UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

VICTOR HUGO GRATÃO DE LIMA

UMA INVESTIGAÇÃO SOBRE CAPACIDADES CIBERNÉTICAS E PROJEÇÃO DE PODER DOS ESTADOS UNIDOS DA AMÉRICA ENTRE OS ANOS DE 2010-2020

BRASÍLIA
2024

VICTOR HUGO GRATÃO DE LIMA

Uma Investigação Sobre Capacidades Cibernéticas e Projeção de Poder dos Estados Unidos da América Entre os Anos de 2010-2020

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais da Universidade de Brasília como requisito para obtenção do grau de mestre em Relações Internacionais.

Área de Concentração: Interconexões Globais, Assimetrias e Conflitos.

Orientador: Prof. Dr. Antonio Jorge Ramalho da Rocha.

Brasília, 2024

“Uma pena não é mais poderosa do que uma espada, e uma espada não é mais poderosa do que uma pena. Penas não lutam, nem espadas fazem poesia. Poderosa é a mão que sabe quando pegar a pena, ou a espada.”
Wiegraf Folles - *Final Fantasy Tactics.*

AGRADECIMENTOS

Eu sou um resultado de ações e esforços coletivos. Logo, é de extrema importância que eu prestigie e agradeça a todos aqueles que me ajudaram a alcançar este espaço, me permitindo chegar até esse ponto.

Primeiramente, gostaria de agradecer a Deus por me auxiliar em todos os passos dessa trajetória acadêmica, por estar ao meu lado, por me iluminar e me guiar em encontro a pessoas magníficas que contribuíram enormemente na produção desta dissertação.

Em segundo lugar gostaria de agradecer a duas pessoas que permitiram o início dessa jornada. Uma delas é a minha mãe, Ludimila de Oliveira Gratão, que esteve comigo em todos os momentos me apoiando e orando por mim, me mostrando que a educação edifica e transforma, e que me incentivou a persistir na busca por um mestrado, me levando a esta ocasião. Outra pessoa é o meu mentor, Felipe Dalcin Silva, da Universidade Federal do Rio Grande do Sul (UFRGS). Agradeço o seu "eu acho que isso vai dar certo, estarei do seu lado te ajudando" que me inspirou a escrever um pré-projeto para o programa de pós-graduação na Universidade de Brasília. Sem seu encorajamento e auxílio, eu não estaria aqui.

Reconheço, estimo e agradeço meu orientador, o professor Antonio Jorge Ramalho da Rocha, na realização desta pesquisa. Desde o primeiro momento que aceitou meu projeto de pesquisa, muito obrigado por ler e reler, com carinho e atenção, todas minhas epifanias e tentativas de tema, além de indicar em nossas reuniões, com todo o profissionalismo e gentileza, as melhores correções e os melhores caminhos temáticos de escrita. O senhor permitiu, através de sua confiança em mim, que eu desenvolvesse e refinasse um tema e um argumento de pesquisa cada vez mais objetivo e interessante, aumentando meu afeto ao estudo de *cyber* segurança.

Sou grato à minha família, em especial minha avó Maria Natividade Gratão, minha irmã Caroline Gratão de Lima e ao meu cunhado Cássio dos Reis Lopes de Sousa, por orarem por mim, me apoiarem, e me ajudarem em etapas complicadas na pesquisa. Não posso deixar de expressar minha gratidão aos meus animais de estimação, em particular minha gata Mimi, que foi meu suporte emocional durante a escrita da dissertação e minha plateia deslumbrada em todos meus ensaios. Por isso e muito mais, aprecio o amor incondicional inerente a esses pequenos seres.

Agradeço também aos meus amigos que deixaram toda essa jornada mais leve. Fico feliz por me mostrarem que uma parte importante no desenvolvimento de uma pesquisa consiste em poder descansar e estar rodeado de pessoas que me fazem bem. Valorizo especialmente a

presença dos meus melhores amigos Anna Caroline Viana, Igor Holanda, Rodrigo Cota, Guilherme Fatel, Aline Vivas e João Henrique Lima por ouvirem todas minhas ideias malucas e meus conceitos temáticos, por me aconselharem em momentos importantes, por me incentivarem e serem uma rede de apoio crucial para mim, por estarem presentes e se divertirem ao meu lado quando eu mais precisei. Vocês são muito importantes para mim, e as ajudas que me forneceram nunca iriam passar despercebido, então com toda a certeza vocês merecem um lugar nesta seção e em meu coração. Sou eternamente grato por ter vocês em minha vida e ao meu lado.

Por fim, sou grato ao Programa de Pós-Graduação de Relações Internacionais da Universidade de Brasília, principalmente as funcionárias da secretaria Vanessa Bottazzini Tavares e Caroline Souto de Morais por dedicarem uma parte de seu tempo me auxiliando com burocracias, pelos professores e colegas que me ensinaram e ampliaram minha visão de mundo, em principal o Prof. Dr. Juliano da Silva Cortinhas e o colega Eduardo Izycki em me motivarem e me ajudarem a fazer um trabalho cada vez melhor.

Aos outros que também tiveram uma importância para a construção desta dissertação, deixo meu muito obrigado!

RESUMO

O espaço cibernético, devido às métricas de desenvolvimento acelerado inerentes à sua construção, permitiu a realização de diversas ações dos atores do Sistema Internacional (SI), amplificadas no final da década de 2010. Esse entendimento afetou e ainda afeta a compreensão, as possibilidades e os atos dos agentes nesse âmbito, que podem recorrer a oportunidades operacionais ou capacitivas com um viés de poder, seja esse tradicional, cinético ou cibernético. Com isso, esta dissertação se focará em investigar como um Estado em particular, os Estados Unidos da América (EUA), conseguiram se utilizar de suas capacidades cibernéticas - ofensivas e defensivas - em prol de conquistar e irradiar poder em um âmbito teórico específico: o Sistema Internacional Cibernético. Serão delimitados como recorte temporal os anos entre 2010 a 2020, conjuntamente com atos cibernéticos realizados a agentes denominados pelos EUA como como aliados - Países Baixos, Reino Unido, Estônia e Índia - ou oponentes - China, Rússia, Irã e Coreia do Norte. Dessa forma, a presente pesquisa realizará um estudo de caso qualitativo aprofundado de apresentação, evolução e consequências das principais ocorrências ofensivas e defensivas presentes nesse período. Para alcançar tal objetivo, foram utilizadas bases de dados qualitativas e quantitativas, fontes primárias e secundárias e do referencial conceitual *S.A.M.* de Kremer e Müller (2013) em conjunto com as teorias de Relações Internacionais acerca do poder e do tema cibernético. Dito isso, foi aplicado um modelo de raciocínio hipotético-dedutivo que avaliou a ampliação deliberada das capacidades cibernéticas dos Estados Unidos em prol de projetar poder, sendo realizado principalmente contra os Estados caracterizados como oponentes.

Palavras-chave: Cyber Segurança; Capacidades Cibernéticas; Estados Unidos da América; Poder Cibernético.

ABSTRACT

The cyberspace, due to the accelerated development metrics inherent in its construction, has enabled the realization of various actions by actors within the International System (IS), actions which were amplified by the end of the 2010s. This understanding has affected, and continues to affect, the comprehension, possibilities, and actions of agents in this realm, who may take advantage of operational or capacitive opportunities with a power bias, whether traditional, kinetic, or cybernetic. Therefore, this dissertation will focus on investigating how a particular state, the United States of America (USA), has been able to leverage its cyber capabilities — both offensive and defensive — in order to gain and project power within a specific theoretical domain: the Cybernetic International System. The temporal scope will be delimited to the years between 2010 and 2020, along with cyber actions carried out against agents designated by the U.S. as allies — The Netherlands, the United Kingdom, Estonia, and India — or adversaries — China, Russia, Iran, and North Korea. Thus, this research will conduct an in-depth qualitative case study, presenting, evolving, and analyzing the consequences of the main offensive and defensive occurrences during this period. To achieve this goal, qualitative and quantitative databases, primary and secondary sources, and the conceptual framework of S.A.M. by Kremer and Müller (2013) will be used, in conjunction with International Relations theories on power and cybernetic themes. With this approach, a hypothetical-deductive reasoning model was applied, evaluating the deliberate expansion of U.S. cyber capabilities in order to project power, primarily against states characterized as adversaries.

Keywords: *Cybersecurity; Cyber Capabilities; United States of America; Cyber Power.*

LISTA DE SIGLAS

APEC - *Asia-Pacific Economic Cooperation*
APT - *Advanced and Persistent Threat*
ARPANET - *Advanced Research and Projects Agency' Network*
ARPEL - *Regional Association of Oil, Gas, and Biofuels Sector Companies in Latin America and the Caribbean*
C&C - *Server of Command and Control* (Servidor de Comando e Controle)
CCD COE - *Cooperative Cyber Defense Center of Excellence*
CDMB - *Cyber Defense Management Board*
CERT - *Computer Emergency Response Team*
CFR - *Council on Foreign Relations*
CISA - *Cybersecurity and Infrastructure Security Agency*
CMF - *US military's Cyber Mission Force*
COT - *Cyber Operations Tracker*
CTIIC - *Cyber Threat Intelligence Integration Center*
DDoS - *Distributed Denial of Service*
DHS - *U.S. Department of Homeland Security*
DICA - Direito Internacional dos Conflitos Armados
DNC - *Democratic National Convention*
DNI - *Office of Director of National Intelligence*
DNS - *Domain Name System*
DoD - Departamento de Defesa dos Estados Unidos da América
GGE - *United Nations Groups of Governmental Experts*
ICS - *Industrial Control Systems*
IP - *Internet Protocol*
IRA - *Internet Research Agency*
ISIS - Estado Islâmico
MoU - *Memorandum of Understanding*
NASA - *National Aeronautics and Space Administration*
NDAA - *National Defense Authorization Act*
NSA - *National Security Agency*
OEA - Organização de Estados Americanos
OEWG - *United Nations' Open-Ended Working Group*

ONU - Organização das Nações Unidas

OTAN - Organização do Tratado do Atlântico Norte

P&D – Pesquisa e Desenvolvimento

PCS - Programa de Cooperação de Segurança

PLA - Exército de Libertação Popular da China

PLC - *Programmable Logic Controllers*

S.A.M. - *Stakeholders, Actions and Motives*

SCADA - *Supervisory Control and Data Acquisition*

TCBM - *Transparency and Confidence-building Measures*

TUBITAK - Conselho de Pesquisa Tecnológica e Científica da Turquia

UE - União Européia

USAID - *United States Agency of International Development*

USCYBERCOM - Comando Cibernético dos Estados Unidos da América

USIS - *U.S Investigations Services*

VPN - *Virtual Private Network*

WWW - *World Wide Web*

SUMÁRIO

INTRODUÇÃO

Perspectivas Históricas e Escopos Analíticos da Dissertação

O espaço cibernético marcou as relações internacionais e as temáticas no mundo contemporâneo. Por ser produto do pensamento humano, o ciberespaço, iniciado na metade do século XX, criou conjunturas históricas, políticas e econômicas, além de ser formado e incrementado por elas. A partir desse pensamento, o estudo de cibersegurança surge com o objetivo de conferir ampla visibilidade à evolução das interações dos atores do sistema internacional (SI) (Ayres Pinto, 2017, p. 03). Os principais agentes dessa afirmação são os Estados nacionais, setor privado, organizações internacionais (OIs) e indivíduos.

Contudo, a partir dos três grandes casos de cibersegurança presentes no início da década de 2000, a percepção geral sobre o tema cibernético ganhou destaque emergencial. Tais ocorrências, via Gratão (2022, p. 03), são apresentadas nos seguintes casos: (1) Estônia, de 2007, com o uso das capacidades cibernéticas como forma de retaliação de temas históricos e culturais; (2) Geórgia, de 2008, pela utilização do poder cibernético em situações cinéticas - físicas; e (3) *Stuxnet*, de 2010, com o emprego das competências de âmbito cibernético como forma de enfrentamento entre Estados. Esses incidentes mudaram o entendimento dos agentes do SI não só por conseguirem aumentar a escala vista em ciberataques, mas por mudar a forma como os agentes maliciosos são vistos no Sistema Internacional Cibernético.

O "Sistema Internacional Cibernético", para os fins desta dissertação, é um conceito formado a partir da inferência proposta por Nye (2010, p. 19), que assume o encontro do espaço cibernético metafísico com os aparatos de comunicação, como redes de *internet*, *intranet*, fibra óptica, satélites, tecnologias de celular, de computador e comunicações entre servidores, em uma tipificação de localidade geográfica definida. De acordo com essa dedução, o espaço cibernético proposto hipotéticamente passa a ter parâmetros territoriais de existência,com substância geográfica, mais especificamente, locais de atuação e posse dos dados de seus usuários.

Isso permite uma interpolação do SI salientada nos estudos das Relações Internacionais, garantindo territorialidade, relações, interações e invasões palpáveis entre atores do Si em um ambiente novo, noção explorada mais a fundo no capítulo 1.

A questão dos agentes maliciosos se transforma no período supracitado, visto que, anteriormente, tais agentes eram definidos apenas como civis (*hackers*) ou grupos de civis, que, por uma variedade de motivos, atacavam usuários e até mesmo sistemas no âmbito cibernético. Todavia, ao perceber que os agentes maliciosos vinculados aos casos apresentados acima são Estados nacionais, a situação se altera.

Isso acontece porque, ao levar em consideração o nível de investimentos em Pesquisa e Desenvolvimento e o poder da tecnologia estatal, uma nova capacidade de destruição pode ser vista nas infraestruturas críticas de outros Estados ou de outros atores do SI (Gratão, 2022. p. 03). A partir de 2010, os atores do SI, em especial as lideranças dos Estados e de seus órgãos públicos, ao perceberem comprovadamente a existência e a atuação estratégica de outros Estados no espaço cibernético e ficarem apreensivos ante a isso, começaram a investir e a aprimorar suas capacidades ofensivas, propagando poder no espaço cibernético a fim de garantir sua própria segurança.

Contudo, tal deslocamento, baseado nos escritos de Valeriano e Maness (2015, p. 21), criou um estado dicotômico no âmbito cibernético, estabelecido mediante a noção de que, por meio da irradiação de poder com um caráter puramente agressivo, o Estado perpetuador obtém uma espécie de segurança individualizada no SI. Ao realizarem tais atos, o contexto de segurança de outros atores fica desestruturado, estimulando esses atores a buscar formas ofensivas no contexto cibernético, garantindo para si uma segurança individual e minando ainda mais a segurança dos atores restantes do SI.

É caracterizada, aqui, a noção do dilema de segurança (Jervis, 1978, p. 169). O ciberespaço passa a ser visto como um domínio conflituoso, governado pelo medo e pela insegurança (Valeriano e Maness, 2015. p. 21), gerando movimentações analíticas abrangentes e cada vez mais importantes ao tópico cibernético.

Nesse contexto, esta dissertação tem como objetivo geral explorar como os Estados conseguem conquistar e irradiar poder no Sistema Internacional Cibernético, a partir da construção e utilização de suas capacidades cibernéticas ofensivas e defensivas. Estuda-se o caso dos Estados Unidos da América (EUA), potência cibernética, explorando a evolução e o emprego de suas capacidades cibernéticas como ferramentas de projeção de poder internacional em um período de 11 anos: entre 2010 e 2020.

O recorte temporal foi escolhido face à necessidade de estabelecer uma década de estudo sobre os Estados Unidos em um tema específico – cibernético –, iniciado a partir do conhecimento e da divulgação do caso *Stuxnet* no mundo, em 2010, e finalizado no

cumprimento da administração de Donald Trump, em 2020. Isso confere à pesquisa um senso de dinamismo e de comparação entre dois governos distintos sobre a temática de cibersegurança, amplificando o estudo proposto.

Esta dissertação realizará um estudo de caso qualitativo aprofundado no desenvolvimento e apresentação de casos estadunidenses cibernéticos contra atores percebidos como aliados - Países Baixos, Reino Unido, Estônia e Índia - e oponentes - China, Rússia, Irã e Coreia do Norte - aos EUA. A escolha desses países deu-se mediante a comprovação, tanto pelos trabalhos de CFR (2024) e de Hitchens e Goren (2017), de que tais Estados foram os que interagiram com maior frequência com os Estados Unidos em âmbitos ofensivos ou defensivos nesses 11 anos.

No que tange aos países vistos como oponentes dos EUA no contexto ofensivo, a seleção fundamentou-se na *Cyber Operations Tracker* (COT), do *Council on Foreign Relations* (CFR), estabelecida em CFR (2024), que indica ciberataques realizados e de autoria comprovadamente estatal. O conceito de ciberataque utilizado nesta dissertação segue as prerrogativas do texto de Brasil (2023, p. 11), em conjunto com CFR (2024), para quem um ataque cibernético é uma ação maliciosa sobre dispositivos, redes, sistemas, dados e comunicações de um ator com o objetivo de ocasionar efeitos cibernéticos ou cinéticos de degradação, destruição, corrupção, negação, roubo, manipulação ou interrupção de informações ou serviços de outro ator no SI.

O CFR (2024) indica a presença de 150 ataques totais realizados contra os EUA entre 2010 a 2020, sendo 132 efetuados pelos quatro Estados-oponentes. A partir desses dados, atribuem-se à China 59 ataques cibernéticos, à Rússia, 27, ao Irã, 31 e à Coreia do Norte, 15.

Já os países vistos como aliados no campo defensivo foram escolhidos com base nos escritos de Hitchens e Goren (2017) e fontes primárias acerca da produção e assinatura de acordos bilaterais ou multilaterais. Entre as 53 convenções realizadas no recorte temporal, os principais Estados que interagiram ou agiram conjuntamente em um caráter normativo com os EUA foram os Países Baixos, com 26 acordos temáticos assinados, o Reino Unido com 26, a Estônia com 24 e a Índia com 6 subscrições.

Uma vez propostas as principais seleções realizadas acerca dos países ponderados, a pesquisa analisará como os EUA perceberam e incorporaram suas capacidades ofensivas, aqui dispostas como estratégias públicas domésticas e internacionais de segurança e defesa, e os casos de matriz cibernética internacional dispostos na COT pelo CFR (2024). Já as capacidades defensivas serão percebidas na forma dos esforços domésticos para o aprimoramento de seus

sistemas defensivos e de tentar consolidar um contexto legislativo e cooperativo internacional de segurança cibernética.

Os casos e atos cibernéticos estadunidenses ofensivos e defensivos serão retratados anualmente, de forma a apresentar os desenvolvimentos e as principais utilizações das tipologias ofensivas e defensivas estadunidenses contra os Estados postos como aliados e oponentes nos 11 anos pesquisados. Através dessa escolha, a pesquisa poderá explorar as possíveis alterações, fomentos e contenções existentes nas capacidades cibernéticas estadunidenses estudadas no espectro temporal selecionado, estimando padrões.

Essa estrutura tentará responder ao seguinte problema de pesquisa: em que medida a aplicação das capacidades cibernéticas - ofensivas e defensivas - afetou a projeção e manutenção de poder dos Estados Unidos contra os atores percebidos como aliados e oponentes entre os anos 2010 e 2020? A hipótese geral (HG) selecionada para responder a tal questionamento afirma que os EUA, entre 2010 e 2020, ampliaram deliberadamente suas capacidades cibernéticas visando projetar poder no SI, principalmente por meio de intervenções no espaço cibernético doméstico de outros Estados nacionais, tendo como foco os atores tidos como seus oponentes.

A partir dessa hipótese geral, foram constituídas três hipóteses secundárias (HS) que estabelecem uma operacionalização mais específica das principais variáveis dispostas na HG, permitindo que o estudo posterior na pesquisa comprove os graus de validação na hipótese. São elas:

HS1 – Os Estados Unidos aumentaram seus níveis de capacidade cibernética através da ampliação, crescente e progressiva, qualitativa e quantitativa, de seus orçamentos e de seus atos ofensivos e defensivos entre 2010 a 2020.

HS2 – Os atos Estados Unidos tiveram como objetivo central a projeção de poder, sendo este realizado principalmente por meio de ataques cibernéticos ofensivos, que visavam intervir no espaço cibernético doméstico de suas vítimas, gerando níveis de dano diversos.

HS3 – O foco das ações ofensivas realizadas pelos Estados Unidos recaiu, principal e exclusivamente, nos quatro Estados postos como oponentes aos Estados Unidos: China, Rússia, Irã e Coreia do Norte.

Logo, as hipóteses serão verificadas mediante identificação e comparação das capacidades cibernéticas ofensivas e defensivas estadunidenses presentes no período proposto. Com isso, será possível salientar - ou não - os níveis de fomento das capacidades dos EUA,

elencando os elementos de ação preponderantes efetuados, para, assim, aceitar ou refutar a hipótese apresentada.

A fim de possibilitar tal estudo, será utilizado o referencial conceitual cibernético *S.A.M. - Stakeholders, Actions and Motives* – Partes Interessadas, Ações e Motivos, em inglês – de Kremer e Müller (2013), em conjunto com as propostas temáticas presentes no estudo de Relações Internacionais (RI) voltadas à temática de construção e projeção de poder em um contexto de *cyber* segurança. Esse referencial analisará dados dispostos no COT (CFR, 2024), nos escritos de Hitchens e Goren (2017) e nas fontes primárias acerca da produção e da assinatura de acordos bilaterais ou multilaterais defensivos durante os 11 anos selecionados.

Uma vez realizada uma comparação gradativa dos dados e casos ofensivos e defensivos designados, o estudo determinará se os atos e os resultados do uso das capacidades estadunidenses alcançaram o objetivo de agregar e aumentar o poder dos EUA no Sistema Internacional Cibernético em relação aos seus aliados e oponentes. Sendo assim, os resultados obtidos destacarão o nível e a natureza da movimentação cibernética estadunidense ofensiva e defensiva para com os Países Baixos, Reino Unido, Estônia, Índia, China, Rússia, Irã e Coreia do Norte, atestando ou não veracidade da hipótese indicada, ponto salientado na utilização do método hipotético-dedutivo por esta dissertação.

Apresentado nos escritos de Prodanov e Freitas (2013, p. 31-34), o modelo hipotético-dedutivo estipula um parâmetro referente a um fenômeno, que pode ou não ser falseado como conhecimento científico ao analisá-lo a partir da formulação de uma hipótese. A tentativa de refutar a hipótese é feita a depender dos resultados advindos de uma série de testes, iniciados com uma coleta de dados significativos acerca da natureza e dos motivadores do problema.

Para utilizar esse método e obter resultados palpáveis, a partir da análise da hipótese e do problema de pesquisa, acredita-se ser necessária a leitura de fontes primárias e secundárias conforme indicadas no trabalho de Thies (2002, p. 356), que se traduzem nos principais marcadores de análise utilizados no referencial conceitual *S.A.M.*, de Kremer e Müller (2013), especificados aqui a fim de salientar as principais seleções, justificativas e possibilidades abordadas na pesquisa e na próxima seção, criando, com isso, um escopo inicial da construção analítica realizada posteriormente nos capítulos.

As fontes primárias incluirão documentos de estratégias cibernéticas anuais, acordos temáticos e bases de dados sobre ataques cibernéticos realizados e confirmados – principalmente o COT, especificado adiante -, além de outros materiais diretamente relacionados ao tema entre 2010 e 2020. Por meio desses elementos, é elencado como o governo

estadunidense percebeu e veiculou informações de cunho cibernético às questões de segurança e defesa, fortalecendo - ou não - os níveis orçamentários dedicados à cibersegurança e à assimilação do tema cibernético à proteção dos Estados Unidos.

Já as fontes secundárias consistem nos estudos realizados por autores reconhecidos na área cibernética e no tópico das RI, na forma de artigos e trabalhos acadêmicos e autorais que oferecem uma visão aprofundada e crítica sobre o estudo de cibersegurança conectado com a temática das RI. Tais autores são considerados relevantes por suas vastas contribuições ao tema e pelo grande número de referências em textos sobre o tema cibernético. Os autores selecionados com base na triagem identificam-se como Anthony Craig, Brandon Valeriano, Herbert Lin, Nilsu Goren, Richard Clarke, Joe Burton, Joe Devanny, Max Smeets, Kim Zetter, Ryan Maness e Theresa Hitchens.

Preferências Teóricas e Temáticas

Esta pesquisa aplicará o COT do CFR como base de dados principal para o agrupamento de informações voltadas às capacidades cibernéticas ofensivas, estabelecendo-o como uma fonte primária e secundária, além de possuir um aspecto metodológico essencial na elaboração dissertativa. Isso se dá graças à estrutura rígida e precisa do COT acerca da construção dos casos disponibilizados, elemento exposto nas seções de glossário e sistematização dessa base de dados.

Segundo CFR (2024), tal processo é fundamentado em uma categorização de todas as instâncias públicas de atividades cibernéticas ofensivas realizadas e custeadas por Estados nacionais a partir de 2005. A seleção desses casos específicos visa conferir transparência nos atos estatais realizados, entendendo, assim, seus interesses nacionais encaminhados ao âmbito cibernético.

A triagem realizada contém apenas casos cibernéticos comprovados de imputação ou financiamento estatal e é proveniente da disponibilidade e confiabilidade dos dados trabalhados pelo COT. Isso faz com que somente informações genuínas sobre ataques cibernéticos estatais sejam selecionadas, pois casos realizados por atores não-estatais não possuem dados materiais acerca da existência do dano ou da atribuição do agente malicioso, complicando seu uso em base de dados confiáveis.

Dessa forma, conforme apontado em CFR (2024), o COT coleta e investiga apenas dados estatais dispostos em empresas de cibersegurança garantidas internacionalmente - como

o grupo Kaspersky e o laboratório *FireEye* -, em repositórios de incidentes cibernéticos de empresas e em grupos acadêmicos de pesquisa. Uma vez reunidas as informações, o COT averigua pontos causais comuns entre os dados, utilizando fontes primárias - comunicados de imprensa, discursos realizados, informes de empresas de cibersegurança, notas presidenciais, além de fontes secundárias - reportagens da mídia e publicações comerciais -, com o intuito de formar dados precisos e detalhados acerca dos casos dispostos.

O COT também tem uma função de *crowdsourcing*, em que há a permissão do público e de outras empresas menores de cibersegurança em sugerir adições de informações à base de dados; porém os materiais oferecidos dessa maneira são julgados com maior precisão, para assim serem integrados aos dados analisados. Ao indicar a metodologia do COT de classificação e apuração dos dados, pode-se considerar o COT como uma fonte primária e secundária de dados, visto que há a possibilidade, como instituído posteriormente, de utilizar tanto os dados analisados pela base quanto as informações brutas criadoras das inferências constatadas por CFR (2024), elemento este que gera mais um nível de peculiaridade e importância de uso para a pesquisa.

Uma vez realizada a etapa de apuração, o COT realiza uma movimentação analítica com o intuito de exprimir e salientar noções comuns das informações díspares e amplas de um caso. Com isso, é criado um marcador temporal do ato cibernético em questão, indicando fatores que identificam: (1) os Estados responsáveis, (2) o tipo de incidente, (3) a data aproximada da realização do ato, (4) possíveis filiações do caso no tempo, (5) os atores afetados, (6) a reação do governo afetado, (7) o nível de resposta governamental nas camadas doméstica e internacional e (8) as informações e os relatórios nos quais se pautaram a construção desses casos na base de dados.

Qualquer registro acerca de um caso cibernético disposto no COT pode ser atualizado, conforme novas informações são verificadas e agregadas à base de dados, normalmente realizada a cada trimestre. Isso permite que as entradas dos casos se tornem cada vez mais fundamentadas no tempo, fortalecendo sua presença e uso nos meios acadêmicos.

Dito isso, ao escolher o COT e a sua metodologia rígida de seleção de casos cibernéticos ofensivos incontestáveis, há uma tentativa de evitar vieses derivados da parca quantidade e veracidade de informações existentes de casos com atribuição expressa. Essa busca pela atribuição de suspeitos é completamente relevante para a pesquisa, pois, quase nenhuma outra base de dados voltada à indicação de casos cibernéticos ofensivos realiza tal movimentação

analítica, visto que há uma problemática derivada dessa circunstância no estudo de *cyber* segurança através da noção de atribuição.

Isso acontece, segundo Lima (2019, p. 39), porque uma atribuição estatal em casos virtuais pode ser percebido como um desafio marcante na área teórica e prática no tópico cibernético. Ainda segundo Lima (2019, p. 39), o ciberespaço é construído e apresentado de forma a manter e facilitar o anonimato de dados e presenças na rede. Isso permite que os usuários da rede, principalmente os agentes maliciosos, se utilizem dessa ausência de identificação para cometer crimes, ataques cibernéticos ou ações oblíquas de forma a manter sua presença desconhecida e deixar nebulosa a existência ou a origem de seu ato. Isso faz com que o anonimato e a falta de uma atribuição clara sejam percebidos como a maior vantagem inerente em um caso cibernético ofensivo (Lima, 2019, p. 48).

Contudo, mesmo com vantagens características, o COT do CFR ainda é uma organização sediada nos Estados Unidos, e, a partir disso, pode ser influenciado por tendências de pensamento intrínsecas desse local. Isso faz com que certas escolhas, dados e casos importantes possam ser desconsiderados por não fazerem parte do *mainstream* acadêmico estadunidense, trazendo possíveis omissões de seleção na metodologia rígida do COT.

Ainda assim, esta dissertação se pautará no uso do *Cyber Operations Tracker* como base de dados de casos cibernéticos ofensivos, pois há um reconhecimento autoral de que as orientações metodológicas, teóricas e práticas estão seguindo uma ampliação de suas capacidades e de seu escopo para além da localidade do CFR, se afastando das lógicas e políticas unitárias. Isso acontece através de uma noção clara, apoiada e enunciada no próprio COT, de que é necessário se utilizar de dados e pareceres técnicos de fontes não-ocidentais, para se ter uma visão clara dos acontecimentos cibernéticos no mundo, com base na comparação de avaliações de fontes e dados díspares, para encontrar informações comuns - e teoricamente verídicas - acerca dos casos estudados.

O uso do CRF, até mesmo podendo ser enviesado em graus distintos, ajuda a entender também como as lógicas e as construções teóricas dos Estados Unidos são construídas e difundidas nessa base de dados. Ponto que indica o grau de influência que os EUA são capazes de difundir nas percepções de envolvimento estadunidense nos casos cibernéticos realizados, permitindo acentuações e desconsiderações aos atos dispostos. Elemento que eleva a importância dos 16 casos de ataques cibernéticos utilizados nessa dissertação, pois, mesmo ao seguir a possibilidade de viés por parte do COT, tais casos foram selecionados e atribuídos aos

Estados Unidos, trazendo, com isso, mérito aos casos, que não conseguiram ser omitidos metodologicamente, trazendo novas nuances e possibilidades de análise aos casos.

Já no que tange os dados acerca das capacidades e casos de orientação defensiva, há poucas margens de problematização, visto que a pesquisa examinará as informações dispostas publicamente pelos Estados Unidos e pelas Organizações Internacionais nas quais os EUA fazem parte nesses 11 anos. Esta dissertação se concentrará principalmente nos dados fornecidos e incluídos no trabalho de Hitchens e Goren (2017), ampliando tais informações para além de 2017, a partir da disponibilidade de dados acerca das construções legislativas e cooperativas científicas.

Dessa forma, a pesquisa seguirá uma filiação epistemológica realista na análise da dissertação. Isso acontece visto que o foco do trabalho destaca a existência, a importância, a construção e o uso do poder no âmbito cibernético. Tal pensamento, reforçado no meio acadêmico, indica que, os Estados do Sistema Internacional Cibernético, em prol de alcançar seus interesses, manter sua própria segurança e conquistar poder, agem agressivamente no ambiente cibernético. Com isso gerou-se percepções de medo e insegurança no Sistema Internacional, se fazendo necessário a utilização do pensamento realista para a explicação de como o poder é criado e garantido na dinâmica entre Estados (Craig e Valeriano, 2018, p. 85, Jervis, 1978, p. 169 e Gratão, 2022, p. 08).

A fim de superar as obliquidades provenientes do realismo nas percepções de poder, será utilizada referências que se distanciam, mesmo que pouco, do pensamento realista. Para isso, serão utilizados os escritos de Joseph Nye e Robert Jervis para atenuar o estudo, e assim trazer novas possibilidades, discussões e resultados acerca do poderio no ambiente cibernético realizado pelos Estados Unidos. A despeito disso, o foco do trabalho continuará sendo orientado ante as percepções realistas para se lidar com assuntos abordados em âmbitos militares, diplomáticos e tecnológicos, trazendo uma visão mais cautelosa e pessimista das movimentações cibernéticas estatais.

Estrutura do Argumento

A presente dissertação foi estruturada em três capítulos. O primeiro capítulo discutirá, teórica e conceitualmente, a temática cibernética, indicando quais são as principais concepções utilizadas, o contexto histórico nos quais estas ideias foram estipuladas, e quais são as dicotomias presentes e marcantes no estudo teórico de cibersegurança, que conseguem construir

definições discrepantes sobre um mesmo pensamento teórico. Serão apresentadas as escolhas teóricas e metodológicas utilizadas na pesquisa.

O segundo capítulo apresentará os principais atos cibernéticos ofensivos e defensivos realizados pelos Estados Unidos entre 2010 e 2020, pautando-se nos pensamentos de Kremer e Müller (2013), Hitchens e Goren (2017), Amoretti e Fracchiolla (2018), Devanny (2021), dentre outros. O capítulo registrará a progressão anual dos atos e movimentações estadunidenses ante a temática cibernética nas áreas militares, diplomáticas e relativas à segurança cibernética nos âmbitos governamentais, institucionais e internacionais. Frisando, com isso, as principais ações e o posicionamento dos Estados Unidos ante a construção de poder para com os atores presentes no Sistema Internacional Cibernético, focando nos Países Baixos, Reino Unido, Estônia, Índia, China, Rússia, Irã e Coreia do Norte.

O terceiro capítulo analisará qualitativa e quantitativamente os dados acumulados. Fundamentado nisso, serão criadas e utilizadas métricas de comparação dos elementos presentes nas capacidades cibernéticas sob as matrizes do referencial conceitual *S.A.M.* de Kremer e Müller (2013), das teorias cibernéticas de Relações Internacionais sobre poder - com um foco no trabalho de Nye (2010) - e do método hipotético-dedutivo, salientando as principais consequências da projeção de poder realizada pelos Estados Unidos e os ganhos alcançados.

Uma vez seguidas tais etapas, será determinado se e em quais graus a hipótese indicada foi provada verídica. Ao realizar uma investigação amparada pelo *framework* cibernético *S.A.M.*, em conjunto com um pensamento das RI sobre poder, será possível ampliar o estudo temático de cibersegurança ao trazer e reforçar perspectivas aos pesquisadores e aos atores do Sistema Internacional Cibernético.

CAPÍTULO 1 – *CYBER* SEGURANÇA: CONTEXTOS E CONCEITOS

Este capítulo tem o intuito de realizar uma construção teórica e contextual ampliada acerca da temática de cibersegurança conectada ao estudo das Relações Internacionais. Esta primeira seção examinará brevemente a conjuntura que fomentou a análise do tema cibernético e indicará os principais conceitos e assimetrias teóricas associadas ao tópico cibernético. A partir disso, serão apresentadas as escolhas realizadas para a produção desta pesquisa, integrando-as em um referencial conceitual temático (*framework S.A.M.*), indicando como as teorias das RI podem se utilizar dessas concepções na explicação e no entendimento do papel desempenhado pelo âmbito cibernético nas relações internacionais.

1.1 Criação e Desenvolvimento da Temática de *Cyber* segurança em RI

O termo e o estudo da cibersegurança, em um contexto amplo, inicia-se na metade do século XX, de acordo com os escritos de Alam (2022, p. 04-05) e Morais, Lima e Franco (2012, p. 41), com a consolidação da *Internet,* a partir da criação da rede de comunicação ARPANET (*Advanced Research and Projects Agency Network* - Rede da Agência Avançada de Projetos e Pesquisas, em inglês). A ARPANET, ainda em um estágio preliminar, segundo Morais, Lima e Franco (2012, p. 42), trouxe uma inovação perceptível na interação entre os agentes utilizadores desta rede - militares e acadêmicos dos Estados Unidos -, em um caráter limitado, por trazer facilidade e rapidez às comunicações, possibilitando realizar transferências de arquivos e acesso remoto aos computadores.

Contudo, mesmo nessa fase, mais especificamente em 1979, houve a primeira presença de um agente malicioso que se utilizou de sua *expertise* a fim de causar graus de inconveniência. Com o nome de *Creeper*, segundo Alam (2022, p. 04), esse *software* benigno tinha como objetivo transitar juntamente com os dados enviados pelos utilizadores da ARPANET, reportando apenas uma mensagem que dizia: “Eu sou o *Creeper*, me pegue se puderem”.

A existência desse programa, o primeiro vírus de computador conhecido, forçou os desenvolvedores a produzir formas de rastrear e destruir tal *software*, criando, com isso, o *Reaper*, o primeiro antivírus da história. Ao perceberem que relações desse porte poderiam existir futuramente, mas com objetivos danosos, os programadores da ARPANET criaram procedimentos e princípios básicos a fim de impossibilitar que estas interações, até então hipotéticas, fossem realmente prejudiciais, desenvolvendo programas e modelos focados em

fazer a rede mais segura e protegida. Esse foi o princípio inaugural do termo de cibersegurança (Alam, 2022, p. 04-05).

Com isso, entende-se que a questão principal e original da cibersegurança seria impedir atos maliciosos, realizados principalmente por indivíduos - *hackers* - de se propagarem nas redes de comunicações, além de estabelecer princípios com o intuito de fortalecer a criação e a manutenção de redes futuras com a finalidade de deixá-las mais consistentes. Com o estabelecimento da *Internet* com a *World Wide Web* (WWW) na década de 1990, foi atraído um grande volume de pessoas e agentes do SI - Estados, organizações internacionais, bancos, centros de pesquisa, empresas, entre outros - com o interesse de utilizar os recursos, na época inovadores, para guardar, utilizar e analisar informações disponíveis em uma alta velocidade (Lima, 2019, p. 13-14).

Esse movimento trouxe um novo desafio para o contexto teórico de cibersegurança, visto que a noção até então existente não estendia sua proteção e projeção especificamente aos participantes da *Internet* ou seus dados, mas somente a rede em si. Isso fez com que fosse necessário, conforme Maness e Valeriano (2018, p. 261), que os conceitos e níveis de proteção vinculados ao tema de *cyber* segurança e à *Internet* - caracterizada como parte do ciberespaço, ponto discutido à frente no capítulo - precisassem ser consolidados e ampliados para abranger novos atores e superar os desafios inerentes, garantindo a segurança dos agentes no espaço cibernético, sendo realizada no final do século XX e início do próximo século.

Contudo, essa situação mudou com a percepção de três grandes casos de cibersegurança, salientados na introdução desta dissertação e postos como atípicos por Valeriano e Maness (2018, p. 260). Esses casos trouxeram frescor ao tema cibernético, além de novos desafios aos estudiosos da área, pois continham evidências do uso de capacidades ofensivas com o objetivo de causar dano material. Não obstante, tais eventos alteraram o pilar do estudo de cibersegurança acerca da identidade dos agentes maliciosos, graças aos indícios que apontavam a ação ou alto financiamento estatal nesses atos cibernéticos.

Até aquele momento, a percepção autoral sobre os agentes maliciosos tendia a caracterizá-los mais como pessoas ou grupos de pessoas - *hackers* - como responsáveis por ataques cibernéticos, desconsiderando a presença dos Estados, que já haviam participado como autores de ciberataques em um período anterior a 2007 (CFR, 2024). Ao se utilizar da lógica focada nos *hackers*, há uma limitação dos possíveis níveis de investimento empregados em atos cibernéticos, diminuindo o alcance de ação e o grau de destruição, de forma a facilitar as análises e possíveis atribuições do atacante.

Porém, quando a identidade de um agente malicioso começa a priorizar os Estados nacionais, a escala de destruição e de possibilidades de ataques aumentam exponencialmente em um ato cibernético. Isso acontece porque, em virtude de ser um Estado, o nível orçamentário é significantemente maior, viabilizando, assim, a construção de aparatos cibernéticos ofensivos mais sofisticados, possibilitadores de *cyber* ataques mais eficientes, com alcances mais amplos e maior capacidade destrutiva.

