essa crise, o governo de Barack Obama criou a Diretiva de Política Presidencial 28, a qual visava indicar quando poderia ocorrer a captação de metadados e reafirmava a importância da privacidade dos cidadãos do país. Contudo, a Diretiva reafirmou a necessidade da obtenção de informações para a segurança nacional e condenou a divulgação dessas afirmações.

O PPD-28 e o *Cyberspace Policy Review* não foram as únicas medidas que o governo tomou para construir a política de segurança cibernética do país. A administração Obama teve outras iniciativas para guiar o desenvolvimento cibernético do país, como o USCYBERCOM, a Estratégia Internacional para o Ciberespaço e o *Cybersecurity National Action Plan*, abordadas a seguir.

2.3 Principais inovações do Governo

A administração Obama foi a primeira que empreendeu vários esforços em construir uma política de cibersegurança robusta para os Estados Unidos. A formulação de relatórios para

que as diversas áreas do governo tivessem um guia de como agir foram um diferencial e avançaram na construção dessa política. O presidente ainda fez avanços na cibersegurança militar, na cooperação internacional e na criação de plano nacional para o próximo comando do país. Essa próxima seção tratará desses avanços. Para isso, analisaremos os documentos *Cybersecurity National Action Plan*, *International Strategy for Cyberspace* e a criação do USCYBERCOM.

Pouco tempo após a publicação do *Cyberspace Policy Review*, o governo estadunidense anunciou a criação do Comando Cibernético dos Estados Unidos (USCYBERCOM). Como foi apontado no relatório do CPR (2009), era necessário criar mais integração entre as agências do governo para que a resposta aos ciberataques fosse mais rápida e eficiente. Conforme a internet se torna parte essencial do governo, ela se torna uma questão de segurança nacional, demandando que forças capacitadas possam operar e defender.

Além da necessidade de manter a segurança nacional, assim como outros setores da sociedade, as forças de segurança norte-americanas dependem cada vez mais da internet para seu funcionamento e realizam cada vez mais operações nas redes. Com essa maior presença no ambiente online, cresce a ameaça de ataques cibernéticos a estruturas militares críticas do país. Refletindo esse cenário, o USCYBERCOM foi criado em 2009 para aumentar a segurança e a presença dos Estados Unidos no espaço cibernético (DEPARTMENT OF DEFENSE, 2010; LYNN III, 2010).

O Departamento de Defesa (DoD) foi responsável pela criação do USCYBERCOM. Essa divisão funciona como um comando sub-unificado subordinado ao Comando Estratégico dos Estados Unidos (USSTRATCOM). Situado no mesmo conglomerado que a NSA, em Fort Mead, o USCYBERCOM conta com vários recursos para defender e responder a possíveis ameaças às redes do país, recebendo parte do orçamento destinado ao DoD. O USCYBERCOM foi pioneiro em centralizar os esforços militares do país em cibersegurança (DEPARTMENT OF DEFENSE, 2010). Sua missão é

> [...] planejar, coordenar, integrar, sincronizar e realizar atividades para: dirigir as operações e defesa específicas das redes de informação do Departamento de Defesa e; preparar-se e, quando direcionado, conduzir as operações militares do ciberespaço em todo o espectro para permitir ações em todos os domínios, garantindo a liberdade de ação dos EUA/Aliados no ciberespaço e negar o mesmo para nossos adversários (DEPARTMENT OF DEFENSE, 2010, tradução nossa).

O Comando trabalha em grande proximidade com o Departamento de Defesa para melhorar a capacidade de combater ameaças e projetar a estrutura cibernética de forma a viabilizar uma resposta à altura por parte dos Estados Unidos e com a menor perturbação possível as redes nacionais (DEPARTMENT OF DEFENSE, 2010).

No final da administração Obama o Comando Cibernético já havia atingido a capacidade máxima estipulada. Isso fez com que o DoD pedisse um repasse de verbas de US$ 6,7 bilhões e aumentasse a capacidade operacional de 5000 agentes para 6200. Esses agentes fazem parte de diversas missões dentro do Comando, que vão desde apoio ao DoD e a defesa das redes militares até a preparação de forças cibernéticas para o combate (SANTOS, 2018).

O Comando Cibernético atua tanto nacionalmente quanto internacionalmente com parceiros nacionais e internacionais, ajudando em operações militares e protegendo as redes governamentais. No plano nacional, ele atua junto a outras agências, como o FBI e o DHS, coordenando operações e prestando o auxílio necessário. O USCYBERCOM supervisiona atividade em cada ramo das forças armadas, isso inclui o exército, marinha, aeronáutica e fuzileiros navais. O Comando auxilia, também, em missões de treinamento para capacitar esses militares a atuarem nas mais diversas condições de redes. Já em âmbito internacional, o Comando Cibernético trabalha com governos aliados compartilhando e recebendo informações que ajudem na melhoria do aparato de cibersegurança do país. O USCYBERCOM conta, também, com a colaboração de empresas privadas para compartilhar informações e ameaças em potencial (LYNN III, 2010).

O USCYBERCOM, assim, tem a função de centralizar os esforços militares, principalmente do Departamento de Defesa, em segurança e defesa cibernética. Sua função é coordenar e supervisionar as missões cibernéticas dos diferentes departamentos prestando auxílio e oferecendo treinamentos. Com sua criação, o governo norte-americano tem o objetivo de aumentar sua presença e influência no espaço cibernético, além de assegurar que suas redes militares permaneçam seguras e o mais preparadas para responder a ataques quanto possível.

A cooperação com parceiros internacionais prevista tanto no *Cyberspace Policy Review* quanto no USCYBERCOM também foi trabalhada pela administração. Em 2011 o governo Obama lançou o documento *International Strategy for Cyberspace* que contava com os princípios que guiariam o país no campo da cooperação internacional para o desenvolvimento de uma rede segura e que contemplasse seus interesses. O documento ressaltou a importância

de se criar um ambiente seguro de colaboração internacional, uma vez que a internet permite que interconectividade entre diferentes áreas do mundo sem qualquer fronteira física. Com isso em vista, o principal objetivo do país é garantir o livre acesso à informação, privacidade e integridade das redes, trabalhando junto com países que tenham a mesma visão (ESTADOS UNIDOS DA AMÉRICA, 2011).

A estratégia principal apontada é baseada em 3 pontos. O primeiro é preservar e aumentar os benefícios trazidos pelas redes, quanto mais informações circularem mais elas poderão ser usadas para o desenvolvimento de novas tecnologias. O segundo diz respeito ao reconhecimento dos novos desafios que a internet traz tanto no campo econômico quanto no da segurança. O documento levanta, principalmente, a questão do roubo de propriedade intelectual, suas consequências para a economia e o livre-mercado, além das mais diferentes categorias de cibercrimes, que tem sua ação facilitada pelo ambiente anônimo que as redes podem proporcionar. Por fim, o último ponto diz respeito a lidar com esses novos desafios tendo em mente os princípios defendidos pelo país de livre acesso à informação, privacidade e proteção das liberdades fundamentais (ESTADOS UNIDOS DA AMÉRICA, 2011).

A estratégia apresenta a livre circulação como um contraponto à tática chinesa de construção de um Firewall. Na época de sua publicação, em 2011, a China já se mostrava como uma concorrente do poder americano levando o relatório a criticar, quase que abertamente, o Firewall chinês. Conforme o documento:

> "Em contraste, vemos outras abordagens - como filtros nacionais e firewalls - como fornecimento apenas ilusório de segurança enquanto dificulta a eficácia e o crescimento da Internet como um meio aberto, interoperável, seguro e confiável de troca" (ESTADOS UNIDOS DA AMÉRICA, 2011, p.5, tradução nossa).

Essa crítica ocorre, pois, o Firewall chinês, o chamado Projeto do Escudo Dourado, funciona censurando aquilo que pode ou não circular no ciberespaço chinês (CHINA'S GREAT FIREWALL, 2011). Essa tática para os Estados Unidos não garantiriam a segurança da população e dificultaria a cooperação internacional, além de violar as liberdades fundamentais.

Tendo como base a estratégia do multilateralismo, o país busca lançar sua posição para a construção de futuras parcerias internacionais relacionadas ao ciberespaço baseadas nos seus interesses nacionais. De acordo com o documento o objetivo é,

> Os Estados Unidos trabalharão internacionalmente para promover uma infraestrutura de informações e comunicações aberta, interoperável, segura e confiável que apoie as trocas e o comércio internacional, fortaleça a segurança

> internacional e promova a liberdade de expressão e inovação. Para atingir essa meta, construiremos e manteremos um ambiente no qual as normas de comportamento responsável guiam as ações dos estados, sustentam parcerias e apoiam o estado de direito no ciberespaço (ESTADOS UNIDOS DA AMÉRICA, 2011, p.8, tradução nossa)

Os principais pontos destacados por essa estratégia são a construção de um ciberespaço aberto e interoperável, seguro e confiável. Diante disso, o país apoiará a construção de um ambiente online compartilhado que garanta o livre acesso de todos, a partir do desenvolvimento de tecnologias confiáveis e que reduzam a vulnerabilidade das redes. Esse objetivo deve ser trabalhado tanto por um viés econômico como político e social, a partir de investimentos, políticas públicas e a formação de usuários conscientes e responsáveis (ESTADOS UNIDOS DA AMÉRICA, 2011).

Para atingir esses objetivos, o documento recomenda a criação de "normas de comportamento responsável" que devem guiar a política externa de defesa e de parcerias do país. O rápido aumento do uso da internet e, por consequência, a maior dependência da sociedade tornaram o ciberespaço um elemento central de política para os Estados. Esse novo ambiente deu aos países uma nova capacidade de ação política. Em função disso tornou-se necessário que novas leis e acordos internacionais fossem criados para contemplar essa nova realidade. O papel dos Estados Unidos, nesse cenário, será empreender esforços para atingir um consenso sobre normas de conduta aceitáveis dentro do ciberespaço (ESTADOS UNIDOS DA AMÉRICA, 2011).

Essas normas, assim como a maioria das normas internacionais, deverão promover, principalmente, a paz, a dignidade humana e o livre-mercado, além de garantir as liberdades fundamentais, o respeito à propriedade, a garantia da privacidade, proteção contra crimes e o direito à autodefesa. Ademais, é necessário que as normas abordem a interoperabilidade global, a estabilidade das redes, acesso confiável, a participação de outras partes-chave para o desenvolvimento das redes e a garantia da cibersegurança por parte dos governos (ESTADOS UNIDOS DA AMÉRICA, 2011).

Para conseguir dialogar com a comunidade internacional e criar essas normas, o documento divide as ações dos Estados Unidos em três campos, a diplomacia, defesa e desenvolvimento. O objetivo diplomático é

> [...] trabalhar para criar incentivos e construir consenso em torno de um ambiente internacional em que os Estados - reconhecendo o valor intrínseco de um ciberespaço aberto, interoperável, seguro e confiável – para que os

> países trabalhem juntos e atuem como partes interessadas responsáveis (ESTADOS UNIDOS DA AMÉRICA, 2011, p.11, tradução nossa).

Através de sua influência internacional o país deverá envolver o maior número de pessoas e entidades essenciais, nos setores públicos e privados, para o desenvolvimento de sua visão para uma política para o ciberespaço. O documento diz que o objetivo do país é trabalhar com relações bilaterais e multilaterais, dentro de organizações internacionais, como a ONU e a OTAN, e junto com o setor privado. As discussões com essas partes será para construir, aplicar e expandir as normas desenvolvidas para todo o sistema internacional (ESTADOS UNIDOS DA AMÉRICA, 2011).

No campo da defesa, o país planejou trabalhar em duas esferas, na dissuasão e na intimidação. O documento deixa claro que qualquer ameaça a suas redes será combatida, seja por parte de grupos terroristas ou por parte de outros Estados. No campo internacional, o país também combaterá qualquer agente que ameace as redes como um todo, trabalhando em parceria com outros atores internacionais (ESTADOS UNIDOS DA AMÉRICA, 2011). O documento destaca o objetivo central para o campo da defesa, dizendo que:

> Os Estados Unidos, junto com outras nações, encorajarão o comportamento responsável e se oporão àqueles que procuram interromper redes e sistemas, dissuadindo e intimidando atores mal-intencionados e reservando o direito de defender esses ativos nacionais vitais conforme necessário e apropriado (ESTADOS UNIDOS DA AMÉRICA, 2011, p.12, tradução nossa).

O país deixa claro que continuará investindo em sua infraestrutura cibernética e na habilidade de responder e se recuperar de ataques. No âmbito doméstico, o plano traçado segue na mesma linha daquilo sugerido pelo *Cyberspace Policy Review*, isto é, o fortalecimento através das parcerias com a indústria e um maior alinhamento das agências governamentais. No plano internacional, no que lhe concerne, o país investirá na educação, treinamento e nas relações políticas e operacionais. Além disso, empregarão maiores esforços em suas parcerias militares e técnicas. A partir dessa colaboração, os Estados Unidos trabalharão com o compartilhamento de informações úteis para aperfeiçoar a resposta a cibercrimes. Já para os países subdesenvolvidos e em desenvolvimento o país se mostra disposto a, junto com outros parceiros, investir na construção de um sistema de cibersegurança (ESTADOS UNIDOS DA AMÉRICA, 2011).

O documento ressalta, além disso, que deixará explícito os riscos a qualquer entidade que tente atacar as redes nacionais. É destacado que, assim como qualquer outra ameaça à

segurança nacional, o país retaliará quaisquer ameaças cibernéticas, em outros termos isso significa que o país se reserva o direito de utilizar todos os meios cabíveis como resposta a um ataque. Nesse sentido, o papel do sistema internacional seria ter meios para que um responsável por um ataque possa ser investigado e julgado de acordo (ESTADOS UNIDOS DA AMÉRICA, 2011).

No campo do desenvolvimento, o documento exalta a capacidade econômica e tecnológica estadunidense colocando-se como o centro das discussões acerca do tema da cibersegurança e o desenvolvimento cibernético. O governo continuará trabalhando no compartilhamento de conhecimentos e tecnologias para que consiga alcançar a formação de um comportamento comum à maioria dos países em relação à cibersegurança (ESTADOS UNIDOS DA AMÉRICA, 2011). Com isso, a estratégia proposta é que

> Os Estados Unidos facilitarão a construção de capacidade de segurança cibernética no exterior, bilateralmente e por meio de organizações multilaterais, para que cada país tenha os meios para proteger sua infraestrutura digital, fortalecer redes globais e construir parcerias mais estreitas no consenso para abertura, interoperabilidade, segurança e confiabilidade nas redes (ESTADOS UNIDOS DA AMÉRICA, 2011, p.14, tradução nossa).

O governo norte-americano investirá no aperfeiçoamento de suas tecnologias e de sua cibersegurança na esfera nacional e internacional. O país trabalhará junto com outros governos e empresas privadas no desenvolvimento de tecnologias que construam uma rede global mais segura, que facilitem o comércio, que garantam as liberdades fundamentais e contribuam para a maior interconectividade ao redor do mundo. Isso será feito a partir da promoção iniciativas e investimento em pesquisas que colaborem para satisfazer cada um dos pontos mencionados (ESTADOS UNIDOS DA AMÉRICA, 2011).

A cooperação entre os países, no campo do desenvolvimento, e nos demais campos mencionados, é apontada como fundamental para alcançar a visão que o país traz no documento. O governo norte-americano pretende formar parcerias estratégicas que ajudem tanto a aperfeiçoar sua capacidade nacional como desenvolver a capacidade de outros atores internacionais (ESTADOS UNIDOS DA AMÉRICA, 2011).

Com o investimento em desenvolvimento, a construção de um aparato de defesa e a formação de parcerias diplomáticas estratégicas, o documento separa sete áreas com prioridade na formação de consenso e condutas internacionais.

Tabela 1 – Estratégia Internacional para o Ciberespaço: Áreas de Investimentos

Áreas	Ações
Economia	Defender e desenvolver o livre mercado; Proteger a propriedade intelectual; Criar padrões para cibersegurança de produtos e serviços
Cibersegurança	Padronizar normas de conduta e de cibersegurança
Aplicação e Desenvolvimento de Normas	Desenvolver normas junto a comunidade internacional e trabalhar para que sejam seguidas
Garantia da segurança nacional	Garantir a segurança das redes nacionais; Capacitar as forças armadas para operarem no ciberespaço
Governança da internet	Investir em inovações e em uma internet aberta
Desenvolvimento da internet	Elevar a capacidade das redes com o investimento em pesquisa e em pessoal especializado na área
Preservar a privacidade e as liberdades individuais	Garantir o livre acesso a informações

A economia é a primeira área mencionada, o país empregará esforços para a defesa e o desenvolvimento do livre comércio, da proteção da propriedade intelectual e da criação de padrões de cibersegurança, de serviços e de produtos. A partir desse investimento o país garantirá que o ciberespaço continue servindo a seus interesses e das demais nações (ESTADOS UNIDOS DA AMÉRICA, 2011).

A segunda área é a cibersegurança, a qual é essencial para o resguardo econômico e nacional. O governo priorizará a cooperação bilateral e multilateral para padronizar normas de conduta e de segurança cibernética. Políticas que reduzam ataques e problemas nas redes também serão uma prioridade, assim como o fortalecimento de sua infraestrutura e de sua capacidade de recuperação e resposta. O país tem o objetivo de, através da cooperação internacional, fortalecer sua rede a partir do compartilhamento de informações com parceiros estratégicos. Nesse ponto a colaboração com a indústria também é essencial para o desenvolvimento de tecnologias mais seguras e a criação de políticas que facilitem a atuação do setor privado (ESTADOS UNIDOS DA AMÉRICA, 2011).

A terceira área que o documento prioriza é a aplicação e desenvolvimento de normas. O país deverá participar na criação de políticas contra os diversos tipos de cibercrimes, seja

através de acordos bilaterais ou em fóruns internacionais. Essa participação na criação de políticas permitirá que os Estados Unidos trabalhem para a harmonizar as diferentes políticas para o ciberespaço em diferentes países, principalmente nas legislações contra cibercrimes. Isso possibilitaria um melhor combate aos problemas de cibersegurança e prevenção a ataques (ESTADOS UNIDOS DA AMÉRICA, 2011).

Na esfera militar o principal foco será a garantia da segurança nacional. Para isso, o país investirá em capacitar suas forças armadas e criar uma rede de operações seguras para elas. Além disso, devem ser dedicados esforços em formar alianças militares com países estratégicos que ajudem no combate a ameaças nas redes e que ajudem na promoção da segurança cibernética.

No campo da governança da internet, o documento ressalta a importância de investir em estruturas que satisfaçam a necessidade de todos os usuários das redes. Segundo a Cúpula Mundial sobre a Sociedade da Informação (CMSI) governança da internet se trata do

> [...] desenvolvimento e a aplicação por parte dos governos, do setor privado e da sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos decisórios e programas compartilhados que dão forma à evolução e uso da Internet (WORLD SUMMIT..., 2005, p.6, tradução nossa).

Assim, nesse campo os Estados Unidos priorizarão políticas que tratem da inovação e abertura da internet a partir de parcerias com governos, organizações internacionais, o setor privado e ONGs. O governo estadunidense se compromete a participar e promover a discussão sobre a governança cibernética nos fóruns internacionais levantando questões sobre cibersegurança, estabilidade e outros problemas pertinentes (ESTADOS UNIDOS DA AMÉRICA, 2011).

Já na área do desenvolvimento da internet a estratégica do país é elevar a capacidade das redes, garantindo a segurança e o sucesso dos sistemas. Para isso, será feito investimento em treinamentos e pesquisas que garantam tanto o desenvolvimento das redes nacionais como internacionais. O governo estadunidense se propôs a capacitar o pessoal necessário em países que estão desenvolvendo sua capacidade, através de investimentos diretos e criando protocolos de cibersegurança internacionalmente (ESTADOS UNIDOS DA AMÉRICA, 2011).

Por fim, o país tem como prioridade investir para que a privacidade e as liberdades fundamentais sejam preservadas. O governo trabalhará junto com a sociedade civil, organizações internacionais e ONGs para garantir o livre acesso a informações. Na questão da privacidade, principalmente, o governo deve trabalhar em conjunto com outros agentes para

assegurar a segurança dos dados tanto no comércio, quanto pessoal (ESTADOS UNIDOS DA AMÉRICA, 2011).

A Estratégia Internacional para o Ciberespaço (2011) tem o propósito de servir de guia para a atuação e destacar o papel do país no desenvolvimento do ciberespaço global. A administração Obama foi a primeira a elaborar um documento do tipo colocando o país no centro das discussões sobre o tema, chegando inclusive a deixar explícito que o país "liderará pelo exemplo" (ESTADOS UNIDOS DA AMÉRICA, 2011, p.4, tradução nossa). Durante todo o documento fica evidente que os Estados Unidos apenas colaborarão e firmarão parcerias com países que pensem como os Estados Unidos e tenham interesse em criar uma conduta internacional para as práticas no ciberespaço.

As questões da segurança e da defesa também são muito exploradas durante o documento, deixando claro que o país responderá a ataques a suas redes. Já no campo internacional promoverá a criação de condutas para a resposta a cibercrimes. No entanto, cerca de dois anos depois, em 2013, as revelações de Snowden mostraram que o próprio país não estava seguindo o que foi proposto no documento. O país violou os próprios valores de liberdade e privacidade que pregou durante todo o documento e condenou outros países, como a China, por violarem. No entanto, não sofreu nenhuma sanção internacional por essa violação; a única consequência foi a diminuição da confiança da comunidade internacional na liderança do país (MAIER, 2019).