Em conjunto com a necessidade de modificação do conceito, novos desafios surgem e consolidam o estudo de cibersegurança no *mainstream* acadêmico, fazendo com que a temática precisasse se desenvolver de uma forma mais consistente, para assim conseguir analisar esses novos exemplos sem precedentes notáveis. Isso fez - e ainda faz - com que sejam criados argumentos temáticos, voltados a tentar reestruturar e consolidar os conceitos que trabalham o ambiente cibernético, seus atores e todas as dinâmicas presentes nesse âmbito, ponto que gerou novas perspectivas e nuances pertinentes à pesquisa.

1.2 Conceitos Cibernéticos - Escolhas, Desafios e Dicotomias

Em razão da contextualização acima, o estudo de cibersegurança após 2010 teve que se desenvolver rapidamente a fim de conseguir ser capaz de responder e analisar os desafios, casos e ações dos atores presentes no espaço cibernético. Dessa forma, grande parte dos autores voltados à temática cibernética - sejam estes mais consagrados ou iniciantes - se dedicaram a indicar quais seriam suas bases conceituais voltadas ao estudo temático nessa seara. Também foram definidos quais seriam os escopos, os significados, os atores e as contrariedades disponíveis. Esses pontos geraram novos conceitos e análises no meio acadêmico, fomentando e inovando uma área de estudo pouco explorada até 2007.

No entanto, dado o fato de que o pensamento cibernético era parcamente discutido na época, com poucos modelos empíricos ou dados a serem analisados, não houve uma construção acadêmica inicial centrada em debates, troca de ideias ou confrontos temáticos. Isso fez com que os estudos centrais de *cyber* segurança nas RI fossem completamente distintos entre si, mesmo quando abrangiam o mesmo conceito.

Essa movimentação, por estar pautada nas escolhas e nos interesses de quem escrevia, geravam - e ainda geram - pesquisas e resultados empíricos diversos, provindos de diferentes tradições epistemológicas - positivistas ou pós-positivistas -, focos de estudo, atores ou conceitos com maior destaque e escolas de conhecimento distintas do estudo das RI,

constituindo, assim, análises contrastantes acerca da materialidade dos conceitos cibernéticos. Esta subseção aponta, com exemplos, como os conceitos cibernéticos podem divergir entre si, além de indicar quais são as escolhas realizadas nesta dissertação.

Primeiramente, no que tange aos atores relevantes ao estudo cibernético, os autores de cibersegurança variam entre uma perspectiva unitária ou mais abrangente. A abordagem mais profusa aponta que o espaço cibernético é maior do que apenas as relações e as interações entre Estados[1].

Para Nye (2010, p. 09), por exemplo, o espaço cibernético pode abranger todo o sistema computacional e informacional público e privado do mundo, permitindo que pessoas, empresas e instituições nacionais ou internacionais usufruem da capacidade de produzir relações, sejam estas de poder ou não, para a construção e a transformação do espaço cibernético e de seus participantes. Contudo, essa escolha mais extensa revela complexidades, percebidas na atenuação das particularidades dos integrantes desse âmbito, tendo um caráter mais inclinado em entender como as interações acontecem do que na identidade e nas competências desses agentes.

A segunda abordagem apresenta um entendimento e análise mais particularizada, construindo modelos empíricos com testes de validade mais concretos. Isso facilita a previsão de fenômenos similares no futuro, dado o fato de usar padrões presentes na epistemologia positivista das RI, como proposto por Braga (2013, p. 62-64).

Porém, ao estabelecer um ator singular como a lente principal em uma análise, certas interações mais amplas e os resultados derivados disso são desconsiderados, impedindo a realização de um estudo mais completo do tema cibernético. Um exemplo desse pensamento está nas percepções de Valeriano e Maness (2015; 2018), Lindsay (2015) e Lopes (2016), que realizam a escolha de designar o Estado nacional como ator de destaque no estudo cibernético.

Com um tom mais voltado à perspectiva realista das RI, tais autores propõem que somente os atos realizados pelos Estados no domínio cibernético - normalmente as grandes potências, como os EUA, China ou Rússia -, por terem maiores orçamentos militares e capacidade de projetar poder, podem gerar resultados empíricos aceitáveis de mudança ante a

[1] Tal afirmação indica que o espaço cibernético, devido seu fomento extremo derivado do início do século XXI, conseguiu alcançar e conectar vários agentes do Sistema Internacional, comunidades e indivíduos, os colocando, teoricamente, em um mesmo patamar dentro do ciberespaço. Isso faz com que a prioridade da análise voltada somente aos Estados e suas relações sejam desafiadas, pois, em um nível de análise cibernético, todos os agentes dispõem das mesmas capacidades de movimentação nesse domínio, não havendo um protagonismo Estatal efetivo no espaço cibernético. Ponto que estabelece a necessidade de existir análises mais abrangentes acerca das relações não-Estatais ocorridas no âmbito virtual.

temática de *cyber* segurança. Isso faria com que as influências geradas por tais atos sejam reproduzidas por outros atores, trazendo possíveis mudanças ao SI. Tal inclinação de determinar a existência estatal como a mais relevante no estudo cibernético, tende a desconsiderar certas ferramentas conceituais ou outras interações com agentes não-estatais em prol de construir uma análise mais palpável e com resultados mais assertivos.

Dessa forma, neste trabalho, foi escolhido o enfoque mais unitário e particularizado do estudo cibernético, destacando somente um ator, no caso os Estados Unidos da América e seus atos como os pontos centrais da pesquisa. Isso permite a criação de uma análise mais profunda das atitudes estadunidenses, se utilizando de algumas características positivistas no processo, como a concretude dos testes de validade de um modelo teórico, e a tentativa de elaborar padrões de comportamento futuro por parte do Estado estudado (Braga, 2013, p. 62).

A fim de amenizar as questões teóricas oriundas dessa alternativa, foram selecionados conceitos cibernéticos que afirmam a centralidade estatal como ator principal no estudo de cibersegurança, mas também ampliam o universo de atores e interações presentes no âmbito virtual, não anulando seus graus de relevância e participação no ambiente cibernético.

Um exemplo da seleção está na definição e utilização de poder cibernético em um caráter neoliberal apontado por Nye (2010, p. 02-04) e Kuehl (2009, p. 38). Para esses autores, poder, em uma característica cibernética, consiste na capacidade de um ator do SI usar o ambiente cibernético como gerador de possibilidades positivas de ganho, difusão e manutenção de poder, empregado conjuntamente com outras ferramentas de poder tradicionais ou até mesmo realistas. Para Nye (2010, p. 04-05), o ganho ou o uso de poder cibernético pode funcionar de duas formas, sendo a primeira constituída pela obtenção de poder em uma tipologia interna do ciberespaço, ou seja, o poder é exercido no domínio, exemplificadas na realização de ciberataques, criação de leis cibernéticas, ou o apoio e as influências realizadas por um Estado às ações de instituições internacionais voltadas à área de *cyber* segurança.

Já o segundo modo de se conquistar poder no espaço cibernético é garantido externamente, ao se utilizar de formas tradicionais e conhecidas de poder com o objetivo de exercer influência ou dominação às tecnologias de acesso do *cyber* espaço. Ponto exemplificado na forma da destruição ou sabotagem de servidores ou cabos de *Internet*, movimentos de boicote ou constrangimento de empresas de tecnologia ou até mesmo campanhas realizadas por organismos internacionais a favor ou contra movimentações cibernéticas específicas em um momento no tempo (Nye, 2010, p. 05).

O conceito de poder cibernético construído por Nye (2010) e Kuehl (2009) aprimorou os instrumentais presentes em uma análise temática, ampliando os pensamentos realistas de Valeriano e Maness (2015; 2018), Lindsay (2015) e Lopes (2016), acerca da singularidade dos atores no SI, dando importância a todos os agentes presentes ao ciberespaço, e, ao mesmo tempo, estipulando ao Estado uma centralidade nas questões de segurança cibernética. Isso garantiu a integração de percepções internas e externas ao pensamento de construção e difusão de poder cibernético. Dessa forma, Nye (2010) indica como o espaço cibernético e o seu uso são capazes de gerar poder físico para os agentes, além de permitir interação com outros atores, gerando assim novas repercussões.

Já outro exemplo que atesta uma escolha mais particularizada ante ao ator central está no conceito de cibersegurança. Por ser o conceito inaugural deste capítulo, foi percebido que a noção cibernética de segurança manteve a base de pensamento: defender um ponto de destaque do ciberespaço do ato de algum agente malicioso no tempo, mas especificamente "a habilidade de defender e de manterem seguras as redes computacionais e de informação estatais de ataques cibernéticos ou de casos de exploração cibernética em um caráter virtual" (Lin, 2012, p. 48).

Entretanto, devido às constantes mudanças na tecnologia, novas dinâmicas, atores e níveis de análise que irromperam no espaço cibernético, necessitando-se que sejam criadas e ampliadas as bases teóricas acerca da definição de *cyber* segurança, ponto que gera conceitos, argumentos e focos de estudo diversos. Como resultado, esta pesquisa ampliará o pensamento de Lin (2012) ante o conceito de segurança cibernética - constituída de uma percepção mais clássica e estatal na construção teórica de *cyber* segurança -, ao utilizar o pensamento de Burton (2015, p. 03) que aprimora tal definição com uma união de aspectos cinéticos e virtuais igualmente importantes no estudo cibernético voltado à segurança.

Burton (2015, p. 03) inclui ao conceito as formas nas quais o ator em destaque - o Estado - deve proteger suas infraestruturas críticas em casos de ataques cibernéticos, diferenciados na forma de crime cibernético[2] (*cyber crime*), *cyber* espionagem[3] (*cyber espionage*), terrorismo

[2] O crime cibernético se caracteriza na forma de "ataques efetuados originalmente por indivíduos ou grupos privados – apoiados ou não por Estados - que buscam, através de falhas - sejam elas humanas sejam elas na rede – adulterar informações, realizar fraudes ou roubar dados valiosos e únicos de pessoas ou empresas" (Burton, 2015, p. 03 e Lima, 2019, p. 19).

[3] A espionagem cibernética é descrita como uma atividade *online* maliciosa normalmente conduzida por Estados - como participantes ou financiadores -, que, "através de roubo de informação vital de outros Estados e empresas privadas, tentam aumentar seu conhecimento e capacidade para conseguir vantagens nos ramos comerciais, políticos e militares" (Burton, 2015, p. 04 e Lima, 2019, p. 19).

cibernético[4] (*cyber terrorism*) e *cyber* conflito[5] (*cyber warfare*). Através dessa percepção, Burton (2015, p. 03) fomenta o estudo temático ao colocar as intenções, a tipologia e as escolhas de alvos dos atacantes ao conceito de *cyber* segurança, facilitando o entendimento e a preparação dos Estados em tentar mitigar os danos gerados por tipos distintos de ataques, produzindo, assim, uma construção teórica mais acessível de ser utilizada por Estados e por OIs voltadas à área de segurança cibernética - como a Organização do Tratado do Atlântico Norte (OTAN).

O segundo tipo de seleção envolve a localização do foco do estudo, ou seja, a designação das bases de análise utilizadas. Assim sendo, optou-se por realizar uma pesquisa das capacidades cibernéticas estadunidenses, ao invés de um estudo completo acerca da construção da política externa cibernética dos Estados Unidos. No entanto, esse trabalho frisou que o uso e as determinações das capacidades cibernéticas ofensivas e defensivas dos Estados Unidos são produtos de uma estruturação temática de política externa realizada no recorte temporal proposto. É necessário, então, conceituar as competências tipificadas como ofensivas e defensivas.

Para se categorizar as capacidades ofensivas, essa pesquisa se utilizará dos escritos de Smeets e Lin (2018, p. 58) e Bellovin, Landau e Lin (2017), trabalhados em conjunto com os documentos de Brasil (2023, p. 07), que inferem o conceito de capacidades ofensivas como a preparação ou a atuação instrumentalizada de um ator ou grupo de atores do SI para o acesso ou degradação de um sistema de comunicação ou rede na forma de ataques cibernéticos estruturados com objetivos de gerar danos a entidades, infraestruturas críticas ou até mesmo seres vivos e assim cumprir com objetivos operacionais estabelecidos previamente. Através desse conceito, é seguida a lógica proposta por Zetter (2014, p. 38) e continuada por várias empresas de cibersegurança acerca da construção de um *cyber* ataque composto por duas partes.

Segundo Zetter (2014, p. 38), uma arma ou um dispositivo cibernético precisa ter dois componentes agindo simultaneamente para ser considerado um instrumento de um ataque

[4] O terrorismo cibernético é definido como uma ação realizada no âmbito virtual que atinge pode atingir dois objetivos: se (a) seus efeitos forem comparados a um ataque terrorista: "quando um ataque cibernético resulta em efeitos que são disruptivos o suficiente para gerar medo comparado à um ato terrorista", ou (b) se o intuito é coagir uma mudança política: "*cyber* terrorismo existe quando um ataque ora desleal ou politicamente motivado são feitos para intimidar ou coagir um governo ou as pessoas em prol de um objetivo político"" (Rollins e Wilson, 2007, p. 03 - tradução nossa e Burton, 2015, p. 04)

[5] O conflito cibernético é apresentado como um ato ofensivo - ou um *cyber* ataque - realizado ou financiado por outro Estado voltado a se utilizar de vulnerabilidade de um ator no espaço cibernético em prol de causar um grande impacto contra as infraestruturas críticas do alvo, dano esse cinético - físico - ou virtual - contra os dados desse agente (Burton, 2015, p. 04 e 05)

cibernético, sendo eles um *Missile* (ou um sistema de entrega) e um *Payload* (uma carga com objetivos). O *Missile* consiste nas formas que um *malware* consegue se locomover, avariar ou infectar um sistema ou rede de dados e informações, criando ou se aproveitando de vulnerabilidades dispostas nos dispositivos-alvo (Zetter, 2014, p. 38, 61). Já o *Payload* corresponde aos conjuntos de códigos liberados por um *malware* a um dispositivo específico com um objetivo a ser cumprido (Zetter, 2014, p. 38).

Para Zetter (2014), a definição e união desses segmentos são significativos para a noção e constatação de um ataque cibernético, já que, sem a existência de ambos em um período aproximado, um *cyber* ataque não pode ser reconhecido oficialmente. Isso ocorre graças à frequência na incidência de erros, *bugs* ou infecções acidentais na rede e para com seus usuários, não garantindo ou provando a existência de uma arremetida cibernética com base em um episódio isolado de *Missile* ou *Payload*. Este aspecto faz necessária a presença de tais detalhes para se provar a existência de uma operacionalização engendrada em um ataque cibernético, asseverando sua existência, seus detalhes e seus alvos prioritários no tempo.

Tal lógica salientada por Zetter (2014) é significativa para esta dissertação, pois, em algumas das ocorrências de uso das capacidades cibernéticas ofensivas utilizadas, são identificados traços de movimentação anterior à sua oficialização em bases de dados, sejam estas a própria COT ou empresas utilizadas por essa base. Isso indica que houve a existência, mesmo que nebulosa, de uma atividade cibernética - um *Missile* ou *Payload* - inerente e precursora a um caso.

Contudo, por estar ligado apenas a um dos elementos evidenciados por Zetter (2014), não há a comprovação dessa antecedência ao caso em si, deixando a circunstância inexata ante ao ato cibernético ofensivo. No entanto, para esse trabalho, serão observados e utilizados esses tipos de informação, normalmente salientados nos relatórios de empresas de *cyber* segurança, a fim de identificar elementos de intenção e preparação do agente malicioso nas movimentações ante o objetivo pressuposto de aumento de projeção de poder.

Dito isso, o conceito utilizado acerca da capacidade cibernética ofensiva derivado da reunião de percepções e lógicas propostas por Smeets e Lin (2018), Bellovin, Landau e Lin (2017), Brasil (2023) e Zetter (2014) trazem consigo novos padrões e percepções que fortalecem os fundamentos originários, adequando as matrizes de pensamento utilizadas na pesquisa. O principal exemplo desse raciocínio está no desenvolvimento e na especificação da natureza do dano gerado por um ataque cibernético, que agora compreende uma tipologia direta

e indireta, não existente nos escritos de Smeets e Lin (2018) por desconsiderar casos de roubo de dados ou espionagem cibernética como parte de seu espectro de estudo.

Por consequência, foi adicionada, graças aos níveis de similaridade disponíveis entre suas instâncias categóricas de capacidades - apontadas a seguir - um nível de aprimoramento do conceito, que agora consegue ajustar as características amplas de dano. Tipologia exemplificada no tipo direto de Smeets e Lin (2018, p. 58-60), indireto decorrente da característica de espionagem cibernética para Burton (2015) como potencial, colateral ou não intencional de Romanosky e Goldman (2017)[6], ou no tipo oriundo dos Efeitos Significativos propostos por Acton (2020)[7].

Para Smeets e Lin (2018, p. 58-60), os atos de gerar dano direto derivado do uso das capacidades cibernéticas ofensivas são identificados em três categorias: (1) falha na distribuição de serviço; (2) avaria em dados; e (3) destruição física, sendo todos advindos e conceituados na obra de Bellovin, Landau e Lin (2017). O primeiro tipo pode apresentar-se na forma de um DDoS (*Distributed Denial of Service* - Negação de um Serviço Distribuído, em inglês), normalmente conhecido e amplamente divulgado na mídia por ser uma tipologia de ataque bem comum.

Um ataque DDoS, para Bellovin, Landau e Lin (2017, p. 62), visa sobrecarregar um site ou até mesmo um servidor inteiro via inundação de solicitações de acesso. Tal ato, por ser artificialmente criado e de grande volume, gera uma falha de resposta dos pedidos realizados, impedindo a circulação de dados até as solicitações anteriores serem atendidas, fazendo com que o servidor em si e as suas comunicações parem de responder.

O problema nesse tipo de ataque é que, a depender do servidor atacado, muitos sites ou canais de compartilhamento de dados importantes podem vir a ser prejudicados, gerando consequências sérias de falta de comunicação, formas de pagamento, distribuição de serviços, entre outros. Ataque exemplificado em dois dos três grandes casos de *cyber* segurança - o caso da Estônia de 2007 e o caso da Geórgia de 2008.

---

[6] Para Romanosky e Goldman (2017, p. 256), os efeitos de dano de um ataque cibernético podem ter decorrências múltiplas intencionais ou até mesmo involuntárias, normalmente não especificadas ou planejadas, possibilitando graus diferentes e ampliados de destruição às infraestruturas críticas. Ponto que faz com que as escalas voltadas ao dano presente em um ataque cibernético possam ser vagas e amplas em detrimento daqueles vistos em doutrinas de operações militares convencionais, facultando, com isso, novas percepções e análises.

[7] Segundo Acton (2020, p. 134), ataques cibernéticos possuem uma característica própria chamada de "Efeitos Significantes" no tempo. Tais efeitos trazem consequências diferentes, a depender da intenção do agente malicioso ou da interpretação da vítima a ocorrência cibernética em si, podendo ser verificada rápida ou tardiamente. As consequências mais comuns dos efeitos se constatam na identificação incorreta do agente malicioso, do objetivo ou até mesmo da existência do ataque, ocasionando implicações imprevisíveis da vítima em relação a um caso cibernético particular, ou danos potenciais a serem incorridos no futuro.

Outra categoria de ataque, para Smeets e Lin (2018, p. 58) e Bellovin, Landau e Lin (2017, p. 62), é a de avaria nos dados. Essa condição consiste no ato de danificar, manipular ou deletar dados de um servidor por parte de um agente malicioso, desconsiderando, inicialmente, atos de roubo de dados ou espionagem cibernética como parte de seu espectro de atuação.

Nesse ponto, a vinculação de espionagem cibernética ao conceito amplo de capacidades cibernéticas ofensivas é evidenciada, visto que, em uma análise de capacidades, o ato de roubar um dado e apagá-lo posteriormente ou apenas deletar um dado sem roubá-lo têm o mesmo valor. É assim porque o objetivo do agente malicioso foi alcançado - desaparecer com o dado em específico - e, graças às circunstâncias que permitem a anonimidade e as trajetórias oriundas desse tipo de ataque, não há provas empíricas que confirmam de fato o roubo de um dado, ponto que permite a integração da espionagem ao conceito.

A última categoria se apresenta na forma da destruição física, que para Smeets e Lin (2018, p. 58) e Bellovin, Landau e Lin (2017, p. 62-63), é o uso das capacidades ofensivas cibernéticas como forma de causar destruição visível e material de um alvo através de uma parada forçada de seu funcionamento ou sobrecarga, sendo assim o auge da utilização desses tipos de capacidades e o tipo de ataque mais perigoso a ser realizado segundo os autores. Um ataque cujo foco é realizar somente a destruição renuncia ao anonimato inerente a um ataque cibernético (Lima, 2019. p, 48) e requer níveis altos de orçamento e planejamento, tendo sido percebido pouquíssimas vezes no mundo e normalmente atribuído às ações Estatais, visto no caso *Stuxnet* de 2010.

Logo, a definição e a classificação das capacidades cibernéticas ofensivas oferecidas por Smeets e Lin (2018), Bellovin, Landau e Lin (2017), Brasil (2023) e Zetter (2014) traz à pesquisa o dinamismo, a ampliação, o uso e os resultados advindos das capacidades nos atos cibernéticos estatais. Ponto que se reflete na escolha da utilização do COT como base de dados para a análise. Ao realizar tal movimentação, as categorias indicadas anteriormente por Smeets e Lin (2018) e Bellovin, Landau e Lin (2017) são colocadas em destaque no COT de CFR (2024), que ao separar por tipo de ataque fundamentado nas tipologias de uso de capacidades cibernéticas ofensivas, traz uma maior comprovação dos arcabouços teóricos e conceituais supracitados.

Já o outro aspecto consequente da identificação e do uso das capacidades cibernéticas advém da tipificação defensiva, que aparece de maneira vaga em várias estratégias de defesa, segurança e *cyber* segurança dos Estados Unidos, classificada um conjunto de esforços e estratégias voltadas a fortalecer as estruturas de defesa cibernéticas domésticas ou

internacionais. Dada a superficialidade desse conceito, essa pesquisa utilizará as contribuições de Hadji-Janev e Bogdanoski (2015) e Brasil (2023) para refinar essa noção, agora indicadas como um ato de aprimoração de sistemas tecnológicos - individuais ou em caráter doméstico geral - voltados a mitigar ataques cibernéticos contra suas infraestruturas críticas, reduzindo, em um primeiro nível de ação, a dependência de outros atores presentes no SI - principalmente com os órgãos internacionais normativos ante a temática cibernética.

Ainda segundo esses autores, a outra dinâmica de movimentação está no fomento da cooperação - doméstica ou internacional - e na criação, implementação e assinatura de normas cibernéticas com abrangência internacional, com o objetivo de construir um Sistema Internacional Cibernético com maiores níveis de concordância ante a temática. Tais atos e conceitos são exemplificados por Hitchens e Goren (2017), que mostram o esforço dos Estados de construir redes de cooperação e legislação conjuntas, através de assinaturas de tratados e acordos temáticos voltados à elaboração de temas defensivos de *cyber* segurança em um nível internacional. Já no âmbito doméstico, a demonstração dessas capacidades aparece nas estratégias estadunidenses de defesa e segurança cibernética, que indicam quais são os parâmetros de idealização e uso destas capacidades em um período específico.

O último tipo de seleção discute a materialidade dos conceitos, que, assim como pontuada na escolha dos atores principais na temática cibernética, variam a partir dos autores e dos padrões epistemológicos utilizados (Braga, 2013). Essa movimentação autoral realça e determina os níveis de objetividade ou subjetividade presentes no campo cibernético, gerando análises, resultados e conceitos que tentam entender como o campo teórico cibernético funciona e se constitui. Tal trama pode ser exemplificada na noção do ciberespaço - ponto focal no estudo de cibersegurança - que, em uma concepção mais ampla, pode ser identificado como uma área intangível, resultante somente das interações entre agentes como forma para determinar sua existência.

Ao se utilizar de tal noção mais subjetiva e normalmente mais pós-positivista, a construção do pensamento e da realidade cibernética se torna mais ampliada, metafísica e socialmente construída, focada em entender como as relações sociais e de poder são perpetradas no SI. Isso gera conceitos mais abstratos sobre o tema cibernético, pontos promotores de análises voltadas à indicação dos desafios pertencentes ao âmbito e aos processos vinculados a ele, distanciando-se, com isso, da elaboração de respostas a problemas empíricos apresentados nesse espaço.

Já uma conceituação mais objetiva e positivista - escolhida por essa pesquisa - se afasta dos aspectos metafísicos inerentes à temática cibernética, pois tenta explicar como os processos cibernéticos conseguem repetir noções determinadas cineticamente, ancorando o entendimento e as conceituações temáticas nas bases tradicionais de pensamento e análise. Um exemplo claro disso está na utilização da definição de *cyber* território ou *cyber* espaço de Nye (2011, p. 04) que engloba todas as redes de *Internet*, *Intranet*, conexão entre computadores, redes de cabos de fibra óptica e comunicações espaciais.

Ao usar tal conceito, Nye (2011) concede ao espaço cibernético, normalmente amplo e impalpável, vinculação física e geográfica, citando como necessário o cumprimento de todas as leis anexadas a estes locais. Com essa determinação, o espaço cibernético se torna material, palpável, com limites e fronteiras domésticas, ponto que ajuda a construir análises mais fundamentadas em concepções já existentes, gerando assim modelos positivistas de entendimento acerca de fenômenos cibernéticos variados.

Não obstante, ao considerar o conceito de Nye (2011) que percebe o ciberespaço como diversos microcosmos domésticos com a definição de poder cibernético de Nye (2010), infere-se a existência de um Sistema Internacional Cibernético. Este aspecto amplia o pensamento do SI convencional, que agora compreende as interações dos agentes presentes em um ciberespaço geograficamente fixado em um caráter internacional.

Com isso, a produção de um Sistema Internacional Cibernético, decorrente da soma de todas as unidades domésticas do ciberespaço, assimila e se utiliza de percepções já consolidadas e discutidas, mas determinadas agora em um outro nível de análise - o cibernético. Isso traz o desafio de indicar e compreender as similaridades e as diferenças provenientes de uma análise cibernética construída por conceitos positivistas tradicionais, criando, assim, associações temáticas e conceituais.

Outro exemplo que se utiliza de padrões positivistas e materiais é o de infraestrutura crítica, que é definido por Ferreira (2017), em conjunto com Brasil (2018; 2023, p. 03), como um espaço, normalmente físico, que contém dados, instalações, serviços, bens e sistemas com um papel essencial e estratégico para a segurança e soberania de um Estado e sua população. Dessa forma, qualquer interrupção ou destruição - total ou parcial - consegue provocar sério impacto social, ambiental, econômico, político e internacional a uma infraestrutura crítica de um ator do Sistema Internacional Cibernético.

Uma demonstração desse conceito está no entendimento que uma hidrelétrica estatal é uma infraestrutura crítica da mesma forma que um servidor com dados pessoais de empregados

também o é. Isso acontece, pois a orientação dessa definição não está na grandeza do dano a ser realizado, mas, sim, nas possibilidades de interferência futuras ou nas problemáticas derivadas do ato, visto que ambas as condutas conseguem gerar preocupação e efeitos - mesmo que em graus diferentes contra setores diferentes - em uma sociedade ou a um ator em específico, caso sejam invadidas.

Somada tal noção ao pensamento geográfico cibernético presente nos trabalhos de Nye (2010; 2011), a ideia de infraestrutura crítica, de Ferreira (2017), ganha atribuição material ante a localização[8] do que se deve proteger e da origem da ação do agente malicioso atacante. Ao realizar tal mobilização, é trazida à análise cibernética marcos legais de proteção cinética já existentes, podendo gerar até mesmo uma responsabilização concreta ante um ataque cibernético.

Não obstante, o pensamento sobre imputações geográficas dos atos realizados também é utilizado pelo COT de CFR (2024) a fim de estabelecer e indicar com maior eficiência as operações cibernéticas e seus principais suspeitos atacantes em sua base de dados. Ressalta-se a exclusão, para esta dissertação, de pensamentos de defesa e proteção de infraestrutura crítica voltados ao tráfego de dados submarinos, e suas possíveis atribuições nas dimensões culturais e informacionais. Dessa forma, a pesquisa se focará somente nos âmbitos militares, diplomáticos e econômicos advindos dos casos cibernéticos abordados.

Definidos os conceitos cibernéticos, as dicotomias e os desafios teóricos e as seleções utilizadas nessa pesquisa, o capítulo se encerrará com a indicação de como estas deliberações podem construir um modelo analítico coerente, baseado em algumas premissas oferecidas no referencial conceitual cibernético *S.A.M.* (*Stakeholder, Actions and Motives* - Partes Interessadas, Ações e Motivos em inglês) de Kremer e Müller (2013). Primeiramente, o *S.A.M.* de Kremer e Müller (2013, p. 45 e 46) é uma concepção teórica qualitativa que enfatiza, esquematiza e dispõe logicamente um ato cibernético através de três pontos focais.

Dessa forma, o referencial *S.A.M.*[9] entende quem seria o agente mais importante em uma dada ação cibernética - (1) as Partes interessadas ou *Stakeholders* -; qual é a ação realizada, como ela será promovida e quais foram os resultados percebidos - (2) as Ações -; e quais seriam as principais motivações e intenções dos atos em si; e (3) os Motivos. Neste trabalho, ao retomar

[8] Localização alcançada mesmo em pontos geográficos legalmente limitados, como em águas internacionais ou no espaço sideral, sendo realizado através da determinação do local da infraestrutura crítica em questão.

[9] A fim de desintrincar o referencial *S.A.M.*, os elementos Partes Interessadas, Ações e Motivos, serão escritos nesta dissertação com letras maiúsculas. Com isso, há um entendimento de que elementos retratados possuem características e conceituações próprias definidas nesta pesquisa por Kremer e Müller (2013), diferenciando-os de seus substantivos-fonte.

as preferências relatadas anteriormente e conectá-las aos princípios do referencial *S.A.M.*, terá como Parte Interessada os Estados Unidos da América e suas ações com outros Estados percebidos pelos próprios EUA como aliados - Países Baixos, Reino Unido, Estônia e Índia - ou oponentes - China, Rússia, Irã e Coreia do Norte.

No que tange às Ações realizadas pelos Estados Unidos, será utilizada a conceituação e ampliação de atos cibernéticos de Burton (2015) voltados à construção e utilização das capacidades cibernéticas ofensivas de Smeets e Lin (2018) e Bellovin, Landau e Lin (2017) e defensivas de Hadji-Janev e Bogdanoski (2015) e Brasil (2014) representadas por CFR (2024) no âmbito ofensivo e pelo trabalho de Hitchens e Goren (2017) no campo defensivo, para assim indicar como estas capacidades foram utilizadas, quais foram seus alvos centrais, como tal ato se encerrou no Sistema Internacional Cibernético e quais foram as consequências advindas dos atos. Em relação aos Motivos, foi considerado o teste das hipóteses geral e secundárias da projeção de poder cibernético de Nye (2010) visando a ampliação de influência e capacidades de intromissão no espaço cibernético e nas infraestruturas críticas determinadas através das percepções de Nye (2010 e 2011) e Ferreira (2017).

O próximo capítulo se utilizará do elemento (2) do referencial *S.A.M.*, as Ações, voltadas a apresentar como as capacidades cibernéticas ofensivas e defensivas dos Estados Unidos foram realizadas entre 2010 a 2020. Dessa forma, serão indicados os principais fatos e ocorrências presentes na utilização das capacidades cibernéticas estadunidenses nos 11 anos selecionados.

CAPÍTULO 2 - 11 ANOS DE CAPACIDADES CIBERNÉTICAS: PROGRESSÃO ANUAL DOS ATOS ESTADUNIDENSES

Este capítulo dará prosseguimento ao referencial conceitual de Kremer e Müller (2013) apresentado na seção anterior, expandindo e informando seu segundo tópico de análise teórica: as Ações. De acordo com Kremer e Müller (2013, p. 49), uma Ação é constituída por um ato malicioso, realizado com um objetivo prévio, que tem como propósito a criação de um impacto, seja esse cinético ou cibernético, direto ou indireto.

Tal fundamento será explicitado através de uma exposição dos principais empreendimentos cibernéticos ofensivos realizados pelos Estados Unidos entre 2010 a 2020 para com seus principais aliados e oponentes. Embora Kremer e Müller (2013) não disponham em seu conceitual a utilização das capacidades defensivas como forma de uma Ação, esta dissertação irá considerar as condutas cibernéticas defensivas estadunidenses como parte desse conceito específico, visto que tais atos também geram repercussões diretas e indiretas aos atores envolvidos.

Os atos ofensivos abordados no capítulo perpassam pelos orçamentos anuais divulgados publicamente pelo Departamento de Defesa (DoD) dos EUA para a área de segurança e defesa doméstica e internacional, manifestando a devida parcela externada para a estratégia cibernética no período. A fim de trazer informações mais exatas acerca do nível orçamentário estadunidense, a dissertação usará somente os informes de orçamento promulgado, disponíveis apenas no ano fiscal posterior ao ano analisado. Ou seja, com o intuito de analisar os recursos oficiais orçamentários de 2010, foram avaliados apenas os valores proclamados e oficializados no orçamento de 2011, e assim sucessivamente.

Após sinalizar o nível orçamentário utilizado em cada sessão anual, serão evidenciados os principais atos de construção legislativa ou demonstração das capacidades cibernéticas ofensivas realizadas pelos Estados Unidos, selecionando as principais ocorrências dispostas. Com o propósito de detalhar as Ações estadunidenses nos anos de uma forma descomplicada, as seções deste capítulo assinalarão os atos cibernéticos ofensivos realizados e atribuídos aos Estados Unidos, seguindo a lógica de Zetter (2014), de forma a apontar uma breve contextualização do caso e seguir os fatores de apresentação salientados pelo CFR (2024).

São eles: o tipo de incidente, a data aproximada da realização do ato, possíveis filiações do caso no tempo, os atores afetados, a reação do governo afetado e o nível de resposta governamental nas camadas domésticas e internacionais. No fim de cada seção ofensiva anual, serão expostos os atos ofensivos relevantes realizados contra os Estados Unidos, cometidos

especificamente pelos grupos selecionados por esta dissertação - aliados ou oponentes dos EUA.

Seguidamente, serão indicadas as principais construções das capacidades cibernéticas defensivas dos EUA, ressaltadas nos escritos de Hitchens e Goren (2017) e nas fontes voltadas à produção ou participação de reuniões cibernéticas relevantes e da assinatura de acordos temáticos bilaterais ou multilaterais, realizadas com os Estados propostos ou em associação a eles. Serão pontuados, quando existentes, pareceres, anuências e detalhes acerca das principais conjecturas legislativas cibernéticas internacionais dispostas nos anos.

2.1 - O ano de 2010: Capacidades Ofensivas Estadunidenses

Composta no segundo ano do primeiro mandato de Barack Obama, o ano de 2010 teve como base orçamentária para os assuntos de defesa e segurança uma soma de 531 bilhões de dólares, com um aumento de 2,9% ao ser comparado com os 516 bilhões de dólares do ano anterior. Desse valor, o Departamento de Defesa destinou 18 milhões de dólares para a construção e aprimoramento do tópico de cibersegurança, elemento que se tornou gradual e politicamente mais relevante nos últimos anos.

O interesse crescente à matéria cibernética não surgiu estritamente do governo Obama, visto que desde 2003, assim como pontuado por Maier (2019, p. 114-115) e Zetter (2014, p. 92), estavam sendo criados arquétipos legislativos domésticos para a defesa das infraestruturas críticas dos EUA e para o fortalecimento das capacidades cibernéticas Estatais. Um exemplo desse posicionamento está na criação da *"National Strategy to Secure Cyberspace"* (Estados Unidos da América, 2003) em 2003 pelo governo George W. Bush, que definiram as principais prioridades ante a ação de agentes maliciosos.

Já outro modelo foi constituído pela *"Comprehensive National Cybersecurity Initiative"* (Estados Unidos da América, 2009a) de 2008 que elaborou as principais diretrizes cibernéticas para serem seguidas e fomentadas nos anos posteriores. Ponto cumprido com a oficialização, em 2009, da pedra basilar "*Cyberspace Policy Review"* (Estados Unidos da América, 2009b) criadora do Comando Cibernético dos Estados Unidos da América, a USCYBERCOM.

A USCYBERCOM foi oficializada em 2010 como um comando conjunto de todos os departamentos e agências militares, de defesa, inteligência e de informação voltado a "sincronizar, coordenar, planejar e estabelecer operações militares cibernéticas em prol da

defesa dos interesses nacionais estadunidenses, com uma colaboração doméstica ou com seus aliados" (Dziwisz e Romaniuk, 2023, p. 307 a 308 - tradução nossa).

Sumariamente, este órgão tem como prerrogativa central a proteção, suporte e fortalecimento das matrizes cinéticas militares ofensivas e defensivas. Adicionalmente, essa instituição lida com a associação dos aparatos tecnológicos e cibernéticos em dois níveis - doméstico e internacional -, podendo ser cooperativo ou não. Dessa forma, o Comando Cibernético pode ser visto como um elemento potencializador e agrupador dos instrumentos militares estadunidenses, usados no Sistema Internacional de forma a garantir sua defesa (Amoretti e Fracchiolla, 2018, p. 04).

Ao progredir com a seção ofensiva cibernética, CFR (2024), Zetter (2014) e Clarke e Knake (2012) reconhecem e identificam, entre julho e agosto de 2010, *Missile* e o *Payload* do ataque contra o Irã. De acordo com esses autores, o *malware* denominado *Stuxnet* comprometeu ICS[10] (*Industrial Control Systems* - Sistemas de Controle Industriais, em inglês) voltadas às PLCs[11] (*Programmable Logic Controllers* - Controladores de Lógica Programável, em inglês), que monitoravam todas as centrífugas presentes nas instalações de enriquecimento nuclear iranianas.

Em junho de 2010, foi constatado, principalmente pela empresa californiana Symantec, que o *Stuxnet* lançou *Missiles* - de junho de 2009 a abril de 2010 - contra cinco empresas iranianas voltadas às áreas de engenharia, eletricidade, tecnologia e automação cerca de 12.000 vezes (Zetter, 2014, p. 65). Circunstância que permitiu o alastramento do *malware* em mais de 100.000 máquinas disponibilizadas em cerca de 100 países.

A partir da investigação dos analistas da Symantec, foi descoberto em julho de 2010, que o principal *Payload* do *Stuxnet* era a usina de enriquecimento de urânio em Natanz, no Irã. A fim de alcançar tal objetivo, esse *malware* se utilizava de *Zero-Day Exploits*[12] (Inventos de

[10] Thomas et al. (2020, p. 50 - tradução nossa) define os Sistemas de Controle Industrial como todos os dispositivos, ferramentas tecnológicas, unidades remotas, *softwares* e serviços que proporcionam controle e informação aos processos físicos em fábricas, usinas de energia, instalações de tratamento de água dentre outras infraestruturas críticas dispostas por um Estado.

[11] Segundo Zetter (2014, p. 13 e 87) e Thomas et al. (2020, p. 50), os Controladores de Lógica Programável são microcomputadores, normalmente autônomos, que são usados para regular, informar ou controlar operações sensíveis presentes nas indústrias e nas infraestruturas de todo o mundo, garantindo sua total operacionalização de forma semi autônoma.

[12] *Zero-Day Exploits* são definidas como falhas raras presentes em um *software*, criadas no momento de seu desenvolvimento, que podem gerar vulnerabilidades de ataque a serem utilizadas por agentes maliciosos. A tamanha especificidade derivada desse equívoco permite que nenhuma ferramenta de defesa ou antivírus consiga detectar e consertar as fragilidades atacadas em um momento anterior a sua identificação e uso (Zetter, 2014, p. 08)

Dia-Zero, em inglês) para infectar uma máquina e assim conseguir difundi-la em outra, fazendo, com isso, uma movimentação de *botnet*[13] e *worm*.

Ao seguir essa estratégia, foi criado um caminho eficiente em direção à infraestrutura crítica das PLCs de Natanz, sobrecarregando e sobreaquecendo as centrífugas utilizadas para o enriquecimento de urânio. A sabotagem realizada pelo *Stuxnet* permitiu um aumento exagerado na rotação das centrífugas enquanto indicava leituras irregulares de temperatura e aceleramento, mostrando-as como normais. Com isso, algumas falhas suspeitas foram percebidas doméstica e internacionalmente no território iraniano, como explosões em canos de transporte de gás e trocas massivas das próprias centrífugas em Natanz, chegando até mesmo a alcançar o número de 1.000 centrífugas compradas entre janeiro e abril de 2010, trazendo a inferência que cerca de 2.000 centrífugas foram avariadas no período (Zetter, 2014, p. 07, 83).