Outro ponto importante a ser considerado é o estímulo à colaboração multilateral e a maior participação da comunidade internacional na construção de um ciberespaço comum. Mais uma vez as revelações do Snowden mostraram que, por mais que a administração Obama colocasse o multilateralismo como carro chefe nas discussões, a postura do país, em muitas situações, foi unilateral e agressiva. O país fez diversas operações sem consentimento que, inclusive, podem ser consideradas como violação à soberania nacional – como a espionagem da presidenta Dilma e da chanceler alemã Angela Merkel (MAIER, 2019).

De maneira geral, a estratégia traçada pelo país dá um bom panorama de onde empregarão os esforços do governo e as formas pelas quais ele trabalhará. O documento leva para o plano internacional aquilo que a administração Obama tinha traçado para os objetivos nacionais com o CPR (2009). A administração lançou estratégias para cada campo que pode contribuir para o ciberespaço e buscou assegurar seus interesses e valores ao levar essa discussão para fóruns internacionais. A formação de uma conduta para o ciberespaço se mostrou

essencial para o país atingir os objetivos estipulados. Os investimentos em segurança, privacidade e propriedade estão presentes em todos os âmbitos que o país planeja trabalhar. Apesar de as ações do governo Obama não terem seguido exatamente o que foi proposto, o documento contribuiu para a formação e desenvolvimento da política cibernética do país.

Após a publicação da *International Strategy* e da criação do USCYBERCOM, Obama terminou seu governo publicando o *Cybersecurity National Action Plan* (CNAP), em fevereiro de 2016. O CNAP é um plano para a próxima administração seguir e fortalecer a política cibernética do país. O documento conta com medidas de curto e longo prazo para assegurar a privacidade, proteção e confiança nas redes e propõe investimentos na área da cibersegurança (ESTADOS..., 2016; MAIER, 2019).

O CNAP propôs novas medidas de cibersegurança para o governo federal seguir. A primeira proposta é a criação da Comissão de Melhoria da Cibersegurança Nacional. Essa comissão será composta por pessoas de fora do governo, envolvendo pesquisadores e membros da indústria e do Congresso do país. Seu objetivo será

> [...] fazer recomendações sobre ações que podem ser tomadas ao longo da próxima década para fortalecer a segurança cibernética nos setores público e privado, protegendo a privacidade; manutenção da segurança pública e da segurança econômica e nacional; fomentar a descoberta e o desenvolvimento de novas soluções técnicas; e fortalecimento de parcerias entre o governo federal, estadual e local e o setor privado no desenvolvimento, promoção e uso de tecnologias, políticas e melhores práticas de segurança cibernética (ESTADOS UNIDOS DA AMÉRICA, 2016, tradução nossa).

A Comissão terá o apoio do Instituto Nacional de Padrões e Tecnologia (NIST, em inglês) e reportará ao presidente as conclusões e recomendações específicas até o fim de 2016.

Enquanto o relatório é elaborado, o documento propõe que se continue a investir na cibersegurança. Uma das propostas é a criação de um Fundo de Modernização de Tecnologia da Informação de 3,1 bilhões de dólares. A finalidade desse fundo, como o próprio nome diz, é garantir que a área de Tecnologia da Informação (TI) do governo esteja sempre atualizada com a tecnologia mais recente e segura. Esse orçamento deve priorizar os itens de maior risco e valor. O DHS e outras agências disponibilizarão serviços compartilhados de TI e cibersegurança para melhorar o desempenho e segurança das redes. Além disso, o Departamento de Segurança Interna investirá no aumento de civis trabalhando na defesa cibernética do país. Essas equipes de civis formadas deverão proteger as redes, os sistemas e os dados em toda parte civil do Governo e responder a eventuais ataques. Além da criação do

Fundo, é proposto o investimento adicional de US$ 19 bilhões de dólares em cibersegurança para o orçamento do ano fiscal de 2017, aumentando em 35% o orçamento de 2016. (ESTADOS UNIDOS DA AMÉRICA, 2016).

Parte do orçamento do Fundo deve ser destinado à educação – o CNAP prevê o investimento de US$ 62 milhões – em especial na Iniciativa Nacional para a Educação em Cibersegurança (NICE). O governo deverá investir em educação e treinamento em cibersegurança em todo o país para a formação de especialistas na área. O NICE deverá expandir as bolsas de estudo para a tema para cidadãos que desejem trabalhar com o governo e montar um Currículo Básico de Cibersegurança. De maneira geral, o investimento em educação deve ter como objetivo, além do desenvolvimento de mão-de-obra capacitada, o estímulo que essas pessoas trabalhem para o governo (ESTADOS UNIDOS DA AMÉRICA, 2016).

O governo federal deverá investir na proteção dos dados de seus cidadãos. Para isso, deve colaborar com as empresas de comunicação – como Google, Apple, Microsoft, etc. – para capacitar os cidadãos estadunidenses a protegerem suas informações online. Na esfera pública, o NIST junto com outras agências trabalhará com pequenas empresas promovendo um treinamento de cibersegurança para negócios. O governo ainda deve continuar a investir em iniciativas que previnem o roubo de identidade e clonagem de cartões bancários (ESTADOS UNIDOS DA AMÉRICA, 2016).

Por fim, o governo deverá continuar seus investimentos na infraestrutura crítica, deixando-a mais segura e confiável. Isso será feito por meio de parcerias público-privadas que o Centro de Excelência de Cibersegurança Nacional impulsionará. O Centro é a colaboração dos setores para pesquisa e desenvolvimento para a elaboração de soluções técnicas de segurança cibernética de alta prioridade. Ademais, o país deve continuar dedicando esforços para aumentar a cooperação internacional (ESTADOS UNIDOS DA AMÉRICA, 2016).

O *Cybersecurity National Action Plan*, assim como o *International Strategy for Cyberspace* e o *Cyberspace Policy Review*, tem o objetivo de sugerir medidas que contribuam para que o país fique na liderança do desenvolvimento tecnológico. Ao propor medidas para a próxima administração, o governo busca dar continuidade à política de cibersegurança construída durante toda a era Obama. Seguindo a mesma linha dos outros dois documentos, o CNAP continua dando a importância para a proteção de dados e da privacidade, do investimento em educação, pesquisa e desenvolvimento, a formação de pessoal capacitado e que trabalhe com o governo e a colaboração entre agentes públicos e privados internacional e nacional tanto

nacional quanto internacionalmente. A Estratégia Internacional para o Ciberespaço, por sua vez, estimula o multilateralismo, a cooperação entre os mais diversos agentes para a criação de comportamentos e valores comuns no ambiente cibernético e mostra o cunho das parcerias a seres feitas pelo país. Além disso, ressalta que o país defenderá e retaliará ataques as suas redes por todos os meios necessários, o que eleva a importância do ciberespaço. Apesar do multilateralismo e os valores defendidos muitas vezes não terem sido seguidos pelos Estados Unidos, o documento ainda assim é relevante pois destaca as principais áreas que o país destinaria investimentos e o tipo de parcerias que buscava. Por fim, a criação do USCYBERCOM, também, está de acordo com o que foi proposto pelo CPR em 2009 e desenvolve a capacidade tanto defensiva quanto de ataque do país centralizando nesse Comando as operações cibernéticas militares facilitando, assim, a capacidade de resposta do país.

No próximo capítulo abordaremos as políticas criadas por Donald Trump, o 45º presidente dos Estados Unidos, em especial a Ordem Executiva 13800 e a Estratégia Cibernética Nacional. Ademais, será abordado também as eleições presidenciais de 2016 que expuseram a vulnerabilidade do país a ciberataques orquestrados tanto por meio de *hacking* quanto por meio das redes sociais.

3. GOVERNO TRUMP (2017-2020)

As eleições de 2016 nos Estados Unidos causaram polêmica no cenário internacional e dentro dos Estados Unidos. O primeiro ponto de controvérsia foram os ataques de Donald Trump aos governos democratas, ao multilateralismo, a China, ao México, a Coreia do Norte, entre outros, externalizando a culpa pelo declínio americano. O segundo ponto foi o uso das redes sociais para a campanha, o que levou a disseminação descontrolada de *fake news* e as acusações de interferência russa nas eleições em prol do candidato republicano.

A eleição de Trump significou a vitória do pensamento conservador em suas mais diversas formas, seja do mais radical até o mais moderado. Com o partido republicano tendo maioria tanto no Senado quanto na Câmara, o 45º presidente representou a recolocação das forças conservadoras e neoconservadoras à frente da política estadunidense. Seus slogans de campanha, *Make America Great Again* e *America First*, refletiam esse pensamento e ditavam quais seriam os pilares de seu governo – xenofobia, racismo, misoginia, nacionalismo, protecionismo, unilateralismo e militarismo (PECEQUILO, 2017).

No campo da cibersegurança, o tema se tornava cada vez mais importante com o avanço da tecnologia, que aumentou a dependência de pessoas, empresas e países. A questão foi de extrema importância para o governo, principalmente face ao crescimento de empresas de tecnologia chinesas e a corrida pelo desenvolvimento da tecnologia 5G. A posição de Trump, nesse cenário, foi em consonância com o restante de sua política externa, e seguiu o viés unilateralista e militarista. As ações da administração Trump foram no sentido de capacitar as forças armadas e aumentar o poder de resistência e dissuasão do país (MAIER, 2019).

Esse capítulo, dessa forma, tratará das políticas e ações adotadas pela administração Trump em relação à cibersegurança. O primeiro ponto a ser considerado será a interferência russa nas eleições de 2016, suas consequências e as ações tomadas em resposta a isso. Outro ponto de análise será as principais políticas e iniciativas de segurança cibernética desenvolvidas pelo governo como, a Ordem Executiva 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017), *National Cyber Strategy* (2018) e algumas outras ações tomadas pelo governo.

3.1 Eleições de 2016

Donald Trump entrou na presidência em meio ao escândalo de uma interferência russa em seu benefício com sua possível participação. Desde a campanha sua postura foi marcada pela agressividade e pelo intenso uso das mídias sociais para promover ataques à candidata democrata Hillary Clinton. Na principal mídia utilizada pelo ex-presidente, o Twitter, uma série de *fake news* foram criadas e espalhadas, a maioria sobre o partido democrata e sua candidata. Essas notícias falsas tiveram grande repercussão nas redes, algumas sendo compartilhadas pelo próprio Trump, como o envolvimento de Obama e Hillary Clinton na criação do grupo terrorista Estado Islâmico (GIBSON, 2016).

Além desse compartilhamento de informações falsas, durante o período eleitoral milhares de e-mails do Comitê Nacional Democrata (DNC, na sigla em inglês) e do Comitê de Campanha Parlamentar Democrata (DCCC) foram vazados no website *WikiLeaks*. Os e-mails, pertencentes a sete funcionários do DNC – incluindo o chefe de campanha de Clinton, John Podesta, e a chefe do partido, Debbie Wasserman Schultz – revelaram uma preferência do Partido Democrata a Clinton ao invés de Bernie Sanders causando uma crise interna no partido e levando os republicanos a acusarem o partido de fraude nas eleições primárias (SCHLEIFER, 2016).