Esses fatos, somados às omissões informacionais realizadas pelo governo iraniano em prol de disfarçar a existência e os danos gerados pelo *Stuxnet*, permitiram uma ação e disseminação mais intensa do *malware* durante o ano de 2010. O nível de periculosidade do vírus cresceu de tal forma que começou a infectar máquinas e dispositivos não iranianos.

Elemento reforçado através da indicação do CFR (2024) da presença do vírus em PLCs de mais 11 Estados, como Azerbaijão, Reino Unido, Estados Unidos, Indonésia, Paquistão, Uzbequistão, Coreia do Sul, Índia, Malásia, Rússia e Taiwan, trazendo o temor de que *Payload* conseguisse sabotar PLCs industriais involuntariamente. Vale ressaltar que a identificação de todas as informações a respeito dos inconvenientes, possibilidades, vetores e objetivos de ataque referentes ao *Stuxnet* só foram identificados e dispostos ao público em agosto de 2010, possibilitando somente nesse momento a criação de soluções ante o combate desse *malware* (Zetter, 2014, p. 93).

Zetter (2014), Sanger (2012) e CFR (2024) em uma investigação aprofundada do caso, conseguiram inferir a responsabilidade do ataque realizado pelo *Stuxnet* prioritariamente aos Estados Unidos, associando o ataque a uma operação cibernética militar de codinome "*Olympic Games*" datada de 2006, que tinha como objetivo reduzir, através de manobras militares sigilosas, a ampliação de poder e influência realizada pelos países do oriente médio que tinham acesso a energia nuclear. Tal operação visava principalmente o Irã, pois havia um temor advindo

[13] Uma ação de *botnet*, assim como salientado no trabalho de Clarke e Knake (2012) e Lima (2019, p. 29), foca na infecção de vários computadores ou dispositivos, os deixando em um estado de acesso remoto com o objetivo de realizar um *worm*, que se trata de uma situação quando várias máquinas infectam automaticamente outras máquinas em um curto período, para assim esperar por uma ordem específica de ação.

dos EUA de que as aspirações nucleares iranianas não poderiam ser pacíficas (Zetter, 2014, p. 32).

O medo do crescimento do programa nuclear iraniano também aumentou as questões e tensões geopolíticas já existentes entre Israel e Irã, se dedicou a operacionalizar e financiar ataques cibernéticos com a intenção de frear qualquer fomento indesejado em Natanz (Zetter, 2014, p. 51, 116 e 124). Dito isso, foi percebida, através dos trabalhos de Zetter (2014, p. 159 e 183), Sanger (2012), Clarke e Knake (2012) e CFR (2024), uma participação posterior de Israel no desenvolvimento de versões mais avançadas do *Stuxnet* em conjunto com os Estados Unidos realizadas entre janeiro de abril de 2010, variante essa mais direcionada às PLCs de Natanz.

O incidente de sabotagem militar *Stuxnet* foi considerado por Zetter (2014) e CFR (2024) como a primeira operação cibernética militar Estatal publicamente conhecida que gerou dano físico em infraestruturas críticas estatais. Tal ocorrência gerou diversas consequências no mundo, sendo a principal as denúncias internacionais realizadas pelos países afetados pelo *Stuxnet*, principalmente o Irã. Isso minou a confiança internacional estadunidense em um âmbito cibernético, pois, por ser o principal Estado suspeito[14]; foram levantadas incertezas e temores perante as novas políticas pacíficas e multilaterais voltadas a esse âmbito iniciadas por Barack Obama a partir de 2009 (Maier, 2019, p. 114).

Já outro produto dessa circunstância resulta do fato de que, por realizar uma manobra de *botnet* e *worm*, o *malware* e seus códigos de atuação e criptografia foram difundidos amplamente pela *internet*. Isso, ao ser somado às possibilidades de destruição inerentes desse *malware*, permitiu que os agentes maliciosos se utilizassem de partes do código para desenvolverem novos tipos de ataques e viabilizarem danos distintos as ICS, permitindo com que fossem criados novas categorias de ciberataques utilizadas no mundo. Contudo, o caso *Stuxnet* também possibilitou que diversas legislações, acordos e movimentações cooperativas defensivas internacionais pudessem ser criadas para a mitigação e proteção da ameaça criada por esse *malware*, criando reflexos positivos futuramente.

No que tange aos ataques cibernéticos efetuados contra os Estados Unidos, o CFR (2024) atribui apenas duas ocorrências existentes no período, presentes no caso *Operation Aurora* e *Night Dragon*. Ambos os atos ofensivos foram imputados à China e foram identificados como ocorrências de espionagem. Apenas o caso *Operation Aurora* teve uma

[14] Vale ressaltar que, segundo Feitosa (2017, p. 40) e apoiado por CFR (2024), os líderes dos Estados Unidos ainda não assumiram publicamente a autoria ante o ataque *Stuxnet*.

reação dos EUA, disposta através de uma denúncia internacional realizada, seguida da negação pública do envolvimento chinês ante o acontecimento.

2.1.1 - O ano de 2010: Capacidades Defensivas Estadunidenses

O ano de 2010 no quesito defensivo, a partir das deliberações de Hitchens e Goren (2017) e Maier (2019), abarcou a construção e o fomento estadunidense de suas capacidades em três circunstâncias marcantes. A primeira se encontra no foco do governo Obama em promover ações cooperativas cibernéticas multilaterais, se utilizando mais assertivamente de seu *soft-power*[15] internacionalmente, alçando novos temas e inaugurando posicionamentos realizados pelos EUA no Sistema Internacional. Com isso, segundo Maier (2019, p. 114), seria garantida confiança e percepção renovada por outros agentes aos Estados Unidos - sejam eles parceiros ou adversários.

A segunda movimentação defensiva realizada pelos Estados Unidos baseia-se na participação e assinatura de tratados e acordos bilaterais e multilaterais temáticos internacionalmente. Posto isso, as lideranças dos EUA subscreveram na *"NATO and Estonia Agreement on Cyber Defense"* em conjunto com outros 28 países, sendo alguns deles a Estônia, o Reino Unido e os Países Baixos. Definida pela Organização do Tratado do Atlântico Norte (OTAN - *NATO - North Atlantic Treaty Organization* em inglês) esse acordo tem como premissa a criação de um arquétipo de cooperação voltada à defesa cibernética. O tratado também facilitou a troca de informações entre os integrantes e forneceu mecanismo de assistência em casos de *cyber* ataques (Hitchens e Goren, 2017, p. 61).

A última movimentação das capacidades defensivas estadunidenses em 2010 está na reafirmação estatal na *United Nations Groups of Governmental Experts (GGE* - Grupo Governamental de Especialistas da Organização das Nações Unidas em inglês) voltado ao desenvolvimento no campo de informação e telecomunicação ante o contexto da segurança internacional. A partir do texto de Klaar (2021, p. 03) e Hitchens e Goren (2017, p. 30), um grupo de GGE surge da necessidade comum entre diversos atores da Organização das Nações Unidas (ONU) para identificar e mitigar cooperativamente um assunto específico visto como uma adversidade. Isso é realizado através do estabelecimento de reuniões bianuais que discutem

[15] *Soft Power* (poder brando - em inglês) é um conceito definido por Joseph Nye que aponta um espectro no qual um ator pode conseguir e exercer poder no Sistema Internacional, criando relações com atores diversos ao seguir padrões de criação de agendas, atração e persuasão para influenciar pacificamente as preferências dos atores, obtendo, com isso, resultados favoráveis ao ator que utiliza essa tipologia de poder (Nye, 2010, p. 02).

e particularizam as temáticas abordadas, criando no final destes dois anos um relatório de intenções e possíveis ações realizadas pelos Estados-membros.

A partir disso, em 2004, surge na ONU o primeiro comitê de GGE com 15 membros[16] voltado a definir uma tipologia comum sobre as ameaças cibernéticas aos atores do Sistema. Não obstante, a delegação criada tentou especificar formas de combate às ameaças, utilizando-se das capacidades cibernéticas conjuntamente às capacidades militares existentes. O grupo também pontuou as melhores práticas de intercâmbio de informações - proposta pela Rússia - e de defesa das infraestruturas críticas de acesso à informação - tencionado principalmente pelos Estados Unidos. Contudo, o primeiro conselho da GGE de 2004 a 2005 não obteve nenhum sucesso prático nas definições devido a falta de consenso entre os membros participantes, impossibilitando, com isso, a criação de um relatório oficial com premissas a serem seguidas.

No entanto, a segunda conferência da GGE ocorrida entre 2009 a 2010 obteve resultados palpáveis ante o desenvolvimento de práticas positivas voltadas à temática cibernética. Tal progressão só foi possível devido ao aumento da percepção da periculosidade dos incidentes cibernéticos no mundo, principalmente após dois dos três grandes casos de cibersegurança - o caso da Estônia de 2007 e o caso da Geórgia em 2008 (Gratão, 2022, p. 03). Isso fez com que os Estados e as Organizações Internacionais (OIs) se movimentassem em prol de entender e criar regras comuns que criem limites de ação dos Estados no espaço cibernético (Klaar, 2021, p. 04).

O entendimento gerado fez com que os mesmos 15 Estados se reunissem em julho de 2010 com a missão de "continuar a estudar ameaças potenciais e factíveis em conformidade à esfera da segurança da informação e assim definir possíveis medidas de cooperação a fim de enfrentá-las" (Klaar, 2021, p. 04 - tradução nossa). Com isso foi produzido o relatório oficial A/65/201 que fundamentou princípios básicos de definição de ameaças cibernéticas, criadas a partir da necessidade de se proteger as infraestruturas críticas em um nível Estatal. Também foram expressas no documento recomendações de fomento à cooperação internacional cibernética de forma a reduzir conflitos (Klaar, 2021, p. 05 e Hitchens e Goren 2017, p. 31).

O segundo encontro do GGE, segundo Klaar (2021), foi um marco multilateral para o desenvolvimento e irradiação da agenda de segurança cibernética no mundo, visto que países distintos e muitas vezes adversários - como Estados Unidos, China e Rússia - conseguiram estabelecer um diálogo acerca da normatização das práticas cibernéticas realizadas pelos

[16] Hitchens e Goren (2017) especificam que os membros da GGE nesse período foram a África do Sul, Alemanha, Bielorússia, Brasil, Catar, China, Coreia do Sul, Estados Unidos da América, Estônia, França, Índia, Israel, Itália, Reino Unido e Rússia.

Estados. Isso fez com que fossem discutidos, pela primeira vez, práticas e noções puramente técnicas de *cyber* segurança aos decisores políticos estatais, criando uma ponte de diálogo valiosa (Klaar, 2021). No entanto, a manutenção e o respeito desse diálogo eram tidos como nebulosos, carecendo de uma observação mais específica acerca do acato dessas legislações.

2.2 - O ano de 2011: Capacidades Ofensivas Estadunidenses

O ano de 2011 no contexto cibernético foi marcado pela falta de utilização das capacidades ofensivas estadunidenses contra os atores do Sistema Internacional Cibernético, elemento indicado pela ausência de *cyber* ataques confirmados e atribuídos aos Estados Unidos pelo CFR (2024). Essa inação também pôde ser observada no orçamento anual do DoD nos assuntos de segurança e defesa, através de uma diminuição de cerca de 0,9% em relação ao ano anterior, na soma de 526 bilhões de dólares. A reserva destinada ao tema cibernético também sofreu uma retração neste ano, com um decrescimento de 19,3% representados nos 14,6 milhões de dólares divulgados em seus relatórios orçamentários.

No entanto, durante esse ano, foi percebido um aumento nas posturas voltadas à potencialização dos arquétipos legislativos domésticos, estabelecendo uma unilateralidade ofensiva e uma maior multilateralidade no aspecto defensivo - abordado na seção defensiva a seguir. Relativamente aos parâmetros ofensivos, em 2011 foi publicada a *International Strategy for Cyberspace* (Estados Unidos da América, 2011), que tem como argumento central a criação de parâmetros cibernéticos domésticos comuns em prol de avançar medidas de combate ou cooperação no espaço cibernético (Maier, 2019, p. 115). Tais preceitos focam no desenvolvimento de políticas e acordos voltados a garantir as liberdades de expressão, privacidade e propriedade intelectual, pontos centrais para continuidade da segurança e manutenção do ciberespaço (Maier, 2019, p. 115 e 116 e Estados Unidos da América, 2011, p. 12-13).

Dessa forma, os representantes das estruturas públicas dos Estados Unidos tentaram estabelecer com a *International Strategy for Cyberspace* um papel de liderança cibernética ao demonstrar seu comprometimento com a criação e respeito às leis internacionais voltadas ao espaço cibernético, de forma a “sinalizar ao mundo que estamos sérios acerca do enfrentamento do desafio com forte liderança e visão. A liderança deve ser elevada e fortemente ancorada na Casa Branca para fornecer orientação, coordenar ações e alcançar resultados” (Estados Unidos da América, 2011, p. 03 - tradução nossa). Ao instituir esse pensamento, a atração e a

cooperação de Estados interessados e semelhantes (*likeminded States*) seria inevitável, gerando uma estabilidade no âmbito cibernético pautada pelo respeito e garantia das normas, defesa das liberdades individuais, respeito a propriedade - que seguirá normativas cinéticas estabelecidas no capítulo 1 -, valorização da privacidade, à proteção contra o crime e o direito à autodefesa (Maier, 2019, p. 116).

A fim de assegurar o cumprimento dos direitos supracitados, as organizações dos Estados Unidos indicam em sua estratégia uma ampliação unilateral ao direito de ação possível contra atos hostis presentes no ciberespaço. Tal ato legítima aos EUA o uso de qualquer meio necessário - cinético ou não - a fim de garantir sua autodefesa no Sistema Internacional contra ações de agentes maliciosos caracterizados como "ameaças aos Estados Unidos, seus parceiros e seus interesses" (Estados Unidos da América, 2011, p. 12 e 14).

O *International Strategy for Cyberspace* também definiu critérios de classificação destes agentes maliciosos, identificando-os como "terroristas, cibercriminosos ou Estados e seus mandatários" (Estados Unidos da América, 2011, p. 12 - tradução nossa). Através dessa movimentação política e estratégica, sugere-se uma tentativa estadunidense no governo Obama de garantir graus de domínio e relevância no Sistema Internacional Cibernético em um nível ofensivo (Maier, 2019, p. 117).

Dito isso, é percebido através das informações dispostas em CFR (2024) uma triplicação de *cyber* ataques realizados contra os EUA em 2011, com oito ataques registrados. Esses episódios variaram entre ataques de negação de serviço e espionagem dispostos nos comprometimentos dos *tokens* de identificação da empresa estadunidense de *cyber* segurança RSA; nos ataques à Força Conjunta Estados Unidos-Coreia do Sul; nas investidas contra Laboratório Nacional de Oak Ridge; contra à Câmara de Comércio dos EUA; nas interferências dos satélites *LandSat* 7; e Terra (EOS AM-1) da NASA (sigla referente a *National Aeronautics and Space Administration* - Administração Nacional da Aeronáutica e Espaço em inglês) e nos casos *Shady Rat* e *Nitro Attacks*.

Dos ataques supracitados, sete deles foram responsabilizados à China e apenas um à Coreia do Norte, através da participação nos ataques à Força Conjunta Estados Unidos-Coreia do Sul. Nota-se reação em somente uma das ocorrências indicadas, presente no caso de interferência do satélite LandSat 7 da NASA, realizada pela China através da negação ante a autoria do ataque.

2.2.1 - O ano de 2011: Capacidades Defensivas Estadunidenses

No ano de 2011, os representantes dos Estados Unidos participaram de duas deliberações de natureza legislativa com aliados. O exemplo dessa comoção está na presença estadunidense no *Memorandum of Understanding* (MoU) - Memorando de Entendimento em inglês - em conjunto com a Índia em janeiro de 2011.

Preliminarmente, um MoU, a partir dos escritos da Agência dos Estados Unidos de Desenvolvimento Internacional (em inglês *United States Agency of International Development*) USAID (2024, p. 01), se trata de um documento que descreve as principais intenções, papéis e responsabilidades dos atores em prol de uma temática específica, minuciando os principais desafios e soluções. Um MoU, em um contexto amplo, não tem um aspecto juridicamente vinculativo ante a sua assinatura, ou seja, ele não carrega em si direitos ou deveres a serem obrigatoriamente cumpridos entre as partes (USAID, 2024, p. 01). Contudo, em alguns casos, um MoU pode ter vínculos legais mais brandos, caso esteja especificada no tratado, variando a depender do caso e do tratado a ser analisado.

O *Memorandum of Understanding* entre os EUA e a Índia em 2011 tem um vínculo legal e trata da criação das melhores práticas em torno do fomento do tema de cibersegurança crítica - voltada à defesa prioritária das infraestruturas críticas governamentais (Hitchens e Goren, 2017, p. 60). O foco desse documento estava na ampliação da cooperação entre CERTs[17] governamentais (*Computer Emergency Response Team* - Time Emergencial de Resposta Computacional - em inglês) para assim serem desenvolvidas as melhores métricas de ação entre os grupos, aprimorando os níveis de perícia cibernética voltadas à defesa e os *timings* de ambos os CERTs na mitigação do dano ocasionado por um ataque cibernético.

Já o último acordo assinado pelos representantes dos EUA ocorreu em fevereiro de 2011 com o "*Poland Agreement with NATO Consultation, Command, and Control Agency*". Esse acordo tinha como objetivo o desenvolvimento cibernético entre governos - principalmente a Polônia - e a OTAN para facilitar pesquisas conjuntas e assim baratear os custos utilizados na ciberdefesa.

[17] Segundo o Departamento de Segurança Interna dos Estados Unidos *(Department of Homeland Security* - DHS) (Estados Unidos da América, 2024 p. 01), um CERT se trata de um time responsável por analisar e reduzir as vulnerabilidades e as ameaças presentes no espaço cibernético. Para isso, os CERTs fazem ações de disseminação de informações e avisos acerca do tema, cooperam doméstica e internacionalmente com outros CERTs, ajudam em investigações federais e forenses e propõem as melhores técnicas de análise e ação voltada ao combate de agentes maliciosos.

O intuito desta deliberação era estipular práticas comuns de fomento técnico para impedir exclusividade tecnológica em aspectos básicos da defesa cibernética entre os países-membros da Organização do Tratado do Atlântico Norte. Através desse acordo, houve uma tentativa de criar homogeneidade nas práticas e nas ferramentas de detecção e proteção ante a ataques cibernéticos entre todos os membros da OTAN (Hitchens e Goren, 2017, p. 60).

2.3 - O ano de 2012: Capacidades Ofensivas Estadunidenses

O período de 2012 foi um ano importante para a temática cibernética. No que diz respeito ao orçamento anual focado nas áreas de segurança e defesa, foi aprovada publicamente uma quantia de 529 bilhões de dólares, um aumento de 0,5% em relação ao ano anterior, tendo nessa soma de 16,6 milhões de dólares reservados aos assuntos cibernéticos estatais, com um aumento de 13,6%. A conjuntura doméstica cibernética também teve um desenvolvimento visível com a Ordem Executiva 13.618 que ajudou o governo Obama a trazer uma reforma mais assertiva à *cyber* segurança estadunidense (Amoretti e Fracchiolla, 2018, p. 14).

Tal determinação enfatizava a necessidade dos órgãos públicos dos Estados Unidos de atualizar suas capacidades cibernéticas domésticas para assim lidarem e se prepararem mais ativamente contra as ameaças advindas do ciberespaço, identificando, investigando e mitigando os riscos virtuais. Dessa forma, foram iniciados, em 2012, os primeiros ajustes do estabelecimento de um órgão público três anos depois, em 2015, o *Cyber Threat Intelligence Integration Center* (CTIIC - Centro Integrado de Inteligência contra as Ameaças Cibernéticas, em inglês), abordado posteriormente neste capítulo.

Dito isso, os exemplos marcantes de ações ofensivas estadunidenses se baseiam em dois ataques cibernéticos descobertos no ano de 2012 - os casos *Flame* e *Gauss*. Inicialmente, segundo CFR (2024) e Zetter (2014, p. 179), *Flame* foi um *spyware*[18] altamente sofisticado desenvolvido para a espionagem de dados de diversas empresas e organizações governamentais iranianas, adquirindo documentos, gravando conversas e memorizando todas as teclas digitadas das máquinas infectadas, determinando, com isso, as senhas e os usuários utilizados, repassando posteriormente ao Servidor de Comando-e-Controle[19] (C&C) do agente responsável pelo ataque.

[18] Segundo CISA (2024, p. 01), um *spyware* é um tipo de *malware* direcionado a espionagem coletando todo tipo de informação sem o consentimento ou percepção de seu alvo.

[19] Um Servidor de Comando-e-Controle (*Command and Control* - C&C - em inglês), segundo Gardiner (2014, p. 03), se trata de uma infraestrutura digital voltada a controlar remotamente um ataque cibernético. Tal servidor pode instruir como um *malware* se comporta antes de um ataque ser realizado. Além de funcionar como um local de

Mesmo sendo 20 vezes mais pesado do que o *malware Stuxnet* (CFR, 2024 e Zetter, 2014, p. 180) com 650.000 linhas de código, *Flame* não tinha um setor prioritário de ataque, infectando, roubando e destruindo dados de mais de 1.000 máquinas pertencentes a civis, empresas privadas e públicas, organizações governamentais e instituições educacionais. Segundo CFR (2024), o *Flame* teve como alvo principal o Irã, com cerca de 189 infecções confirmadas. Contudo, assim como no caso *Stuxnet*, foram percebidas infecções e subtrações de informações por parte desse *spyware* em outros 14 países - foco nos respingos do *Flame* na Rússia e em Israel[20].

Tal ataque obteve uma reação governamental por parte do Irã em maio de 2012, que se dispôs, em conjunto com o grupo Kaspersky - o proclamador do *Flame*, descobrindo o *Payload* e o *Missile* do ataque -, em desenvolver um detector que revele e combata o *spyware* de seus dispositivos. Além dessa movimentação, não houve nenhuma denúncia internacional para se descobrir ou penalizar o ator central desse ataque.

Já o *malware Gauss*, descoberto em junho de 2012 pelo grupo russo Kaspersky - graças ao seu fomento específico de suas capacidades de detecção devido ao caso *Flame* -, indica um esforço estatal em praticar uma operação de vigilância cibernética contra países do Oriente Médio (CFR, 2024 e Kaspersky, 2012). Sendo aparentemente projetado pelos mesmos agentes maliciosos que desenvolveram os vírus *Stuxnet* e *Flame* - pois certas linhas de código são parecidas -, *Gauss* tinha como *Payload* principal a espionagem do setor privado, mais especificamente, ao roubo de informações de sistemas bancários presentes nos servidores do Líbano (Zetter, 2012 e CFR, 2024).

Com esse objetivo primário em seu código, *Gauss* infectou mais de 1.660 máquinas referentes aos bancos Bank of Beirut, EBLF, *BlomBank, ByblosBank*, *FransaBank, Credit Libanais, Citibank e PayPal*, de forma a roubar todas as credenciais, senhas e movimentações bancárias dispostas nos servidores libaneses para seu C&C. Contudo, dada a natureza de expansão do *malware* em servidores utilizadores da tecnologia de nuvem, *Gauss* conseguiu invadir mais de 890 máquinas adicionais e obter dados dos servidores do Citibank e PayPal em mais nove países - com os respingos aos Estados Unidos, Irã e Israel sendo destacados para a pesquisa (Zetter, 2014, p. 190 e CFR, 2024).

---

retorno para os dados obtidos, o C&C cria um canal de comunicação para o vírus em movimento no espaço cibernético.

[20] Assim como no caso *Stuxnet*, Israel é tido como um participante secundário na criação das linhas de código do *spyware Flame* (CFR, 2024).

Gauss marca o estudo de capacidades ofensivas visto que esta foi a primeira ocorrência conhecida do uso de um *malware* estatal com propósitos de contrainteligência (Zetter, 2012). Isso acontece pois, embora essa tipologia de ataque seja bastante comum, ela só era realizada - até aquele momento - por grupos de agentes maliciosos que visavam o roubo do dinheiro pertencente às credenciais adquiridas, ponto que não foi constatado no caso *Gauss*, pois os dados roubados não foram utilizados em nenhuma circunstância conhecida para se obter ganhos econômicos.

Todavia, essas mesmas informações também não foram usadas constatadamente em nenhuma outra situação, gerou-se a suspeita de seu uso para atos de contrainteligência Estatal, e a criação de danos potenciais futuros, realizada principalmente pelos Estados Unidos e Israel, suspeitos basilares desse caso para CFR (2024). Para além do temor aos atores do Sistema Internacional Cibernético, não houve reações ou denúncias públicas das vítimas desse *malware*.

No que se refere aos ataques cometidos contra os Estados Unidos durante o ano de 2012 foram confirmadas seis ocorrências por parte dos dados dispostos em CFR (2024). Desses eventos, três deles tiveram o Irã como autor principal - nos incidentes *Madi*; *Operation Abadil* e *ITSecTeam* - e três deles a China - nos casos *Sabpub*; *Sneaky Panda* e o ataque à filial da Coca-Cola. Durante o ano de 2012, apenas uma das ocorrências supracitadas teve reação internacional e legal por parte dos EUA e de seus representantes, obtidas na ocorrência iraniana *Operation Abadil*, com denúncias criminais ao país executor e penas de prisão de dez anos aos agentes maliciosos responsáveis pelo caso - sete iranianos que faziam parte da Guarda Revolucionária do Irã (Estados Unidos da América, 2016a e CFR, 2024).

2.3.1 - O ano de 2012: Capacidades Defensivas Estadunidenses

A data de 2012 foi marcada por mais um aumento nas movimentações legislativas internacionais com a participação dos Estados Unidos na terceira conferência do GGE da ONU e a assinatura de quatro acordos temáticos. Primeiramente, foi percebida que a terceira instância do GGE conseguiu progredir o estudo e o entendimento dos temas cibernéticos tidos como desafios na edição anterior (Hitchens e Goren, 2017, p. 31 e Klaar, 2021, p. 05).

Nesta edição da GGE, de acordo com o texto de Hitchens e Goren (2017, p. 31), foram desenvolvidos três tipos de recomendações: criação e fomento de normas, regras e princípios de comportamento responsivo; a efetivação das Medidas para a Construção de Transparência e Confiança (MCTC - do inglês *TCBM - Transparency and Confidence-building Measures*); e a

necessidade de amplificar o trabalho conjunto na consolidação das capacidades cibernéticas dos membros. Durante a reunião em 2012 (Klaar, 2021, p. 05), foi iniciada a elaboração de um relatório e de um *framework* para se definir comportamentos responsáveis e responsivos de um Estado no ciberespaço, parecer consolidado em 2013 e trabalhado na seção defensiva de 2013.

No tocante aos acordos assinados, as autoridades temáticas dos Estados Unidos celebraram, em janeiro de 2012, o MoU da *Cyber Defense Management Board* (CDMB - Conselho de Administração de *Cyber* Defesa - CACD) da OTAN com a autoridade da República Tcheca. Esse documento teve como foco o fomento das práticas militares cibernéticas para a proteção da OTAN e de seus membros. Esse Memorando criava direitos e deveres entre as partes, caracterizando sua obrigatoriedade. Entretanto, Hitchens e Goren (2017, p. 59) indicam em seu trabalho, uma alta confidencialidade presente nesse acordo, impedindo o conhecimento de informações adicionais.

Outro MoU subscrito em janeiro se referiu-se à cooperação entre a OTAN com o governo da Letônia em relação à defesa cibernética. Segundo Hitchens e Goren (2017, p. 58), o acordo buscava aumentar a contribuição da Letônia na cooperação internacional de ciberdefesa por conta de sua localização geográfica, que ao ser ao sul da Estônia e ao leste da Rússia, o torna um alvo acessível à ataques cibernéticos ou a roubos de informações. Dessa forma, todos os membros da OTAN se comprometeram em desenvolver operações militares conjuntas com o propósito de fortalecer suas capacidades defensivas, e, assim, mitigar os riscos advindos dos agentes maliciosos no espaço cibernético.

Em fevereiro de 2012, foi firmada uma Carta de Intenções bilaterais entre os Estados Unidos e os Países Baixos em prol da cooperação ampla em *cyber* segurança. Esse documento com características não jurídicas, tentou construir iniciativas positivas de segurança com o intuito de promover um ambiente cibernético seguro e resiliente entre as partes. Isso permitiria uma maior velocidade de reação para a proteção das infraestruturas críticas governamentais (Hitchens e Goren, 2017, p. 58).

A carta tentava estabelecer um diálogo entre os Departamentos de Segurança Interna dos países em cinco áreas vitais de cooperação cibernética defensiva: perícia cibernética; ações maliciosas em ambientes de comunicação móvel; gerenciamento de identidade transfronteiriça; infraestruturas críticas e SCADA *(Supervisory Control and Data Acquisition* - Sistemas de Supervisão e Aquisição de Dados em inglês); e computação em nuvem. Uma vez realizada tal movimentação, possíveis operações cibernéticas conjuntas poderiam ser produzidas entre os Estados Unidos e os Países Baixos.

Já o último acordo firmado em 2012 diz respeito ao convênio dos programas de cooperação realizados entre a OTAN e a Nova Zelândia em junho. Naquele momento, todos os países-membros da OTAN se comprometeram a cooperar assiduamente com a Nova Zelândia com o intuito de elaborar abordagens comuns para desenvolvimento de operações militares conjuntas. Para esse acordo (Hitchens e Goren, 2017, p. 57), a temática de cibersegurança é apenas um dos tópicos presentes, não sendo, ao contrário dos tratados abordados até então, o elemento principal de elaboração do documento, tendo, com isso, uma presença mais concisa nessa deliberação.

2.4 - O ano de 2013: Capacidades Ofensivas Estadunidenses

O ano de 2013 apresentou, assim como visto em 2011, uma queda orçamentária em relação ao seu ano anterior com uma diminuição de 0,3% ao valor destinado aos temas de segurança e defesa - 527 bilhões de dólares. A contração também foi salientada na repartição do orçamento designado à cibersegurança, com um decréscimo de 53% indicado no cálculo público de 7,8 milhões de dólares para a área. Em relação a ataques cibernéticos realizados ou financiados pelos Estados Unidos, CFR (2024) não obteve nenhum dado que consiga atribuir a presença ofensiva estadunidense no ano de 2013.

Entretanto, os Estados Unidos foram atacados ciberneticamente nove vezes pelos Estados oponentes centrados nesta dissertação. A partir dos dados dispostos em CFR (2024), todos os casos foram de espionagem cibernética, e entre os ataques realizados, um dos casos foi atribuído à Rússia - *The Dukes* -, um dos casos foi atribuído ao Irã com o Comprometimento da rede da Marinha dos Estados Unidos e os outros sete são de autoria chinesa - *PLA Unit* 61398; *NetTraveler*; *Anchor Panda*; *Sykipot*; *Deep Panda*; *Icefog* e *Admin@338*. Ainda segundo a CFR (2024), não foi observado nenhum ato público de denúncia ou investigação internacional.

2.4.1 - O ano de 2013: Capacidades Defensivas Estadunidenses

Em 2013, as lideranças temáticas dos Estados Unidos, defensivamente, assinaram dois tratados temáticos, participaram do desenvolvimento do relatório da terceira GGE e formularam, em conjunto com a OTAN, um exemplo legislativo importante para a temática de cibersegurança - o Manual de Tallinn. Em princípio, ao considerar as convenções subscritas

pelos Estados Unidos, em janeiro de 2013, houve o comprometimento estadunidense com a Convenção de Pesquisa e Desenvolvimento (P&D) realizada entre a OTAN e o Conselho de Pesquisa Tecnológica e Científica da Turquia (TUBITAK).

Este tratado criou uma tipologia de cooperação científica voltada ao fomento da pesquisa no âmbito cibernético, permitindo trocas de informações entre o centro turco e os países-membros da OTAN. Vale frisar que assim como o MoU da *Cyber Defense Management Board* de 2012, esse acordo não divulgou publicamente informações adicionais acerca de suas alíneas, mantendo algumas de suas partes em sigilo (Hitchens e Goren, 2017, p. 57).

Em junho de 2013, ocorreu a primeira[21] interação legislativa bilateral defensiva entre os Estados Unidos e a Rússia com o Acordo de Cooperação Estados Unidos-Rússia em Tecnologias de Informação, Comunicação e Segurança. Essa convenção, segundo Hitchens e Goren (2017, p. 56), determinou as principais medidas para o aumento de transparência. além da redução na escalação de animosidade entre as partes em um nível cibernético, para assim alcançar um grau de cooperação entre as CERTs russas e estadunidenses.

A cooperação visaria a coordenação dos CERTs ante a troca de informações e dados técnicos, além de permitir uma integração entre esses institutos governamentais com infraestruturas críticas importantes - a dar de exemplo os Centros de Detecção de Risco Nuclear -, criando pontos de confiança através da troca de informações. Por fim, essa convenção autorizou uma comunicação direta entre o coordenador de *cyber* segurança dos Estados Unidos - naquele momento o primeiro diretor da USCYBERCOM, o general Keith B. Alexander - e o secretário do conselho de segurança da Rússia - Nikolai Klimashin. Em princípio, essa movimentação geraria uma ponte de confiança entre os Estados Unidos e a Rússia no tocante à temática cibernética defensiva.

Em 2013, no final do terceiro encontro do GGE da ONU para assuntos cibernéticos, foram acordados entre as partes cerca de 11 normas voluntárias e não legalmente vinculativas acerca dos comportamentos estatais para o ciberespaço. Sob o nome de relatório A/68/98, ficou pactuada a necessidade de criação de uma lei internacional que permita o desenvolvimento de um espaço cibernético mais aberto, seguro, pacífico e acessível (Hitchens e Goren, 2017, p. 31). O parecer também estabeleceu que enquanto a legislação supracitada não for criada, as normas internacionais sobre assuntos de segurança e paz cinéticas já existentes deveriam ser utilizadas

[21] Hitchens e Goren (2017, p. 62 e 64) afirmam em seu trabalho que houve outros episódios de cooperação legislativa cibernética entre os Estados Unidos e a Rússia ocorridas em 2002 com o *APEC Cybersecurity Strategy* e em 2005 com a Declaração de Lima. Contudo, as autoras apontam a natureza multilateral desses tratados, colocando o Acordo de Cooperação supracitado como a primeira ocorrência bilateral verificada em sua base de dados.

na temática de cibersegurança como forma de reduzir os riscos à paz, segurança e estabilidade internacional, se utilizando como exemplos a Carta da ONU no Direito Internacional dos Conflitos Armados (DICA) (Klaar, 2021, p. 05).

À vista disso, o relatório A/68/98 reforçou os conceitos de soberania Estatal, território, e fronteiras ante o âmbito cibernético para assim tentar construir parâmetros de atribuição aos atos pertencentes ao ciberespaço, permitindo comportamentos mais evidentes de cooperação e defesa das infraestruturas críticas dos 15 Estados-membros. Segundo Klaar (2021, p. 05), a questão da aplicabilidade das leis gerou controvérsia em alguns Estados - principalmente China e Rússia - sobre a recomendação e o acatamento de leis prioritariamente ocidentais em um contexto internacional para a cibersegurança, ponto que traz novos desafios a serem superados nas próximas reuniões do GGE.

Finalmente, no ano de 2013 foi consolidada uma tentativa mais específica de criação e orientação dos princípios internacionais ante a temática cibernética. Criada como uma reação a fim de impedir a repetição de episódios como o da Estônia em 2007, o *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Manual de Tallinn Sobre a Lei Internacional Aplicável ao Conflito Cibernético - em inglês) recorre aos *experts* presentes no Centro de Excelência Cooperativo de *Cyber* Defesa - CECCD (em inglês *Cooperative Cyber Defense Center of Excellence* - CCD COE) da OTAN para responder questões de legalidade, neutralidade e proteção em casos de *cyber* cibernético (Robinson, Jones e Janicke, 2015 p. 83 e Jensen, 2017 p. 737).

Com um foco juridicamente não-vinculativo, o Manual construiu 95 tipos de normas de percepção e auxílio das leis já existentes sobre conflitos armados em um contexto cibernético para os Estados, criando um arcabouço legal de citações de regras e exemplos cinéticos possíveis. Segundo Robinson, Jones e Janicke (2015, p. 83), os preceitos são separados em duas partes, perpassando pelos temas de (a) Estados e Espaço Cibernético e Uso da Força; e (b) Condutas de Hostilidade, Leis sobre Conflito Armado, Neutralidade, Ocupação e Certas Pessoas, Objetivos e Atividades relevantes cinética e ciberneticamente.

Embora Robinson, Jones e Janicke (2015, p. 84) indiquem um alto nível de detalhamento e possibilidades presentes no Manual de Tallinn, também apontam duas fraquezas dispostas nessa tentativa normativa da OTAN, sendo a primeira o viés ocidental presente na cartilha. Ponto demonstrado em seu preâmbulo que aponta o uso dos guias militares da Alemanha, Canadá, Reino Unido e Estados Unidos como principais fontes utilizadas para a criação do Manual, admitindo o uso do pensamento ocidental na criação de um guia

internacional, gerando dificuldades de comunicação e aceitação do modelo em países não ocidentais.

A segunda dificuldade indicada pelos autores está na falta de uma deliberação unânime por parte dos *experts* da CECCD de como as leis presentes no Manual deveriam ser utilizadas em casos de conflito cibernético. Isso faz com que o objetivo principal do Manual não seja realmente cumprido, pois há discordâncias na própria Cartilha de como se agir nos exemplos propostos, representando uma falha de consonância do Manual, trazendo mais questionamentos sobre a adoção das normas indicadas.

Essas complexidades fizeram com que, em um primeiro momento, o Manual de Tallinn de 2013 não servisse como uma orientação jurídica assertiva sobre como o direito internacional se aplica a casos de conflito cibernético. Tendo em vista esses desafios, os *experts* da CECCD se empenharam, nos anos seguintes, em aprimorar o Manual, tentando, com isso, fomentar a temática cibernética defensiva aos atores do Sistema Internacional Cibernético.

2.5 - O ano de 2014: Capacidades Ofensivas Estadunidenses

O ciclo de 2014, no que se refere às capacitações orçamentárias dos Estados Unidos, teve um leve decréscimo de 0,18% em relação ao ano anterior, com um total de 526 bilhões de dólares destinados à área de segurança e defesa. Todavia, essa diminuição não foi contabilizada no âmbito de cibersegurança, que indicou um aumento de 12720% ao apresentar uma soma de um bilhão de dólares para o ano em detrimento dos 7,8 milhões identificados em 2013, trazendo um fomento estadunidense para a área cibernética.

Esse incentivo, a partir do pensamento de Amoretti e Fracchiolla (2018, p. 17 e 18 - tradução nossa), também se teve em uma perspectiva legislativa doméstica, visto que houve uma movimentação do governo Obama em usar os meios cibernéticos em apoio aos planos militares, operacionais e de contingência para "garantir e defender a pátria dos Estados Unidos e seus interesses contra ataques cibernéticos significativos dispostos no mundo". Para isso, o governo Obama, com o apoio principal do congresso, colocou no *National Defense Authorization Act*[22] (NDAA - em inglês: AADN - Ato de Autorização da Defesa Nacional) de 2014 a necessidade do Departamento de Defesa em designar oficialmente um conselheiro

[22] Um *National Defense Authorization Act* segundo Estados Unidos da América (2014, p. 02) se trata de um ato legislativo anual realizado em conjunto com a câmara, o senado e o governo que recomenda e autoriza as principais atividades, construções, estratégias e prescrições militares aos Departamentos de Defesa e de Energia para maximizar o melhor uso do orçamento disposto para o ano fiscal.

cibernético para a Secretária de Defesa, em prol de "analisar as atividades militares e as operações cibernéticas ofensivas e defensivas" (Amoretti e Fracchiolla, 2018, p. 17 - tradução nossa).

Tal movimentação tentou ampliar e integrar a comunicação das agências de segurança e inteligência, tendo como objetivo a criação de medidas cibernéticas mais diligentes, além de desenvolver as capacidades do Comando Cibernético dos Estados Unidos (USCYBERCOM) e dos órgãos interconectados a ele - como a Agência de Segurança Nacional (NSA) e o Departamento de Segurança Interna (DHS). Embora a implementação oficial do cargo de conselheiro cibernético tenha falhado em 2014 (Amoretti e Fracchiolla, 2018, p. 18), o AADN possibilitou uma movimentação cooperativa entre as Instituições domésticas de segurança estadunidense com a indicação e admissão do almirante de quatro estrelas Michael S. Rogers como o diretor da USCYBERCOM e da NSA, facilitando a comunicação e a movimentação doméstica desses órgãos.

Posto isso, em fevereiro de 2014, foi verificada uma atuação cibernética ofensiva responsabilizada - por meio da identificação do *Payload* do ataque - aos Estados Unidos através do caso *Regin*. *Regin*, a partir dos dados dispostos em CFR (2024) e Kaspersky (2014) foi um ato de espionagem cibernética no qual os objetivos centrais eram extrair informações sensíveis de diversos setores institucionais e governamentais, além de criar vulnerabilidades ocultas nas redes e infraestruturas críticas de suas vítimas, permitindo novos ataques no futuro.

Fundamentado no relatório da Kaspersky (2014), o *malware Regin* infectava os dispositivos de suas vítimas e se disfarçava de *plug-ins* comuns dispostos na máquina afetada, para assim copiar e salvar dados e informações listadas como importantes em um Servidor de Comando-e-Controle, a citar de exemplo o registro de tráfico computacional, senhas usadas e capturas de tela constantes do dispositivo. Finalmente, a máquina infectada criaria *backdoors*[23] como uma forma de vulnerabilidade, permitindo acessos posteriores e se lançando a outros dispositivos usando a rede existente como intermediário, realizando novas vítimas e aumentando a quantidade de dados adquiridos ao C&C.

Kaspersky (2014) também elenca que o *malware Regin* focava suas ações principalmente nas infraestruturas críticas das operadoras de telecomunicações, instituições governamentais, instituições financeiras, órgãos políticos multinacionais, instituições de pesquisa e em pesquisadores individuais envolvidos em estudos avançados sobre matemática e

[23] Um *backdoor* é um método, normalmente anônimo, de acesso criado para permitir entradas posteriores de agentes para o controle de um dispositivo (Yang et al., 2023).

criptografia. CFR (2024) e Kaspersky (2014) conseguiram identificar a presença e possível ação de *Regin* em cerca de 15 países em um período que chega a datar 11 anos - os códigos do *missile* datam uma ação presente em 2003.

Vale ressaltar a presença de Estados como o Irã, a Rússia e a Índia dentre as vítimas do caso *Regin*, embora não haja nenhuma reação pública por parte das vítimas em denunciar e investigar os autores responsáveis por este caso. Outra especificidade deste caso advém da indicação de CFR (2024) da suspeita de coautoria por parte do Reino Unido no *malware Regin*. Essa responsabilização é apresentada de forma diferente ao comparar com os casos *Stuxnet* e *Flame* – onde há indícios de participação israelense - pois há evidências de que o Servidor de Comando-e-Controle desse ataque situava-se em algumas infraestruturas localizadas no Reino Unido, marcando, com isso, uma suspeita de atribuição.

Relativamente aos ataques realizados contra os Estados Unidos, CFR (2024) atesta a presença de 18 ataques realizados pelos Estados oponentes. Tais ocorrências perpassam por atos de espionagem, destruição de dados e de *doxing*[24] com a autoria dos quatro Estados escolhidos para a pesquisa. A atribuição realizada aponta a participação da Rússia em três casos de 2014 - *Turla*; *Crouching Yeti* e o Comprometimento do Departamento de Estado estadunidense -, o Irã em quatro atos - *Operation Clever*; *Charming Kitten*; *Saffron Rose* e no *Sands Casino* -, a China em dez ocorrências - *Axiom*; APT18; caso de acusação formal aos oficiais do Exército de Libertação Popular da China (PLA); *Moafee*; *Putter Panda* e os Comprometimentos da *Boeing*, da USIS (*U.S Investigations Services*); do *Community Health Systems* e do Comando de Transporte e dos Serviços Postais - e a Coreia do Norte em um episódio - incidente na indústria cinematográfica Sony.

Nesses incidentes, de acordo com o CFR (2024), apenas em cinco deles foi relatado algum tipo de reação por parte dos Estados Unidos, sendo dois na forma de denúncias internacionais da ação derivada do caso de destruição de dados do *Saffron Rose* e do comprometimento dos contratados do Comando de Transporte. Já nos episódios restantes a movimentação se baseou na incriminação dos agentes maliciosos em nome do Estado atacante, como visto na prisão de cinco oficiais do Exército de Libertação Popular da China responsáveis pelo ato de espionagem ao setor privado supracitado, no confinamento de Su Bin, responsabilizado pelo incidente de espionagem chinês da *Boeing* e na detenção de Park Jin Hyok, autor do *doxing* norte-coreano presente no ataque à Sony. Consequentemente a isso,

[24] Segundo CFR (2024), *doxing* se trata de um ato de busca e rastreio de informações pessoais, sensíveis ou importantes de uma vítima, para assim conseguir publicá-las na *internet* com intenções maliciosas e difamatórias.

somente a China em relação ao caso do PLA se apresentou publicamente para negar a participação no episódio indicado.

2.5.1 - O ano de 2014: Capacidades Defensivas Estadunidenses

Em 2014, as lideranças diplomáticas dos Estados Unidos reuniram-se para sua quarta sessão do GGE da ONU, tendo como objetivo principal seguir as recomendações e simplificar os desafios dispostos na deliberação do relatório anterior. À vista disso, foi percebida uma dedicação dos países-membros em tentar estabelecer diálogos cooperativos sobre a defesa das infraestruturas críticas, trocas de informações ante a incidentes transnacionais e discutir relações cibernéticas transfronteiriças (Hitchens e Goren, 2017, p. 31). A reunião de 2014 ajudou no desenvolvimento de um relatório mais específico e em sintonia com os participantes, como visto na subseção defensiva de 2015.

Em relação aos acordos assinados, as lideranças temáticas dos EUA participaram de cinco acordos temáticos em 2014, com o primeiro sendo o Memorando de Entendimento entre a Organização de Estados Americanos (OEA) e a Estônia. Esse tratado, de natureza juridicamente vinculativa, promoveu o desenvolvimento das capacidades cibernéticas dos signatários através de treinamentos conjuntos e participação em operações militares mirando a criação de manuais de treinamento para a área militar futuramente. Esse MoU contou com a participação de todos os 34 Estados-membros da OEA em conjunto com a Estônia, que disponibilizou boa parte da tecnologia utilizada para os exercícios coletivos.

Tendo em vista o incentivo tecnológico oferecido pela Estônia em acordos anteriores, a OTAN elaborou e estabeleceu, em janeiro de 2014, um compromisso legislativo entre a Liga Estoniana de Defesa e o Centro de Excelência Cooperativo de Ciberdefesa. Esse tratado, segundo Hitchens e Goren (2017, p. 55) formalizou a parceria entre as duas agências governamentais e consolidou suas práticas militares cibernéticas através de exercícios conjuntos anuais, com o nome de grupamento *Locked Shields* (escudos bloqueadores - em inglês). Aqui, todos os países-membros da OTAN assinaram e formalizaram o presente acordo.

Similarmente aos acordos supracitados, em janeiro também foi deliberado o Programa de Cooperação e Parceria Individual entre o Japão e a OTAN. Com o foco exclusivo na pesquisa e desenvolvimento, essa resolução governamental estipulava formas cooperativas para se compartilhar e aprender as principais tendências tecnológicas e teóricas utilizadas nos governos e na academia dos Estados-membros da OTAN, fomentando assim o tema defensivo.

Em julho de 2014, foi realizado entre 25 Estados[25], um arranjo legislativo acerca do reconhecimento de critérios comuns para a *cyber* segurança. Estipulados conjuntamente entre os signatários, o tratado determinou medidas regulatórias partilhadas para se adquirir peças de tecnologia e *softwares* sem avaliações adicionais (Hitchens e Goren, 2017, p. 54). Essa movimentação permitiria uma velocidade na compra e venda de ferramentas para a cibersegurança, facilitando o desenvolvimento conjunto dos governos assinantes.

O último acordo assinado pelos Estados Unidos em 2014 criou uma força de ação voltada ao combate do crime cibernético. Formado por nove Estados - Alemanha, Áustria, Canadá, Espanha, Estados Unidos, Finlândia, Itália, Países Baixos e Reino Unido -, essa equipe de trabalho evidenciou o intercâmbio de informações para a identificação e o combate de ameaças comuns.

Uma vez identificados os padrões comuns de ação, a força-tarefa treinará conjuntamente os serviços policiais e de inteligência dos signatários na área de detecção e combate de crimes cibernéticos e investigações forenses. O arranjo legislativo indicou a criação de encontros cooperativos regulares entre os líderes de *cyber* segurança dos Estados com profissionais renomados na área acadêmica e industrial com o intuito de desenvolver continuamente as capacidades teóricas e práticas das partes ciberneticamente (Hitchens e Goren, 2017, p. 54).

2.6 - O ano de 2015: Capacidades Ofensivas Estadunidenses

Em 2015 foi percebida, em relação aos atributos orçamentários dos Estados Unidos, a menor diminuição entre os anos fiscais indicados nesta dissertação com uma quantia total de 496,1 bilhões de dólares dedicados à temática de defesa e segurança, uma contração de 5,68% em relação ao ano anterior. Apesar disso, a parcela orçamental dedicada aos assuntos cibernéticos no Departamento de Defesa dos EUA sofreu um aumento de 410% ao registrar cerca de 5,1 bilhões de dólares para o ano fiscal de 2015.

Esse aumento orçamentário temático pode ser explicado através da consolidação das políticas e sugestões de Obama de 2012 para deixar o assunto cibernético mais integrado entre os setores políticos, militares e estratégicos, ponto que permitiu a concepção do *Cyber Threat Intelligence Integration Center* (CTIIC) (Amoretti e Fracchiolla, 2018, p. 14 e 23). Ao seguir

[25] Os Estados signatários deste arranjo são: Alemanha, Austrália, Canadá, Coreia do Sul, Dinamarca, Espanha, Estados Unidos, Finlândia, França, Grécia, Hungria, Índia, Israel, Itália, Japão, Malásia, Noruega, Nova Zelândia, Países Baixos, Paquistão, Singapura, Reino Unido, República Tcheca, Suécia e Turquia.

os parâmetros e as visões políticas presentes em 2012 e em 2014, esse Centro Nacional focava no desenvolvimento de uma abordagem sistemática e integrada dos departamentos e agências militares e de inteligência estadunidenses para reconhecer o que viria a ser uma ameaça cibernética aos Estados Unidos, para assim serem criados esforços de combate e atuação contra esses perigos.

Os objetivos centrais indicados na criação do CTIIC seriam alcançados pelo diretor do Departamento de Inteligência Nacional, cujo cargo compartilhado ajudaria na disseminação e produção de avaliações coordenadas acerca das ameaças cibernéticas vistas nos Departamentos de Defesa e nos órgãos cibernéticos estadunidenses (Amoretti e Fracchiolla, 2018, p. 23). Uma vez analisados, os dados sobre os perigos cibernéticos aos EUA poderiam ser usados como base para missões de inteligência internas e externas, padronizando, assim, as noções e as ações cibernéticas realizadas.

Ooutra indicação cibernética estabelecida domesticamente durante o governo Obama advém da Estratégia do Departamento de Defesa ante a temática cibernética. Nesse documento foram elaborados critérios que norteiam as principais ações e oponentes dos Estados Unidos ciberneticamente. Com base na Estratégia de 2015, o DoD introduziu medidas mais agressivas e sofisticadas de respostas às ameaças cibernéticas identificadas por outros departamentos - principalmente o USCYBERCOM e o CTIIC - de forma a proteger as infraestruturas críticas e os interesses estadunidenses no ciberespaço (Estados Unidos da América, 2015 e Amoretti e Fracchiolla, 2018, p. 24).

Para isso, segundo Amoretti e Fracchiolla (2018, p. 24) e Estados Unidos da América (2015), foi estabelecido, como um ato anexado à Estratégia, a *US military's Cyber Mission Force* (CMF - a Força Militar de Missão Cibernética dos Estados Unidos em inglês) com cerca de 6200 militares, civis e empreiteiros de suporte dispostos entre diversos Departamentos e complexos militares e de defesa dos Estados Unidos. A CMF teve como escopo central a defesa das infraestruturas críticas de comunicação do governo contra ataques cibernéticos, além de disponibilizar suporte e comando em missões militares cibernéticas e cinéticas realizadas.

Outro diferencial da Estratégia do DoD de 2015 está na declaração categórica dos oponentes a serem combatidos no espaço cibernético, atribuídos como a China, a Rússia, o Irã e a Coreia do Norte. Segundo Amoretti e Fracchiolla (2018, p. 24) e Estados Unidos da América (2015), essa agnição ajudará o DoD e outras Agências estadunidenses a responder ou negar preventivamente ataques cibernéticos direcionados aos EUA, deixando a estratégia temática e

o desenvolvimento das capacidades cibernéticas estadunidenses mais transparentes, seguindo uma orientação diferente dos governos predecessores (Amoretti e Fracchiolla, 2018, p. 24).

Em referência aos ataques cibernéticos responsabilizados aos Estados Unidos por CFR (2024), em 2015 foi encontrado pelo grupo Kaspersky a comprovação do *Missile* e do *Payload* do *malware Equation Group*. Voltado principalmente à espionagem, CFR (2024), Kaspersky (2015) e Goodin (2015) relatam as particularidades presentes na codificação desse *malware*, ponto que possibilitou o uso de mais de 300 domínios de *internet* e de 100 servidores para aumentar a velocidade de ações adaptativas de infecção vistas em mais de 5.000 máquinas e sistemas em todo o mundo.

Um exemplo das operações realizadas pelo *Equation Group* em máquinas infectadas está na capacidade de reprogramar os *hard drives* - áreas de armazenamento de dados e programas em uma máquina - para assim se encriptar nos registros do sistema operacional, apagando completamente seus rastros de existência e de ação. A partir disso, esse vírus conseguiu roubar informações sensíveis de governos, instituições financeiras, embaixadas, grupos de pesquisa, companhias de telecomunicação e mídia, departamentos de energia e do setor militar e aeroespacial em mais de 42 países - grifando para esta dissertação a presença confirmada do Irã, Rússia, Índia, China e Reino Unido como vítimas.

Vale ressaltar que disposto em seu código, o *malware* tinha uma especificação de autodestruição em caso de inspeção minuciosa de antivírus mais potentes, indicando a possibilidade de que os números de infectados sejam apenas uma pequena porcentagem do total de vítimas (Goodin, 2015 e Kaspersky, 2015). A partir do relatório da Kaspersky, foi constatado a presença de códigos de *Missile* e da presença do Servidor de Comando-e-Controle do *Equation Group* a datar de agosto de 2001, indicando muita sofisticação e atuação do agente malicioso no ciberespaço.

Não obstante, Kaspersky (2015) infere - a partir da forma de escrita do *malware* - a possibilidade do *Equation Group* ser o molde de associação para outros vírus e ataques cibernéticos estadunidenses indicados neste capítulo, como o *Stuxnet* de 2010, *Gauss* de 2012, *Flame* de 2012 e o *Regin* de 2014, aumentando, com isso, seu nível de periculosidade como uma capacidade cibernética ofensiva. Dito isso, não houve reações conhecidas ante ao caso internacionalmente por parte das vítimas afetadas, apenas o temor do uso das informações adquiridas.

Quanto aos ataques realizados contra os Estados Unidos atestados pelo CFR (2024), foi relatada a existência de 13 ataques empreendidos por três dos quatro Estados oponentes

trabalhados. A Rússia foi responsabilizada em três comprometimentos cibernéticos - nos atos de ataque contra a rede da Casa Branca; o Sistema de Legado do Pentágono e as redes sigilosas associadas do Conjunto do Estado-maior dos Estados Unidos.

Já o Irã teve a participação confirmada em um dos episódios - comprometimento das contas de mídias sociais dos oficiais do Departamento de Estado. Por fim, relativamente a China foi comprovada sua ação em nove circunstâncias - no caso de negação de serviço do Escritório de Gestão de Pessoal dos Estados Unidos (United States Office of Personnel Management); nos comprometimentos na empresa de seguros de saúde *Anthem*; a companhia de aviação *United airlines*; na interrupção do desenvolvedor de *softwares* de código-fonte *GitHub*; nos incidentes *Hellsing*; *Emissary Panda*; APT 3; APT 17 e APT 30.

Em relação às circunstâncias supracitadas, foram percebidas publicamente apenas duas reações dos Estados Unidos ante aos ataques cibernéticos exercidos, sendo a primeira uma denúncia pública internacional contra a Rússia no caso de envolvimento nos Sistemas do Pentágono, onde não foram destacadas consequências posteriores. A outra atitude estadunidense foi corroborada no caso contra a *Anthem* com a imputação criminal por parte do Departamento de Segurança Interna dos Estados Unidos contra o Estado chinês, que negou a participação no ataque cibernético.

2.6.1 - O ano de 2015: Capacidades Defensivas Estadunidenses

O ano de 2015 foi bastante produtivo ao se notar a quantidade de acordos e relatórios assinados pelos Estados Unidos em relação à temática de cibersegurança, com oito tratados assinados e a produção do parecer final no quarto encontro do GGE da ONU. Segundo Hitchens e Goren (2017, p. 31) e Klaar (2021, p. 06), a resolução oficial A/70/174 seguiu e tentou deliberar algumas das problemáticas consideradas na última reunião e criou algumas recomendações que enfatizam na centralidade de proteção das infraestruturas críticas governamentais em um caráter transfronteiriço.

Foi percebido também, através de 11 normas não juridicamente vinculativas para comportamentos responsáveis de Estados, o esforço dos participantes em se comprometer futuramente na "cooperação, assistência e consulta mútua em casos de incidentes cibernéticos, abstenção em atividades que possam afetar as infraestruturas críticas de outros atores e fomentar a ação de equipes de resposta a ciberataques" (Klaar, 2021, p. 06 - tradução nossa). Para Klaar (2021), essas medidas significaram um avanço temático nos elementos de atribuição,

transparência ante os atos realizados e ampliação das medidas de construção de confiança e capacitação dos CERTs dos Estados-membros.

Posto isso, o relatório de 2015 ainda se pautou minimamente no Direito Internacional dos Conflitos Armados, tentando aumentar sua aplicabilidade no ciberespaço e seu reconhecimento aos Estados não-ocidentais. Mesmo não podendo ser mencionado diretamente e juridicamente nas alíneas do A/70/174, os itens dispostos no DICA tentavam ser ampliados e diluídos nos princípios de humanidade, necessidade, proporcionalidade dessa convenção, elemento que criou um certo consenso entre as partes, que aceitaram essa tentativa elaboração de uma lei internacional que respeite os objetivos de todos os signatários (Klaar, 2021, p. 06).

Em relação aos tratados assinados pelos Estados Unidos, Hitchens e Goren (2017, p. 53) indicam inicialmente o Memorando de Entendimento entre a OTAN e a República Tcheca realizado em janeiro de 2015. Esse pacto com nexos jurídicos se focou no fortalecimento das tecnologias de informação e de defesa cibernética presentes nas operações militares de todos os países-membros da OTAN, estabelecendo assistência multilateral no combate contra ameaças e agentes maliciosos dispostos no ciberespaço.

Também em janeiro, foi firmado um acordo entre a *Raytheon Technologies* - uma empresa estadunidense de defesa e aeronaves - e o governo da Estônia. Com um foco voltado às operações militares cibernéticas, a parceria acordada pretendia avançar as em participações já existentes e fomentar, com a ajuda da *Raytheon*, as capacidades cibernéticas defensivas da Estônia através de ações colaborativas conjuntas.

O último convênio de janeiro foi o acordo entre o Ministério de Defesa da Bulgária e a Organização de Comunicações e Informações da OTAN. Tal resolução, voltada principalmente para a área militar, iniciava a estratégia 2020 da OTAN de defesa cibernética por parte da Bulgária, promovendo, com isso, avanços nos âmbitos tecnológicos de automação, modernização nos serviços de comunicação, atualização nos equipamentos de criptografia e aquisição de serviços cibernéticos defensivos dos países-membros.

Já em março, segundo Hitchens e Goren (2017, p. 52), foi subscrito um MoU bilateral entre a Comissão Federal de Comércio dos Estados Unidos e os Países Baixos acerca do Ato de Proteção de Dados Pessoais e do Setor Privado. Esse Memorando com autoridade legal aumentava a aplicabilidade e integrava alíneas dispostas nos Atos de Proteção de Dados já existentes dos signatários - o Ato de Proteção de Dados Pessoais dos Países Baixos e o Ato Geral da Comissão Federal de Comércio dos Estados Unidos. Ao realizar essa movimentação, foi facilitada a pesquisa e o intercâmbio de informações temáticas entre os Estados, aumentando

o nível de *expertise* via treinamentos conjuntos e trocas de profissionais especializados, impulsionando as capacidades cibernéticas defensivas dos EUA e dos Países Baixos.

Em abril de 2015 foi criado um documento legal para o desenvolvimento de uma iniciativa de cibersegurança entre os países da OEA em conjunto com a Noruega e o Reino Unido: o Centro de Capacidades de *Cyber* Segurança Global (CCCSG). Voltada a construir instruções das melhores práticas a serem realizadas tematicamente, o CCCSG tentou auxiliar os Estados-membros a entender suas prioridades para o investimento e desenvolvimento de seus órgãos de resposta a incidentes cibernéticos, determinando com isso, o nível de maturidade de cada signatário em relação a temática cibernética.

Para isso, a declaração firmada definiu as principais dimensões de maturidade nas quais o CCCSG ajudará na construção e fomento das capacidades cibernéticas estatais de proteção de infraestruturas críticas. São elas: (1) estratégias de segurança, defesa e resiliência; (2) cultura e sociedade; (3) desenvolvimento educacional; (4) lei e regulação; e (5) referências e controles legislativos de tecnologia (Hitchens e Goren, 2017, p. 52). Dessa forma, foi indicada a participação e o apoio de todos os 34 países-membros da OEA, sincronicamente à Noruega e ao Reino Unido, que ficaram incumbidas da utilização das variáveis de maturidade para a identificação e extensão das competências cibernéticas dos subscritores.

No que tange à esfera de pesquisa, foi assinalado por Hitchens e Goren (2017, p. 51) a Declaração Conjunta bilateral entre os Estados Unidos e a Índia sobre o crime cibernético. Realizado em agosto de 2015, a quarta edição desse diálogo contínuo conseguiu produzir inusualmente um compromisso legal voltado ao aumento da colaboração temática para o desenvolvimento das capacidades ofensivas e defensivas. Também foi indicado no acordo uma possível evolução nas pesquisas conjuntas e no combate aos crimes cibernéticos mirados contra os EUA e a Índia, criando, com isso, redes de apoio entre os departamentos de segurança e defesa cibernética das partes.

Em setembro de 2015, foi realizada a primeira ocorrência legislativa bilateral entre os Estados Unidos e a China. O presente acordo criava deveres para a interação das partes nos âmbitos cibernético e cinético, trazendo conjuntamente questões de intercâmbio de informações. A partir dos escritos de Hitchens e Goren (2017, p. 51), as alíneas do contrato estipularam o cessamento e a proibição de qualquer apropriação indevida de propriedade intelectual adquirida ciberneticamente, a mitigação contínua dos crimes cibernéticos perpetuados em território chinês ou estadunidense, a criação e promoção de leis internacionais

multilaterais que respeitem os direitos dos signatários e o estabelecimento de um diálogo colaborativo de alto nível diante o combate do crime cibernético.

Posterior a isso, percebeu-se a criação e assinatura de um Memorando de Entendimento bilateral entre os Estados Unidos e os Países Baixos realizados pela empresa neerlandesa de segurança *Hague Security Delta*, a companhia estadunidense *Virginia Economic Development Partnership* de exportação e a agência de desenvolvimento econômico *Fairfax County Economic Development Authority* em outubro de 2015. Esse MoU com liames legais enfatizava a pesquisa e o desenvolvimento e a criação de vínculos de negócio entre os países, permitindo intercâmbio de informações. Vale ressaltar que esse Memorando foi produto da *Joint Dutch-Flemish Mission*, um encontro internacional nas áreas econômicas e de inovação realizado em Atlanta no mesmo período.

2.7 - O ano de 2016: Capacidades Ofensivas Estadunidenses

Para o ano de 2016, foi verificado nos relatórios orçamentários do Departamento de Defesa dos Estados Unidos um aumento na estimativa financeira utilizada para a esfera de segurança e defesa em relação ao ano anterior. Com uma quantia de 585,2 bilhões de dólares, foi indigitado um incremento de 17,9% sobre 2015. Essa amplificação orçamental também foi presenciada no segmento para a configuração cibernética de segurança e defesa, com um crescimento de 7,8% relativo ao ano pregresso, chegando em 5,5 bilhões de dólares destinados à cibersegurança.

Esse incremento orçamentário, geral e temático, produziu uma duplicação nos casos cibernéticos ofensivos responsabilizados pelos Estados Unidos pelo CFR (2024) em relação ao ano anterior, atribuindo-o aos casos *Project Sauron* e ao ataque cibernético contra o Estado Islâmico. Diante disso, será trabalhado inicialmente o *Project Sauron*. Também conhecido como *Strider*, o *malware* descoberto pelo grupo Kaspersky em julho de 2016 se apresentou como um *Advanced and Persistent Threat*[26] (APT - Ameaça Avançada e Persistente, em inglês) voltada à espionagem de alto nível.

[26] A partir dos textos de Bahrami *et al.* (2019, p. 886), Siddiqi (2016) e Gratão (2022, p. 06), um APT se trata de um *malware* com altos níveis de sofisticação em suas linhas de código, elemento no qual permite com que certas metodologias de ataque possam ser realizadas ante a vítima potencial. Tais métodos perpassam por uma identificação mais precisa do alvo a ser infectado e *Payloads* mais eficazes que facilitam a destruição de dados e uma retirada idônea, proporcionando uma dificuldade de atribuir o responsável e até mesmo a constatação da existência do ataque. É importante ressaltar que um APT tem como característica principal sua adaptação a rede na qual ele está inserido, ou seja, este *malware* se utiliza do espaço cibernético para ficar dormente e se aprimorar no tempo, se tornando uma ameaça cada vez mais difícil de ser identificada e combatida.

Segundo Kaspersky (2016) e Goodin (2016), o *Project Sauron* infectava as máquinas de forma a não gerar nenhum efeito imediato, se tornando operante somente se alguns comandos específicos fossem realizados no tráfego de rede das vítimas. Uma vez ativo, o *malware* obtinha senhas, chaves de criptografia, arquivos de configuração, endereços de IP e chaves de servidores utilizadas pelo dispositivo atacado, enviando todos os dados a um Servidor de Comando-e-Controle.

Vale ressaltar que, para o *Project Sauron*, cada vítima atacada tinha um Servidor de Comando-e-Controle próprio para armazenar as informações roubadas, evitando reusos e dificultando o rastreio de *softwares* anti-*malwares* comuns (Kaspersky, 2016, p. 16). Dito isso, a partir dos dados da Kaspersky (2016), foi constatada a existência inicial de 28 domínios para servidores que atacaram cerca de 30 alvos diferentes, perpassando por agências governamentais, centros científicos de pesquisa, órgãos militares, provedores de telecomunicação e instituições financeiras dispostas em 6 países - destacando para a dissertação a presença do *malware* na Rússia, China e Irã. Perante o exposto, não foi divulgada publicamente nenhuma reação das vítimas ante o ataque, além de não ser percebido nenhum uso para os dados roubados pelo APT, trazendo novamente o temor de dano potencial derivado desse ato de espionagem cibernética.

Outro caso responsabilizado aos Estados Unidos pelo CFR (2024) foi em relação aos ataques cibernéticos efetuados contra o Estado Islâmico (ISIS) em fevereiro de 2016. A partir dos escritos de Sanger (2016), os porta-vozes dos EUA anunciaram a ação da USCYBERCOM em conjunto com os grupos militares do Reino Unido em uma campanha militar cinética e cibernética contra o grupo terrorista ISIS. Sanger (2016) e CFR (2024) especificam que os objetivos desse esforço se concentraram na criação de distúrbios na rede de comunicação e pagamentos do grupo, dificultando a ação e a ampliação do grupo ciberneticamente.

Para alcançar tal propósito, ambos os Estados se focaram em estabelecer ações coordenadas para liberar "bombas cibernéticas" contra o ISIS, caracterizadas como quantidades massivas de *malwares* cujo *Payload* era a sabotagem das infraestruturas críticas de comunicação, propaganda e pagamento atribuídas ao Estado Islâmico na Síria e em certos países da Europa. Sanger (2016) indica que esta ação foi a primeira operação cibernética ofensiva do Comando Cibernético Estadunidense de forma publicamente exposta, marcando o esforço do país em combater um oponente no âmbito internacional cibernético.

Contudo, Sanger (2016) e CFR (2024) ressaltam as problemáticas dessa ação, já que não foram especificadas as métricas de atribuição das infraestruturas críticas atacadas ao grupo

terrorista. Elemento que fez com que os ataques realizados pudessem ser vistos como uma quebra na soberania dos Estados vitimados, potencializados pela inexistência na identificação de quais países europeus foram o foco da operação. Exceto as preocupações salientadas acima, o caso de ataque contra o Estado Islâmico não obteve nenhuma reação ou retaliação publicamente disposta em um contexto doméstico ou internacional.

Posto isso, acerca das informações de ataques realizados contra os Estados Unidos, CFR (2024) indica a atribuição de nove ataques realizados pelos Estados-oponentes. Tais atos, prioritariamente de espionagem, continham a presença dos quatro atores destacados nesta dissertação, responsabilizando a Rússia em quatro conjunturas ofensivas - o comprometimento ao Comitê Democrata Nacional; a tentativa de comprometimento aos *think-tanks* dos Estados Unidos; o ato de *Spear-phishing*[27] contra contas do *google*; e a Falha do *Yahoo* -, o Irã em duas ocorrências - o caso *Prince of Persia* e *Oilrig* -, a China em dois episódios - o comprometimento a organizações de *software* e de jogos estadunidenses e sul coreanos e ao caso *Mofang* - e a Coreia do Norte em um incidente - *Lazarus Group*.

CFR (2024) atesta em seu banco de dados a presença de apenas uma reação aos atos supracitados em 2016, através da denúncia pública e internacional dos Estados Unidos à falha do *Yahoo*, evoluindo a uma acusação criminal e a prisão de quatro russos responsáveis pelo caso de espionagem, sendo dois deles funcionários do Serviço de Segurança da Rússia (Estados Unidos da América, 2016b). Em reação a essa movimentação legal, a Rússia, a partir dos escritos de CFR (2024), respondeu às acusações negando o envolvimento do Estado ante o caso, salientado a existência das ações individuais dos réus.

2.7.1 - O ano de 2016: Capacidades Defensivas Estadunidenses

No tocante às movimentações legislativas de 2016, esta seção inicia-se com o esforço estadunidense para a manutenção e realização da sessão da GGE de 2016-2017 (Schmitt, 2021). Instaurado ainda em 2015 para fortalecer os consensos realizados no relatório A/70/174, a quinta reunião foi marcada pela mudança no quadro de membros, aumentando para 25 Estados

[27] Segundo a *Office of Director of National Intelligence* (DNI - Diretoria de Inteligência Nacional, em inglês), um ato de *Spear-phishing* consiste na tentativa, roubo de informações ou entrada não autorizada em um servidor com informações sensíveis de forma a enganar um colaborador a clicar em *links* falsos com aparências legítimas. O *Spear-phishing* tem como característica central a especificidade do alvo atacado, criando *links* personalizados à pessoa atacada, aumentando, com isso, a eficácia do ataque (DNI, 2024, p. 01).

participantes[28] e indicando a ausência de cinco países regulares em outras edições, como Israel, Coreia do Sul, Bielorrússia, Catar e Itália. Esse encontro de 2016, criou movimentações temáticas distintas das anteriores, ressaltadas com detalhes no subtema do ano de 2017.

Acerca dos acordos cibernéticos assinados em 2016, Hitchens e Goren (2017) mencionam a subscrição dos Estados Unidos em cinco novos tratados temáticos e a reiteração em uma determinação multilateral na *NATO and Estonia Agreement on Cyber Defense* de 2010, mantendo, com isso, as mesmas alíneas e compromissos acordados. Dessarte, em janeiro de 2016, foi firmado um Plano de Ação Estratégico sobre a área de Telecomunicações entre os países participantes da APEC (*Asia-Pacific Economic Cooperation* - Cooperação Econômica Ásia-Pacífico, em inglês), no qual a Rússia e a China faziam – e ainda fazem – parte.

Ao estar concentrado nas áreas de pesquisa, criações de políticas e operações cibernéticas não-militares, a convenção se concentrou no fomento e suporte das inovações das tecnologias dos 21 signatários[29]. Ao realizar essa movimentação, Hitchens e Goren (2017, p. 50), indicam nas alíneas desse contrato a necessidade de promoção do desenvolvimento tecnológico para a economia digital, promovendo maior cooperação entre os membros.

Já em abril foi constatada a Cooperação Técnica entre a ARPEL (*Regional Association of Oil, Gas, and Biofuels Sector Companies in Latin America and the Caribbean*, em inglês, a Associação Regional das Companhias de Óleo, Gás e Biocombustíveis na América Latina e no Caribe) e o Centro Industrial de Cibersegurança da Espanha. Esse pacto foi realizado com o intuito de consolidar a proteção das infraestruturas críticas organizacionais, construindo e compartilhando informações, conhecimentos técnicos e experiências para reduzir as vulnerabilidades e os *cyber* ataques realizados aos membros da ARPEL[30], a Espanha, a Suíça, Gana e os Países Baixos. Também foi indicado nessa coadjuvação a concepção de reuniões e oficinas entre os signatários e as empresas envolvidas para o fomento das competências de gestão à respostas conjuntas contra emergências.

Uma coadjuvação bilateral de 2016 assinalada por Hitchens e Goren (2017, p. 49) foi o *Framework* de Relacionamento Cibernético Estados Unidos-Índia, também realizado em junho.

---

[28] A partir dos relatórios de comparecimento da sexta GGE, os novos Estados constituintes são: Austrália, Cazaquistão, Ilhas Maurício, Indonésia, Japão, Jordânia, Marrocos, México, Noruega, Países Baixos, Quênia, Romênia, Singapura, Suíça e Uruguai.

[29] Os atores-membros da APEC são: Austrália, Brunei, Canadá, Chile, China, Coreia do Sul, Estados Unidos, Filipinas, Hong Kong, Indonésia, Japão, Malásia, México, Nova Zelândia, Papua Nova Guiné, Peru, Singapura, Tailândia, Taiwan, Rússia e Vietnã.

[30] Os membros da ARPEL constituem principalmente de Estados e empresas de combustíveis, gás e óleo presentes na Argentina, Bolívia, Brasil, Chile, Colômbia, Costa Rica, Estados Unidos, Equador, Jamaica, México, Paraguai, Suriname, Uruguai e Venezuela.

Com um caráter extenso, porém flexível de compromissos, esse acordo possuía cláusulas para o desenvolvimento de pesquisas, melhores práticas temáticas, exercícios cibernéticos não-militares e treinamentos conjuntos, de forma a manter um intercâmbio claro de informações em tempo real. Com isso, seria facilitado as colaborações temáticas futuras entre os parceiros, melhorando a percepção e o combate ao crime cibernético dos EUA e Índia.

Realizado em julho de 2016, o Juramento de Defesa Cibernética da OTAN estabeleceu objetivos importantes para a temática multilateral defensiva. Esse convênio tinha como meta o melhoramento das infraestruturas críticas governamentais e dos protocolos de *cyber* defesa dos assinantes.

Para isso, foi recomendado a parceria temática com outros atores do Sistema Internacional, principalmente a academia, as indústrias e a União Européia (UE), enfatizando a cooperação por meio de criações de pesquisas, treinamentos cibernéticos militares conjuntos, intercâmbio de informações e elaboração de legislações conjuntas e internacionais cibernéticas. A partir dos escritos de Hitchens e Goren (2017, p. 48), somente 25 dos 28 Estados-membros da OTAN assinaram a convenção supracitada, havendo abstenções da Hungria, Países Baixos e da Polônia. As motivações da recusa não foram indicadas.

Por fim, com o intuito de fortalecer o tratado anterior, a OTAN em conjunto com a UE, instituiu um Acordo Técnico entre seus centros de respostas a incidentes - CERTs - nas áreas políticas e de operações cibernéticas militares. Firmado em outubro de 2016, a coalizão era orientada na prevenção, detecção e combate a episódios cibernéticos de maior escala, fomentando a interação entre as Organizações Internacionais com a construção de exercícios militares anuais e troca de informações relevantes entre as partes. Hitchens e Goren (2017, p. 48), indicam a presença e subscrição de todos os 28 países da OTAN nesta resolução em adição a seis Estados-membros da União Europeia como Áustria, Chipre, Finlândia, Irlanda, Malta e Suécia.

2.8 - O ano de 2017: Capacidades Ofensivas Estadunidenses

Ao serem utilizados os documentos do Departamento de Defesa estadunidense para 2017, foi atestado uma queda de 0,4% no orçamento, com a quantia de 582,7 bilhões de dólares para o ano fiscal. Esse declínio, contudo, não foi percebido na parcela orçamental dirigida à área de *cyber* segurança, obtendo seu quinto aumento consecutivo no recorte temporal estudado,

com um incremento de 21,8% representado na forma de 6,7 bilhões de dólares deliberada ao tema em 2017.

Com uma substituição presidencial advinda da vitória de Donald Trump, houve também mudanças nas políticas e estratégias domésticas e internacionais realizadas pelos Estados Unidos em relação ao espaço cibernético. Isso trouxe novos modelos de ação e movimentações distintas das percebidas no governo anterior. O governo Trump, com base nas inferências de Maier (2019, p. 121 e 122) e Amoretti e Fracchiolla (2018, p. 26 - tradução nossa) foi marcado, em 2017, pelo uso e benefício das elaborações políticas, técnicas e estratégicas realizadas pelos governos anteriores - principalmente o empreendido na administração Obama - para "repor as forças neoconservadoras na cena política estadunidense", objetivo viabilizado por conta da leve maioria republicana na câmara e no senado.

Isso fez com que as políticas de Trump pudessem ser vistas como uma movimentação agressiva da agenda estadunidense para com o Sistema Internacional (Maier, 2019 e Brânda, 2018, p. 164). Deslocamento visível através do esforço em concretizar os *slogans* apresentados em sua campanha eleitoral - "América Primeiro" (*America First*) e "Torne a América Poderosa Novamente" (*Make America Great Again*) - em decisões políticas, militares e estratégicas doméstica e internacionalmente.

Essas atitudes criaram políticas voltadas ao afastamento dos EUA em questões cooperativas, minando, com isso, as chances estadunidenses de alcançar um papel de liderança global multilateral iniciada pelos governos anteriores (Brânda, 2018, p. 162). Não obstante, as relações exteriores de Trump, ao seguir um movimento de insulamento derivado de vieses nacionalistas, criou mais acentuadamente inimigos externos que impediam a consolidação dos EUA em padrões ideais, fator possibilitador de uma militarização aguda nas agendas criadas e na existência de possíveis confrontos no Sistema Internacional.

Posto isso, a política internacional de Trump ante a temática cibernética repete e consolida estes mesmos parâmetros de ação, segundo Maier (2019, p. 122), mas com um foco maior nos aspectos e possibilidades beligerantes dos processos cibernéticos, assumindo uma postura resolutamente intervencionista para as políticas de cibersegurança (Amoretti e Fracchiolla, 2018, p. 26). Ponto indicado na Estratégia Nacional de Segurança (Estados Unidos da América, 2017a, p. 04 - tradução nossa), que trouxeram linhas voltadas a "preservar a paz pela força" e "avançar a influência estadunidense no mundo para quem apoia seus interesses" para os âmbitos cinéticos e cibernéticos, sendo consolidado no *"America First: A Budget*

Blueprint to Make America Great Again", também de 2017 (Estados Unidos da América, 2017b).