Após o vazamento dos e-mails do DNC, o Departamento de Segurança Interna, o FBI e o Diretor Nacional de Inteligência publicaram um relatório mostrando haver fortes indícios de que o ciberataque ao Partido Democrata fora financiado pelo governo russo. Após divulgado, o relatório Obama impôs uma série de sanções ao país incluindo suas agências de inteligência, o Departamento Central de Inteligência (GRU) e o Serviço de Segurança Federal (FSB), expulsando 35 de seus oficiais dos Estados Unidos (THIELMAN, 2016).

As evidências levantadas pelo relatório das agências de inteligência do país e pela investigação que o FBI conduzia desde julho de 2016 levaram o Congresso americano a abrir sua própria investigação em 2017. O inquérito aberto pelo Congresso, contudo, investigaria além da participação russa, um possível conluio entre a campanha de Trump e a Rússia. O Departamento de Justiça dos Estados Unidos, então, nomeou Robert Mueller III como procurador especial encarregado de investigar

> (i) quaisquer ligações e/ou coordenação entre o governo russo e indivíduos associados à campanha do presidente Donald Trump; e (ii) quaisquer questões que tenham surgido ou possam surgir diretamente da investigação; e (iii)

> quaisquer outros assuntos dentro do escopo do Título 28 do C.F.R. § 600.4(a). (MUELLER, 2019, p.11, tradução nossa)[1]

O relatório final da investigação foi apresentado em março de 2019 para o Procurador Geral e parte dele foi divulgada para o público em abril de 2019. O relatório conta com 448 páginas sendo dividido em dois volumes. O primeiro trata da interferência russa e do possível envolvimento de Trump e de sua campanha. Já o segundo volume trata dos casos de obstrução de justiça durante as investigações (MUELLER, 2019).

Durante os dois anos de investigação, de 2017 a 2019, foram ouvidas mais de 500 testemunhas, sendo 80 perante um Grande Júri, emitidas quase 3000 intimações e cerca de 500 mandados de busca e apreensão. Mueller e sua equipe, ainda conseguiram indiciar 34 indivíduos e três empresas russas.

As principais figuras indiciadas foram a Agência de Pesquisa de Internet russa (IRA, na sigla em inglês) juntamente com outras duas empresas de fachada de Yevgeniy Progizhin, oligarca próximo de Vladimir Putin, por distribuição de propaganda russa; 12 oficiais russos foram indiciados pelo ciberataque ao Partido Democrata; o presidente de campanha de Trump, Paul Manafort foi condenado a sete anos de prisão por crimes financeiros; Konstantin Kilimnik, funcionário de Manafort, foi acusado de obstrução de justiça; Roger Stone, próximo de Trump, condenado por mentir para o Congresso; Michael Flynn, ex-conselheiro de Segurança Nacional se declarou culpado por mentir para o FBI, Rick Gates, assessor de campanha de Trump, se declarou culpado de mentir para os investigadores; Michael Cohen, advogado de Trump, se declarou culpado por irregularidades financeiras na campanha; George Papadopulos, assessor de política externa de Trump, condenado a 12 dias de cadeia por mentir para os investigadores. (MUELLER, 2019; TIME, 2019).

A primeira forma de intervenção russa analisada pelo relatório foi a produção de *fake news* pela IRA, uma organização russa fundada pelo oligarca Yevgeniy Progizhin. A investigação apurou evidências de ações da organização desde 2014. A Agência de Pesquisa de Internet criou contas falsas nas redes sociais, principalmente Facebook, Twitter e YouTube, personificando cidadãos americanos para espalhar informações falsas e, a partir disso, criar páginas e grupos que tratavam de assuntos sociais e políticos. A organização conseguiu imitar

[1] A saber C.F.R. é o Código de Regulamentos Federais dos Estados Unidos. O parágrafo 600.4 (a) o qual estabelece a jurisdição do procurador especial, que vai desde o fato pelo qual ele foi nomeado até outros crimes federais cometidos no curso da investigação como perjúrio, obstrução da justiça, destruição de evidências e intimidação de testemunhas (https://www.law.cornell.edu/cfr/text/28/600.4)

páginas oficiais como a conta do Partido Republicano do Tennessee (@TEN_GOP) fingindo ser associada ao partido. A Agência, também, chegou a mandar funcionários para os Estados Unidos para colher informações para as postagens, que ao final das eleições de 2016 tinham milhões de visualizações dentro dos Estados Unidos (MUELLER, 2019).

Os agentes da IRA encarregados das contas eram instruídos a disseminar conteúdo através de fazendas de *trolls*, isto é

> [...] um grupo organizado que se uniu com o propósito específico de afetar a opinião pública por meio da geração de informações erradas e/ou desinformação na Internet. Um indivíduo envolvido em tal atividade é chamado de troll ou troll da Internet. (MCCOMBIE, UHLMANN e MORRISON, 2019, p.5, tradução nossa)

Esse conteúdo era compartilhado com o objetivo de influenciar alvos específicos, como grupos conservadores, grupos religiosos e grupos de justiça social.

A partir de 2016 o principal objetivo da Agência se tornou apoiar a campanha de Donald Trump. Os agentes, então, passaram-se por voluntários para saber como melhor interferir nas eleições. A maneira encontrada foi focar em estados pendulares – Flórida, Ohio, Pensilvânia, Virgínia e Winconsin – com postagens contra Hillary Clinton e outros candidatos republicanos durante as eleições primárias. A confusão causada pelo vazamento dos e-mails também foi aproveitada pela IRA, que aumentou os ataques à candidata democrata a partir da disseminação de *fake news* (MUELLER, 2019; MCCOMBIE et al. 2019).

A principal estratégia do grupo era explorar conflitos já existentes no país para aumentar a tensão em torno dos tópicos. Alguns dos temas abordados pela IRA são

> ● Cultura negra, comunidade, Black Lives Matter ● Blue Lives Matter, pró-polícia ● Reforma anti-refugiados e pró-imigração ● Cultura, comunidade e orgulho do Texas ● Cultura do sul (história da Confederação) ● Movimentos separatistas e secessão ● Cultura, comunidade e orgulho muçulmano ● Cultura, comunidade e orgulho cristãos ● Cultura, comunidade e orgulho LGBT ● Cultura, comunidade nativa americana e orgulho ● Cultura de memes e 'pílula vermelha' ● Patriotismo e cultura Tea Party ● Cultura liberal e feminista ● Questões dos veteranos ● Direitos de armas, pró-2ª Emenda ● Conteúdo político pró-Trump e anti-Clinton ● Conteúdo pró-Bernie Sanders e pró-Jill Stein ● Síria e ISIS, pró-Assad, contra o envolvimento dos EUA ● Confiança na mídia (MCCOMBIE; UHLMANN; MORRISON, 2019, p. 6, tradução nossa).

A partir das discussões geradas por esses temas a IRA conseguiu alcançar visibilidade suficiente para organizar comícios pró-Trump em diversos Estados, como Flórida, Nova Iorque e Washington. No Facebook, o grupo comprou diversos anúncios a favor de Trump e contra

Clinton para aumentar seu alcance. O relatório de Mueller estima que aproximadamente US$ 100.000 dólares foram gastos em anúncios. Em todas as redes sociais os agentes da IRA compravam anúncios e subiam *hashtags* em favor a Trump e atacando Hillary Clinton. Essa campanha chegou a atingir cerca de 126 milhões de americanos (MUELLER, 2019; MCCOMBIE; UHLMANN; MORRISON, 2019).

O Relatório de Mueller (2019) aborda, além do esquema das *fake news*, os ciberataques ao grupo Democrata, como mencionado no início da seção. O ataque foi orquestrado pela principal agência de inteligência do governo russo, o GRU, e foram vazados para o *WikiLeaks* pelos perfis anônimos chamados de "Guccifer 2.0" e "DCLeaks". A invasão da rede de computadores do DNC começou em abril e teve como alvo os e-mails de funcionários e voluntários próximos a Clinton. O GRU conseguiu acesso aos e-mails através de operações militares utilizando principalmente a técnica de *spearphishing*[2] em larga escala, com o objetivo de achar e-mails que prejudicassem a candidata democrata.

Uma vez que os e-mails foram tornados públicos, a agência de inteligência russa continuou com os ataques a membros da campanha de Clinton e aos responsáveis pelo sistema eleitoral. Outro alvo da GRU foram softwares e hardwares das empresas de tecnologia encarregadas das eleições de novembro. O único relato de interferência da agência no sistema eleitoral foi quando a agência conseguiu invadir o sistema de registro de eleitores do estado de Illinois em julho de 2016. Mesmo com esse ocorrido, o relatório reporta não ter encontrado nenhuma evidência de contagem errada de votos nem de manipulação dos resultados da eleição (MUELLER, 2019).

Em relação à participação da campanha de Trump nos ciberataques e na produção de *fake news*, o relatório achou vários links entre membros da campanha próximos de Trump e o governo Russo. No entanto, Mueller e sua equipe foram incapazes de achar conexões entre o comitê eleitoral do presidente e os russos envolvidos no ataque ao DNC e os agentes da IRA. Ainda assim, as informações coletadas na investigação mostram que tanto George Papadopoulos, quanto Donald Trump Júnior sabiam que o governo russo tinha informações que poderiam prejudicar a campanha de Hillary Clinton (MUELLER, 2019).

[2] Um e-mail de spearphishing é projetado para parecer originário de uma fonte confiável e solicita informações para permitir que o remetente obtenha acesso a uma conta ou rede, ou faz com que o destinatário baixe malware que permite ao remetente obter acesso a uma conta ou rede (MUELLER, 2019, p.37, tradução nossa).

Após ser eleito e em resposta às acusações da influência russa nas eleições, a primeira reação de Donald Trump foi negar que teria acontecido e acusar o Partido Democrata de mentir sobre o ocorrido para deslegitimar sua vitória. O presidente chegou a substituir os chefes do FBI e da CIA após assumir o cargo. Mesmo com relatórios do diretor da CIA apontado por ele afirmando a intervenção, o presidente continuou negando a interferência russa e culpando a oposição e criticando as medidas tomadas por Obama face ao ocorrido. O presidente só foi, de fato, reconhecer a interferência em 2020 (BLACKWILL; GORDON, 2018).

A resposta insatisfatória da administração Trump à presença externa nas eleições levou o Congresso e outras instituições federais a agir. O Congresso aprovou uma lei em julho de 2017 com o propósito de retaliar a intervenção russa nas eleições, a chamada Lei de Combate aos Adversários da América por Sanções (CAATSA). A lei foi estruturada de forma que a administração Trump não conseguiria suspendê-la sem a aprovação do parlamento do país e coloca sanções à Rússia em suas principais áreas econômicas. Além disso, impõe sanções a países e organizações que ajudem a Rússia a atacar o ciberespaço de outra instituição democrática. Mesmo com esse aparato legal a administração Trump demorou para aprovar o projeto e só o fez após pressão do Congresso (BLACKWILL; GORDON, 2018).

As agências federais, no que lhes concerne, em especial a Agência de Segurança Cibernética e Infraestrutura (CISA) e o DHS, tomaram a frente e implementaram medidas para garantir a segurança cibernética das próximas eleições. As medidas tomadas giraram em torno de fortalecer toda a infraestrutura cibernética eleitoral a partir da parceria entre o governo federal, estadual, municipal e o setor privado. Programas para prevenção e defesa foram desenvolvidos e consultores de cibersegurança foram colocados à disposição. As medidas tiveram resultado e o pleito de 2020 foi considerado como o mais seguro na história do país mesmo com a pandemia de COVID-19 (DEPARTMENT OF HOMELAND SECURITY, 2021).

Em resposta às acusações o presidente russo, Vladimir Putin, negou qualquer envolvimento do governo do país nas eleições estadunidenses. Putin acusou as agências de inteligência norte-americanas de tentar deslegitimar a vitória de Trump e piorar a relação entre os dois países (KHURSHUDYAN, 2020).

Segundo a pesquisa de McCombie et al. (2019) foi analisada a influência que as operações russas tiveram no resultado das eleições, observando principalmente os estados pendulares que a IRA focou. Os autores concluíram que

> [...] o efeito do IRA nas tendências dos eleitores é inexistente ou, no máximo, contribui de forma moderada para outros fatores mais poderosos. Ao considerar o número de votos do Colégio Eleitoral que mudou de democrata para republicano em 2016 e, em seguida, procurar atribuir a mudança à ação do IRA, não podemos sustentar nenhuma afirmação de que o IRA teve um papel significativo na entrega da vitória de Hillary Clinton a Donald Trump. (MCCOMBIE et al., 2019, p. 14, tradução nossa)

Os locais onde a operação da IRA teve maior sucesso foram em estados que já normalmente votam no partido republicano, como Texas e Kansas.

Ainda segundo a pesquisa (2019) o verdadeiro sucesso da operação russa não foi interferir e influenciar nas eleições presidenciais e sim contestar a funcionalidade e a validade das democracias na era digital. Nas palavras dos autores

> Ao parecer um meio válido e eficaz de subverter o processo eleitoral – a operação troll-farm veio a lançar mais dúvidas sobre a viabilidade da democracia eleitoral na era digital de forma mais geral, rompendo ainda mais a narrativa hegemônica da classe política das democracias parlamentares do Ocidente. (MCCOMBIE et al., 2019, p. 16, tradução nossa)

A vitória de Donald Trump chocou a classe política do país principalmente pela forma que o 45º presidente usou as redes sociais a seu favor. As campanhas russas no ciberespaço americano expuseram a vulnerabilidade que as redes sociais trazem para seu próprio ciberespaço, coisa que os Estados Unidos viram apenas na Primavera Árabe (MCCOMBIE et al., 2019).

As operações russas no ciberespaço norte-americano, seja a disseminação de notícias falsas, seja a invasão dos e-mails do Partido Democrata tiveram como objetivo promover Donald Trump como candidato e explorar os conflitos internos dos Estados Unidos. A investigação levada a cabo pelo Congresso liderada por Robert Mueller e as investigações das agências de inteligência do país obtiveram sucesso descobrindo os pormenores da atividade russa tanto do Departamento Central de Inteligência quanto da Agência de Pesquisa de Internet mesmo que Putin tenha negado tal intervenção. Ao investigar se existia cooperação entre a IRA e o GRU com a campanha de Trump, Mueller não conseguiu estabelecer nenhum vínculo, ainda que diversos membros perto de Trump tenham sido indiciados e condenados posteriormente. Ao assumir a presidência, Trump não tomou nenhuma medida direta para responder aos ataques russos e negou qualquer interferência russa acusando a oposição de tentar deslegitimar sua vitória. Isso foi considerado um grande fracasso do presidente em termos de cibersegurança. O Congresso, então, toma a frente e aprova uma lei de sanções como forma de retaliação, a

CAATSA. As agências federais, principalmente CISA e DHS, também agem em resposta à intervenção russa fortalecendo a infraestrutura cibernética do país, principalmente no que diz respeito às eleições.

No tópico seguinte serão analisadas as iniciativas e políticas criadas pela administração de Trump. Em especial a Ordem Executiva 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017), *National Cyber Strategy (2018)* e outras iniciativas do governo para garantir a cibersegurança nacional.

3.2 Principais ações do Governo

Apesar dos diversos ataques a Obama e as políticas implementadas durante sua administração, Trump não faz muitas alterações na política de segurança cibernética que o ex-presidente havia desenvolvido. A administração continuou trabalhando para fortalecer a política e a infraestrutura cibernética do país. Esse trabalho seguiu a lógica do lema de sua campanha *America First* buscando fortalecer as capacidades ofensivas e de defesa. Assim, examinaremos os seguintes documentos, a Estratégia Cibernética Nacional (2018*)* e a Ordem Executiva 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017).

Alguns meses após assumir a presidência o presidente emitiu a Ordem Executiva 13800 (EO 13800), com o título *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. A Ordem Executiva tem como objetivo fazer uma revisão da política de segurança cibernética do país. O documento é dividido em cinco seções, cibersegurança nas redes federais, cibersegurança em infraestruturas críticas, cibersegurança para a nação, uma seção para definições acerca dos termos utilizados e uma para as disposições gerais (ESTADOS UNIDOS DA AMÉRICA, 2017).

O primeiro ponto levantado no documento diz respeito à modernização e ao gerenciamento de riscos das redes do governo. A modernização constitui parte fundamental da manutenção dos riscos enfrentados pelas redes federais. O documento instrui as agências a estarem preparadas para possíveis invasões dos sistemas, vazamentos, destruição ou modificação de dados sem autorização. Além disso, é exigido que todas as repartições do governo sigam as recomendações estabelecidas pelo Instituto Nacional de Padrões e Tecnologia (NIST) e produzam um relatório para o Departamento de Segurança Interna e para o Gabinete de Gestão e Orçamento (OMB, na sigla em inglês). Esse relatório deve

> (A) documentar as escolhas de mitigação de risco e aprovação feitas por cada chefe de agência na data desta ordem, incluindo: (1) as considerações estratégicas, operacionais e orçamentárias que informaram essas escolhas; e (2) qualquer risco aceito, inclusive de vulnerabilidades não mitigadas; e (B) descrever o plano de ação da agência para implementar o Framework. (ESTADOS UNIDOS DA AMÉRICA, 2017, p.2, tradução nossa).

Uma vez enviado ao DHS e ao OMB, esses departamentos têm a função de analisar os relatórios. Essa análise leva em conta se as medidas são cabíveis e suficientes para a proteção da infraestrutura cibernética. A partir dessa análise os dois departamentos mencionados devem formular um plano alinhado com as políticas do NIST que proteja as redes de todas as agências e inclua o orçamento necessário para que as modernizações sejam feitas. O plano, então, deve ser enviado ao gabinete presidencial para ser apurado (ESTADOS UNIDOS DA AMÉRICA, 2017).

Para o segundo tópico, o documento coloca ser dever do governo e de seus departamentos trabalharem para preservar e prestar suporte aos responsáveis pelas infraestruturas críticas do país. Baseando-se na legislação criada por Obama, a Ordem Executiva instrui os principais setores de defesa do país a identificarem esferas que possam ajudar na proteção da segurança cibernética da infraestrutura essencial do país. Isso significa que o governo deve proteger os sistemas que, se comprometidos, podem causar adversidades ao nível nacional ou regional (ESTADOS UNIDOS DA AMÉRICA, 2017).

O Comércio também engloba a infraestrutura crítica do país, sendo assim, manter sua segurança e transparência é um dos deveres colocados pela ordem executiva. O DHS e o Departamento do Comércio devem trabalhar juntos e mapear as medidas de segurança já implementadas pelo governo e avaliá-las de modo a promover um comércio seguro e transparente. Os departamentos devem aprimorar a resiliência da internet e serviços de comunicações contra possíveis ataques de *botnets*[3] (ESTADOS UNIDOS DA AMÉRICA, 2017).

Além da questão do comércio, o documento aborda a segurança cibernética nos setores energético e na indústria de defesa. Para o setor energético, a EO 13800 determina que o Departamento de Energia junto com o DHS e o Diretor de Inteligência Nacional devem avaliar as consequências de um potencial ataque cibernético à rede elétrica do país; a prontidão com

[3] Uma **botnet** é uma rede de computadores que foram infectados por softwares maliciosos e podem ser controlados remotamente, obrigando-os a enviar spam, espalhar vírus ou executar ataques de DDoS sem o conhecimento ou o consentimento dos seus donos (AVAST ACADEMY TEAM, 2016)

que o país possa resolver o incidente e suas consequências; e as limitações dos recursos necessários para mitigar às repercussões de um ciberataque (ESTADOS UNIDOS DA AMÉRICA, 2017).

Da mesma maneira que os outros setores mencionados, para o setor industrial de defesa também deve-se fazer um relatório dos possíveis riscos de cibersegurança que as redes, a base industrial, a cadeia de produção e as forças armadas do país podem enfrentar. Essa avaliação será entregue ao presidente junto com sugestões de melhorias para o aumento da capacidade defensiva das redes (ESTADOS UNIDOS DA AMÉRICA, 2017).

Para o terceiro ponto abordado na Ordem Executiva, a administração define como objetivo

> [...] promover uma internet aberta, interoperável, confiável e segura que promova a eficiência, inovação, comunicação e prosperidade econômica, respeitando a privacidade e protegendo contra interrupções, fraude e roubo. Além disso, os Estados Unidos buscam apoiar o crescimento e a sustentação de uma força de trabalho qualificada em segurança cibernética e áreas afins como base para alcançar nossos objetivos no ciberespaço (ESTADOS UNIDOS DA AMÉRICA, 2017, p.5, tradução nossa).

A partir desse objetivo os departamentos devem fazer um relatório com as principais medidas de defesa e estratégias adotadas para a proteção dos cidadãos do país contra ameaças cibernéticas.

O tópico aborda a questão da cooperação internacional e fica determinado que as agências estabeleçam prioridades no campo da cibersegurança internacional, o que inclui compartilhamento de dados e outras informações. O governo utilizará os relatórios produzidos para a criação de uma estratégia de cooperação para a cibersegurança internacional, sugerindo a substituição da *International Strategy for Cyberspace* (2011) criada pelo governo Obama (ESTADOS UNIDOS DA AMÉRICA, 2017; MAIER, 2019).