Esse documento formal salientou a necessidade de realizar cortes orçamentais em todos os departamentos do governo em prol de aumentar o investimento nos órgãos voltados aos temas e gastos de defesa a partir de 2018. Segundo Trump (Maier, 2019, p. 122 e Estados Unidos da América, 2017b, p. 16 - tradução nossa) esse investimento garantirá que os Estados Unidos "permaneçam a força militar melhor comandada, melhor equipada e melhor preparada no mundo para garantir superioridade americana, não só na terra, no mar, no ar e no espaço, mas também no ciberespaço". Ademais, a justificativa desse projeto se deu pois, para Trump, as capacidades cibernéticas como um todo precisavam estar em conjunto com as capacidades militares cinéticas, para assim possibilitar modernizações às Forças Armadas (Maier, 2019, p. 122).

Complementarmente, o governo Trump realizou, em 2017, uma alteração importante na estrutura de *cyber* segurança militar, estratégica e de defesa mais relevante dos Estados Unidos: a USCYBERCOM. Ao ser divulgada na Ordem Executiva de 2017 (The White House, 2017), foi percebido um retorno ao *National Defense Authorization Act* de 2014 através da ampliação das competências, mobilizações possíveis e no destaque do órgão governamental temático, que foi elevado ao patamar de um "Comando Combatente Unificado" (Maier, 2019, p. 124). Essa progressão outorgou ao USCYBERCOM um aumento no nível orçamentário para compra de equipamentos, maiores graus de autoridade e autonomia no que se refere a elaboração e exercício de operações cibernéticas internacionais, colocando essa instituição subordinada somente à Agência de Segurança Nacional (*National Security Agency*), devido a identidade única de sua diretoria.

Ainda em 2017, o governo Trump estendeu os tópicos legislativos iniciados pela *International Strategy for Cyberspace* de 2011 ante a defesa, retaliação e legitimação de *cyber* ataques realizados à agentes maliciosos antagônicos que ameaçam os Estados Unidos e seus interesses (Amoretti e Fracchiolla, 2018, p. 27). A partir desse documento, os EUA passaram a seguir parâmetros transparentes para a identificação dos oponentes, realizados, nesse período, por Michael S. Rogers, diretor USCYBERCOM e da Agência de Segurança Nacional. Advindo de escritos desclassificados, Rogers (2017, p. 05 e 06) constatou que os principais opositores dos EUA são a China, a Rússia, o Irã, a Coreia do Norte, grupos terroristas diversos e *cyber* criminosos.

Esses agentes, ainda segundo Rogers (2017, p. 06), se utilizavam de táticas avançadas para criar ou se aproveitar das vulnerabilidades cibernéticas dos Estados Unidos, causando danos ao Estado. Desta forma, é necessária a existência de respostas coercitivas, ou até mesmo preemptivas, como forma de defender as infraestruturas críticas governamentais e os interesses estadunidenses desses oponentes.

A partir das indicações e estratégias pontuadas, CFR (2024) conseguiu atribuir aos Estados Unidos autoria em três casos de ataques cibernéticos em 2017, sendo o maior número de ocorrências até aquele ano. Dentre esses episódios, foi descoberto em 2017, o *Payload* do *spyware* global *Longhorn*. Com base nos relatórios da Kaspersky (2017), *Longhorn* - também conhecido como *The Lamberts* - foi um APT que se utilizou de *Zero-Day Exploits* além de outras ferramentas avançadas para roubar dados relevantes dos setores privados e governamentais e transmiti-los aos múltiplos Servidores de Comando-e-Controle. Esse *malware* também salvava o tráfego de rede utilizado pelas vítimas, executava *plug-ins* - recursos adicionais de um aplicativo - sem o conhecimento do *hard drive*, criava *backdoors* para acessos futuros e se utilizava das informações roubadas para se aprimorar no tempo, aumentando seu nível de periculosidade.

Essa movimentação particular do *Longhorn* fez com que se este APT mantivesse ativo com *Missiles* recorrentes desde 2004 (Kaspersky, 2017), se refinando com tanta sofisticação, que possibilitou com que o *malware* desenvolvesse "famílias" voltadas a tipos diferentes de vítimas, com tipos distintos de Servidores de Comando-e-Controle utilizados. Segundo Kaspersky (2017), até o ano de 2017, foram descobertos a ação de seis tipos diferentes de *malwares* da tipologia *Longhorn* - os *Lamberts*[31] preto, branco, azul, cinza, verde e rosa.

Os *Missiles* utilizados, mesmo com diferenças no estilo de codificação e nas configurações utilizadas, operavam com um mesmo formato de criptografia e de linhas de códigos, escolhendo a mesma base de Servidores de Comando-e-Controle, facilitando a conexão entre esses *spywares* (Kaspersky, 2017). Entretanto, mesmo com um nível de semelhança e um alto período de pesquisa dedicado ao estudo do *Longhorn*, os grupos Kaspersky e *FireEye* - empresa estadunidense de *cyber* segurança - não conseguiram conjuntamente estipular as formas de infecção e o número de vítimas afetadas pelos *Lamberts*.

Ponto agravado ao indicar o fato desse APT deletar e suprimir facilmente sua existência em caso de uma busca minuciosa, fazendo com que esse *malware* fosse classificado como um

[31] A ordem indicada representa a evolução da tipologia presente neste *malware* no tempo, sendo o *Lambert* rosa o mais sofisticado e o último a ser encontrado em 2017 (Kaspersky, 2017)

ato de espionagem cibernética refinada com objetivos e vítimas globais (CFR, 2024). Devido às características supracitadas, não houve nenhuma reação ou denúncia internacional derivada desse caso de ciberataque.

A segunda ocorrência realizada em 2017 pelos EUA, conforme relatado pelo CFR (2024), foi identificada em março e se focou na sabotagem cibernética realizada contra o programa de mísseis da Coreia do Norte. Entre 2014 e 2017, segundo Sanger e Broad (2017), foi percebido que durante exercícios militares norte-coreanos, diversos mísseis balísticos dificilmente acertavam os alvos, falhando seu lançamento ou explodindo em pleno ar. Naquela época, os militares da Coreia do Norte consideravam a presença de erros de manufatura ou até mesmo descuido humano no transporte ou uso desses armamentos como os motivos desses eventos problemáticos.

Contudo, no início de 2017, foi entendido através de entrevistas com os oficiais do Pentágono e de documentos, uma vez confidenciais, mas agora extensivos, de que havia uma estratégia estadunidense em execução com o objetivo de criar avarias nos armamentos da Coreia do Norte (Sanger e Broad, 2017). Planejamento esse que se originava da administração Obama e se tratava de uma medida emergencial de controle dos programas militares e nucleares norte-coreanos. A partir dos dados obtidos, os principais órgãos de defesa dos Estados Unidos não conseguiriam deter ou contra-atacar rapidamente a faixa de alcance balístico da Coreia do Norte, que crescia anualmente, podendo logo serem capazes de se utilizar com precisão mísseis intercontinentais (Sanger e Broad, 2017).

Com isso, era necessário que os Estados Unidos e suas instituições aumentassem os investimentos na área de defesa, além de realizarem fomentos nos atos de desaceleração preemptiva do desenvolvimento armamentístico da Coreia do Norte. Com essa perturbação, realizada de forma sigilosa, as tecnologias antimísseis estadunidenses poderiam ser fomentadas para proteger seu espaço aéreo e de seus aliados - caracterizando como o *Payload* do ataque.

Na administração Trump, foi percebido por Sanger e Broad (2017) a transição desse planejamento cibernético de sabotagem, porém agora em um caráter mais transparente devido às preferências presidenciais mais agressivas ante a resolução dessa problemática, implicando o uso e as intenções estadunidenses prévias contra a Coreia do Norte nos eventos supracitados, criando uma circunstância belicosa entre os Estados. Apesar disso, não foi percebida nenhuma reação ou resposta norte-coreana por parte do caso (CFR, 2024).

Já o último ciberataque atribuído aos Estados Unidos em 2017 foi um caso de negação de serviço efetuado contra o Escritório Geral de Reconhecimento da Coreia do Norte, a

principal agência de inteligência desse Estado. Identificado em setembro de 2017, o ataque se focou em criar um DDoS massivo contra o setor da empresa de telecomunicação russa *TransTelekom* - fornecedor de *internet* à Coreia do Norte, mais especificamente aos servidores do Escritório Geral de Reconhecimento (Gallagher, 2017 e DeYoung, Nakashima e Rauhala, 2017). O ataque durou apenas dois dias - entre 29 e 30 de setembro - e interrompeu os trabalhos dos oficiais de inteligência norte-coreanos em um caráter temporário, premeditado e não-destrutivo.

Essa ocorrência, no entanto, teve como diferencial o reconhecimento do Comando Cibernético Estadunidense - USCYBERCOM - ante a autoria do *cyber* ataque, caracterizando-o como uma operação militar (DeYoung, Nakashima e Rauhala, 2017). Segundo entrevistas com oficiais do Pentágono e do secretário de defesa dos EUA, o objetivo da ação era "sinalizar a Coreia do Norte uma postura agressiva advinda dos Estados Unidos", sendo realizada através do uso das capacidades cibernéticas ofensivas de uma forma disruptiva (DeYoung, Nakashima e Rauhala, 2017). Mesmo com a possível existência de uma retaliação, facilitada pela transparência estadunidense ante ao ato, as reações norte-coreanas foram desconhecidas (CFR, 2024).

Em relação aos ataques cibernéticos realizados contra os Estados Unidos, CFR (2024) identificou 13 ataques atribuídos aos atores estudados. Dentre elas, quatro das ocorrências de espionagem foram responsabilizadas à Rússia - nos casos *NotPetya*; *Whitebear*; os ataques à campanha presidencial do senador Marco Rubio e as ofensivas aos colaboradores de companhias de usinas elétricas nucleares. Já o Irã foi imputado em três eventos, também de espionagem cibernética - nos eventos *MuddyWater*; *Copy Kittens* e APT 33.

A China foi acusada de realizar também quatro casos de espionagem em 2017, como indicado nas circunstâncias do APT 10, APT 40, na denúncia formal acerca dos atores responsáveis pelo APT 3 de 2015 e nas arremetidas cibernéticas à *websites* de notícias dos Estados Unidos em língua chinesa. Por fim, a Coreia do Norte foi indicada em dois casos - o de espionagem presente nos ataques às companhias elétricas estadunidenses e no ato de destruição de dados disposto no caso *WannaCry*.

No que tange às reações estadunidenses ante aos incidentes dispostos, em três desses eventos foi constatada uma denúncia internacional da existência do ataque e uma atribuição formal de culpados, indicado pelo CFR (2024) nas ocorrências de acusação a China pelo APT 3, pelo *malware* russo *NotPetya*, cujo último foi atestado uma negação pública da Rússia em relação aos envolvimento estatal ante o incidente. A última atitude formal dos Estados Unidos

em 2017 foi a respeito do caso norte-coreano *WannaCry*, onde Park Jin Hyok - autor do *doxing* presente no ataque à Sony de 2014 - foi condenado novamente pela corte de Justiça dos Estados Unidos pelos crimes de conspiração e fraude eletrônica como o agente responsável pelo *malware WannaCry* (Estados Unidos da América, 2017c p. 01).

2.8.1 - O ano de 2017: Capacidades Defensivas Estadunidenses

Sobre as movimentações defensivas, foi constatado três atos durante o ano de 2017, com a finalização do quinto encontro do GGE da ONU, a realização da segunda versão do Manual de Tallinn e a assinatura[32] em dois acordos internacionais de ciberdefesa. Essa seção inicia com o encontro de 2015-2017 da GGE, que, segundo Hitchens e Goren (2017, p. 30-34), Klaar (2021, p. 06) e Schmitt (2021), falhou em alcançar uma conformidade entre as partes e elaborar algum relatório para condutas estatais cibernéticas.

O principal problema percebido na reunião se pautou em como as normas discutidas - não somente neste encontro, mas nos anteriores - conseguiriam produzir resultados legais para serem aplicadas internacionalmente. Segundo alguns oficiais da reunião do GGE, as principais queixas advinham do fato de que os procedimentos engendrados nos relatórios tinham uma natureza não legalmente vinculativa, dificultando seu cumprimento. Outra problemática provém novamente do fato que as leis internacionais pretendidas se utilizavam de preceitos que não são aceitos plenamente entre todos os Estados-membros como base - contando de exemplo o Direito Internacional dos Conflitos Armados (DICA) para a Rússia a China (Hitchens e Goren, 2017, p. 30, Klaar, 2021, p. 06 e Schmitt, 2021).

Isso fez com que houvesse um descontentamento entre as partes e um questionamento sobre a continuidade do projeto no futuro, causando um colapso na reunião em junho de 2017. Ocorrência que fez com que as reuniões posteriores da GGE fossem canceladas em um prazo indefinido, criando incertezas do desenvolvimento temático defensivo em um caráter internacional (Klaar, 2021, p. 06-07). Circunstância avançada somente em 2018, conforme indicado na próxima subseção defensiva.

[32] A partir do ano de 2017, perde-se a contribuição de Hitchens e Goren (2017) como a base de dados principal para apresentação das capacidades cibernéticas defensivas, dado o recorte temporal realizado pelas autoras. Com isso, a presente dissertação tenta engendrar as mesmas escolhas metodológicas das autoras na busca e apuração dos dados defensivos dispostos nos anos posteriores. Dessa forma, foi gerada uma investigação circunstanciada em todos os arquivos públicos estadunidenses e em todas as Instituições Internacionais nas quais os Estados Unidos fazem parte em busca de relatórios e documentos que atestem a participação ou assinatura desse Estado em tratados com tipologias cibernéticas. A contar da seção 2.8.1, esses foram os resultados alcançados.

Também em 2017 foi repensada e publicada uma atualização da principal legislação para conflitos armados em um âmbito cibernético: o Manual de Tallinn. Chamada de "Manual de Tallinn Sobre a Lei Internacional Aplicável ao Conflito Cibernético versão 2.0", esse documento, segundo Jensen (2017, p. 738), teve como intuito principal a superação dos desafios e as controvérsias advindas de seu modelo anterior.

Elemento reparado na ampliação dos autores utilizados em sua produção, que agora continham mais *experts* em diversas áreas complementares - direitos humanos, leis espaciais e legislação internacional de telecomunicações. Não obstante, esses profissionais tinham origens diversas, com naturalidades japonesas, tailandesas, chinesas e bielorrussas trabalhando em conjunto com o Centro de Excelência Cooperativo de *Cyber* Defesa - CECCD - da OTAN, autor da primeira versão.

Ainda com a finalidade de ser caracterizada como uma reformulação legislativa com aspectos não legalmente vinculativos, o Manual de 2017 forneceu definições, explicações e comentários de como as regras já existentes poderiam ser aplicadas em cenários e exemplos cibernéticos (Jensen, 2017, p. 738). Dessa forma, o documento foi dividido em quatro partes, salientando sobre as leis gerais e internacionais sobre o *cyber* espaço (parte I); os regimes especializados para as leis internacionais sobre o ciberespaço (parte II); a paz internacional, segurança e atividades cibernéticas (parte III); e uma reformulação da segunda parte do Manual 1.0 de 2013 sobre Condutas de Hostilidade, Leis sobre Conflito Armado, Neutralidade, Ocupação e Certas Pessoas, Objetivos e Atividades relevantes (parte IV).

Posto isso, os autores dessa versão também se preocuparam em abranger uma solução para a segunda grande problemática do Manual de 2013: a discordância entre as recomendações realizadas. A partir dos escritos de Jensen (2017, p. 739 e 740), a falta de consenso foi indicada no documento a partir da quantidade de *experts* divergentes, expressando maioridade ou menoridade na seção disposta. Ou seja, em uma alínea específica da publicação, caso houvesse divergências, o manual indicou transparentemente o nível de concordância, discordância ou reconhecimento dos *experts* acerca das definições ou exemplos de resolução utilizados, facilitando a noção da visão autoral ampliada no assunto e esclarecendo dúvidas aos leitores.

Mesmo com mudanças perceptíveis, o Manual de Tallinn de 2017 ainda não pôde ser considerado como um iniciação legislativa ante a área cibernética, necessitando de maiores alterações, participantes e concordâncias internacionais para ser classificado como um modelo normativo a ser seguido. Entretanto, devido à falta de uma lei internacional cibernética, Jensen

(2017, p. 778), indicou o uso e as recomendações da versão 2.0 entre os Estados ocidentais a partir de 2017.

Dessarte, como resultado da mudança do governo, em 2017 foi encontrada publicamente a participação e assinatura dos Estados Unidos em apenas dois acordos internacionais voltados a área cibernética realizados em apoio com a OTAN. Segundo a OTAN (2024), o primeiro tratado foi o Acordo-Quadro em Cooperação de Ciberdefesa entre a OTAN e a Finlândia. Firmado em fevereiro de 2017, este tratado teve como objetivo o fortalecimento das redes de comunicação dos signatários, criando uma relação cooperativa temática fomentada através do intercâmbio de informações e treinamento conjunto entre as partes.

Já o último acordo subscrito foi a Cooperação OTAN-UE Sobre Ameaças Cibernéticas realizado em dezembro de 2017. Segundo OTAN (2017, p. 09) e OTAN (2024), essa convenção priorizava a construção conjunta de capacidades cibernéticas para a identificação e mitigação das ameaças cibernéticas entre os membros. Dito isso, o acordo estipulava operações cibernéticas e treinamentos conjuntos entre os CERTs organizacionais, a criação de parâmetros de boas práticas cibernéticas, intercâmbio de informações entre as agências de segurança e defesa cibernética e a criação de um time conjunto para o gerenciamento de crises cibernéticas e cinéticas. Vale ressaltar a presença de 29 Estados-membros da OTAN assinantes desse tratado com a entrada de Montenegro em junho de 2017.

2.9 - O ano de 2018: Capacidades Ofensivas Estadunidenses

Devido às ações e os comprometimentos definidos na *America First: A Budget Blueprint to Make America Great Again"* (Estados Unidos da América, 2017b), a questão orçamentária dos Estados Unidos para o ano de 2018 foi caracterizada de uma forma distinta em relação aos períodos anteriores, ponto constatado no aumento de 9,6% advindo da quantia de 639,1 bilhões de dólares destinadas aos âmbitos de segurança e defesa. Contudo, conforme ressaltado na subseção ofensiva anterior, esse acréscimo foi garantido a partir de redistribuições de renda de outros setores e departamentos para a temática securitária, indicando singularidade no processo.

Em 2018, a partir dos documentos oficiais, a repartição orçamental destinada à cibersegurança sofreu uma diminuição de 99% em relação ao ano anterior, com 51 milhões de dólares outorgados ao setor. O motivo dessa atenuação específica não foi estabelecida nos relatórios orçamentários, criando possibilidades analíticas alternativas em relação à transparência estatal na divulgação de dados oficiais.

No que se refere a postura legislativa estadunidense, em 2018, a administração Trump realizou duas movimentações em prol ao âmbito cibernético: a construção da Estratégia Nacional de Defesa (Estados Unidos da América, 2018a) e a Visão de Comando do USCYBERCOM (Comando Cibernético dos Estados Unidos, 2018). Segundo os escritos de Dziwisz e Romaniuk (2023, p. 308 - 309) e Estados Unidos da América (2018a), a Estratégia Nacional de Defesa incluía tópicos voltados em mais uma ampliação no alcance das funções do Comando Cibernético Estadunidense, recebendo uma anuência da Casa Branca para realizar operações militares ofensivas contra os principais adversários dos Estados Unidos.

Não obstante, a Estratégia retomou pontos de seu documento estratégico de 2017 e fortaleceu a noção de "preservar a paz pela força", indicando que o espaço cibernético não será mais categorizado como algo distante da política ou dos elementos tradicionais do poder nacional dos Estados Unidos, recomendando o uso e a integração das opções cibernéticas em todas as possibilidades inerentes ao uso de poder estadunidense (Dziwisz e Romaniuk, 2023, p. 309 e Defesa, 2018). Para isso, a partir de 2018, os órgãos dos EUA não só passaram a se utilizar das capacidades cibernéticas ofensivas contra seus principais oponentes, mas o fizeram de uma forma evidente, destacando que os Estados Unidos queriam "identificar, constranger, degradar, dissuadir e se opor a qualquer comportamento que desestabilize ou contrarie seus interesses nacionais" (Nelson, 2018; Dziwisz e Romaniuk, 2023, p. 309 - tradução nossa), confirmando o avanço ofensivo dos EUA para o âmbito cibernético.

Desenvolvimento esse também percebido organizacionalmente através da Visão de Comando do USCYBERCOM de abril de 2018 e da mudança nas lideranças do Comando e da Agência de Segurança Nacional, com a integração do General Paul M. Nakasone. Conforme salientado nos escritos de Devanny (2021, p. 06) e Comando Cibernético dos Estados Unidos (2018, p. 02), o documento organizacional enfatizou a estruturação e o uso, em um padrão oficializado, de dois conceitos à doutrina cibernética estadunidense: defesa dianteira (*forward defense* em inglês) e o combate persistente (*persistent engagement* em inglês) de forma a garantir uma superioridade no espaço cibernético.

Segundo Fischerkeller e Harknett (2018, p. 04) e Smeets (2020, p. 03) ambos os conceitos de defesa dianteira e combate persistente tratam da redefinição da estratégia estadunidense a fim de facilitar uma operacionalização mais fluida no espaço cibernético, posto pela USCYBERCOM como um âmbito dinâmico. Dessa forma, a ação dos órgãos militares dos EUA se concentrariam em criar um estado de combate persistente, que indica formas de estabelecer uma postura mais ativa no ciberespaço, que prioriza atos de "resiliência, defesa,

contestação e reação aos atos cibernéticos maliciosos de seus oponentes", para assim forçar com que seus adversários reduzam seus atos de ataque por estarem ocupados com a defesa de suas próprias infraestruturas críticas – caracterizado como defesa dianteira – (Fischerkeller e Harknett, 2018, p. 04).

Através desses atributos de planejamento, seriam criadas oportunidades favoráveis de predominância à ação e à defesa das infraestruturas críticas estadunidenses e de seus interesses (Comando Cibernético dos Estados Unidos, 2018, p. 09). Ou seja, a nova visão de combate persistente da USCYBERCOM com a liderança de Nakasone propunha o uso e o desenvolvimento estadunidense de um estado de vigilância constante no *cyber* espaço, que salienta os principais riscos e oponentes presentes, para assim conseguir criar formas operacionalizadas de ataque - agora mais facilitadas - com o intuito de trazer uma segurança temática mais perceptível e de vanguarda aos EUA e seus aliados.

Posto isso, mesmo com um aprestamento legislativo e estratégico mais ressaltado ante ao tema de cibersegurança, em 2018 não foi comprovada nenhuma ação cibernética ofensiva aos Estados Unidos pelo CFR (2024). No entanto, com relação aos ciberataques realizados contra os EUA, a base de dados da CFR (2024) relatou a existência de 22 casos atribuídos aos Estados oponentes estudados, o maior número de ocorrências neste recorte temporal. Os incidentes em questão englobam atos cibernéticos de espionagem, sabotagem, *doxing* e roubo financeiro.

Dito isso, CFR (2024) responsabilizou a Rússia em sete desses atos - dispostos nos ataques às infraestruturas críticas dos EUA de fornecimento de energia; às campanhas políticas durante as eleições de meio de mandato no congresso dos Estados Unidos; ao gabinete da senadora Claire McCaskill; à Agência Anti-Doping; à companhia elétrica *Westinghouse Electric Corporation*; aos comprometimentos aos equipamentos de rede estatais; as salas de controle de utilidade elétrica estadunidenses. Foi atribuída a autoria ao Irã em três desses episódios - nos casos *Cobalt Dickens*; APT 35 e no assalto aos dados do Instituto *Mabna*.

CFR (2024) indicou o envolvimento da China foi culpabilizada em oito incidentes - nas ocorrências *Winnti Umbrella*; *Mustang Panda*; *Thrip*; nos comprometimentos às companhias provedoras de serviços conjuntos; às organizações associadas com atividade comercial chinesas; às companhias estadunidenses aeroespaciais; aos contratados da Marinha dos Estados Unidos em dois momentos distintos. Já a Coreia do Norte foi responsabilizada em quatro atos cibernéticos ofensivos - presentes nas impugnações à rede de cinemas *AMC*; aos principais

empreiteiros de defesa estadunidenses; a diversos bancos globais sediados nos EUA e no caso *GhostSecret*.

Os Estados Unidos e suas instituições, no que se concerne aos atos realizados, reagiram através de denúncias internacionais em nove desses casos - os ataques russos à equipamentos de rede estatais, às infraestruturas críticas dos EUA de fornecimento de energia e as salas de controle de utilidade elétrica estadunidenses; o incidente iraniano contra o Instituto *Mabna*; os atos norte-coreanos contra a rede de cinemas *AMC*, aos principais empreiteiros de defesa estadunidenses e a diversos bancos globais sediados nos EUA; e nos incidentes chineses de comprometimento às companhias provedoras de serviços conjuntos e às companhias estadunidenses aeroespaciais - sendo respondido seis[33] vezes por parte dos Estados suspeitos, que negaram o envolvimento estatal no incidente cibernético. Em oito[34] dos 22 casos supracitados, houve movimentações jurídicas por parte dos Estados voltadas para criar sanções internacionais contra os Estados atacantes, condenando e sentenciando os principais indivíduos envolvidos (CFR, 2024).

2.9.1 - O ano de 2018: Capacidades Defensivas Estadunidenses

Em 2018 foram constatadas três movimentações legislativas internacionais dos Estados Unidos defensivamente, vistas no desenvolvimento da OEWG (*Open-Ended Working Group* - Grupo de Trabalho Aberto, em inglês) da ONU, na criação de uma agência de segurança doméstica focada na proteção das infraestruturas críticas - a *Cybersecurity and Infrastructure Security Agency* (CISA - em inglês, Agência de Segurança Cibernética e de Segurança à Infraestruturas) e na subscrição em um acordo multilateral com a OTAN. A OEWG, a partir dos escritos de Klaar (2021, p. 07) e Schmitt (2021), surgiu do espaço deixado pelo fim abrupto da GGE em 2017, como uma possibilidade de manter o tópico cibernético estruturado e discutido entre os membros das Nações Unidas.

[33] Os três casos que não foram negados estatalmente foram: o ataque russo contra a rede de fornecimento de energia; o incidente chinês contra companhias estadunidenses aeroespaciais e o ato norte-coreano contra os bancos globais.

[34] Os atos russos contra a rede de fornecimento de energia; aos equipamentos de rede estatais e à companhia elétrica *Westinghouse Electric Corporation*; o incidente iraniano de ataque ao Instituto *Mabna*; as ocorrências norte-coreanas contra a rede de cinemas *AMC* e aos principais empreiteiros de defesa estadunidenses; e os casos chineses de espionagem às companhias provedoras de serviços conjuntos e às companhias estadunidenses aeroespaciais.

Iniciado a partir dos intentos da Rússia, o grupo foi criado através do relatório A/RES/73/27, que indicou os principais desafios e oportunidades dispostos no Sistema Internacional Cibernético, necessitando com que haja um esforço contínuo dos atores internacionais em prol de discutir, entender e mitigar os riscos inerentes do espaço cibernético. Um diferencial do OEWG é que esse grupo de trabalho tentou ampliar as discussões para outros setores, não se mantendo somente como um grupo Estatal (Klaar, 2021, p. 07 e Schmitt, 2021).

Essa flexibilidade também foi vista no próprio documento produzido, que se focou apenas em estabelecer diálogos legislativos, se abstendo do rigor técnico que era visto como uma problemática entre os participantes do GGE. Esse prospecto permitiu a atração de novos participantes, expandidos a todos os membros da ONU e Organizações interessadas (Klaar, 2021, p. 07). A partir de sua primeira reunião em dezembro de 2018 em Nova York, a OEWG se tornou um sucesso ante a disseminação de conhecimento inclusivo sobre os principais temas de *cyber* segurança, criando recomendações legislativas mais acessíveis aos Estados e aos atores do Sistema Internacional. Com isso foi possibilitado com que fossem realizados consensos internacionais com maior facilidade nos anos posteriores.

A CISA, criada a partir da lei pública 115-278 em novembro de 2018 (Estados Unidos da América, 2018b), surgiu da necessidade dos Estados Unidos e de seus órgãos em estabelecer uma Organização única voltada a proteger as infraestruturas críticas nacionais em um contexto específico (CISA, 2021a, p. 02). Dessa forma, a Agência teve como missão principal conduzir e manter os programas, as operações e as políticas de proteção de *cyber* segurança nas áreas de defesa das infraestruturas críticas e comunicação emergencial, doméstica e internacionalmente (CISA, 2021a, p. 02 e CISA, 2021b, p. 01).

A fim de garantir seus pretextos fundadores, a CISA foi desenvolvida para detectar, prevenir e compartilhar informações acerca dos principais riscos cibernéticos aos seus parceiros, nas áreas públicas - principalmente nos CERTs governamentais - e privadas, além de realizar operações integradas de defesa nacional e internacional das infraestruturas críticas estadunidenses e de seus aliados. A CISA também ajudou no desenvolvimento das capacidades defensivas a partir do intercâmbio de informações emergenciais e da criação de sistemas de comunicação conjuntos entre os parceiros, facilitando a proteção de seus dados no espaço cibernético, fomentando a cooperação técnica no contexto de *cyber* segurança (CISA, 2021a, p. 05 a 07 e CISA, 2021b, p. 02).

Por fim, a Agência, ao dispor de dez centros regionais, realizou treinamentos e seminários das melhores práticas cibernéticas aos seus parceiros e colaboradores, além de se

utilizar desses recursos para manter e potencializar as políticas e os acordos temáticos firmados pelos Estados Unidos. É válido destacar que não foram identificados nas plataformas da CISA as métricas de atuação da Organização dos tratados firmados, e nem quais tratados tiveram a participação dessa Agência.

Já a última participação estadunidense em um contexto defensivo foi obtida na anuência e assinatura para a construção de um Centro de Operações do Ciberespaço em parceria com os Estados aliados à OTAN. Realizado como um produto da Cúpula de Bruxelas, esse esforço temático fortaleceu a estrutura de comando cibernético dos signatários, proporcionando um intercâmbio de informações rápida e possibilitando a realização de operações militares cibernéticas conjuntas, treinamentos e seminários entre os CERTs institucionais e estatais (OTAN, 2024).

2.10 - O ano de 2019: Capacidades Ofensivas Estadunidenses

Ao ainda seguir as prioridades políticas e orçamentárias derivadas do *blueprint* de 2017, o quantitativo destinado à temática de segurança e defesa recebeu mais um aumento, dessa vez de 7,3% em relação ao ano anterior, determinado no valor de 686 bilhões de dólares para o ano fiscal de 2019. O segmento reservado especificamente ao setor de *cyber* segurança também ganhou um incremento visível neste ano, com um crescimento de 26700% em referência a 2018, com 13,7 bilhões de dólares distribuídos na área cibernética. Amplificação temática que retoma a discussão acerca da veracidade dos dados específicos dispostos no ano de 2018.

No que concerne às movimentações domésticas para o âmbito de *cyber* segurança, Devanny (2021) indicou os empreendimentos de Paul M. Nakasone - agora diretor da USCYBERCOM e da NSA - em estabelecer as novas estratégias do Comando, elevando o poder cibernético empregado internacionalmente pelos EUA. Para Nakasone (2019) e Devanny (2021), o Comando e os Estados Unidos ainda deveriam se utilizar dos parâmetros propostos no ano anterior sobre o combate persistente e a defesa dianteira para alcançar uma predominância no espaço cibernético, elemento tido como necessário após o aumento de *cyber* ataques dirigidos aos EUA em 2018 - ampliação de 69,2% entre 2017 e 2018.

Esse pensamento trouxe a necessidade de estabelecer e aumentar as operações cibernéticas pautadas na demonstração das capacidades ofensivas estadunidenses, para que os "oponentes sejam alertados de que os anos de passividade acabaram, e que os aliados se tranquilizem pois agora os Estados Unidos estavam em marcha no espaço cibernético"

(Devanny, 2021, p. 10 e Bolton, 2020, p. 182 - tradução nossa). Esses preceitos retomam os escritos de Rogers (2017) sobre a operacionalização do Comando e os tornam mais transparentes, ressaltando um novo modo de atuação estadunidense cibernética. Comportamento pronunciado nos informes de CFR (2024) que evidenciaram a participação dos Estados Unidos em cinco ataques cibernéticos durante o ano de 2019, sendo quatro deles com afiliação direta ou do governo dos EUA ou do próprio USCYBERCOM.

O primeiro caso que seguiu esses critérios foi estabelecido entre novembro de 2018 a fevereiro de 2019 - data de seu *Payload* oficial - e se tratou de uma operação cibernética ofensiva contra a desinformação russa. Com base nos escritos de Barnes (2018) e CFR (2024), esse ataque consistiu principalmente na localização dos principais agentes maliciosos responsáveis pela divulgação de informações falsas sobre os Estados Unidos durante as eleições de meio de mandato em 2018. Uma vez identificados, os autores - pontuados pela USCYBERCOM como russos - eram dissuadidos na continuação de suas atitudes criminosas através do uso de *Missiles* de negação de serviço.

Barnes (2018) indicou, que através dos testemunhos dos oficiais do Departamento de Defesa e do Comando Cibernético, não foram especificadas as formas de identificação desses agentes maliciosos ou a maneira na qual eles foram persuadidos a parar com suas ações. Contudo, foi ressaltado que esses indivíduos não foram ameaçados. Paul Nakasone, durante a operação, indicou publicamente que esse ato deveria ser visto como uma advertência dos Estados Unidos aos seus oponentes dispostos no ciberespaço, implicando o início de "uma competição entre grandes poderes" (Barnes, 2018 - tradução nossa). CFR (2024) ressalta a falta de reação pública e internacional por parte da Rússia sobre o caso.

A operação cibernética ofensiva Estadunidense contra a Rússia foi expandida com mais um ato durante fevereiro de 2019, agora com um ataque de sabotagem à empresa *Internet Research Agency* (IRA - Agência de Pesquisa na Internet, em inglês). Fundamentado nos relatórios de CFR (2024), essa arremetida ainda teve como objetivo o combate a desinformação das eleições de 2018, e, apoiado nos dados disponibilizados pela USCYBERCOM, a IRA tinha, na época, associações com o governo russo, criando e disseminando notícias falsas compartilhadas nas redes sociais.

Dito isso, Greenberg (2019) apontou que no ataque foram utilizados *Missiles* que derrubaram os servidores de rede da empresa por um tempo indeterminado, impossibilitando que os funcionários realizassem nenhum tipo de movimentação ou difamação. Greenberg (2019 - tradução nossa) também ressaltou, a partir de entrevistas com oficiais do Comando

Cibernético, o relato público de que, essa operação, assim como a supracitada, tinha como propósito secundário sinalizar ao governo russo que os "Estados Unidos poderiam ter feito pior, podendo destruir os computadores ou vazar comunicações internas do IRA". O analista de *cyber* segurança Robert Knake foi entrevistado para o artigo de Greenberg (2019) e questionou como o caso e a mensagem poderiam ter sido interpretados pela Rússia, visto que, mais uma vez, não houve nenhuma reação pública e internacional na época.

Em junho de 2019, CFR (2024) relatou outra ação cibernética ofensiva realizada pelo Comando Cibernético dos Estados Unidos. Ao ver a queda de um drone estadunidense por parte do exército iraniano como provocação, o governo dos Estados Unidos permitiram a condução da USCYBERCOM em realizar ataques cibernéticos contra as redes da Agência de Inteligência do Irã (CFR, 2024 e Barnes e Gibbons-Neff, 2019). Os ataques continham *Missiles* com *Payloads* voltados a sabotagem militar em múltiplas camadas, chegando a utilizar de vulnerabilidades já existentes - como *Zero-Day Exploits* - para tomar o controle dos sistemas de mísseis e foguetes iranianos, que pararam de responder.

Barnes e Gibbons-Neff (2019) indicam a natureza transitória do ataque, uma vez que as redes e os sistemas militares foram rapidamente retomados, segundo as declarações dos líderes militares iranianos. Posto isso, CFR (2024) e a agência Reuters (2019 - tradução nossa) revelam a existência de uma denúncia internacional do Irã ao ataque dos Estados Unidos, não levada adiante por conta da "vontade de não escalar as tensões e as consequências".

Quatro meses após essa circunstância, em outubro, foram encontradas evidências de ação do governo dos Estados Unidos em mais um ataque cibernético contra o Irã. Ao considerar as informações citadas por CFR (2024) e Ali e Stewart (2019), a ofensiva cibernética teve dois motivadores, sendo o primeiro uma forma de retaliação a um suposto ataque do Irã contra navio-petroleiro dos Estados Unidos em maio. O segundo ato promotor foi percebido em setembro, com um bombardeio a instalações petrolíferas na Arábia Saudita, cujo ataque foi atribuído publicamente pelos Estados Unidos, Arábia Saudita, França, Alemanha e Reino Unido como de responsabilidade iraniana.

Por conseguinte, a operação ofensiva enviou vários *Missiles* contra servidores localizados no Teerã, capital do Irã, que tinham como *Payloads* a destruição de dados e a danificação dos componentes presentes na infraestrutura, causando avarias físicas ou perda total nos *hardwares* existentes (Ali e Stewart, 2019). Fora isso, não foi divulgada nenhuma informação específica sobre as tecnologias empregadas nos *Missiles*.

Nesse incidente, ao contrário dos reportados anteriormente, o Pentágono e a USCYBERCOM não se pronunciaram abertamente sobre a existência do caso ou a participação estadunidense nele. Ponto que permitiu com que a identificação e a atribuição do ato ofensivo fosse realizada através das denúncias iranianas sobre o dano causado, reação única percebida pela investigação de CFR (2024) sobre as trilhas de códigos dispostas na rede pelo ataque realizado.

O último episódio cibernético ofensivo de responsabilidade estadunidense foi notificado em junho de 2019, com o ataque à empresa russa *Yandex*. CFR (2024) e Bing, Stubbs e Menn (2019) relatam que esse *malware*, com a codificação semelhante ao *Regin* de 2014, se utilizou de *Missiles* voltados a criação de vulnerabilidades nas métricas de autenticação dos colaboradores entre outubro e novembro de 2018, para assim se infiltrar na rede de dados pessoais e corporativos da *Yandex*, uma companhia de serviços tecnológicos que abarcou *e-mails* e o principal motor de busca na Rússia, Bielorússia, Cazaquistão e Turquia, com mais de 108 milhões de usuários mensais (Bing, Stubbs e Menn, 2019).

Em junho de 2019, foi identificado o *Payload* do *malware*, que não consistia apenas no roubo dos dados, mas na vigilância externa das pesquisas e acessos realizados na *Yandex*, se mantendo indetectável por semanas no sistema. Por conta desse ataque, o governo russo contratou a empresa de cibersegurança Kaspersky, que ao identificar o *Payload* do ataque, conseguiu rastrear e relevar que três desenvolvedores da *Yandex* foram responsáveis pela disseminação do vírus.

Posteriormente à identificação, foi atestado, através de uma investigação extensa, uma ligação e comunicação desses indivíduos com governos ocidentais - principalmente com os Estados Unidos - garantindo, com isso, suas prisões (Bing, Stubbs e Menn, 2019). Após isso, diversas empresas internacionais de cibersegurança tiveram acesso aos relatórios da Kaspersky sobre o caso e os códigos de *malware* utilizados, confirmando a existência e as atribuições realizadas nesse incidente.

Em referência aos ataques efetuados contra os Estados Unidos em 2019, CFR (2024) indica a existência de 13 ataques cibernéticos, responsabilizados aos quatro Estados oponentes. Posto isso, dentre as ocorrências reportadas, duas delas são atribuídas a Rússia - nos ataques aos *think-tanks* europeus e estadunidenses e ao *Democratic National Convention* (DNC - Convenção Nacional Democrata em inglês) - e seis são irrogados ao Irã - nos casos de comprometimentos a mais de 60 universidades no mundo em 2019; ao DNS (*Domain Name System* – Sistema de nome de domínio, em inglês) global; às corporações privadas dos EUA;

às campanhas presidenciais estadunidenses; aos oficiais de campanha presidenciais jornalistas e expatriados iranianos proeminentes e ao governo dos Estados Unidos e outros órgãos e entidades privadas em um grau amplo.