Sobre o desenvolvimento de uma força de trabalho capacitada para trabalhar com o assunto é revisado o escopo das atuais políticas para desenvolvimento dessa mão-de-obra do país. As políticas de educação básica e superior, programas de estágio, treinamentos no setor público e privado devem ser revistos e as devidas recomendações devem ser feitas. O Diretor Nacional de Inteligência deve ficar responsável por monitorar desenvolvimentos na mão-de-obra de outros países que possam afetar os Estados Unidos. Além disso, as agências têm que garantir a manutenção ou aperfeiçoamento da posição de liderança do país no campo da segurança cibernética (ESTADOS UNIDOS DA AMÉRICA, 2017).

Os relatórios foram analisados e seu resultado serviu de base para o governo montar a Estratégia de Defesa Nacional (2017) e para o *National Cyber Strategy* (NCS). O primeiro documento coloca as seis áreas centrais para o governo aprimorar a cibersegurança e defender: segurança nacional, energia, bancos e finanças, saúde e segurança, comunicações e transporte. A estratégia do governo para segurança cibernética dessas áreas será melhor desenvolvida no documento *National Cyber Strategy* de 2018.

O NCS (2018) coloca que a visão estadunidense de um ambiente online seguro, aberto e que defenda as liberdades individuais, o livre mercado e a propriedade privada juntamente com a segurança dos cidadãos americanos foram ameaçadas por países como Rússia, Irã, Coreia do Norte e China. Segundo o documento esses países se aproveitam do ambiente aberto e anônimo da internet para promover ciberataques contra os Estados Unidos e outras nações aliadas. Assim, a administração de Trump se compromete a proteger o ciberespaço e garantir que os valores do país sejam respeitados. Para isso o documento divide as ações do governo em quatro pilares:

> • Defender a pátria protegendo as redes, sistemas, funções e dados; • Promover a prosperidade americana alimentando uma economia digital segura e próspera e promovendo uma forte inovação doméstica; • Preservar a paz e a segurança fortalecendo a capacidade dos Estados Unidos - em conjunto com aliados e parceiros - de dissuadir e, se necessário, punir aqueles que usam ferramentas cibernéticas para fins maliciosos; e • Expandir a influência americana no exterior para estender os princípios fundamentais de uma Internet aberta, interoperável, confiável e segura (ESTADOS UNIDOS DA AMÉRICA, 2018, p.1, tradução nossa).

Tabela 2 – Estratégia Cibernética Nacional: Ações do Governo Trump para Ciberespaço

Pilares	Ações
Defender a pátria protegendo as redes, sistemas, funções e dados	Proteger as redes e as informações federais; proteger as infraestruturas críticas; e combater os cibercrimes e melhorar as comunicações de incidentes
Promover a prosperidade americana	Promover uma economia digital resiliente, proteger invenções americanas e desenvolver uma mão-de-obra para a cibersegurança altamente capacitada.
Preservar a paz através da força	Melhorar a estabilidade cibernética do país e atribuir e impedir comportamentos considerados inaceitáveis no ciberespaço

Expandir a influência americana	Promover uma internet segura, interoperável, confiável e aberta e construir uma capacidade cibernética internacional

Para o primeiro pilar são colocados três focos de ação: proteger as redes e as informações federais; proteger as infraestruturas críticas; e combater os cibercrimes e melhorar as comunicações de incidentes. Ao trabalhar nessas áreas mencionadas o governo aumentará a resiliência e a segurança cibernética das redes e dos sistemas de informação do país (ESTADOS UNIDOS DA AMÉRICA, 2018).

Para se comprometer em garantir a segurança das redes e informações dos sistemas federais, a primeira medida a ser tomada é centralizar no DHS o gerenciamento e a supervisão da cibersegurança civil. A segunda medida é dar aos chefes de departamentos e de agências um papel mais ativo na aquisição e escolha de novas tecnologias para proteger as redes. O governo também se compromete a colocar os riscos da cadeia de produção dentro dos riscos a serem considerados pelas agências. Outra medida a ser implementada é aumentar a segurança das redes dos serviços contratados para evitar o vazamento de dados. Por fim, garantir a liderança do governo em inovações no setor da cibersegurança e garantir os investimentos federais nesse setor (ESTADOS UNIDOS DA AMÉRICA, 2018).

Em relação à proteção das infraestruturas críticas, a primeira medida a ser trabalhada pela administração é a redefinição de papéis e de responsabilidades. Isso significa que o governo de Donald Trump detalhará e especificará as funções e quais expectativas se tem tanto do setor privado quanto do público em relação à proteção da segurança das infraestruturas. A segunda medida é a priorização das seis áreas definidas na Estratégia de Defesa Nacional. Outra medida é aumentar o compartilhamento de informações com os provedores de tecnologia de informação e comunicação. O documento também coloca o incentivo a pesquisa e investimentos na área de cibersegurança, o aumento a segurança das redes marítimas de transporte, a proteção dos processos democráticos e a proteção de tecnologias de monitoramento do espaço, como satélites GPS e tecnologias de monitoramento do clima (ESTADOS UNIDOS DA AMÉRICA, 2018).

Por fim, para o terceiro ponto do pilar, combate ao cibercrime e melhorar a comunicação de incidente, as medidas a serem tomadas são incentivar a denúncia de invasões de ameaças as redes; modernizar a vigilância nas redes e as leis para cibercrimes; ajudar na criação de leis que

sejam capazes de combater cibercrimes em um ambiente transnacional; trabalhar com outros países aliados para a criação de uma prática internacional de combate a transgressões no universo online (ESTADOS UNIDOS DA AMÉRICA, 2018).

Passando para o segundo pilar, que diz respeito a promoção da prosperidade americana, o objetivo do governo é "Preservar a influência dos Estados Unidos no ambiente tecnológico e o desenvolvimento do ciberespaço como um motor aberto de crescimento econômico, inovação e eficiência" (ESTADOS UNIDOS DA AMÉRICA, 2018, p.14, tradução nossa). O documento coloca três pontos de ação que o governo deve tomar, promover uma economia digital resiliente, proteger invenções americanas e desenvolver uma mão-de-obra para a cibersegurança altamente capacitada.

Para garantir a prosperidade e a segurança da economia digital do país, a primeira medida a ser tomada é incentivar uma tecnologia adaptável e segura no mercado. Para tal, o governo deve trabalhar junto com atores públicos e privados, nacionais e internacionais, para promover a adoção de tecnologias seguras, a transparência das práticas de cibersegurança adotadas e a livre circulação de dados através das fronteiras. Outra providência a ser tomada é priorizar inovações, atualizando sempre os sistemas e redes do país para torná-los cada vez mais seguros. Além disso, o documento coloca que o país deve facilitar e investir no desenvolvimento das infraestruturas, principalmente em relação ao setor de telecomunicações, como no caso do 5G. Por fim, é necessário que o governo trabalhe para manter a liderança do país e seu poder de influência no ciberespaço (ESTADOS UNIDOS DA AMÉRICA, 2018).

Proteger as invenções e inovações dos Estados Unidos é uma das medidas necessárias para manter a liderança do país no ciberespaço. Para isso, o governo deve modernizar os mecanismos de revisão de investimentos e operações estrangeiros, protegendo principalmente as telecomunicações do país. O país deve, também, manter um sistema forte e seguro para proteção, confidencialidade e integridade de sua propriedade intelectual (ESTADOS UNIDOS DA AMÉRICA, 2018).

Para formar trabalhadores capazes de trabalhar com a estrutura cibernética do país e garantir sua segurança e integridade, o governo deve construir e investir em programas de desenvolvimento de talentos. Ademais, o governo deve expandir oportunidades educacionais para trabalhadores, aumentar o número de trabalhadores responsáveis pela cibersegurança nas agências federais e criar um sistema que destaque e recompense talentos (ESTADOS UNIDOS DA AMÉRICA, 2018).

Partindo para o terceiro pilar, preservar a paz através da força, o objetivo do governo é "identificar, combater, interromper, degradar e deter o comportamento no ciberespaço que seja desestabilizador e contrário aos interesses nacionais, preservando a liderança dos Estados Unidos no e através do ciberespaço." (ESTADOS UNIDOS DA AMÉRICA, 2018, p.20, tradução nossa). Para concretizar isso, dois grupos de ação são necessários, melhorar a estabilidade cibernética do país e atribuir e impedir comportamentos considerados inaceitáveis no ciberespaço.

Para o primeiro grupo, o país deve encorajar a adoção de normas de cibersegurança internacionalmente, contribuindo com a criação de um ciberespaço seguro, estável e seguro. Já para o segundo grupo, o país deve, através da Comunidade de Inteligência e da colaboração com outros governos, liderar o restante do mundo na identificação de atividades nocivas ao meio cibernético. O NCS coloca à importância de o país impor consequências àqueles que praticarem cibercrimes e contenha a disseminação de informações falsas. O documento coloca, por último, a criação de uma iniciativa de dissuasão cibernética com Estados aliados para manter a segurança do ambiente cibernético (ESTADOS UNIDOS DA AMÉRICA, 2018).

O último pilar, por fim, diz respeito a aumentar a influência americana. Seu objetivo é "Preservar a abertura, interoperabilidade, segurança e confiabilidade a longo prazo da Internet, que apoia e é reforçada pelos interesses dos Estados Unidos." (ESTADOS UNIDOS DA AMÉRICA, 2018, p.24, tradução nossa). Para isso o país deve promover uma internet segura, interoperável, confiável e aberta e construir uma capacidade cibernética internacional.

Para viabilizar tal coisa, o país deve defender e incentivar a liberdade com o respeito aos direitos humanos, às liberdades fundamentais e à privacidade. O governo deve, ainda, trabalhar com Estados aliados, a indústria, o setor privado e a academia para propiciar um ambiente cibernético aberto e seguro. O país deve, ainda, desenvolver e manter mercados para a tecnologia estadunidense no restante do mundo e incentivar a adoção de um modelo de governança da internet em que governos, o setor privado trabalhem juntos e a sociedade civil trabalhem juntos (ESTADOS UNIDOS DA AMÉRICA, 2018).

Para construir uma capacidade cibernética internacional o país trabalhará com outros governos para fortalecer a segurança e outras habilidades necessárias para um ciberespaço seguro. Essa colaboração internacional vale também para o campo da defesa a ataques terroristas e outros ciberataques, seja pelo compartilhamento de tecnologias e informações, seja pela criação de leis internacionais (ESTADOS UNIDOS DA AMÉRICA, 2018).

Além dos dois documentos mencionados, é importante destacar outras algumas ações implementadas pela administração de Donald Trump no campo da cibersegurança. A competição com a China pelo domínio da tecnologia 5G teve um papel bastante importante no mandato de Trump. O presidente atacava constantemente a China com alegações de roubo de dados, espionagem e roubo de propriedade intelectual. Trump, também criticava o controle chinês aos conteúdos que seus cidadãos podiam ou não acessar, dizendo que o país trabalhava contra a construção de uma internet aberta. Com essas acusações em mente e para combater os avanços do país asiático, uma das medidas tomadas foi a proibição da empresa chinesa, Huawei no país, pioneira na utilização da tecnologia 5G, a partir da acusação de espionagem comercial. O país também liderou campanhas diplomáticas e impôs sanções para barrar a expansão chinesa (FIDLER, 2020).

O presidente assinou o Ato que estabeleceu a Agência de Segurança Cibernética e de Infraestrutura (CISA) em 2018. A agência surgiu de uma divisão do DHS e foi transformada em agência para que melhor direcionar as ações de proteção às redes e infraestruturas críticas do país. A agência tem a função de proteger as redes e os sistemas de informação federal; coordenar os esforços nacionais para proteger e defender as infraestruturas críticas do país; fazer parcerias com outros agentes federais e civis, nacionais e internacionais; prestar assistência aos operadores das infraestruturas críticas; e realizar outros trabalhos de comunicação estipulados por leis (GAO, 2021). A agência começou a operar no início de 2019 e foi essencial para a segurança das eleições de 2020. Após perder as eleições que o levariam ao segundo mandato, Trump alegou fraude, o que foi negado pelos relatórios da Agência levando seu diretor, Chris Krebs, a ser demitido (MARKS, 2021).

No campo militar, o presidente buscou aumentar a capacidade cibernética de suas forças armadas. Para isso mudou o USCYBERCOM de um subcomando para um “Comando Combatente Unificado focado em operações no ciberespaço (THE WHITE HOUSE, 2017, tradução nossa). Além disso, a administração colaborou para tornar o Departamento de Defesa autoridade em operações cibernéticas militares junto com o Comando (FIDLER, 2020).

Juntamente com a elevação do USCYBERCOM, o presidente revisou algumas políticas criadas por Obama de modo a facilitar operações militares nas redes. A Diretiva de Política Presidencial 20 (PPD-20), que estabelecia diretrizes necessárias para que as forças armadas conduzissem operações no ciberespaço foi rescindida por Trump, dando maior autonomia ao

Comando. As operações do USCYBERCOM, a partir dessa decisão passam a ser baseadas nas decisões estratégicas do governo, sem a necessidade de aprovação para cada ação (CFR, 2018).

Ainda no campo militar, Trump, também, foi responsável por criar um Plano de Segurança Cibernética para a Marinha do país, em 2020, visando a proteção, em especial, do Sistema de Transporte Marítimo responsável por um quarto do PIB do país. O Plano segue as mesmas ações previstas na Estratégia Cibernética Nacional, de defesa do livre-mercado, parceria com o setor privado, construção de parâmetros de defesa das redes, entre outros mencionados no NCS. Seu objetivo é

> [..] unificar os recursos, as partes interessadas e as iniciativas de cibersegurança marítima, mitigando agressivamente as ameaças e vulnerabilidades do ciberespaço marítimo atuais e de curto prazo e complementa os sete planos de apoio da Estratégia Nacional para Segurança Marítima (ESTADOS UNIDOS DA AMÉRICA, 2020, p.1, tradução nossa).

No campo da colaboração internacional, o presidente assinou Acordo com o México e Canadá (USMCA) que, entre outras disposições, lida com o comércio digital entre os países. Através do acordo o presidente conseguiu melhorar o compartilhamento de dados digitais entre esses países. O acordo também coloca a cooperação dos países para fortalecer a segurança das redes responsáveis pelo comércio e o compartilhamento de informações sobre cibercrimes e outras informações pertinentes (ESTADOS UNIDOS DA AMÉRICA, 2020; FIDLER, 2020).

O governo de Donald Trump, dessa forma, trabalhou para aumentar a segurança das infraestruturas do país e o poder de defesa do país, além de trabalhar para manter o país uma liderança no campo cibernético. Tanto a Ordem Executiva 13800 quanto a Estratégia Cibernética Nacional tem o objetivo aumentar a resiliência das redes do país e construir uma política de cibersegurança robusta. A Ordem Executiva propôs uma revisão de toda a política cibernética da nação para que as devidas atualizações fossem feitas. A partir dessa, as principais infraestruturas cibernéticas que o país deve proteger são definidas – segurança nacional, energia, bancos e finanças, saúde e segurança, comunicações e transporte. A partir dessa avaliação o governo elabora a Estratégia Cibernética Nacional que traça planos de ação para assegurar a proteção dessas infraestruturas, o desenvolvimento e investimentos em novas tecnologias, aumentar o combate internacional a cibercrimes e expandir a influência dos Estados Unidos. Além desses documentos, o governo tomou outras medidas para garantir os objetivos mencionados, como o aumento da capacidade militar nas redes, com a elevação do USCYBERCOM e a criação do Plano de Segurança Cibernética para a Marinha. O conflito

com a China teve um papel central na administração, principalmente com a corrida para o 5G, que fez com que sanções fossem impostas à China e suas empresas de tecnologia. Por fim, no campo da colaboração internacional, o presidente trabalhou para a garantia do comércio digital seguro com o Acordo entre Estados Unidos, México e Canadá.

A seguir partiremos para as considerações finais com uma breve análise do que foi exposto.

4. CONSIDERAÇÕES FINAIS

Tendo feito a exposição de cada governo voltemos à pergunta feita no início do trabalho: quais são as semelhanças e diferenças entre a abordagem que as administrações de Barack Obama e de Donald Trump tiveram em relação a cibersegurança?

É possível analisar que a principal diferença se dá no foco que cada presidente deu na construção das políticas para a segurança cibernética. Enquanto Trump focou e promoveu principalmente em seus esforços de desenvolver a capacidade militar do país de conduzir operações cibernéticas, o foco de Obama foi a construção de uma base robusta para a política de cibersegurança estadunidense, a partir da elaboração de diretrizes e relatórios. Trump deu maior autonomia as forças armadas para operarem no ciberespaço, tornado o USCYBERCOM um comando unificado e criando um documento específico para proteger a segurança das redes da marinha do país. Além de enfatizar em seus discursos a necessidade de o país aumentar sua capacidade e defesa e ataque nas redes. No caso de Obama, por mais que houvesse a preocupação com a segurança das redes militares, o que levou a criação do Comando mencionado, e o governo tenha conduzido operações militares no ciberespaço, a questão não foi um foco de promoção da administração, que preferiu divulgar as questões relacionadas a cooperação internacional e ao desenvolvimento das políticas para o assunto.

É possível notar, também, que Trump retorna ao Departamento de Segurança Interna a função de coordenar as atividades de cibersegurança, que passa depois à CISA. O presidente dispensou a necessidade de um Coordenador de Cibersegurança em seu governo, cargo criado por Obama como forma de centralizar as operações sobre o tema e criar maior harmonia entre as políticas do governo. Além de tornar a resposta a incidentes mais rápida, visto que ele se reportaria diretamente ao presidente.

Passando para a consideração acerca das semelhanças entre os dois governantes, ambos operaram para construir suas políticas de maneira semelhante, realizando primeiro uma revisão da política existente e depois a elaboração de uma estratégia. Obama fez uma revisão de toda a política cibernética do país, o que resultou no *Cyberspace Policy Review* que apresenta as 24 medidas a serem implementadas pela administração e dá as principais áreas que o governo deve trabalhar. Trump fez o mesmo com a publicação da Ordem Executiva 13800 que, por sua vez, originou a Estratégia Cibernética Nacional, a qual destaca as principais áreas de defesa e as principais ações a serem implementadas em cada área.

Podemos destacar, além disso, que os documentos produzidos pelos dois governos têm o mesmo objetivo, a criação de um ambiente cibernético seguro, interoperável, confiável, que proteja a privacidade e as liberdades fundamentais e garanta o livre-comércio e o direito à propriedade. Os governos também destacam áreas semelhantes para atuação do governo, como a formação de uma mão-de-obra especializada; proteção da economia; proteção e o fortalecimento das infraestruturas críticas; combate a cibercrimes nacional e internacionalmente; e a cooperação com o setor privado para o desenvolvimento de melhores tecnologias e protocolos de segurança.

É possível notar semelhanças, ainda, na forma como os dois governos lidaram com os escândalos enfrentados e mencionados no trabalho. A resposta de Obama aos vazamentos feitos por Snowden pode ser vista como insatisfatória uma vez que o presidente falhou em criar mecanismos concretos de controle para a Comunidade de Inteligência do país. Trump, no que lhe concerne, falhou ao demorar a reconhecer as intervenções russas nas eleições de 2016 e relutar em impor sanções ao país, deixando a cargo das agências federais a criação de mecanismos que fortalecessem a infraestrutura cibernética nacional.

A questão da cooperação internacional também não apresenta grandes rupturas entre os governos, conforme apontado por Maier (2019). O governo Obama, por mais que exortasse a cooperação internacional e o multilateralismo, teve posicionamentos unilaterais, os quais podem ser observados na forma como o governo desenvolveu sua Comunidade de Inteligência e promoveu a espionagem desenfreada de diversas pessoas e governos. No caso de Trump, por mais que sua postura tenha sito majoritariamente unilateral, ele, ainda assim, firmou o Acordo entre os Estados Unidos, México e Canadá, que trata do compartilhamento de dados entre os países, e colocou a colaboração internacional como um dos pontos de sua estratégia.

Assim, embora os dois presidentes possuam algumas diferenças entre suas políticas, ambos têm o objetivo de proteger e manter a liderança do país no campo cibernético. Obama desenvolve o *Cyberspace Policy Review* para destacar as principais medidas a serem tomadas por sua administração, a Estratégia Internacional para o Ciberespaço para direcionar as parcerias a serem firmadas e colocar o país nas discussões sobre o tema e o CNAP para fazer com que os investimentos na área sejam enquadrados como prioridade no próximo governo. Contudo, apesar de sua contribuição, o ex-presidente enfrentou a falta de confiança nacional e internacionalmente após as revelações de Edward Snowden. Já Trump desenvolve tanto a EO 13800 quanto a Estratégia Cibernética Nacional para elaborar um plano de ação para cada área

destacada como prioridade. O 45º presidente reforça, também, a capacidade militar de operar nas redes e toma medidas para tentar barrar o crescimento chinês. Apesar disso o presidente falhou em reconhecer e agir contra a interferência russa no pleito de 2016.

APÊNDICE A - LINHA DO TEMPO GOVERNO OBAMA



APÊNDICE B - LINHA DO TEMPO GOVERNO TRUMP



REFERÊNCIAS BIBLIOGRÁFICAS

AVAST ACADEMY TEAM. **Botnet**. [*S.l.*], 2016. Disponível em: https://www.avast.com/pt-br/c-botnet#gref. Acesso em: 21 jan. 2022.

BLACKWILL, Robert D.; GORDON, Philip H. **Containing Russia**: how to respond to Moscow's intervention in U.S. democracy and growing geopolitical challenge. *[S.l]*, Council on Foreign Relations Press, 2018. 56 p. Disponível em: https://www.cfr.org/report/containing-russia. Acesso em: 04 jan. 2022.