Ainda segundo CFR (2024), três episódios cibernéticos são responsabilizados à China - indicados nos atos de impugnação de segredos militares das universidades da marinha, espionagem a empresas privadas de manufaturados dos Estados Unidos e no caso APT 41. Os últimos dois casos são imputados à Coreia do Norte - nas arremetidas de intimidação usadas no caso *Autumn Aperture* em dois momentos distintos no ano de 2019.

Os órgãos competentes dos Estados Unidos, em 2019, reagiram publicamente a dois desses incidentes, sendo percebida uma ação de denúncia internacional a conduta chinesa contra as universidades da marinha e ao *cyber* ataque iraniano de destruição de dados tida às corporações privadas dos Estados Unidos, evento esse que teve uma confirmação internacional ante sua existência. CFR (2024) destacou a falta de negações advindas da China e Irã sobre o envolvimento estatal nos ataques e nas contestações estadunidenses.

2.10.1 - O ano de 2019: Capacidades Defensivas Estadunidenses

Ao continuar com as premissas presentes da administração Trump, os Estados Unidos em 2019 se mantiveram minimamente participativos na construção e fomento das capacidades cibernéticas defensivas internacionais. Contudo, foi notada a presença estadunidense em uma reunião internacional e na assinatura de um acordo multilateral de temática cibernética. O primeiro compromisso indicado acima se tratou da reformulação da sexta iteração GGE da ONU em setembro de 2019.

A GGE da ONU em 2019, segundo Schmitt (2021) e Klaar (2021, p. 08), foi repensada a partir dos esforços das lideranças dos Estados Unidos - presente na resolução A/RES/73/266 de 2018 - e da noção do sucesso da OEWG no ano anterior, criando novamente a necessidade de *experts* voltados a área cibernética criarem e se utilizarem de *frameworks* legislativos para entender e se mobilizar no espaço cibernético. A associação desses atores na GGE permitiria e retomaria a construção das capacidades cibernéticas conforme os resultados dialogados na OEWG, criando, com isso, um elo proveitoso entre os grupos de teoria e prática.

Dito isso, a nova GGE ainda possuiria um caráter mais formal e exclusivo dos 25 membros dispostos na reunião de 2016-2017, fundamentados para a discussão e a formulação de normas, práticas e princípios de construção de capacidades e na definição das principais

aplicações da leis internacionais aos questionamentos existentes ao espaço cibernético. Contudo, para que a mudança no órgão fosse concretizada, o GGE teria que integrar e consultar opiniões e pareceres de vários *experts* mundialmente - sendo temáticos ou não - para assim permitir uma ampliação mais assertiva e completa do tema cibernético e de seus principais atores.

Schmitt (2021) indicou que a primeira reunião GGE 2019-2021 conseguiu reativar os principais pontos de sucesso do grupo da ONU, salientando e progredindo o tema cibernético em múltiplas camadas de entendimento e alcançando consensos não percebidos na reunião de 2017. Essa continuidade e amplitude da área de diálogo permitiu com que as normas legalmente não vinculativas criadas pela GGE conseguissem ser aceitas com maior facilidade pelos participantes não ocidentais, possibilitando o início de reflexões responsáveis no espaço cibernético. Contudo, ainda é importante salientar que, pelos relatórios anteriores ainda não possuírem força legislativa internacional, os avanços criados pela GGE ainda são de natureza teórica, não produzindo resultados palpáveis aos Estados-membros.

Assim sendo, o governo dos Estados Unidos também participou e subscreveu em um acordo temático em 2019, sendo o Guia da OTAN de Fortalecimento das Capacidades Cibernéticas. Tal documento, segundo OTAN (2024), ajudou a Instituição, seus signatários e seus aliados a intensificar seus tempos de reação contra as atividades ofensivas dispostas no espaço cibernético. Para isso, Estados-membros se encarregam de aumentar sua resiliência cibernética através de treinamentos e seminários e de criar forças-tarefas conjuntas no futuro para se defender e combater as ameaças cibernéticas em um contexto amplo.

2.11 - O ano de 2020: Capacidades Ofensivas Estadunidenses

O último ano disposto no recorte temporal desta dissertação indicou, ao consultar os documentos oficiais do Departamento de Defesa dos Estados Unidos, um incremento orçamental no ano de 2019, reportando aumento de 4,7%, representado na forma de 718,3 bilhões de dólares. Essa movimentação, no entanto, não foi percebida no recorte orçamentário reservado aos temas de cibersegurança, que teve uma retração de 29,9% no ano, com um montante de 9,6 bilhões de dólares para a área.

O período de 2020 foi um ano no qual não se teve operações legislativas estadunidenses evidentes voltadas ao âmbito cibernético. Elemento motivado tanto pelo agravamento da doença COVID-19 pelo mundo, necessitando de ações prioritárias voltadas a outras áreas que

não a cibernética, e dado ao fato de que as eleições presidenciais estariam ocorrendo no final daquele ano, e, junto com ela, uma movimentação acentuada do presidente Donald Trump em alcançar sua reeleição, dispensando, com isso, a necessidade de criar orientações novas para a política estadunidense cibernética (Devanny, 2021, p. 15).

Posto isso, CFR (2024) atribuiu participação estadunidense em apenas um caso ofensivo em 2020, sendo uma continuação da sabotagem cibernética realizada contra a Rússia no ano anterior. Ponto indicado pelo lançamento de *Missiles* contínuos realizados pela USCYBERCOM contra as redes de informação e servidores de dados russos, assim como reportados no episódio contra à IRA entre 2018-2019. Com isso, o sistema russo foi boicotado, impedindo o uso dos dados da rede entre agosto e outubro de 2020, atingindo cerca de um milhão de máquinas em todo o território nacional da Rússia (Nakashima, 2020). O *Payload* central do ataque estadunidense estava na desativação do *botnet* chamado *TrickBot*, responsável por lançar diversos tipos de *Ransomwares*[35] capazes de sabotar a eleição presidencial daquele ano.

O *TrickBot*, a partir dos conceitos da CISA (2021c, p. 02-03), se tratou de um *Trojan* - um vírus facilitador para criação de *backdoors* - usado em estratégias de *Spear-phishing* cujo objetivo está ou no roubo de credenciais de acesso e de informações importantes; ou na facilitação para a ação de outros *malwares* responsáveis por manipular, interromper, e inutilizar dados ou sistemas em um servidor, tendo assim módulos de atuação dupla: de Reconhecimento e de Impacto. Nesse episódio, não foram relatados quais setores ou agências do governo foram atacados por esse *malware*, contudo, foram realizadas confirmações por Donald Trump e Paul Nakasone acerca da investida cibernética estadunidense na forma de entrevistas e participações públicas, na qual foram indicados o envolvimento estatal e da USCYBERCOM contra a Rússia.

Segundo esses atores, o ato se tratava de mais uma "operação para a proteção dos Estados Unidos e de seus interesses" (CFR, 2024, Nakashima, 2020 e Thiessen, 2020 - tradução nossa). CFR (2024) revela uma falta de reação pública e internacional russa acerca do caso supracitado.

Por fim, em relação aos ataques realizados contra os Estados Unidos em 2020, CFR (2024) constatou a existência de 19 ocorrências cibernéticas realizadas pelo grupo estatal oponente. Nesse conjunto ofensivo, foi atribuída à Rússia a autoria em três ataques - dispostos

[35] Segundo Simoiu et al (2019, p. 01) um *Ransomware* se trata de uma forma perniciosa de *malware* voltada a acessar e restringir o uso de dados em um servidor ou uma máquina, bloqueando seu acesso por parte do usuário. Esse vírus então obriga o utilizador a realizar uma ação - normalmente financeira - pela a liberação de suas informações ou o retorno do funcionamento do servidor atacado.

nas campanhas políticas de 2020 e aos consultores de advocacia filiados a partidos políticos; contra as redes governamentais da CISA e um ato de roubo de dados a uma agência governamental não identificada. O Irã, em 2020, foi responsabilizado em oito ações cibernéticas - nos eventos de personificação de jornalistas a fim de comprometer figuras públicas; nos comprometimentos às redes elétricas dos EUA; aos principais colaboradores do governo; às companhias privadas usando VPNs - *Virtual Private Network*, em inglês Rede Virtual Privada -; a diversas agências governamentais e companhias privadas dos Estados Unidos; à campanha presidencial de Donald Trump; às indústrias de informação do governo, planos de saúde, finanças e mídias sociais e no caso *Fox Kitten*.

A China foi imputada como principal autora em quatro ocorrências de 2020 - nos ataques a mais de 75 organizações públicas e privadas durante o ano; aos funcionários da campanha eleitoral de Joe Biden; à Comunidade de Assuntos Internacionais dos Estados Unidos; à agência de rede do governo dos EUA e na espionagem derivada do *malware Zirconium*. Já a Coreia do Norte foi acusada em quatro cenários de ataque - os casos *Zinc*; *Cerium*; as arremetidas cibernéticas contra diversos empreiteiros de defesa estadunidenses e contra uma entidade estadunidense não nomeada se utilizando de *Spear-Phishing*.

Dentre esses atos ofensivos, CFR (2024) indicou apenas uma denúncia internacional, relativa ao caso russo de ataque às campanhas políticas de 2020 e aos consultores de advocacia. Adicionalmente, em quatro ocorrências desse ano foram indicadas confirmações da existência das ocorrências internacionalmente, manifestadas nos atos russos de roubo de dados de uma agência governamental não identificada e na investida contra a CISA, no ataque iraniano às indústrias de informação do governo, planos de saúde, finanças e mídias sociais e no episódio chinês de espionagem à agência de rede do governo dos Estados Unidos.

2.11.1 - O ano de 2020: Capacidades Defensivas Estadunidenses

No último ano do recorte temporal estabelecido, as lideranças temáticas dos Estados Unidos assinaram e sancionaram apenas um tratado internacional com o foco cibernético, contudo esse acordo não foi realizado com um Estado-aliado foco desta dissertação. Os Estados Unidos, também em 2020, reafirmaram sua participação nos dois principais grupos de trabalho governamental voltados à temática cibernética defensiva: a GGE e a OEWG da ONU. A reunião da sexta sessão da GGE, ocorrida em fevereiro, ainda estava em período de discussões entre os

membros e não produziu nenhum relatório oficial para a aplicação de leis internacionais no ciberespaço, sendo realizada somente em 2021 (DIG, 2021, p. 01).

Já a OEWG perpassou por uma sessão e quatro reuniões virtuais para estabelecer consensos e possíveis construções de capacidades entre os participantes interessados, ampliando o debate temático com mais Estados e atores do Sistema Internacional Cibernético. Ponto que permitiu, em dezembro de 2020, a criação da resolução A/RES/75/240 que renovou o Grupo de Trabalho Aberto para um segundo mandato entre 2021 a 2025, trazendo novas possibilidades teóricas a serem consideradas por seus membros (DIG, 2024 e Klaar, 2021, p. 08).

Em face do exposto, este capítulo relatou e catalogou as principais Ações cibernéticas ofensivas e atos defensivos dos Estados Unidos em um período de 11 anos. Dito isso, o próximo capítulo analisará os dados dispostos a partir da metodologia *S.A.M.* com o pensamento autoral de Relações Internacionais voltada a poder usado na temática de *cyber* segurança. Elemento que permitirá a construção de métricas de avaliação de capacidades e a possível validação das questões propostas por esta dissertação.

CAPÍTULO 3 - ANÁLISE DAS CAPACIDADES CIBERNÉTICAS DOS ESTADOS UNIDOS: MOTIVOS, IMAGENS E PODER.

Uma vez estabelecidos os principais conceitos e os dados a serem utilizados nesta dissertação, o presente capítulo reunirá e analisará as informações dispostas a partir da temática de poder e *cyber* segurança no âmbito das RI. Tendo em vista esses objetivos, o terceiro capítulo se dividirá em três seções, com a primeira voltada para o aprofundamento categórico das informações estabelecidas no capítulo anterior, evidenciando características, especificidades e questões significativas nos 11 anos estudados, criando padrões para o estudo das capacidades estadunidenses.

Fundamentada nisso, a seção seguinte salientará as interpretações de poder estatal sob o âmbito cibernético de Nye (2010), reunindo os dados e os indicadores com a teoria das RI sobre cibersegurança, evidenciando principalmente as concepções das imagens de Jervis (1970) em conjunto com os Motivos de Kremer e Müller (2013). A última seção do capítulo estipulará as consequências perceptíveis dos atos dos Estados Unidos, avaliando o possível sucesso nas movimentações cibernéticas pretendidas no recorte pesquisado. Com isso, serão objetificadas as noções centrais acerca das capacidades cibernéticas estatais, incorporando premissas teóricas com a *práxis* dispostas nos dados.

3.1 - Exame Inicial dos Elementos Cibernéticos entre 2010 a 2020 - Um Olhar Aplicado

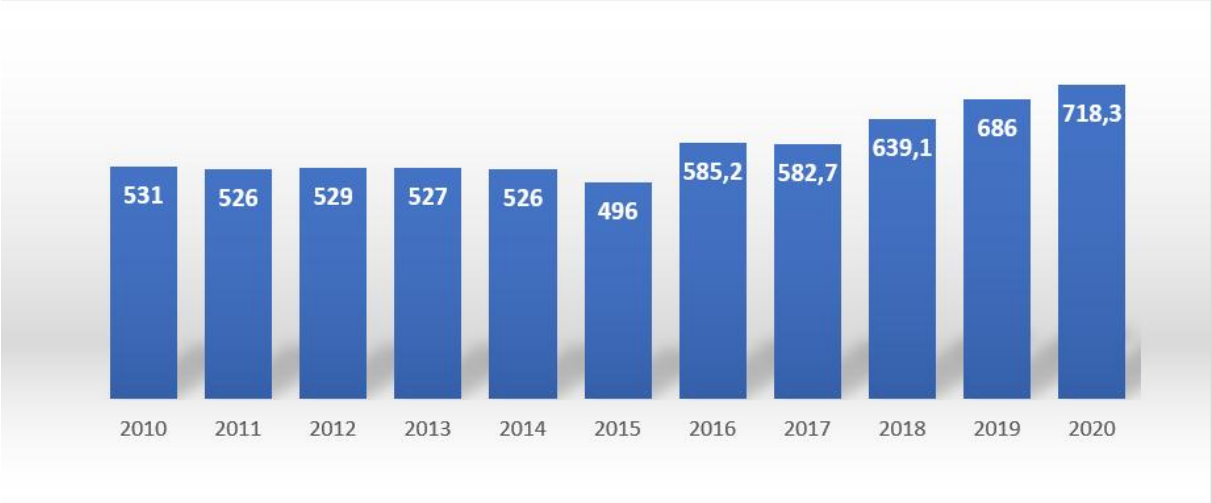
A fim de examinar as capacidades cibernéticas estadunidenses, este subtema irá expor as principais características presentes nos dados, casos, documentos, relatórios e acordos salientados no capítulo anterior, ressaltando elementos necessários para a investigação. Dessa forma, as capacidades cibernéticas ofensivas e defensivas entre 2010 a 2020 serão separadas, apresentadas e ilustradas em três tipologias: (1) estudo dos dados de orçamento para a defesa e segurança estadunidense, de forma geral e cibernética; (2) fundamentos percebidos nos casos de ciberataques, sendo esses ou realizados pelos EUA ou mirados a este Estado; e (3) informações derivadas dos acordos cibernéticos realizados e assinados no recorte temporal.

Primeiramente, ao congregar as informações orçamentárias abertamente divulgadas pelo Departamento de Defesa dos EUA, observou-se constância seguida de aumento nas quantias totais destinadas à temática de segurança e defesa. O acréscimo orçamentário, assim como estipulado no capítulo anterior, teve seu início em 2017 com o *Budget Blueprint to Make*

America Great Again (Estados Unidos da América, 2017b), que estimulou a área em detrimento da realocação de recursos advindos de outros departamentos.

A partir dessa movimentação, foi constatada uma progressão total de 35,2% no orçamento estadunidense entre 2010 a 2020, tendo o maior aumento anual em 2016 com 17,9% em relação ao seu ano anterior. O fluxo orçamentário supracitado também pode ser averiguado no apêndice abaixo:

Apêndice A – Gráfico orçamentário dos Estados Unidos para o Departamento de Defesa – em bilhões de dólares.



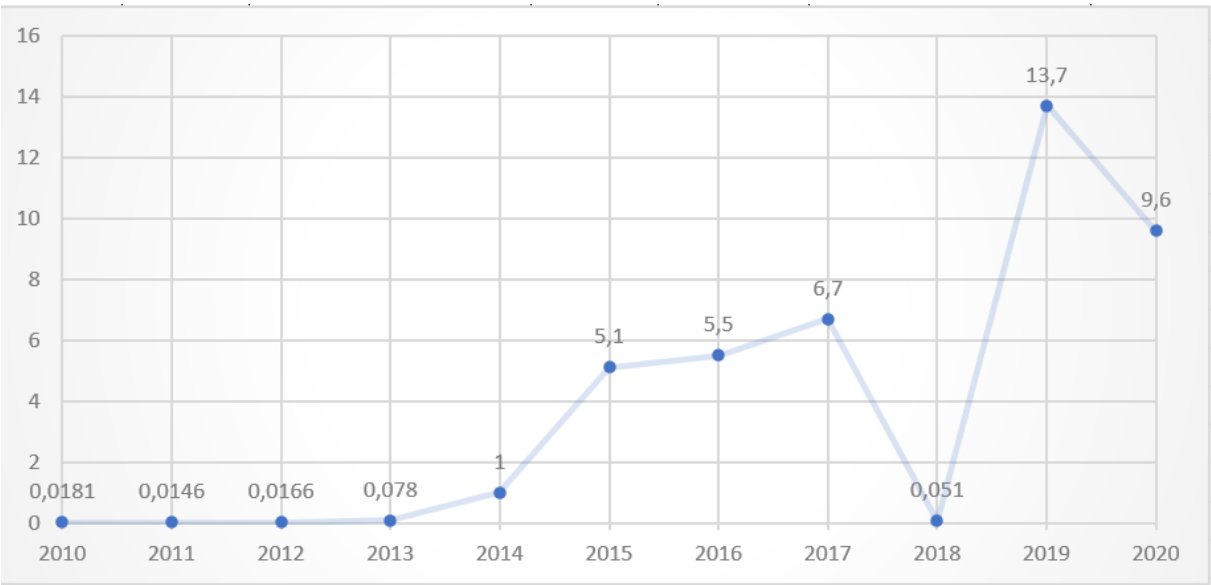
Fonte: Compilação do autor com base nos dados públicos do Departamento de Defesa dos EUA.

Oriunda principalmente de políticas e estratégias temáticas realizadas em dois governos distintos, parte da quantia orçamentária foi focalizada e amplamente divulgada à *cyber* segurança, permitindo e categorizando fomentos e utilizações diversas às capacidades cibernéticas dos Estados Unidos. Baseando-se nesses dados, ao contrário do percebido nos valores integrais, o desdobramento de valores cibernéticos foi efetivamente oscilante durante os anos.

Fundamentado nas informações compiladas no apêndice B, os recursos destinados pelo Departamento de Defesa ao domínio cibernético foram ampliados gradativamente durante os anos estudados - com uma adição de 52938% do início ao fim do recorte -, chegando a patamares orçamentários bilionários teoricamente crescentes, adquiridos principalmente entre 2014 e 2015. Contudo, em 2018, mesmo com aportes orçamentários notáveis decorrentes do governo Trump, o valor remetido à cibersegurança alcançou cerca de 51 milhões de dólares para o ano fiscal, o menor montante financeiro constatado entre 2010 a 2020.

Vale ressaltar que essa diminuição financeira se normaliza em 2019, elevando o orçamento a quantia de 13,7 bilhões de dólares, maior valor registrado no período. Tal questão faz com que o retrato orçamentário reportado pelo DoD dos EUA seja questionado em relação à veracidade de seus dados, ponto que retornará nas seções de análise posteriores.

Apêndice B - Gráfico da parcela orçamentária reservada à temática de *cyber* segurança - em bilhões de dólares.



Fonte: Compilação do autor com base nos dados públicos do Departamento de Defesa dos EUA.

A partir desses dados, foi percebido um reconhecimento crescente dos governos estadunidenses para a segurança cibernética, garantindo construções domésticas de suas capacidades nos anos estudados. Ponto visto através do uso da verba temática, que ao se utilizar das *National Defense Authorization Act* anuais, permitiram definições e desenvolvimentos domésticos cibernéticos, salientados na criação e oficialização da USCYBERCOM entre 2009 e 2010, na concepção do *Cyber Threat Intelligence Integration Center* em 2015 e no estabelecimento da *Cybersecurity and Infrastructure Security Agency* em 2018. Também foram verificados destaques progressivos nos órgãos domésticos criados - principalmente no Comando Cibernético do EUA -, que garantiu modernizações e fortalecimentos nas práticas cibernéticas realizadas.

Quanto aos ciberataques realizados pelos Estados Unidos, a CRF (2024) conseguiu atestar e comprovar 16 casos de utilização das capacidades ofensivas estadunidenses, realizadas com o intuito de causar dano ou adentrar indevidamente nas redes de outros agentes do SI. Tais

ações se focaram em atos de espionagem cibernética e no roubo de dados, com a presença de seis ocorrências, que variavam em relação aos alvos atingidos, com um volume maior no furto de dados governamentais, seguido por informações militares sigilosas.

Também foram comprovados, com seis incidentes, ataques cibernéticos que objetivaram a sabotagem de servidores, dados ou equipamentos dos atores afetados, caracterizando-os às tipologias de dano especificadas no capítulo 1. Esses casos se voltaram principalmente ao dano - e o provável roubo de informações técnicas - de tecnologias governamentais com três casos. Já os três incidentes de sabotagem diversificaram os alvos, perpassando pelo setor privado, sociedade civil e pelo âmbito militar. Os quatro atos cibernéticos restantes tinham como objetivo especificamente ou a destruição de dados com duas ocorrências ou realizar DDoS massivos aos atores afetados.

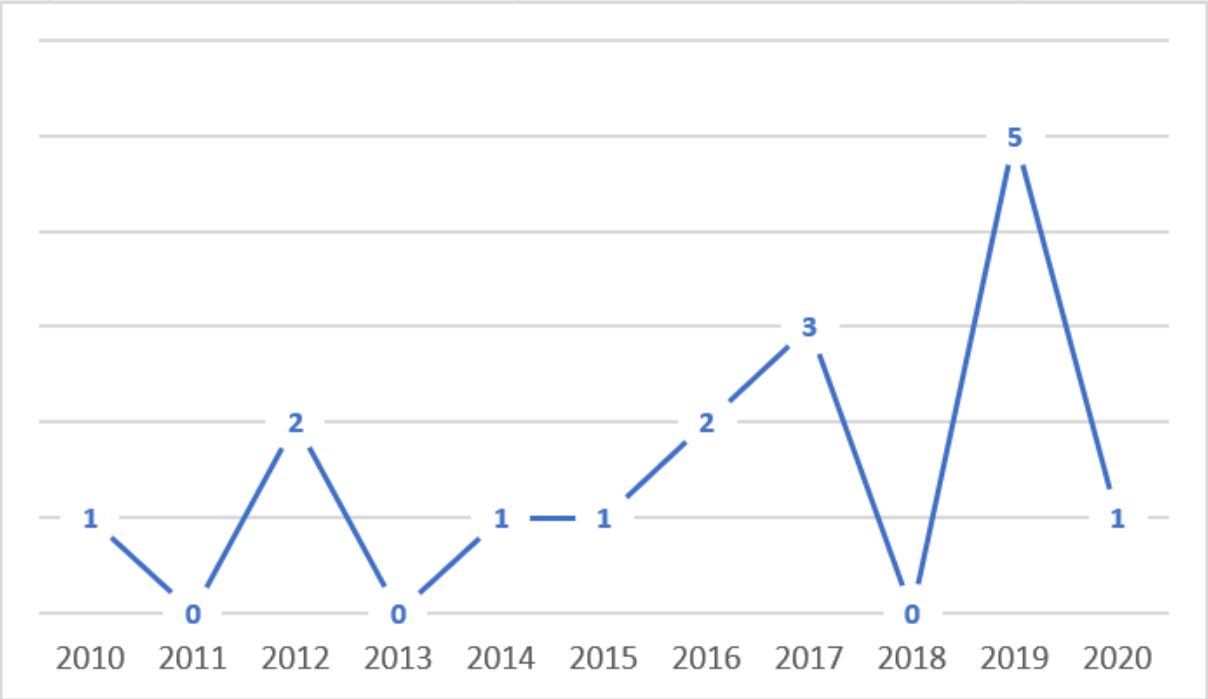
De acordo com a CFR (2024), nos 16 ataques reportados, as estruturas militares dos EUA miraram especificamente a Rússia e o Irã - com dez e nove casos, respectivamente - e a China e a Coreia do Norte foram atacadas três vezes. Vale ressaltar que os Estados Unidos e suas administrações também investiram ciberneticamente contra seus aliados, atacando a Índia quatro vezes, o Reino Unido três vezes e a Estônia e os Países Baixos uma vez. Destaca-se o caso *Longhorn* de 2017, visto que, dada as suas peculiaridades e o seu *status* global de ataque concedido pela CRF (2024), sua presença no escopo de ataque dos EUA foi garantida em um à soma e a caracterização realizada em todos os Estados atacados.

Nesses incidentes, até 2017 - com exceção ao ataque ao Estado Islâmico de 2016 -, os ataques tinham uma característica multilateral, ou seja, visavam atacar, direta ou indiretamente, vários alvos simultaneamente. No entanto, a partir da metade de 2017, as ocorrências cibernéticas se pautaram em causar dano direto contra apenas um ator, sendo esse um dos quatro Estados-oponentes aos EUA abordados na dissertação. Também é enfatizada nos dados a noção de que, em 16 casos, apenas dois tiveram denúncias internacionais acerca da existência e da requisição de investigações e punições adequadas. Ambas as reações - percebidas no caso *Stuxnet* de 2010 e no ataque à Agência de Inteligência iraniana em 2019 - foram realizadas pelo Irã e não tiveram uma continuidade efetiva em relação à veracidade dos agentes responsáveis.

Abaixo está disposto, no apêndice C, uma compilação anual dos *cyber* ataques realizados e comprovados pelos Estados Unidos de acordo com o CFR (2024). Frisa-se o fato de que, ao comparar com o apêndice B, as linhas de matriz dos dados começam a ser emparelhadas a partir do ano de 2014, crescendo uniformemente. O mesmo acontece com a queda brusca percebida em 2018, seguida pelo maior aumento no recorte percebido no ano

posterior. Ambos os apêndices foram realizados pela compilação de fontes primárias e secundárias distintas, entretanto esse respeito a uma lógica existente entre o orçamento temático e o número de ataques cibernéticos criou um padrão observável considerável que será utilizado na análise de poder especificada no subitem seguinte.

Apêndice C - Gráfico da quantidade de ataques cibernéticos de realização comprovada dos Estados Unidos entre 2010 a 2020.



Fonte: Compilação do autor baseado nos dados dispostos pelo CFR (2024).

A CFR (2024) também foi utilizada para indicar os casos de *cyber* ataques sofridos pelos Estados Unidos durante os anos. Essas informações, embora tenham sido repassadas de forma breve entre os períodos abordados, ajudam na dissertação através de um entendimento amplo de como a percepção ofensiva dos Estados oponentes foi transmitida aos EUA na forma de ataques cibernéticos, podendo ser notadas como possíveis respostas às ações estadunidenses. O mesmo pode ser realizado com os Estados Unidos, ao observar as reações realizadas por este Estado ante as investidas realizadas.

A partir dessa visão, foram compilados 132 ciberataques oficializados e direcionados aos Estados Unidos. Nesse agrupamento, somente os Estados-oponentes atacaram os EUA, e, conforme salientado na introdução, a China foi o Estado com a maior quantidade de movimentações ofensivas realizadas, com 59 casos, seguido do Irã com 31, a Rússia com 27 e,

por fim, a Coreia do Norte com 15. O CFR (2024) aponta a existência de apenas 16 respostas estadunidenses em consequência aos ataques empreendidos, realizados normalmente na forma de denúncias internacionais e do requerimento de atuações jurídicas para sancionar e deter os agentes maliciosos e seus mandantes, movimento visto 11 vezes no período. As últimas cinco reações conseguiram culpabilizar consistentemente os participantes, realizando condenações e prisões dos principais suspeitos.

Analisando os dados de ataques em uma segmentação anual e por Estados, ressaltado no apêndice D abaixo, verifica-se um crescimento seguido por uma leve estabilização nas ocorrências cibernéticas ofensivas. Esse fluxo perpassa principalmente ao observar Estados como a Rússia, o Irã, e a Coreia do Norte, havendo, irregularmente, certos aumentos no período proposto. Já a China realiza um movimento contrário, diminuindo a quantidade de ataques realizados durante os anos, mas ainda tendo um alto volume de ocorrências anuais.

Com exceção do Irã e da China, os Estados ampliam seu nível de atuação a partir da troca de governo dos Estados Unidos, trazendo a noção de reatividade advinda dos ataques cibernéticos realizados. Aqui também é retomada a questão e a possível relevância de 2018 à análise, visto, que tal ano foi observado a maior quantidade de investidas cibernéticas para com os Estados Unidos, com um total de 22 casos reconhecidos, estabelecendo o recorde anual de ofensivas no período da Rússia e da Coreia do Norte, e o terceiro maior valor ao considerar a China.

Apêndice D - Tabela representativa dos ataques cibernéticos realizados contra os Estados Unidos entre 2010 e 2020 pela CFR (2024).

ANOS	Ataque da Rússia aos EUA	Ataque do Irã aos EUA	Ataque da Coreia do Norte aos EUA	Ataque da China aos EUA	Total Anual
2010	0	0	0	2	2
2011	0	0	1	7	8
2012	0	3	0	3	6
2013	1	1	0	7	9
2014	3	4	1	10	18
2015	3	1	0	9	13
2016	4	2	1	2	9
2017	4	3	2	4	13
2018	7	3	4	8	22
2019	2	6	2	3	13
2020	3	8	4	4	19
TOTAL	**27**	**31**	**15**	**59**	**132**

Fonte: Compilação do autor baseado nos dados dispostos pelo CFR (2024).

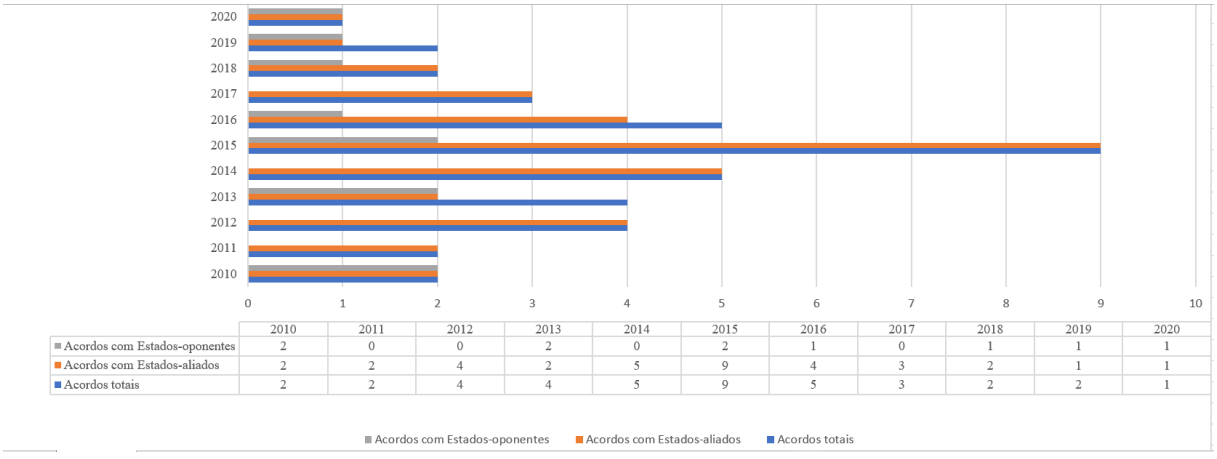
Em referência aos acordos internacionais de segurança e defesa cibernética, expostos no trabalho de Hitchens e Goren (2017) em conjunto com fontes primárias e secundárias, foi

fixada a anuência seguida de assinatura dos Estados Unidos em 53 acordos temáticos cibernéticos. Dentre eles, apenas 39 seguiram as métricas propostas por esta dissertação. Tais resoluções possuíam tanto natureza jurídica, com a criação de direitos e deveres entre as partes, quanto percepções não-juridicamente vinculativas, recaindo a uma condição recomendativa acerca das melhores práticas a serem realizadas pelos signatários.

Dito isso, no que tange os 39 acordos pontuados no capítulo 2, cerca de 35 foram realizados com um ou vários dos Estados-aliados aos Estados Unidos, conferindo ao Reino Unido um total de 26 assinaturas conjuntas, assim como evidenciado pelos Países Baixos. A Estônia realizou 24 tratados bilaterais ou multilaterais no período, já as lideranças da Índia subscreveram em 6 convenções.

Também foi reportada a existência de compromissos legais com os oponentes estadunidenses, principalmente a Rússia e a China. Tais atores assinaram dez convenções, tendo a assinatura da Rússia em oito delas. Tal circunstância se repete com a China, que conta com oito subscrições. Ressalta-se que em oito dos dez tratados assinados foram celebrados em condições multilaterais, sendo realizados exclusivamente em conjunto com a ONU, vide a GGE e o OEWG. Essas representações foram ilustradas no apêndice E abaixo.

Apêndice E - Gráfico que ilustra os acordos cibernéticos defensivos realizados pelos Estados Unidos entre os signatários aliados e oponentes de 2010 a 2020.



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Acordos com Estados-oponentes	2	0	0	2	0	2	1	0	1	1	1
Acordos com Estados-aliados	2	2	4	2	5	9	4	3	2	1	1
Acordos totais	2	2	4	4	5	9	5	3	2	2	1

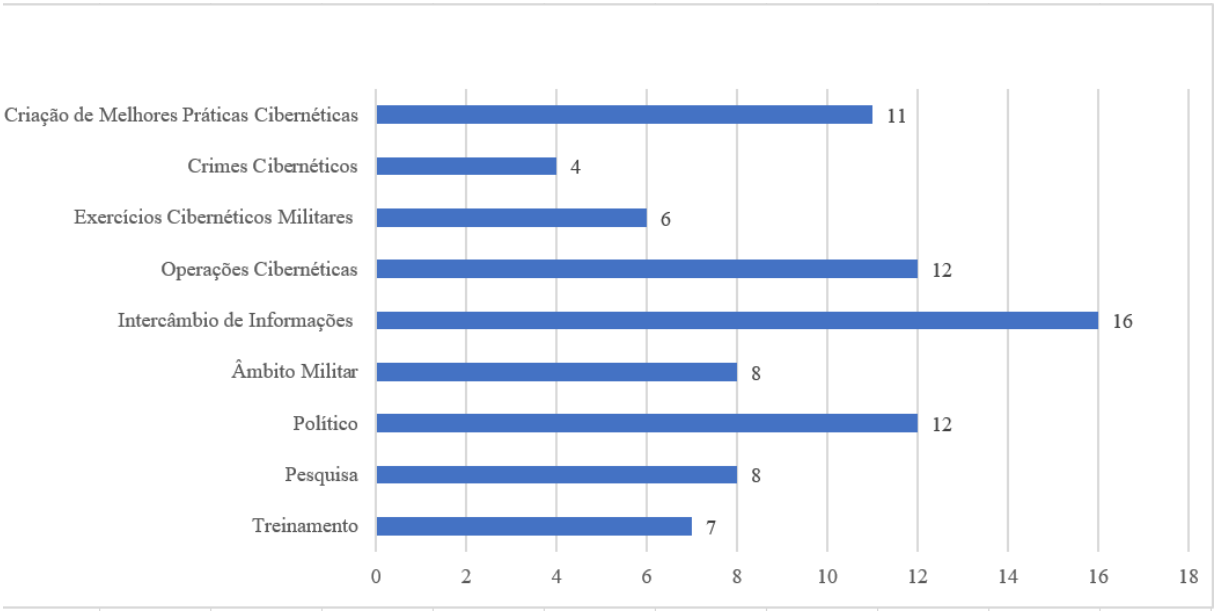
Fonte: Compilação do autor baseado nos dados dispostos em fontes primárias e no trabalho de Hitchens e Goren (2017).

Ao salientar os principais termos e temas existentes nas alíneas dos tratados elaborados, foi constatada a presença de nove termos temáticos distintos que foram aceitos 84 vezes. Tais elementos, difundidos de forma discrepante nos 39 tratados apresentados no capítulo 2, se

propuseram principalmente a abordar o intercâmbio de informações entre as partes, manifestando-se em 16 compromissos. Em segundo lugar, foram assinados os termos de criação ou da continuação de operações cibernéticas conjuntas em caráter não militar e o âmbito político, ambos com 12 acordos.

As tipologias subsequentes presentes nos compromissos perpassam pelo âmbito da produção das melhores práticas cibernéticas ou legislações para a área, com 11 manifestações, seguida das áreas de pesquisa e militar, com oito assinaturas cada. Os últimos três temas assinados desdobram-se ao treinamento - sete -, ao desenvolvimento de exercícios militares cibernéticos – seis – e à esfera de combate ao crime cibernético com quatro subscrições. Essas informações estão presentes no apêndice F a seguir.

Apêndice F - Gráfico representativo da quantidade de termos temáticos existentes nos acordos defensivos de 2010 a 2020.



Fonte: Compilação do autor dos dados dispostos em fontes primárias e no trabalho de Hitchens e Goren (2017).

As informações aqui coligidas oferecem uma base de entendimento intrínseco, utilizada nesta dissertação para investigar a projeção de poder efetuada pelos Estados Unidos. Com isso, os registros orçamentários, ofensivos e defensivos, ajudam a classificar padrões de movimentações estatais de domínio, influência e motivações, pontuados na subseção seguinte.

3.2 - Poder Cibernético: Investigação dos Motivos e da Imagem Estadunidense

Com o intuito de tornar a análise do poder cibernético factível, é necessário construir o cenário que possibilita a atuação estadunidense ante o escopo temático. Dito isso, o texto de Kremer e Müller (2013) ajuda na especificação e na investigação de um elemento possibilitador para as Ações cibernéticas indicadas no Sistema Internacional: os Motivos.

Definidas por Kremer e Müller (2013, p. 50 e 51) como um elemento "versátil e não mutuamente exclusivo", os Motivos impulsionadores de uma Ação podem ser variados e abstratos a depender do contexto e das agendas realizadas pelas Partes Interessadas em um período. Posto isto, Kremer e Müller (2013, p. 51) exemplificam esta afirmação ao manifestar os principais Motivos possíveis, definidos em escopos econômicos, psicológicos, ideológicos, políticos e relacionados ao poder (*power-related* em inglês).

Os Motivos, ao considerar sua natureza abstrata, permitem a criação de parâmetros cíclicos de Ações, que são incorporados nas estratégias das Partes Interessadas de forma a se salvaguardar, ou seja, os Motivos que regem um ato cibernético tem como objetivo principal a defesa e manutenção do Motivo em si. Isso faz com que tal ato se torne algo intermitente, caso não haja mudanças nas definições motivacionais da Parte Interessada. Nesse ponto, caso a Parte Interessada seja um Estado nacional, a mudança na liderança e nas políticas militares e de defesa, podem permitir mudanças na elaboração e na efetivação dos Motivos. Salienta-se a noção de Kremer e Müller (2013, p. 50) que estabelece a facilidade dos Estados em se utilizarem dos Motivos relacionados ao poder no espaço cibernético.

Com base nos dados e nas atribuições dos elementos *S.A.M.* de Kremer e Müller (2013) nos capítulos anteriores, os Estados Unidos e os governos estudados realizaram ações ofensivas contra atores do Sistema Internacional Cibernético. Tais atos tiveram Efeitos Significativos distintos, causando danos diretos ou indiretos às vítimas atacadas. Adicionalmente, foi inferido que o Motivo central das Ações realizadas foi a defesa das infraestruturas críticas e dos interesses nacionais estadunidenses.

Essa determinação advém das repetições destacadas nos dados do capítulo 2, principalmente nos documentos públicos e nos tratados internacionais realizados. Isso trouxe a necessidade de construção de medidas de defesa e proteção desses elementos - sua infraestrutura crítica e seus interesses. Com isso, os atos de preservação desse Motivo poderiam pender para a criação de estratégias tanto ofensivas - a base das Ações cibernéticas - quanto defensivas - a legislação, normalmente não observada no conceitual de Kremer e Müller (2013).

Ao se basear nessa motivação, os Estados Unidos, durante o recorte pesquisado, criaram estratégias de ação temáticas que oportunizaram atos concretos no Sistema Internacional

Cibernético. É enfatizada nesse ponto, a ausência na definição exata do que seriam os interesses nacionais salvaguardados pelas estratégias efetuadas, deixando-os em um contexto amplo e abrangente nos documentos oficiais. Isso faz com que haja uma variedade nas ações e ponderações possíveis, trazendo um complicador à categorização motivacional exata.

A fim de solucionar esse dificultador, será utilizado o trabalho de Jervis (1970) acerca das imagens, que consegue analisar como uma estratégia de ação pode ser construída por um Estado e concretizada no SI, determinando assim as prováveis representações criadas, passadas e interpretadas por outros atores. Ao realizar tal investigação, os interesses estadunidenses podem ser enfim inferidos, permitindo a categorização dos Motivos que regeram os EUA no período, viabilizando uma análise acerca do poder cibernético.

Primeiramente, Jervis (1970, p. 06; 18; 28 e 32) salienta que um Estado tende a compor uma imagem de si próprio e apresentá-la a outros atores no Sistema Internacional. Essa imagem determina as formas nas quais o Estado pode ou quer ser visto, designando-o como um elemento crucial para a consecução de seus objetivos. Entender uma imagem estatal permite categorizar as atitudes, comportamentos e intenções inerentes a um ato realizado no SI, criando manobras distintas de poder. Dessa forma, Jervis (1970) elabora duas bases que ajudam o Estado a conceber sua imagem no Sistema. São elas: os Sinais e os Índices.

Os Sinais, para Jervis (1970, p. 18), são declarações ou ações públicas que expressam significados e entendimentos explícitos para os receptores. Os Sinais servem principalmente para influenciar e consolidar uma imagem predeterminada, aumentando a probabilidade do ator ser visto de uma determinada maneira, em um contexto preterido.

Para Jervis (1970, p. 18), os Sinais são entendidos na forma de notas diplomáticas, operações militares, ampliação ou rompimento de relações diplomáticas, discursos ou entrevistas públicas ou escolhas realizadas em mesas de negociação. Salienta-se a incerteza derivada do uso de Sinais, pois, a imagem que se deseja passar pode não ser notada da forma esperada. É assim devido ao peso que as noções pré-concebidas dos atores têm sobre o sobre o utilizador de Sinais, ponto que leva à desvalorização das evidências e das falas apresentadas e à diminuição da credibilidade do locutor e da incerteza acerca das ações futuras, visto que não há garantias de que o ator atenderá às expectativas definidas por si próprio.

Já os Índices, ao contrário dos Sinais, são afirmações ou atos que inerentemente carregam evidências, promulgando certeza da imagem, visto que a postura indicada normalmente se complementa às capacidades e as intenções do ator (Jervis, 1970, p. 18). O uso de Índices promove com maior facilidade a construção de uma personificação desejada, já que

estará pautada em dados visíveis e públicos, facultando o entendimento e a pressuposição de um comportamento específico no Sistema Internacional.

Contudo, observa-se a possibilidade de fraudar ou confundir os atores com os Índices adulterados, originando circunstâncias convenientes ao emissor, pois podem gerar liberdades de ações diante outros atores do SI. Isso gera um entendimento da construção e do uso de Índices traduzidos em uma Ação no tempo, ponto que será usado em uma perspectiva cibernética adiante neste capítulo.

Ao se basear nos conceitos de Jervis (1970) sobre Sinais e Índices, este trabalho consegue traduzir e perceber tais elementos nas estratégias cibernéticas estadunidenses, elemento trabalhado principalmente por Maier (2019). Tais processos indicam, de formas distintas, como cada governo estudado se preparou e organizou seus recursos em prol de alcançar um objetivo no espaço cibernético, materializando, assim, em um ato cibernético ofensivo e defensivo.

Posto isso, conforme apresentado brevemente no capítulo anterior, Maier (2019) sustenta uma percepção de que as movimentações políticas e as definições das estratégias cibernéticas praticadas nos governos Obama e Trump seguiram vertentes distintas, mas se pautaram no mesmo direcionamento. Para ele, esses empreendimentos estabelecidos entre as administrações oscilavam entre uma postura multilateral mais pacífica e uma prática unilateral mais agressiva aos agentes do SI.

No que tange ao governo Obama, Maier (2019, p. 114) nomeia a conduta estadunidense como uma "retórica multilateral", pois, a depender do momento no tempo, a imagem governamental alternaria fortemente entre padrões uni e multilaterais. Informação esta que traz a percepção de Jervis (1970) a análise, visto que muitos dados utilizados no capítulo anterior derivados da documentação utilizada na administração Obama podem ser deduzidos como modelos de Índices para a transmissão de uma alegoria estadunidense pré-determinada.

Ao categorizar os documentos de consolidação e fomento das agências cibernéticas dos Estados Unidos - com um foco nas manifestações da USCYBERCOM em 2010, do CTIIC em 2015 e nos fortalecimentos conjuntos por parte das CERTs governamentais em movimentos cooperativos - como Índices e reuni-los com os esforços multilaterais de realização de acordos internacionais em múltiplos termos temáticos, conforme salientado nos apêndices E e F, é indicado, em um primeiro momento, a construção de uma imagem estatal branda, moderada, resistente e confiável, apresentada doméstica e internacionalmente. Figura essa que salienta um

posicionamento novo por parte dos Estados Unidos durante a presidência Obama, sendo distinto dos governos anteriores.

Isso garantiria credibilidade e percepção renovada ao Estado por parte de outros agentes, se focando tanto nos aliados quanto nos oponentes através dessa estratégia (Maier, 2015, p. 113-114). Entretanto, também havia nesses documentos Índices que permitiam uma imagem inclinada a definição e consolidação de empreendimentos unilaterais mais incisivos, oscilando a visão supracitada. Elemento exemplificado nas prerrogativas dos documentos de estabelecimento do Comando Cibernético Estadunidense, que propuseram atos de potencialização de seus aparatos cibernéticos militares a serem utilizados no Sistema Internacional Cibernético, tendo a salvaguarda de sua defesa como objetivo central.

Esse pensamento, ampliado em 2011 com o *International Strategy for Cyberspace*, viabilizou atos ativos e reativos, legitimando o uso de qualquer meio necessário contra agentes maliciosos presentes no Sistema, que, através de suas práticas, ameaçavam a segurança e os interesses dos Estados Unidos e de seus aliados no espaço cibernético (Estados Unidos da América, 2011, p. 14). Não obstante, tal documento apresentou uma caracterização abrangente de quem seriam esses agentes, possibilitando ataques retaliatórios ou até mesmo preemptivos contra alvos distintos. Com isso, foi ampliado a escala de ação possível por parte dos Estados Unidos com Obama.

Dessa forma, ao considerar os processos realizados no governo Obama pela interpretação de Maier (2019) reunida com o trabalho de Jervis (1970), a imagem trazida pelos Índices trazem a noção que de os Estados Unidos de Obama se apresentaram, inicialmente, como um ator confiável para o Sistema Internacional Cibernético. Tal representação realça a ideia de que, baseado nas preferências dos EUA na época, o Estado estaria interessado em se utilizar de suas capacidades cibernéticas - com um foco defensivo maior - para construir um *cyber* espaço mais cooperativo e regular aos seus atores, garantindo possibilidades de apoio e amparo legislativo e multilateral fundamentado nas Instituições Internacionais.

Essa movimentação poderia garantir vantagens aos Estados Unidos durante o governo Obama, que, nesse contexto, estariam fomentando a ideia de serem considerados como exemplos a serem seguidos em questões de segurança cibernética, mas especificamente em pautas legislativas e de defesa. Vale ressaltar que esse pensamento seguiria principalmente uma noção realista, caso a imagem proposta fosse assimilada e os exemplos indicados fossem seguidos pelos atores do Sistema.

Todavia, assim como indicado por Maier (2019), a representação estadunidense também se apresentou como oscilante. Isso é posto através dos Índices subentendidos nos documentos, revelando a ideia de que, embora os Estados Unidos de Obama possam ser vistos como um exemplo a ser seguido em um contexto defensivo, ele também desejava ser considerado como um ator preparado ofensivamente para o enfrentamento no espaço cibernético. Foram determinadas através das diretrizes documentais supra referidas, as principais formas que as estruturas dos EUA poderiam agir em um contexto mais inamistoso, sustentando suas motivações de proteção aos seus interesses, infraestruturas e colaboradores.

A partir das concepções autorais, deduz-se que os interesses abarcados nos Motivos estadunidenses durante o governo Obama tinham como foco a construção e manifestação de poder para o âmbito cibernético. Esses atos visavam, através de um desenho estratégico, conseguir uma imagem dupla no Sistema Internacional Cibernético, obtendo poder através de uma imagética de liderança defensiva, estabelecida em conjunto com a visão e com o uso sistemático e estratégico de poder no espaço cibernético, realizado nas permissões e nos atos que fizeram com que as estruturas cibernéticas ofensivas fossem percebidas como um agente prevenido contra as possíveis problemáticas cibernéticas.

Através desses indícios, pode-se caracterizar, em um ponto de vista estratégico, a definição de Motivos relacionados a poder de Kremer e Müller (2013) na imagem representada pelos Estados Unidos entre 2010 a 2016. Destaca-se nessa representação a inexistência de Sinais nos dados utilizados para representar o governo Obama. A transposição dos intuitos em Atos será verificada à frente no capítulo, ao analisar se a estratégia realizada conseguiu se manter à frente da sua efetivação.

Ao progredir com o recorte temporal, entre 2017 a 2020, durante um novo modelo de administração regido por Donald Trump, os interesses e as imagens definidas por Jervis (1970) receberam alterações visíveis. Salientado principalmente por Amoretti e Fracchiolla (2018) e Devanny (2021), a nova alegoria estadunidense se distanciava da cognição multilateral pretendida por Obama, diminuindo, com isso, a quantidade de acordos e movimentações legislativas realizadas no período, indicado pelo apêndice E.

Essa atenuação, no entanto, não foi percebida nos Índices domésticos, que sofreram aumentos regulares e constantes tanto em uma interpretação orçamentária geral e cibernética - com exceção de 2018 e 2020 - quanto no desenvolvimento de agências governamentais voltadas à área - como a criação da CISA em 2018. O uso dos documentos orçamentários como Índices

em ambos os governos serão retomados adiante, a fim de elaborar uma compreensão total das capacidades, estratégias e atos cibernéticos realizados pelos Estados Unidos.

Porém, enquanto as práticas multilaterais se tornavam escassas na presidência de Donald Trump, os atos unilaterais seguiram um direcionamento mais intenso. Com uma postura mais agressiva, os Estados Unidos de Trump orientaram seus esforços em produzir uma imagem mais beligerante a ser apresentada no SI. Essa conduta se baseava principalmente nas diretrizes de "preservar a paz pela força" e "avançar a influência estadunidense no mundo para quem apoia seus interesses" (Amoretti e Fracchiolla, 2018, p. 26 e Estados Unidos da América, 2017a, p. 04 - tradução nossa).

Para alcançar essas finalidades, recursos foram atribuídos, agências cibernéticas foram modernizadas, unificadas e consideradas autossuficientes - foco principal na USCYBERCOM -, as operações cibernéticas ofensivas realizadas pelos Estados Unidos foram oportunizadas e os principais oponentes estadunidenses foram nomeados, indicando as melhores formas para enfrentá-los (Rogers, 2017). Evidencia-se que esses processos foram potencializados através do uso de Sinais por parte dos Estados Unidos durante o mandato de Donald Trump.

Tais Sinais derivam principalmente de manifestações públicas, discursos e entrevistas realizadas não só pelo presidente, mas também pelos cargos de liderança militar e de defesa dos EUA. Ao realizar tais posturas - não percebidas na administração anterior - complementadas pelos elementos de Índices e Sinais, foi facilitada a noção de que a alegoria estadunidense anteposta conseguisse se materializar no SI e aos seus atores de forma a perpassar uma ideia mais simplista de ação ante ao espaço cibernético.

O retrato intencionado apresentou a noção de que, a pretexto da conjuntura do ciberespaço, ações cibernéticas mais acentuadas são cada vez mais necessárias para salvaguardar as infraestruturas críticas e os interesses dos atores no Sistema. Os governos e órgãos dos EUA se utilizaram dessa lógica para que os atos dos agentes maliciosos dispostos no espaço não se tornem progressivamente mais comuns, garantindo sua proteção.

É fundamental que as preferências dos Estados Unidos na administração Trump assumam uma postura imperativa cibernética para lidar com essas problemáticas, aumentando, com isso, seu nível de poder doméstico para assim projetá-lo no Sistema Internacional Cibernético. Ao realizar essa ação, as estruturas dos EUA ampliaram seus níveis de capacidade, e se tornaram a melhor força militar em todos os âmbitos de combate (Maier, 2019, p. 122 e Estados Unidos da América, 2017b, p. 16 - tradução nossa).

Para alcançar essa finalidade, a diminuição ou até mesmo a abstenção de práticas multilaterais poderiam ser realizadas, manifestadas por meio da redução desses parâmetros durante o governo Trump. Contudo, não houve uma interrupção total dessas ações, salientadas em dez acordos anuídos, manifestando até mesmo atos antagônicos nos contextos multilaterais legislativos. Um exemplo disso está na renovação da sexta sessão do GGE, realizado principalmente como uma resposta à criação da OEWG em 2018 pelos esforços russos.

Dito isso, a imagem e os interesses estadunidenses engendrados por Trump não tentaram disfarçar sua busca por poder para com o espaço cibernético. Ao contrário do que foi percebido no governo Obama, os Estados Unidos entre 2017 e 2020 deixaram claro que seus interesses e Motivos de defesa e proteção de suas infraestruturas críticas abarcavam objetivamente a tipologia relacionada ao poder de Kremer e Müller (2013), se utilizando de Sinais e Índices para criar movimentações favoráveis de cognição por parte dos agentes do Sistema.

Mesmo ao identificar imagéticas distintas entre os governos pesquisados, existe, em um padrão amplo, uma movimentação constante dos Estados Unidos e de seus comandos em reforçar anualmente uma imagem pré-determinada, sendo realizada através do Índice Orçamentário. Através dessa estratégia, conforme salientado por Jervis (1970. p. 28 e 38), representações são facilitadas, pois, há um senso de predicabilidade nos atos futuros de um agente. Dessa forma, ao seguir o pensamento de Jervis (1970), o orçamento publicamente divulgado de um Estado pode ser percebido como um conjunto de dados traduzidos como Índices que revelam e fortalecem uma representação pretendida.

O fundamento de Jervis (1970) é reforçado pelos escritos de Raiffa (1994) acerca da divulgação de informações. Raiffa (1994, p. 07) tem como foco principal o ambiente da negociação, indicando as melhores formas nas quais um ator consegue obter vantagens em uma disputa. Para ele, um negócio é favorável quando uma das partes capta recursos maiores em detrimento do outro, alcançando a capacidade de ajustar a quantidade e a qualidade dos ganhos recebidos.

Aqui, a presença de um Estado em uma negociação atende às mesmas métricas de ação, aumentando apenas a escala dos atores participantes da mesa. Isso acontece pois, para Raiffa (1994), uma interação voltada à disputa de interesses, movimentações estratégicas e ganhos, podem ser consideradas como formas de negociação, mesmo sendo realizadas em um nível formal ou até mesmo informal.

Dessa maneira, segundo Raiffa (1994), informações dispostas do agente negociador são consideradas recursos importantes em um entendimento formal. Adicionalmente, a

disponibilização desses dados deve ser cuidadosamente revelada, pois podem encerrar possibilidades de ganhos. Isso traz a noção de que - ao seguir a lógica de Raiffa (1994) - todo e qualquer dado revelado em uma negociação teve uma intenção prévia de ação para lograr um resultado favorável e específico.

Logo, ao seguir tais premissas, os dados derivados de documentos públicos, os interesses e os contextos orçamentários anuais podem apresentar duas possibilidades ante a sua existência. A primeira assume total veracidade nas informações instituídas nos documentos, afirmando altos graus de transparência realizados pelos Estados Unidos e seus governos. Isso implica uma estratégia consistente em ser visto como um ator completamente confiável no SI.

Já a segunda opção assume que boa parte das informações divulgadas publicamente pelos Estados Unidos têm um viés de desconfiança, pois os dados salientados não assumem completamente com os verdadeiros níveis de capacidade dos EUA. Ao seguir esse pensamento, é destacada a vontade estatal em garantir movimentações específicas para com o espaço cibernético, fazendo com que sejam divulgados somente elementos intencionados e úteis para a estratégia estadunidense, reforçando uma imagem geral apresentada aos atores do Sistema Internacional ou até mesmo garantindo formas de ação extraordinárias derivadas de justificativas abrangentes e imprecisas.

Essa alternativa explica a variação aguda no orçamento para a cibersegurança em 2018 seguido por um aumento em 2019, como ressaltado no apêndice B, além da complexidade inerente aos interesses repetidos nos documentos oficiais. Isso traz a noção de que as promoções, os embaraços e dinâmicas presentes nos dados públicos foram divulgadas seguindo uma conformidade estatal predeterminada. Com isso, fica implícito que as capacidades estadunidenses reais poderiam ser superiores - ou até mesmo inferiores - às indicadas, acentuando artificialidade nos elementos estatais com o intuito de alcançar objetivos prolongados no tempo.

Posto isso, esta dissertação opta por seguir a segunda possibilidade disposta, visto que ela consegue explicar boa parte dos dados dispostos e coaduna com os pensamentos autorais utilizados. Ademais, ao avaliar as informações indicadas no capítulo 2 e compendiada nos apêndices A e B, pode-se deduzir que a imagem e os Motivos relacionados a poder, criados por ambos os governos estudados seguem uma mesma intenção de materializar percepções e oportunidades favoráveis aos Estados Unidos e suas administrações.

Nesse ponto, a diferença está principalmente na forma que os administradores compreenderam e consubstanciaram a estratégia e as representações pretendidas, pendendo ou

para uma dinâmica díade de comportamento - governo Obama - ou para um formato completamente direto e unilateral - gestão Trump. Isso faz com que os Motivos estadunidenses superem as expectativas esboçadas, pois, ao seguir tal ponto de vista, os elementos alegórico e Motivacional dos Estados Unidos são concebidos como algo integral e intrínseco ao seu pensamento estratégico, sendo caracterizados como uma política de estado e não de governo.

Isso posto, destaca-se que, embora haja um esforço contínuo dos Estados Unidos e seus governos em construir e transmitir sua imagem desejada - sendo essa baseada em seus Motivos relacionados ao poder -, esse Estado não tem controle na forma como essas representações são constatadas ou avaliadas pelos agentes do Sistema Internacional Cibernético (Jervis, 1970, p. 13). Tal pensamento se consolida nas ações cibernéticas realizadas pelos EUA, que não deveriam ser consideradas como Sinais ou Índices. Isso acontece, pois tais atos se utilizam normalmente do anonimato inerente da prática para permitir novas oportunidades, execuções ou o alcance de certos objetivos.

Dessa forma, as Ações de Kremer e Müller (2013) podem ser vistas, em um primeiro momento, como a implementação da imagem estadunidense. Ao analisar e avaliar as Ações, não só quantitativamente, mas qualitativamente, se entende um grau de aceitação aos Motivos relativos a poder nos atos, mas também o nível potencial dos atos em relação a sua capacidade de promover dano aos atores do Sistema. Perceber as Ações de uma maneira mais focalizada propicia a manifestação nas interpretações das alegorias estadunidenses, realizadas até mesmo de formas não intencionadas, suscitando em consequências e repercussões contínuas no Sistema.

À vista disso, os 16 casos cibernéticos ofensivos realizados e atribuídos aos Estados Unidos pelo CFR (2024), serão analisados qualitativamente ao usar como base as métricas de Clarke e Knake (2012, p. 147 e 148), de forma a determinar o nível de risco e as possibilidades de dano percebidas nos ataques estadunidenses. As estimativas realizadas levarão em consideração, em conjunto com os anos da manifestação das ocorrências, três fatores de observação: (1) a quantidade de atores afetados; (2) a condição presumida da sofisticação e danificação no ataque e (3) o nível de reconhecimento doméstico e de resposta internacional aos casos.

Esses fatores serão valorados entre 1 e 10 a partir das informações do CRF (2024). Serão percebidos e utilizados padrões de intensidade, repetição e avaliação presentes nos dados, para assim serem estipulados os principais moldes de avaliação. Ressalta-se que nos materiais do fator (1), a investigação estabelecerá de forma literal o número de agentes com a pontuação,

caso a quantia se estabeleça entre 1 e 7, já os valores 8 e 9 representarão designações para além de 10 e 15 vítimas, respectivamente. Uma vez classificados todos os recursos, será realizada uma média simples entre os elementos, atribuindo um valor de análise para os casos.

Salienta-se que a natureza simples desse quadro de análise é intencional, visto que o objetivo do panorama é apenas estimar valores de competência e evolução dos casos cibernéticos, para assim relacioná-los com as premissas teóricas utilizadas nesta dissertação. Caso seja necessário, tal representação poderá ser refinada e utilizada em trabalhos futuros, ampliando seu acesso e sua capacidade de inspeção. Ao realizar as etapas informadas, foi produzido o apêndice G a seguir.

Apêndice G - Tabela de ponderação dos atos cibernéticos ofensivos realizados pelos Estados Unidos entre 2010 e 2020.

Caso Cibenético	Ano da Ocorrência	Atores Afetados	Grau de Dano	Nivel de Reconhecimento	Nota do Ato Cibernético
Stuxnet	2010	8	10	10	9,3
Flame	2012	8	9	2	6,3
Gauss	2012	8	7	2	5,7
Regin	2014	8	7,5	1	5,5
Equation Group	2015	9	9,5	3	7,2
Project Sauron	2016	6	7,5	2	5,2
Ataque ao ISIS	2016	1	4	6	3,7
Longhorn	2017	10	10	5	8,3
Sabotagem ao Programa de Mísseis da Coreia do Norte	2017	1	5,5	7,5	4,7
Ataque à Agência de Inteligência Norte-Coreana	2017	1	4	9	4,7
Operação Contra a Desinformação Russa	2019	1	6	9	5,3
Sabotagem à IRA	2019	1	6	9,5	5,5
Ataque contra a Agência de Inteligência do Irã	2019	1	8,5	8,5	6
Ataque aos Servidores Iranianos	2019	1	8	7	5,3
Comprometimento ao *Yandex*	2019	4	7	6	5,7
Operação contra o *Malware Trickbot*	2020	1	4	5,5	3,5

Fonte: Compilação do autor baseado nos dados e nos relatórios dispostos pelo CFR (2024), seguindo em conjunto com o modelo determinado por Clarke e Knake (2012, p. 147 e 148).

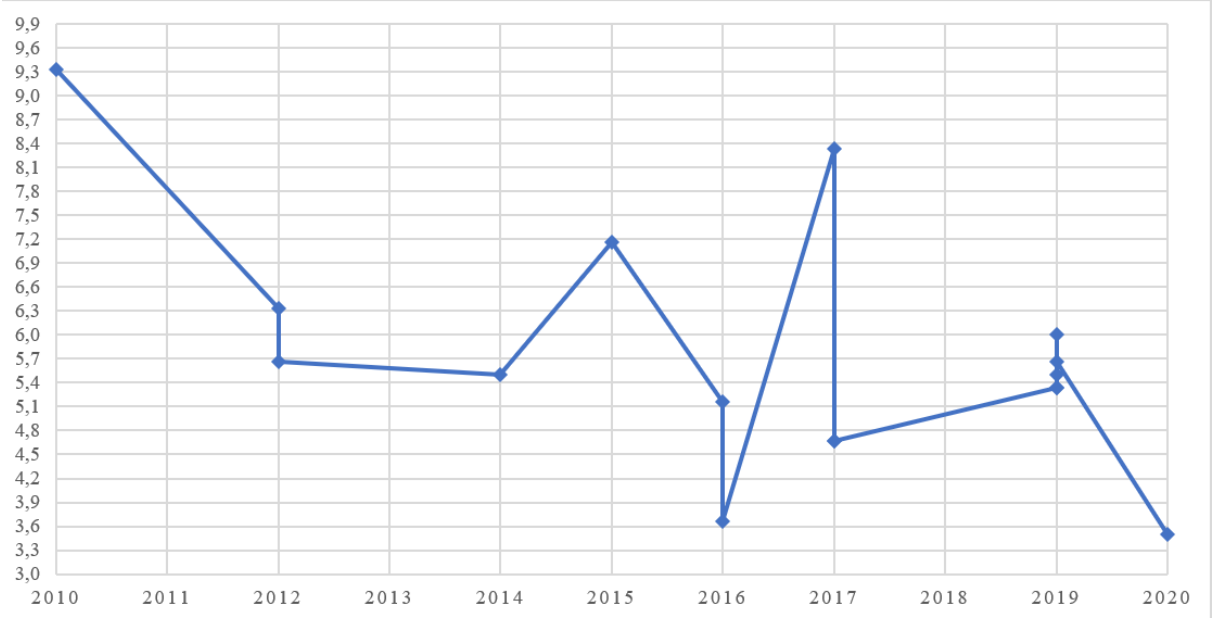
Ao considerar e valorar os Atos cibernéticos estadunidenses, percebe-se uma evolução notável nas métricas e nas pontuações totais estabelecidas através de uma investigação minuciosa. Isso acontece principalmente devido ao seu início, com o caso *Stuxnet*, que, dado ao sua forma de ação, sofisticação, destruição e reconhecimento, obteve a avaliação mais alta do recorte escolhido, pensamento adequado ao considerar que tal ocorrência fez parte dos três grandes casos de *cyber* segurança (Gratão, 2022, p. 03).

Entretanto, nos anos e eventos posteriores, a nota estadunidense oscilou bastante até o ano de 2016, ainda atingindo valores substanciais por conta da quantidade de atores afetados e sofisticação dos códigos presentes nos *malwares*, criando possibilidades de dano e Efeito Significativo de forma direta ou potencial, mas não tendo altos índices de reconhecimento doméstico ou internacional ante os ataques. Tal situação muda a partir de 2017, com o episódio *Longhorn*, recebendo notas máximas nos elementos de atores afetados - graças a sua escala global - e no grau de dano advindo de sua alta sofisticação e longa existência como APT. Isso fez com que esse caso tivesse a segunda maior nota na tabela realizada.

Posterior a esse evento, os casos cibernéticos ofensivos tiveram avaliações constantes em um nível abaixo ao relacioná-lo com os atos anteriores. Essa constatação advém da escolha em realizar somente atos contra atores unitários do SI, garantindo resultados mínimos nessa categoria. Entretanto, durante esse período, as ocorrências ofensivas tiveram as maiores notas recorrentes no elemento de reconhecimento acerca dos episódios, movimentação peculiar ao considerar os atos passados.

Em um contexto geral, a verificação ofensiva cibernética dos Estados Unidos teve um enfraquecimento a considerar seu ponto inicial - o caso *Stuxnet* de 2010 -, se aproximando desse patamar apenas em 2017, com o *malware Longhorn*, embora em uma perspectiva menor. Apesar disso, ao se tratar somente do nível potencial de Acton (2020) de se causar dano através dos casos, as capacidades cibernéticas ofensivas dos EUA mantiveram um padrão levemente alto, indicando, com isso, um grau desenvolvido de preparo e operacionalização cibernética ofensiva. Esse deslocamento avaliativo entre os anos foi indicado no apêndice H a seguir.

Apêndice H - Gráfico demonstrativo da evolução das notas efetuadas aos casos cibernéticos ofensivos realizados pelos Estados Unidos entre 2010 e 2020.



Fonte: Compilação do autor.

Uma vez indicada a movimentação geral das notas estadunidenses, constata-se novamente a concatenação dos materiais empíricos com a teoria de Jervis (1970) sobre as imagens e os pensamentos de Kremer e Müller (2013), Maier (2019), Amoretti e Fracchiolla (2018) e Devanny (2021). Essa relação advém da noção de que as alegorias estadunidenses implementadas continuaram seguindo os moldes em suas Ações, de formas levemente distintas, a depender da administração evidenciada, mas ainda com o foco de defender suas infraestruturas críticas e seus interesses através de uma projeção de poder, concretizando suas Ações como parte do Motivo relacionado ao poder (Kremer e Müller, 2013).

A diferenciação é apontada através do estudo das imagens representadas pelos governos Obama e Trump. Ao trazer os dados empíricos das Ações ao argumento, as notas realizadas no apêndice G são explicadas de forma evidente. Um exemplo dessa afirmação está nos níveis baixos de reconhecimento realizados entre 2012 a 2016, que ainda se utilizava dos benefícios inerentes do anonimato na perpetuação de um ataque cibernético (Lima, 2019, p. 39).

Pontua-se esse elemento como parte da estratégia de imagem dupla presente na gestão Obama (Maier, 2019), pois os atos cibernéticos de ataque não correspondiam[36] com o nível de movimentação cibernética multilateral apresentada e incentivada por Obama, remetendo-o a

[36] Ao seguir essa conjectura, o caso *Stuxnet* de 2010 seria apenas uma exceção, um produto da operação "*Olympic Games"* de 2006, efetuado apenas com o consentimento de Obama e não com sua participação na elaboração do ataque (Zetter, 2014, Sanger, 2012 e CFR, 2024). Contudo, segundo Zetter (2014) e Sanger (2012), a participação de Obama no caso *Stuxnet* também pode ser vista como uma continuação e uma apoderação da estratégia ofensiva construída em 2006, operacionalizando sistematicamente seus atos em um padrão tanto visível quanto anônimo, trazendo consequências a própria imagem multilateral construída na administração Obama, que foi vista como dúbia e até mesmo como hipócrita (Sanger, 2012).

sua postura unilateral. Tal atitude é salientada nos sete casos cibernéticos ofensivos durante o governo Obama. Atos esses que apresentam uma movimentação semelhante entre si, pois atacavam uma tipologia de vítimas englobavam[37] aliados e oponentes, seguido de um alto nível de sofisticação em seus códigos, resultando em possibilidades maiores de dano e a manutenção de um menor reconhecimento no Sistema, oportunizando atos de ataque, espionagem e roubo de dados contínuos.

A verificação dos agentes maliciosos das Ações só foi constatada devido à complexidade metodológica presente nos relatórios das empresas de cibersegurança vinculadas ao CFR (2024), principalmente aos elaborados pelo grupo Kaspersky. Essas empresas realizam uma verificação minuciosa na fonte dos códigos, nos servidores atacados e nas informações faltantes, para assim determinarem as nuances e as possibilidades existentes nas linhas de codificação, que normalmente levam a outros casos, atores ou IPs[38].

Logo, ao realizar essa atividade, as incógnitas e atribuições confusas existentes em um caso ofensivo são pontuadas e testadas, produzindo a dedução lógica mais provável acerca da origem do incidente e dos atores mais capazes de realizar tal ato. Determinando tais premissas, se entende a vontade do agente malicioso em não ser descoberto, garantindo padrões formais ofensivos de atuação e a manutenção de seus objetivos para com o espaço cibernético.

Ao se utilizar dessa lógica, se percebe que as intenções e as possibilidades unilaterais salientadas nos Índices do governo Obama, estavam sendo operacionalizadas da forma desejada. Isso acontece pois, enquanto os Estados Unidos de Obama se manifestavam como um ator multilateral responsável e confiável, atraindo tratados e movimentações legislativas positivas ao Sistema - vide apêndices E e F -, as organizações dos EUA monitoravam, roubavam e destruíam dados de diversos agentes de maneira anônima. O uso dos Índices ajudou a prever a sequência de acontecimentos viáveis, garantindo a exposição da imagem de retórica multilateral desejada, assim como orientado por Jervis (1970, p. 18).

A partir de 2017, com a mudança para o governo Trump, as Ações estadunidenses naturalmente se tornaram análogas à imagem pretendida. Representação essa focada em apresentar uma postura ativamente unilateral, indicando um uso para as ampliações de suas

[37] Ao anexar os dados do CFR (2024) à pesquisa, nos 16 casos de *cyber* ataques efetuados pelos EUA no recorte temporal proposto. Dentre os oponentes, a Rússia foi atacada dez vezes, o Irã nove a China três e a Coreia do Norte em três momentos. Já entre os aliados, houve quatro investidas cibernéticas contra a Índia, três contra o Reino Unido, e apenas um caso notado contra a Estônia e os Países Baixos. É necessário enfatizar a presença do caso *Longhorn* à soma, pois, devido ao seu alcance global sem comprovação, os números de ocorrências apresentadas foram ampliadas em um.

[38] Um IP (*Internet Protocol* - Protocolo de *Internet* em inglês) é segundo Diaz et al. (2022, p. 03) se trata de um identificador único que todo dispositivo de rede possui para indicar padrões de localização geográfica.

capacidades cibernéticas ofensivas e nomeando os principais alvos para essa atividade (Rogers, 2017, p. 05 e 06 e Amoretti e Fracchiolla, 2018, p. 27).

Com exceção do caso *Longhorn* de 2017 e sua condição incomum, os outros[39] oito casos se focaram em ter apenas um ator do Sistema Internacional Cibernético como vítima principal. Isso fez com que a Rússia fosse impactada em quatro ocorrências cibernéticas e o Irã e a Coreia do Norte em dois incidentes respectivamente. Tais elementos foram refletidos nas notas produzidas pelo apêndice G, gerando valores menores ao seguir a lógica avaliativa supracitada. Ressalta-se que a escolha dos alvos medulares dos ataques cibernéticos respeitaram as noções indicadas por Rogers (2017), investindo contra três[40] dos quatro Estados abordados.

A partir desse pensamento, os ataques cibernéticos realizados contra a Coreia do Norte foram enfatizados pois se iniciaram em 2017, em conjunto com a publicação do manuscrito - em um caráter sigiloso naquele período - de Michael S. Rogers, terceiro comandante geral da USCYBERCOM e da NSA. A vontade e seleção de oponentes, nos anos subsequentes, se mantiveram idênticas, pois mesmo com a mudança na liderança ocorrida em maio de 2018, com Paul M. Nakasone, os ataques mantiveram os critérios de preferência - agora nomeado de estratégia de combate persistente e de defesa dianteira -, salientando, com isso, a continuação no padrão cibernético apresentado na administração Trump.

Adicionalmente, foi identificada, durante o governo Trump, outra alteração significativa nas Ações cibernéticas. Tal mudança adveio da divulgação e responsabilização pública dos representantes dos Estados Unidos nos ciberataques realizados, nomeados de operações militares cibernéticas. Ao realizar tal conduta, os EUA de Trump abandonaram o anonimato inerente de um ato ofensivo, e se apresentaram como o principal culpado dos ataques realizados contra esses Estados, se disponibilizando, em um primeiro momento, às movimentações de reprovação em um contexto internacional.

A partir dessa escolha estadunidense, a complexidade relativa a um caso cibernético ofensivo foi reduzida, dispensando a necessidade de serem produzidos relatórios sobre as especificidades das ocorrências. Isso fez com que certos detalhes, nuances e deduções se perdessem devido à transparência do perpetrador do *cyber* ataque, produzindo,

[39] O ato de comprometimento ao *Yandex* de 2019 também segue esses parâmetros, com a Rússia como objetivo principal de ataque. Entretanto, esse incidente respingou também em mais outros três países usuários da plataforma infectada - Bielorússia, Cazaquistão e Turquia.

[40] Nesse período, verificou-se a ausência de dados que comprovaram ataques cibernéticos contra a China, o quarto Estado salientado por Rogers (2017).

consequentemente, notas variadas sobre o dano direcionado às vítimas, pontuado no apêndice G.

Ao afirmar as movimentações ofensivas para com o Sistema Internacional Cibernético, os Estados Unidos durante o governo Trump apresentaram um comportamento singular em suas Ações ao transformá-las em Sinais. Em um contexto regular, Jervis (1970, p. 18) indica que os Sinais não contém credibilidade inata, pois se apresentam como declarações públicas sobre um tópico específico, realizadas para influenciar certos comportamentos e consolidar imagens pré-concebidas. Dessa forma, os Sinais não conseguem se associar aos atos realizados no Sistema, já que não haveria provas de que um Estado forneceria, com suas falas, evidências constantes de sua conduta para com atores do SI (Jervis, 1970, p. 18).

No entanto, os Sinais estipulados por Trump foram associados, quase simultaneamente, ao ato efetivado. À vista disso, foram determinados os cursos de ação prováveis, além de concretizar as intenções e a imagem almejada. Através dessa movimentação, os Estados Unidos de Trump consolidaram a representação unilateral e combativa estruturada por seus Índices, indicando a vontade de travar enfrentamentos contra seus oponentes no Sistema Internacional Cibernético, alcançando, com isso, graus de domínio e influência no espaço.

A conduta estadunidense foi agravada ao considerar as percepções e as falas estadunidenses que apontam a possibilidade dos atos perpetrados poderem ser mais extremos, destacando maiores graus de dano a serem realizados futuramente. Essa noção retoma as inferências de Raiffa (1994) acerca do controle de informações presente em uma mesa de negociação. Baseado nesse pensamento, verifica-se que a movimentação transparente dos Estados Unidos em suas Ações, realizadas em conjunto com as imagens destacadas a partir disso foram definidas como uma pretensão admissível do ator.

As Ações dos EUA assumiram, assim, o risco e as possibilidades dessa decisão em prol de construir circunstâncias vantajosas para si no SI. Com base nos dados utilizados na construção desta dissertação, salvo a consolidação da imagem estadunidense incisiva pelas Ações efetuadas, não é possível especificar[41] quais outros benefícios seriam obtidos por esse padrão operacional.

[41] Nessa afirmação, pode ser utilizada a inferência de Libicki (2020) acerca do conceito de normalização como forma de explicação. Para Libicki (2020, p. 44), na normalização é assumida a noção de que certos atos contraditórios, com normas inexistentes ou intricadas, quando não são discutidos ativamente ou repreendidos internacionalmente, são permitidos no SI, se tornando normais e aceitáveis como uma forma legitima de comportamento. Dessa forma, os atos cibernéticos ofensivos transparentes efetuados no governo Trump assumiriam vantagens ao construir e permitir uma prática normalizada no espaço cibernético em um caráter ofensivo.

Ao incluir os indicadores com os pensamentos autorais dispostos neste capítulo, infere-se que a manifestação estadunidense das capacidades cibernéticas entre 2017 a 2020, seguem, assim como percebido no governo Obama, as mesmas métricas de materialização de sua estratégia em Ações. Conforme indicado anteriormente por Maier (2019), Amoretti e Fracchiolla (2018) e Devanny (2021), o planejamento cibernético do período consistia em passar uma representação mais unilateral e resoluta em relação ao ciberespaço. Elemento realizado a partir do fortalecimento - orçamentário e tecnológico - dos órgãos domésticos e militares voltados à área.

Uma vez estipulada a estratégia cibernética, os Estados Unidos com Trump passaram a difundir essa representação através de suas ações no Sistema. Ocorrências essas voltadas a normalmente atingir apenas um ator - posto como oponente aos EUA (Rogers, 2017) -, e anunciando transparentemente seu envolvimento como o agente malicioso responsável.

Com a ajuda do uso de Sinais realizados em conjunto com as Ações, as escolhas dos Estados Unidos na administração Trump estabeleceram e destacaram uma imagem conveniente a si no espaço cibernético para os atores do Sistema Internacional. Configuração que ainda teve como objetivo central a defesa de seus interesses e de suas infraestruturas críticas, salvaguardadas naquele momento com maior rigidez e possibilidades favoráveis de atuação ofensiva - podendo ser classificada como autodefesa.

Congregando tais informações, se tem a noção de que tanto a estratégia quanto a implementação das capacidades durante o governo Trump continuavam a seguir Motivos relacionados ao poder. Não obstante, essa movimentação, assim como vista na presidência Obama, retomou e desenvolveu os interesses estadunidenses, que ainda perpassam pela construção e projeção de poder no ciberespaço, porém dessa vez com um viés mais belicoso, responsivo e evidente.

Ao analisar os dados e as construções teóricas indicadas neste capítulo e no anterior, percebe-se que os Estados Unidos, mesmo em um recorte temporal amplo com a presença de dois presidentes distintos, recorreram a pensamentos e atividades voltadas à temática de poder para alcançar influência e liderança no espaço cibernético. Adicionalmente, a movimentação efetuada nesses 11 anos consegue ser associada ao trabalho de Nye (2010) acerca do poder cibernético, elemento teórico central para esta dissertação.