CARR, Madeline. Public-private partnerships in national cyber-security strategies. **International Affairs**, *[S.l.]*, v. 92, n. 1, p. 43-62, jan. 2016. Oxford University Press (OUP). http://dx.doi.org/10.1111/1468-2346.12504.

China's Great Firewall. 2011. Disponível em: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html. Acesso em: 11 nov. 2021.

CONSIL ON FOREIN RELARIONS (CFR). **What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?** *[S.l.]*, 2018. Disponível em: https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations. Acesso em: 10 fev. 2022.

CYBERSECURITY AND INFRAESTRUCTURE SECURITY AGENCY (CISA). **What is Cybersecurity?** *[S.l.]*, 2019. Disponível em: https://www.cisa.gov/uscert/ncas/tips/ST04-001. Acesso em: 07 fev. 2022.

DEPARTMENT OF DEFENSE. **U. S. Cyber Command**. Washington, DC, EUA, 2010. Disponível em: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf. Acesso em: 31 out. 2021.

DEPARTMENT OF HOMELAND SECURITY. **Election Security**. EUA, 2021. Disponível em: https://www.dhs.gov/topic/election-security. Acesso em: 14 jan. 2022.

ESTADOS UNIDOS DA AMÉRICA **Foreign Intelligence Surveilance Act**. Washington, 1978, 95th Congress, Public Law No. 95-511, 92 Stat. 1783.

ESTADOS UNIDOS DA AMÉRICA. **Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text**. 2020. Disponível em: https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between. Acesso em: 24 jan. 2022.

ESTADOS UNIDOS DA AMÉRICA. **CYBERSPACE POLICY REVIEW**: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington, Executive Office of the President of the U.S, 2009. Disponível em: https://irp.fas.org/eprint/cyber-review.pdf. Acesso em: 31 de agosto de 2021.

ESTADOS UNIDOS DA AMÉRICA. **EXECUTIVE ORDER 13.800** - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Estados Unidos, 2017.

Disponível em: https://trumpwhitehouse.archives.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure/.Acesso em: 02 nov. 2021

ESTADOS UNIDOS DA AMÉRICA. **FACT SHEET**: Cybersecurity National Action Plan. The White House, Office of the Press Secretary, 2016. Disponível em: https://obamawhitehouse.archives.gov/the-pressoffice/2016/02/09/fact-sheet-cybersecurity-national-action-plan. Acesso em: 31 out. 2021.

ESTADOS UNIDOS DA AMÉRICA. **INTERNATIONAL STRATEGY FOR CYBERSPACE**: Prosperity, Security and Openness in a Networked World. Washington, Executive Office of the President of the U. S., National Security Council, 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_vie wer/international_strategy_for_cyberspace.pdf. Acesso em: 31 out. 2021.

ESTADOS UNIDOS DA AMÉRICA. **NATIONAL CYBER STRATEGY**: of the United States of America. Washington, 2018. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso: 08 fev. 2022

ESTADOS UNIDOS DA AMÉRICA. **NATIONAL MARITIME CYBERSECURITY PLAN**: to the National Strategy for Maritime Security. Washington, 2020. Disponível em: https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-regarding-national-maritime-cybersecurity-plan/#:~:text=President%20Trump%20has%20released%20the,sector%2C%20promoting%20prosperity%20through%20information. Acesso em: 08 fev. 2022.

ESTADOS UNIDOS DA AMÉRICA. **NATIONAL SECURITY STRATEGY**: of the United States of America. Washington, 2017. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf. Acesso em: 17 jan. 2022.

FIDLER, David P. **PRESIDENT TRUMP'S LEGACY ON CYBERSPACE POLICY**. *[S.l.]*, 2020. Disponível em: https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy. Acesso em: 24 jan. 2022.

GIBSON, G. **TRUMP CALLS OBAMA, CLINTON ISLAMIC STATE "CO-FOUNDERS," DRAWS REBUKE**. *[S.l.]*, 2016. Disponível em: https://www.reuters.com/article/us-usa-election-trump-idUSKCN10M146. Acesso em: 11 jan. 2022.

GOVERNMENT ACCOUNTABILITY OFFICE (GAO). **Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed**. Estados Unidos, 2010. Disponível em: https://www.gao.gov/assets/gao-11-24.pdf. Acesso em: 30 set. 2021.

GOVERNMENT ACCOUNTABILITY OFFICE (GAO). **CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY:** Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation. Estados Unidos, 2021. Disponível em: https://www.gao.gov/products/gao-21-236. Acesso em: 4 fev. 2022.

GREENWALD, Eric A.. History Repeats Itself: the 60-day cyberspace policy review in context. **Journal Of National Security Law & Policy**, *[S.l]*, v. 4, n. 1, p. 41-60, 13 ago. 2010.

GREENWALD, Glenn. **NO PLACE TO HIDE**: Edward Snowden, the NSA and the Suveillance State. London: Penguin, 2014.

HARKNETT, Richard J.; A STEVER, James. The Cybersecurity Triad: government, private sector partners, and the engaged cybersecurity citizen. **Journal Of Homeland Security and Emergency Management**, *[S.l.]*, v. 6, n. 1, p. 1-14, 30 jan. 2009. Walter de Gruyter GmbH. http://dx.doi.org/10.2202/1547-7355.1649.

JENSEN, Eric Talbot. President Obama and the changing cyber paradigm. **Admin. & Reg. L. News**. *[S.l.]*, v. 37, p. 3, 2011.

KHURSHUDYAN, I. **Putin denies meddling in U.S. elections**. *[S.l.]*, 2020. Disponível em: https://www.inquirer.com/news/nation-world/vladimir-putin-election-united-states-interference-denial-20201217.html. Acesso em: 03 jan. 2022.

LILLI, Eugenio. President Obama and US cyber security policy. **Journal Of Cyber Policy**, *[S.l.]*, v. 5, n. 2, p. 265-284, 3 maio 2020. Informa UK Limited. http://dx.doi.org/10.1080/23738871.2020.1778759.

LYNN III, William J. Defending a New Domain: the pentagon's cyberstrategy. **Foreign Affairs**, *[S. L.]*, v. 89, n. 5, p. 97-108, set. 2010. Disponível em: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. Acesso em: 02 nov. 2021.

MAIER, F. DE OBAMA A TRUMP: O Contínuo da Política Cibernética Estadunidense. **Caderno de Relações Internacionais**, *[S. l.]*, v. 10, n. 18, 2019. DOI: 10.22293/2179-1376.v10i18.1034. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/relacoesinternacionais/article/view/1034. Acesso em: 31 ago. 2021.

MARGULIES, Peter. Global Cybersecurity, Surveillance, and Privacy: the Obama administration's conflicted legacy. **Indiana Journal of Global Legal Studies**, *[S.l.]*, v. 24, n. 2, p. 459, 2017. Indiana University Press. http://dx.doi.org/10.2979/indjglolegstu.24.2.0459. Disponível em: www.jstor.org/stable/10.2979/indjglolegstu.24.2.0459. Acesso em: 31 agosto 2021.

MARKS, Joseph. **It's been one year since Trump fired the CISA director**. *[S.l]*, 2021. Disponível em: https://www.washingtonpost.com/politics/2021/11/17/it-been-one-year-since-trump-fired-cisa-director/. Acesso em: 10 fev. 2022.

MCCOMBIE, Stephen; UHLMANN, Allon J.; MORRISON, Sarah. The US 2016 presidential election & Russia's troll farms. **Intelligence And National Security**, [S.L.], v. 35, n. 1, p. 95-114, 13 out. 2019. Informa UK Limited. http://dx.doi.org/10.1080/02684527.2019.1673940. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/02684527.2019.1673940. Acesso em: 04 jan. 2022.

MUELLER III, Robert. (2019). “Report on the Investigation into Russian Interference in the 2016 Presidential Election”. Department of Justice of the United States of America. Disponível em: https://www.justice.gov/storage/report.pdf. Acesso em: 10 dez. 2021.

NATIONAL SCIENCE AND TECHNOLOGY COUNSIL. **TRUSTWORTHY CYBERSPACE**: strategic plan for the federal cybersecurity research and development program. Estados Unidos, Executive Office of the President, 2011. Disponível em: https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf. Acesso em: 02 nov. 2021.

NEWHOUSE, William; KEITH, Stephanie; SCRIBNER, Benjamin; WITTE, Greg. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. **National Institute of Standards and Technology**, *[S.l.]*, 1-144, 7 ago. 2017. National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.800-181.

PECEQUILO, C. S. **A política externa de Trump e a Cooperação Sul-Sul**: impactos e potencialidades. Pontes, v. 13, n. 6, p. 12–15, 2017.

SANTOS, Phillipe Dautro dos. **Ciberespaço como domínio de operações militares**: a perspectiva dos Estados Unidos da América. Paraíba, 2018. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/12670/1/PDS14122018.pdf. Acesso em 02 nov. 2021.

SCHLEIFER, T. **DNC’s treatment of Sanders at issue in leaked emails**. *[S.l.]*, 2016. Disponível em: https://edition.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/index.html. Acesso em: 11 jan. 2022.

SQUADRANS, Lyvia Spregacinere. **O Estado de Vigilância de Exceção dos Estados Unidos: a espionagem aos aliados**. Coimbra, 2017. Tese de Doutorado. Universidade de Coimbra. Disponível em: https://estudogeral.sib.uc.pt/bitstream/10316/82464/1/MRI_LyviaSquadrans_Dissertacao%20Final.pdf. Acesso em: 12 set. 2021.

THE WHITE HOUSE. **Presidential Policy Directive 28 (PPD-28).** Signals Intelligence Activities. Estados Unidos da América, 2014. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. Acesso em: 8 out. 2021.

THE WHITE HOUSE. **Presidential Memorandum for the Secretary of Defense**. Office of the Press Secretary, Washington, 18 agosto 2017. Disponível em: https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/. Acesso em: 15 jan. 2022.

THIELMAN, S. **FBI and Homeland Security detail Russian hacking campaign in new report**. *[S.l.]* 2016. Disponível em: https://www.theguardian.com/technology/2016/dec/29/fbi-dhs-russian-hacking-report. Acesso em: 12 jan. 2022.

TIME. **Here Are All of the Indictments, Guilty Pleas and Convictions from Robert Mueller's Investigation**. *[S.l.]* 2019. Disponível em: https://time.com/5556331/mueller-investigation-indictments-guilty-pleas/. Acesso em: 15 jan. 2022.

VAGOUN, Tomas; STRAWN, George O. Implementing the Federal Cybersecurity R&D Strategy. **Computer**, *[S.l.]*, v. 48, n. 4, p. 45-55, abr. 2015. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mc.2015.111.

WORLD SUMMIT ON THE INFORMATION SOCIETY(WSIS). **Tunis Agenda for the Information Society.** Tunísia, 2005. Disponível em: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.pdf. Acesso em: 14 dez. 2010.