Conforme salientado no primeiro capítulo, o poder cibernético se trata da capacidade de um ator do Sistema Internacional em criar e transformar eventos e padrões existentes no espaço cibernético em possibilidades de ganhos favoráveis (Nye, 2010, p. 04). Tais benefícios

poderiam ser garantidos internamente ou externamente ao ciberespaço, a depender dos fatos realizados e dos resultados intencionados. Caso a movimentação logre algum tipo de sucesso ao agente perpetrador dos atos, o poder e as vantagens inerentes à ação seriam assegurados.

Através dessa noção, grande parte das informações trabalhadas na dissertação trazem a concretização do trabalho de Nye (2010) dos atos de poder realizados pelos Estados Unidos. Tais elementos se reúnem com Motivos, caracterizados pela defesa dos interesses estadunidenses em um caráter relativo ao poder, definidores de estratégias cibernéticas focadas em garantir - com nuances de implementação, a depender do governo - oportunidades pertinentes, viabilizadas através das Ações no Sistema Internacional Cibernético (Kremer e Müller, 2013, Jervis, 1970 e Nye, 2010).

Não obstante, todos os atos de desenvolvimento e apresentação das capacidades cibernéticas dos Estados Unidos, tanto defensivas - criação e assinaturas de acordos internacionais salientado por Hitchens e Goren (2017) - quanto ofensivas - exposição dos dados públicos governamentais estadunidenses e as Ações dispostas no CFR (2024) - manifestam a presença de fatores internos ou externos indicados por Nye (2010, p. 02-05) e Kuehl (2009, p. 38) para se alcançar poder no âmbito cibernético. A obtenção de poder a partir do caráter interno adveio principalmente da manifestação das capacidades defensivas estadunidenses. Elemento ressaltado na estruturação da influência dos EUA como o principal formulador e apoiador - principalmente no governo Obama - de legislações positivas para o SI.

Através da construção e implementação dessa imagem, os Estados Unidos, entre 2010 a 2020, conseguiram conduzir que os Memorandos de Entendimento seguissem padrões benéficos aos seus Motivos, realizando-os com seus principais aliados, mas também com seus oponentes. Ponto exemplificado nas reuniões do GGE até 2017 e no desenvolvimento do Manual de Tallinn de 2013 e de sua versão de 2017. Tal tipologia de emprego de poder exclusivamente no domínio cibernético, no entanto, foi percebida com maior intensidade durante a administração Obama, fazendo parte de sua imagem transmitida ao Sistema.

Já a consecução de poder obtido externamente resultou do uso das capacidades ofensivas estadunidenses na forma das ações cibernéticas realizadas. Ressalta-se também a percepção de poder internalizado nos ciberataques realizados segundo Nye (2010, p. 04-05). Entretanto, é constatada nessas ocorrências maiores exemplificações de atos de poder externo nos atos cibernéticos ofensivos, indicados através das formas de destruição e dominação realizadas no Sistema Internacional Cibernético.

Conforme salientado nos apêndices C, G e H, os *cyber* ataques atribuídos perpassaram uma movimentação constante acerca da forma da operacionalização, dos alvos prioritários e do grau de dano disposto, mantendo classificações razoáveis no último componente. Isso fez com que as ofensivas realizadas fossem percebidas, reconhecidas e contestadas de formas distintas, a depender das estratégias governamentais implementadas.

Diferentemente do observado nas capacidades defensivas, a utilização do poder cibernético em uma característica externa foi alcançada de forma significativa por ambas as administrações pesquisadas, com sete e nove casos respectivamente. Contudo, durante o governo Trump, a implementação da estratégia ofensiva seguiu de forma mais visível a utilização de padrões tradicionais de poder - permitidos pelo pensamento de Nye (2010, p. 05) - de forma a fortalecer sua projeção no Sistema Internacional Cibernético.

Ao utilizar essa lógica, evidenciou-se o emprego das noções acerca dos Sinais, Índices e as imagens de Jervis (1970) para o alcance de seus interesses. Nesse ponto, também é percebido o uso das estratégias de negociação de Raiffa (1994) sobre a disposição e divulgação de informações conscientemente planejadas para criar possibilidades favoráveis de ganho. Esses conceitos, dada a época na qual foram concebidos, não indicavam a utilização no pensamento cibernético. Contudo, ao integrá-los ao estudo ampliado e particular de Nye (2010), foi estabelecida uma relação entre as ideias, fortalecendo os fundamentos teóricos utilizados.

Fundamentado nisso, infere-se que a lógica de poder identificada nos Motivos estadunidenses segue o pensamento de poder cibernético de Nye (2010). Tal concepção avalia que os atos de poder internos e externos foram percebidos pelos Estados Unidos como possibilitadores de eventos oportunos para a consolidação de sua imagem e a conquista de seus interesses no Sistema Internacional Cibernético.

O comprometimento Estatal com essa tipologia de poder conseguiu até mesmo ser evidenciada em Índices gerais das informações, dispostas no orçamento específico para a *cyber* segurança. Nesse ponto, salienta-se que houve um padrão entre as informações dispostas nos apêndices B e C, que evidenciam a estimativa orçamentária cibernética e a quantidade de *cyber* ataques atribuídos pela CFR (2024) respectivamente. Esse exemplo indica que os aumentos e as diminuições no cálculo destinado a temática cibernética seguiu a mesma movimentação, podendo indicar um nível de preparação de um ataque cibernético. Através dessa dedução, os apêndices B e C podem ser interpolados em um grau de conformidade razoável, trazendo noções preditivas inerentes a um Índice (Jervis, 1970, p. 19).

Vale ressaltar a possibilidade de a correlação supracitada ser acidental, pois segundo os escritos de Zetter (2014) e Libicki (2007), um ato de *cyber* ataque com padrões elevados pode se apresentar como uma ocorrência demorada. Tal delonga é possivelmente derivada pelo longo processo de contratação e treinamento dos editores de código-fonte - autores das linhas de código presentes em um *malware* - e pelo alto tempo investido no aprimoramento na codificação e na criptografia, pontos que permitem com que um programa malicioso consiga realizar seus objetivos de forma prestativa.

Adicionalmente, os valores investidos para a execução de um ataque cibernético podem demorar a serem angariados e empregados aos setores corretos, trazendo eventuais problemáticas para o fator operacional de um *cyber* ataque. Esses embaraços reunidos fazem com que a remontagem certeira da origem de uma investida cibernética sejam percebidos como mais um fato complicador no pensamento de cibersegurança, tendo exceções em alguns contextos marcantes e prolongados, como nos casos *Stuxnet*, *Equation Group* e *Longhorn*, que conseguiram estipular datas de origem de ação distantes, mas não de seu desenvolvimento.

Assim sendo, através dos dados dispostos e dos pensamentos teóricos utilizados, infere-se a utilização dos Estados Unidos em atos de poder em um caráter cibernético. Não obstante, a construção dessa capacidade segue os parâmetros expostos no trabalho de Nye (2010) associados às concepções de Kremer e Müller (2013), Jervis (1970) e Raiffa (1994). Tal associação deriva do entendimento de que os EUA - Parte Interessada central -, baseado em um Motivo - defesa de suas infraestruturas críticas, adjunto da propagação de seus interesses no Sistema Internacional Cibernético - construiu estratégias de concretização de uma imagem - dupla a depender da administração -, a partir de informações cuidadosamente expressas.

Decorrente disso, o processo é implementado através de Ações contra agentes do SI e por atos internos de consecução de poder, defendendo, com isso, seus Motivos e possibilitando renovações dessa movimentação. Seguindo tal junção teórica, o poder cibernético estadunidense segue um parâmetro cíclico de organização e utilização voltado a garantir sua defesa no Sistema, chegando até mesmo a ter pretensões preemptivas de ação contra diversos atores, podendo caracterizá-los como oponentes.

Comprova-se, mediante a teoria utilizada, a estruturação do poder cibernético pelos Estados Unidos no recorte temporal. Nota-se que o poder alcançado não utilizou exclusivamente de arranjos teóricos realistas – elemento norteador desta pesquisa –, conseguindo compreender o poder cibernético através de perspectivas múltiplas, sejam elas realistas – com o trabalho de Jervis (1970; 1978) – ou até mesmo neoliberais – com o trabalho

de Nye (2010; 2011). Isso se deu por conta da noção de que as preferências e as instituições estadunidenses, durante o recorte temporal escolhido, não se pautaram em uma dinâmica teórica única para construir e projetar poder no espaço cibernético, se concentrando apenas na obtenção de seus objetivos a longo prazo. A partir desse pensamento, esta dissertação conseguiu ampliar a discussão teórica, pois conseguiu entender e definir as formas dinâmicas nas quais o poder consegue ser definido e aplicado em contextos e em teorias distintas.

A partir do conceitual teórico *S.A.M.* de Kremer e Müller (2013), a investigação das capacidades cibernéticas é encerrada, visto que os três componentes centrais foram identificados e atribuídos de forma lógica em um argumento. Essa concepção, no entanto, marca um limite no alcance explicativo desse *framework*, visto que as consequências e os ganhos dos atos estadunidenses não conseguem ser analisados sob a noção desse referencial, ponto considerável para esta dissertação. Isso acontece visto que, Kremer e Müller (2013), ao escolherem pesquisar um caso cibernético segundo suas três categorias de prioridade, é preterido, consequentemente, dispensar fatores mais imprecisos ante a temática cibernética, como as decorrências de episódio no tempo.

Dessa forma, para esta dissertação, se faz necessário entender como composição desse poder cibernético de Nye (2010) foi percebida pelos atores do Sistema Internacional, salientando os efeitos e os possíveis benefícios obtidos pela obtenção de poder seguindo as noções de Nye (2010). Ponto abordado na última seção deste estudo.

3.3 - Poder Cibernético: Consequências, Ganhos e Desfechos

Jervis (1970, p. 19) indica que uma ação, seguida ou não das métricas formuladoras de uma imagem, possuem ambiguidades quando percebidas pelos agentes no SI. Essa incerteza advém do fato de que, seja uma imagem, um ato, uma estratégia, ou até mesmo uma Ação pode produzir resultados inesperados - positivos ou negativos - ao ocasionador do ato e ao Sistema Internacional em si. Logo, é fundamental entender quais foram os produtos derivados das Ações cibernéticas ofensivas e das movimentações defensivas estadunidenses - parte dos elementos de poder para Nye (2010) - para com os atores do Sistema. Com isso, será inferido as principais consequências alcançadas pelos Estados Unidos através de seus atos cibernéticos.

Ao analisar a utilização das capacidades cibernéticas pelos EUA, averigua-se que houve êxito nos atos de poder realizados, obtendo poder por meio dessas práticas. A conquista de poder, no entanto, foi alcançada de formas indiretas e diretas, a depender da movimentação e

do nível de interesse presente dos governos investigados. Uma amostra disso está na utilização das capacidades defensivas - percebida como uma forma interiorizada do poder cibernético -, que, ao considerar as ações realizadas, deduz-se uma dinâmica branda, porém objetiva na projeção de poder no ciberespaço.

Isso é dito pois, embora tenham sido confirmados e assinados 39 acordos temáticos – 53 ao considerar os valores totais –, tais compromissos específicos foram efetivados em sua maioria durante a administração Obama, com 31 ocorrências. Mostrando que a alta dedicação para com as noções legislativas fazia parte somente nesse período, reduzindo o efeito no tempo devido a mudança na liderança dos Estados Unidos, que possuíam outras prioridades.

Porém, mesmo com uma baixa adesão nos tratados temáticos, os Estados Unidos com Trump ainda se mantiveram comprometidos aos acordos realizados. Elemento salientado graças a falta de dados comprovando a descontinuação nos contratos assinados ou até mesmo atos de desrespeito às recomendações presentes nos Memorandos de Entendimento realizados anteriormente. Isso gera a noção de que os Estados Unidos de Trump ainda detiveram um nível razoável de utilidade ao pensamento legislativo defensivo, possibilitando manutenções à pauta, evidenciada oito vezes.

A estratégia defensiva realizada resultou em ganhos indiretos de poder, representados pela influência estadunidense conquistada pelo uso das capacidades defensivas na construção de leis e recomendações, geralmente favoráveis aos Estados Unidos. Ponto notabilizado principalmente nas GGEs - até sua quinta sessão - e no Manual de Tallinn, reafirmados durante o governo Trump. Essa forma de influxo é verificada pela noção de que, tanto as sessões do GGE quanto o Manual, foram baseadas em leis e guias militares ocidentais ou estadunidenses, promovendo vantagens naturais aos EUA ao seguir as interpretações sugeridas (Robinson, Jones e Janicke, 2015, p. 84, Klaar, 2021, p. 06 e Schmitt, 2021).

Mesmo com complicações em relação às escolhas de formação dessas demonstrações, o fato é que, especialmente no caso do Manual de Tallinn, tais recomendações são os exemplos mais avançados ante as questões cibernéticas sobre a segurança cibernética. Ponto que gera a necessidade dos atores do Sistema Internacional em se utilizar dessas orientações, principalmente sobre aspectos territoriais, fronteiriços e jurisdicionais ante a temática cibernética (Jensen, 2017, p. 778 e Bustelo, 2019, p. 55).

Isso faz com que haja uma concretude do uso crescente dessas instruções pelos atores do SI e Estados, de forma a tentar elucidar as problemáticas existentes e dar exemplos tangíveis de sua contribuição e fomentar tópicos de discussão conjuntos e temáticos (Bustelo, 2019, p.

60). Com isso, os Estados Unidos, no período estudado, podem garantir vantagens para si através desse cumprimento, pois, a cada estratégia cibernética defensiva - em um tom internacionalizado - baseada nos parâmetros estadunidenses de interpretação que é acatada no Sistema Internacional, mais influência e poder indireto os EUA garantem para si, criando uma esfera de dominância nas questões de segurança no ciberespaço.

Tal raciocínio explica as reações estadunidenses ante ao OEWG de 2018, que tentaram reformular a própria GGE - uma circunstância tão vantajosa que criou complexidades na garantia de sua continuidade - em prol de não permitir com que um oponente - a Rússia - crie um espaço próprio e aberto de diálogo cibernético. Seguindo o pensamento dos Estados Unidos sob a administração Trump, a movimentação russa poderia estabelecer uma influência na área, gerando a necessidade de rivalizar a partir da revitalização da GGE em 2019 (Devanny, 2021, p. 05).

Posto isso, ao considerar as formas exteriorizadas de ganho de poder, realizadas por meio das Ações, a percepção de captação é direta. Tal afirmação é derivada da tangibilidade dos atos, atribuídos ou até mesmo denunciados em ambos os governos apresentados, conforme indicado no apêndice C, determinando as tipologias de dano e os Efeitos Significativos nas infraestruturas críticas de seus alvos, realizadas mesmo quando o intuito era manter o anonimato - como percebido nos casos entre 2010 a 2016.

Aqui, ao levar em consideração as 16 operações cibernéticas ofensivas realizadas pelos Estados Unidos e seus Motivos instauradores - a defesa das infraestruturas críticas governamentais e seus interesses -, deduz-se uma movimentação positiva do alcance desses elementos, adquiridos de formas distintas. Os interesses de projeção e manutenção de poder, conforme indicado na seção 3.2, foram obtidos de forma facilitada em virtude da configuração dos ciberataques e da forma como eles afetaram suas principais vítimas. Já o primeiro elemento, em um caráter direto, ao observar as ações realizadas e suas consequências, provoca e retoma o pensamento do dilema de segurança de Jervis (1978) vinculado ao conceito de autodefesa apresentado nos documentos estadunidenses.

A autodefesa, segundo Maier (2019), é posta como a capacidade de garantir a defesa dos Estados Unidos por meio de qualquer ato necessário. Essa concepção, a partir do pensamento realista fundamentado por esta dissertação, consegue se mesclar com o pensamento de autoajuda de Gentili (2005) e Palacios Junior (2011, p. 71).

Para esses autores, a autoajuda seria a capacidade do ator de se defender em um momento anterior ao ato de ataque, ou seja, com objetivo de evitar sua destruição, um agente

age preemptivamente contra seu agressor, atacando-o sob a justificativa de que é "impossível para uma vítima realizar uma defesa efetiva depois de ter sido atacada" (Palacios Junior, 2011, p. 71). Nota-se que essa lógica foi utilizada pelos Estados Unidos para salvaguardar suas infraestruturas críticas, conforme apontado em seus documentos oficiais no capítulo 2. Dessa forma, seus principais oponentes foram atacados ciberneticamente com base nesse conceito e justificativa. Em alguns casos, no entanto, Estados-aliados também foram atacados[42].

Ao realizar a obtenção de poder por meio de atos ofensivos contra atores do Sistema, os governos dos Estados Unidos garantiram poder e segurança individualizada e limitada no Sistema. Contudo, também foi estimulada a possibilidade de respostas de igual medida. Assertiva consolidada ao perceber que enquanto os EUA, a partir dos dados da CFR (2024), realizaram comprovadamente 16 ciberataques no Sistema entre 2010 a 2020, esse Estado foi atacado, em contrapartida, 150 vezes, conforme indicado na introdução.

Dentre esses incidentes, cerca de 88% - 132 - foram realizados pelos quatro Estados-oponentes aos EUA. As ocorrências realizadas contra os EUA, apresentadas no apêndice D, se iniciam principalmente após o reconhecimento internacional do caso *Stuxnet*, a partir de 2011, com o aumento de três para oito - nove ao considerar valores totais. Tal padrão segue uma lógica[43] parecida ao considerar os anos dos ataques estadunidenses indicado no apêndice C, havendo aumento ou estabilização em anos nos quais são comprovados atos ofensivos estadunidenses.

Esse encadeamento lógico é reforçado através da noção de que, quando os governos dos Estados Unidos agem ofensivamente no Sistema Internacional Cibernético, suas vítimas obtêm a capacidade de retaliar, fazendo-a contra os EUA. Dessa forma, através de uma ação preemptiva para a defesa de suas infraestruturas críticas, as movimentações estadunidenses

---

[42] Nesse ponto, é notada a falta de explicação que o conceito de autodefesa e autoajuda oferece nos casos cibernéticos ofensivos realizados durante o governo Obama em conjunto com o incidente *Longhorn* de 2017, pois, nesses eventos, atores pontuados como aliados também foram atacados.

[43] Retoma-se o princípio supracitado entre as informações dispostas nos apêndices B e C, que se repete ao considerar esse novo elemento. Em 2018, ano no qual não se reportou nenhum caso cibernético dos EUA, conjuntamente com as informações que propuseram o menor valor orçamentário temático, houve o maior número de ataques contra os Estados Unidos, com 22 incidentes - 30 ao considerar o total. Essa conexão traz questionamentos acerca do que de fato aconteceu ciberneticamente em 2018 e por qual motivo as informações desse ano não seguem os padrões estabelecidos no recorte temporal.
Existe a hipótese de que o valor temático possa ter sido consequência do estabelecimento do congresso em desfavor do presidente Trump. Contudo, segundo os dados da CRS (2020, p. 04), o 116° congresso de 2018 teve maioria republicana - partido de Trump - no senado, enquanto obteve maioria democrata na câmara. Tal diferença poderia causar atritos e diminuições na construção e repartição do orçamento. No entanto, tais decisões e diminuições deveriam se manter por mais de um ano, indo de 2019 a 2020, elemento não observado nos dados dos anos posteriores - apêndices A e B. Baseado nisso, não foram encontradas informações que expliquem essa exceção nos dados estudados, criando questionamentos que podem ser solucionados a partir de pesquisas futuras com novas percepções e dados.

também criaram possibilidades danosas contra elas, aumentando a quantidade e o nível de destruição contra um de seus motivadores. Tal perspectiva é apresentada no trabalho de Mastanduno, Lake e Ikenberry (1989, p. 466) como uma das consequências possíveis e imediatas do uso de poder no Sistema Internacional. Para eles, ao realizar uma ação dimensionada no poder direto, há chances de aumento de ações contra o responsável pelos atos, elemento notado ao considerar os dados desta dissertação.

Ao estabelecer essa postura, as preferências dos Estados Unidos iniciaram e consolidaram, em um contexto cibernético, o pensamento do dilema de segurança proposto por Jervis (1978) e apresentado no início desta pesquisa. É fato notar que o caso *Stuxnet* de 2010 permitiu que atos cibernéticos ofensivos realizados por Estados fossem considerados, temidos e possibilitados no Sistema, visto que seu código ficou disponibilizado, de forma involuntária, na rede.

Também foi viabilizada a noção de que outros Estados também poderiam aumentar seu nível de poder se utilizando do espaço cibernético, expandindo seus níveis de ataque e quantidade de vítimas. Isso fez com que um comportamento belicoso fosse estabelecido no Sistema como resposta às estratégias e aos atos estadunidenses (Devanny, 2021, p. 09).

Com o uso da autodefesa e da autoajuda como pontos basilares de sua estratégia para cumprir seus Motivos, os governos estadunidenses garantiram poder externo mediante o uso de suas ações ofensivas. Não obstante, esses atos também diminuíram a segurança geral de outros atores do Sistema Internacional Cibernético. Isso fez com que tais agentes, a partir do temor consequente dessa atividade, também projetassem poder no ciberespaço para salvaguardar sua condição, de forma a minar ainda mais a segurança no Sistema em si, fundamentando o dilema de Jervis (1978).

Além disso, as práticas cibernéticas dos Estados Unidos realizadas e produtoras do dilema foram evidenciadas por esta dissertação como intencionais. Isso acontece pois para Jervis (1978, p. 169 e 170), o dilema só é causado quando o ator perpetuador da ação escolhe essa forma de projeção de poder como a principal, visto que existem maneiras não belicosas de se alcançar influência no SI, elemento constatado nesta pesquisa ao considerar as capacidades defensivas dos Estados Unidos. Ou seja, ao considerar esse pensamento, não só as inclinações dos Estados Unidos criaram conscientemente essa movimentação combativa no Sistema, como, ao fazê-la, eles conseguiram se tornar o principal alvo de ataques efetuados no *cyber* espaço, também fortalecendo suas justificativas para continuar se mobilizando agressivamente no âmbito cibernético.

Com base nessa atitude, são trazidos os comentários de Healey e Jervis (2020) e Devanny (2021, p. 09 - tradução nossa) que pontuam que, em um contexto cibernético, “os Estados Unidos se esqueceram que são os predadores muito antes de serem as presas”. Esses autores indicam que, os EUA, a partir de suas próprias ações para a criação do dilema e das consequências características desse ato em um contexto cibernético - poderem ser atacados por outros atores que projetarão poder para se defender -, se colocaram ainda mais como a principal vítima a ser defendida, aumentando a necessidade de se agir no Sistema.

Isso mostra que, em um pensamento externalizado de poder, os governos dos Estados Unidos, embora tenham obtido poder através do alcance de seus interesses para com o Sistema Internacional Cibernético, a manutenção da defesa de suas infraestruturas críticas foi lograda, porém dificultada pelas consequências de suas Ações, criando um dilema de segurança no ciberespaço (Mastanduno, Lake e Ikenberry, 1989, p. 466 e Jervis, 1978, p. 169 e 170). No entanto, esse entrave permitiu com que a imagem e o modelo das Ações dos Estados Unidos permaneçam inalteradas, pois ainda há a necessidade em se autodefender, permitindo a continuação de atos de autoajuda no Sistema Internacional Cibernético.

Em suma, através do uso de suas capacidades ofensivas e defensivas, os governos dos Estados Unidos obtiveram poder no Sistema Internacional Cibernético. Tal força, conquistada estrategicamente pela definição de imagens, motivos e interesses, foi concretizada em circunstâncias vantajosas para si no Sistema, que, através de padrões internos e externos, garantiram níveis de poder cibernético previstos no trabalho de Nye (2010).

Contudo, ao analisar os resultados derivados das posturas governamentais estudadas, percebe-se que, enquanto foi constatada a consecução de poder segundo os parâmetros definidos, os ganhos, principalmente na percepção externa de Nye (2010), criaram consequências evidentes. Decorridas principalmente da escolha de agir preemptivamente em nome de sua autodefesa, as preferências governamentais dos EUA iniciaram e consolidaram um dilema de segurança no espaço cibernético, possibilitando crescimento dos *cyber* ataques realizados.

Isso fez com que, naturalmente, as infraestruturas críticas dos Estados Unidos se tornem alvos de ocorrências cibernéticas ofensivas - apêndice D -, criando a necessidade em proteger suas infraestruturas críticas, deixando-as mais resilientes. No entanto, conforme salientado anteriormente, o fato de ser atacado permitiu com que os atos ofensivos fossem vistos como ainda mais necessários para as administrações dos Estados Unidos, perpetuando o dilema. Com

isso é previsto que futuramente haja maiores possibilidades animosas de projeção de poder no Sistema Internacional, tornando o ciberespaço mais inseguro aos atores.

CONCLUSÃO

Após apurar 11 anos das capacidades cibernéticas realizadas pelos Estados Unidos, conectando-as com pensamentos autorais distintos sobre uma lógica de poder realista, é fundamental para esta dissertação responder o questionamento preambular presente na introdução. Com isso, será comparada a hipótese elaborada com os resultados alcançados, determinando a aceitação ou a contestação desse elemento para a pesquisa.

O trabalho estabelecido foi pautado na seguinte pergunta de pesquisa: Em que medida a aplicação das capacidades cibernéticas - ofensivas e defensivas - afetou a projeção e manutenção de poder dos Estados Unidos contra os atores percebidos como aliados e oponentes entre os anos 2010 e 2020?. Derivado disso, foi proposta a seguinte hipótese geral de dissolução, baseada na afirmação de que os EUA, entre 2010 e 2020, ampliaram deliberadamente suas capacidades cibernéticas visando projetar poder no Sistema Internacional, realizado principalmente por meio de intervenções no espaço cibernético doméstico de outros Estados nacionais, tendo como o foco os atores tidos como oponentes aos Estados Unidos - Rússia, Irã, Coreia do Norte e China.

Já as três hipóteses secundárias elaboradas aprofundaram a HG indicando que:

HS1 – Os Estados Unidos aumentaram seus níveis de capacidade cibernética através da ampliação, crescente e progressiva, qualitativa e quantitativa, de seus orçamentos e de seus atos ofensivos e defensivos entre 2010 a 2020.

HS2 – Os atos estadunidenses tiveram como objetivo central a projeção de poder, sendo este realizado principalmente por meio de ataques cibernéticos ofensivos, que visavam a intervenção do espaço cibernético doméstico de suas vítimas, gerando níveis de dano diversos.

HS3 – O foco das ações ofensivas realizadas pelos Estados Unidos recaíram principalmente e exclusivamente aos quatro Estados postos como oponentes aos Estados Unidos: China, Rússia, Irã e Coreia do Norte.

Dessa forma, a verificação da hipótese será realizada a partir de três etapas: (1) indicar os graus de ampliação realizados nas capacidades cibernéticas estadunidenses, presente no HS1; (2) assinalar se o objetivo dos Estados Unidos seguiram as métricas de projeção de poder previstas, exposto no HS2; e (3) se o foco recaiu principalmente sobre os quatro Estados-oponentes, elemento do HS3. Com isso, será realizada uma comparação prevista no método hipotético-dedutivo, salientando uma elucidação concreta da pergunta de pesquisa.

O componente (1) assume uma ampliação deliberada no uso das capacidades cibernéticas - ofensivas e defensivas - dos Estados Unidos no período proposto. Em um caráter ofensivo, esse aumento foi moderadamente correto.

Primeiramente, em um contexto orçamentário geral, a seção 3.1 estabelece um incremento de 35,2% entre 2010 a 2020, mantendo-se anualmente estável até 2016, onde se passou a ter um crescimento progressivo - vide apêndice A. Tal acréscimo teve como principal motivador a mudança de governo, que passou a retirar recursos de outros departamentos para que o Departamento de Defesa estivesse melhor equipado e preparado para as problemáticas dispostas em todos os âmbitos de combate (Estados Unidos da América, 2017b).

Já em um ambiente temático, o orçamento para a cibersegurança amplifica-se imensamente no recorte, com um cálculo de 52938%, registrado na totalidade do recorte temporal. No entanto, tal crescimento não foi totalmente constante, sendo salientado algumas baixas orçamentárias indicadas no apêndice B.

No que tange os ataques cibernéticos realizados pelos Estados Unidos, quantitativamente, constatou-se aumentos nos anos, contudo, tal movimentação não se manteve no final do recorte, encerrando com a mesma quantidade de *cyber* ataques, um, conforme indicado no apêndice C. A maior adição ofensiva foi percebida entre 2018 e 2019, com ampliação de 500% - chegando a cinco ataques constatados em 2019.

Ao pensar nos ataques em termos qualitativos, foi reportada uma queda nas notas das capacidades utilizadas pelos EUA, tendo uma redução de 62,3% entre as datas limites de 2010 a 2020. A partir dos dados presentes no apêndice G e H, as médias realizadas apresentam assimetrias em sua progressão anual, finalizando com a menor pontuação dos atos cibernéticos analisados, com 3,5.

O contexto avaliativo também dispôs de um pico anual, presente entre 2016 e 2017, com um aumento de 124,3%, derivado da nota do caso *Longhorn* de 8,3. Entretanto, esse valor não conseguiu superar as métricas presentes no incidente *Stuxnet* de 2010, colocando-o no segundo maior valor do período.

As indicações das capacidades defensivas, último elemento do item (1), também seguem o pensamento desigual visto quantitativamente nas capacidades ofensivas, visto que, em um contexto amplo, foram constatadas diminuições, indo de duas assinaturas em 2010 a uma subscrição em 2020. Contudo, em um pensamento anual progressivo, foram retratados aumentos significativos, chegando a adições de 62,5% entre 2014 a 2015 - vide apêndice E.

Tais avanços, no entanto, não foram mantidos com a mudança de governo a datar de 2017, marcado pela diminuição de 62,5%.

Estabelecidos os parâmetros, constata-se um aumento irregular na construção e uso das capacidades cibernéticas dos Estados Unidos entre 2010 a 2020. Dito isso, o elemento (1) e a HS1 podem ser considerados parcialmente corretos.

O crescimento é visível e constante nos termos orçamentários, porém desarmônico nas quantidades de acordos assinados e ataques realizados, chegando até mesmo em diminuições nas avaliações realizadas dos atos ofensivos. Foram percebidas adições relevantes nos atos ofensivos e defensivos, dispostos em alguns anos do recorte temporal, contudo, essas movimentações não foram continuadas. Escolha intrigante ao considerar a dimensão ofensiva estadunidense, que, mesmo com aumentos orçamentários, não foi possível retratar o uso desse reforço nos atos ofensivos cibernéticos.

Ao considerar os elementos presentes no item (2), a HS2 levantada é comprovada. Isso é posto graças a noção de que, conforme retratado na seção 3.2, as condutas cibernéticas realizadas pelos Estados Unidos tinham como objetivo a projeção de poder no Sistema Internacional Cibernético, sendo caracterizadas como relativas a poder em seus Motivos através de uma investigação acerca da imagética estadunidense realizada e de seus interesses provocadores.

Não obstante, a movimentação de poder realizada até mesmo excedeu o previsto na hipótese, já que não foram constatadas somente intervenções no espaço cibernético doméstico, mas atos defensivos visando esse objetivo de poder. Ao utilizar Nye (2010) e sua concepção de poder cibernético, comprova-se posturas externas e internas de domínio realizadas pelos Estados Unidos nos 11 anos pesquisados. Com isso, as administrações dos EUA adquiriram poder no ciberespaço, obtido ou através das condutas diretas realizadas, as Ações, ou graças ao aumento da influência defensiva estadunidenses nas questões de *cyber* segurança.

Já no item (3) presente na HS3, é retomada a parcialidade em sua validação. A conjuntura pressuposta previa um foco das condutas cibernéticas realizadas somente aos Estados-oponentes aos Estados Unidos - Rússia, Irã, Coreia do Norte e China - contudo, as ações ofensivas e defensivas atingiram ambas as classificações salientadas, aliados e oponentes.

À vista disso, o capítulo 2 e a seção 3.1 indica que das 16 Ações atribuídas aos Estados Unidos, em quatro circunstâncias, foram vitimados Estados-aliados, realizados entre 2010 e 2017. A partir de 2017, com a mudança na administração estadunidense, os oponentes aos Estados Unidos foram anunciados e combatidos através do fomento de operações cibernéticas

transparentes e com alvos específicos. Contudo, mesmo com a mudança para Ações ofensivas unilaterais derivada do governo Trump, os ataques estadunidenses também respingaram em outros Estados - vide o comprometimento ao *Yandex* de 2019 -, marcando que o interesse ofensivo não se concentra estritamente em alvos postos como oponentes.

Averigua-se também a presença de acordos defensivos bi ou multilaterais realizados com oponentes no recorte temporal escolhido. Através das pontuações realizadas na seção 3.1 e no apêndice E, dez tratados foram subscritos entre os Estados Unidos, Rússia e China, tendo três deles sido realizados durante o governo Trump.

Isso indica que os interesses voltados ao poder realizados pelos Estados Unidos não foram estabelecidos de forma totalmente pragmática, de forma a somente ampliar ou reduzir os escopos estabelecidos de caracterização para alcançar seus objetivos. Seja na forma de ataques contra aliados nesse período ou na criação de compromissos pacíficos contra oponentes - que foram atacados no mesmo ano das convenções assinadas, vale ressaltar. Por conseguinte, devido a essas singularidades, não se pode atestar completamente o elemento (3) da HS3.

Uma vez salientados todos os componentes estabelecidos na hipótese pretendida, é possível determinar uma resposta ao questionamento central desta dissertação. Segundo os dados e as análises realizadas, os Estados Unidos, entre 2010 a 2020, amplificaram o uso de capacidades cibernéticas ofensivas e defensivas. Tal crescimento, presente nas Ações, qualidade dos ataques realizados e nas assinaturas de acordos, no entanto, não se manteve nos anos finais do recorte, ao contrário do âmbito orçamentário, que apresentou um crescimento sólido nesses 11 anos.

Apesar disso, os governos dos EUA obtiveram poder no âmbito cibernético a partir dos parâmetros de Nye (2010). Baseados principalmente nos Motivos relacionados a poder de Kremer e Müller (2013) e nos elementos que os compõem, tal Estado se utilizou do ciberespaço como um possibilitador de vantagens favoráveis a si, garantindo poder em uma escala interna e externa do contexto cibernético, empregando de suas capacidades ofensivas e defensivas para esse propósito. A partir desses atos, foi comprovado que as presidências dos Estados Unidos não projetaram poder apenas aos Estados caracterizados como oponentes conforme pontuado em seus documentos oficiais, pois ampliaram a escala ofensiva a seus aliados e defensiva a seus oponentes.

Dessa forma, ao comparar a resposta obtida com as hipóteses gerais e secundárias produzidas, conclui-se uma validação parcial. Isso acontece visto que certas especificidades e

proporções dos atos estadunidenses não foram considerados, diferenciando, mesmo que pouco, a resposta final investigada ao seguir os contextos e os recortes escolhidos.

Posto isso, é importante destacar que, ao realizar tais atos contra o Sistema Internacional Cibernético e aos atores presentes nele, os Estados Unidos e seus governos criaram e progrediram o pensamento do dilema de segurança de Jervis (1978) no espaço cibernético. Ao realizar essa movimentação, foi permitido que outros atos cibernéticos ofensivos pudessem ser fomentados no *cyber* espaço, produzindo escalas maiores e mais constantes de dano nas infraestruturas críticas dos agentes do SI. Elemento utilizado pelos Estados Unidos e suas administrações a fim de perpetuar seus atos de autodefesa no âmbito cibernético.

Por fim, esta dissertação, através de um estudo preciso acerca das capacidades cibernéticas estatais, conseguiu estabelecer associações teóricas tradicionais das Relações Internacionais com o pensamento acerca do poder ante ao domínio cibernético. Essa conexão, admitida nas premissas de Nye (2010), aumenta o escopo analítico em um caráter positivista, trazendo novas perspectivas sobre o uso da temática de cibersegurança nos estudos futuros.

Destaca-se que, dada a orientação específica existente na produção dessa pesquisa, certas nuances, casos, consequências e padrões não conseguiram ser incorporados ao estudo. Isso cria pendências e questionamentos que não conseguem ser respondidos com os dados e as teorias utilizadas, a contar de exemplo a carência de explicação acerca da lacuna existente no ano de 2018 em relação aos padrões estipulados. Elemento que cria perguntas e pontos de discussão a serem replicadas em pesquisas subsequentes, realizadas até mesmo por outros pesquisadores da área.

A cibersegurança foi, e ainda é, um elemento transformador nos atos e percepções dos atores do Sistema Internacional. Graças ao desenvolvimento tecnológico acelerado, novas perspectivas, temáticas e desafios são colocados nas pautas existentes. Pontos que fazem com que os agentes, principalmente os Estados, se adequem e usem da tecnologia e das teorias vinculadas a ele ao seu favor, integrando-os às suas capacidades.

O problema surge quando as movimentações decorrentes criam rupturas e disputas no espaço cibernético, gerando novas viabilidades de destruição, interação e busca por poder nesse âmbito. Unido ao fato de que existem novas tecnologias da qual ainda não se sabe as limitações, como a Inteligência Artificial (IA), há uma maior facilidade do uso desses recursos em atos cada vez mais acessíveis e destrutivos no Sistema. Com isso, é trazido, mais uma vez, a importância do pensamento cibernético unido ao estudo das Relações Internacionais como forma de entender e analisar como essas integrações conseguem produzir resultados materiais

dos atos, seja de poder ou não, no ciberespaço, um domínio recente, mas ainda cheio de possibilidades.

REFERÊNCIAS

ACTON, James M. Cyber Warfare & Inadvertent Escalation. **Daedalus**, v. 149, n. 2, p. 133-149, abr. 2020. MIT Press - Journals. http://dx.doi.org/10.1162/daed_a_01794.

ALAM, Shahid. **Cybersecurity**: past, present and future. 2022. Disponível em: https://arxiv.org/ftp/arxiv/papers/2207/2207.01227.pdf. Acesso em: 07 set. 2023.

ALI, Idrees; STEWART, Phil. **Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack**. 2019. Disponível em: https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-say-idUSKBN1WV0EK/. Acesso em: 16 maio 2024.

AMORETTI, Francesco and FRACCHIOLLA, Domenico, **The Cyber Security Policy of the USA under the Obama Administration**: A Case Study of a Constituent Policy (November 15, 2018). GigaNet: Global Internet Governance Academic Network, Annual Symposium 2018.

AYRES PINTO, Danielle Jacon . Segurança e Defesa Cibernética: Desafios e Perspectivas para os países da América do Sul. In: **6º Encontro da Associação Brasileira de Relações Internacionais - ABRI, 2017**, Belo Horizonte. Anais Complementares, 2017. p. 1-15.

BAHRAMI, P. N. et al. Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. **Journal of Information Processing Systems**, v. 15, n. 4, p. 865–889, 31 ago. 2019.

BARNES, J. E. U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. **The New York Times**, 23 out. 2018.

BARNES, J. E.; GIBBONS-NEFF, T. U.S. Carried Out Cyberattacks on Iran. **The New York Times**, 22 jun. 2019.

BELLOVIN, Steven M. , LANDAU, Susan and LIN, Herbert S. , "**Limiting the undesired impact of cyber weapons: technical requirements and policy implications**", Journal of Cybersecurity, 3:1 (2017)59–68.

BING, Christopher; STUBBS, Jack; MENN, Joseph. **Western intelligence hacked 'Russia's Google' Yandex to spy on accounts**. 2019. Disponível em: https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources-idUSKCN1TS2SX/. Acesso em: 17 maio 2024.

BOLTON, J. R. **The room where it happened**: A white house memoir. 2020. Simon & Schuster.

BRAGA, Nathalia Rocha Carneiro Ferraz. **PERSPECTIVAS POSITIVISTAS E PÓS POSITIVISTAS NAS RELAÇÕES INTERNACIONAIS**: as divergências epistemológicas levariam a distinções em seu modo de fazer ciência?. Rio de janeiro: Pólemos, 2013.

BRÂNDA, Oana-Elena. Changes in the American Foreign Policy: from Obama to Trump. **International Conference Knowledge-Based Organization**, 2018, v. 24, n. 2, p. 160-165. Walter de Gruyter GmbH. http://dx.doi.org/10.1515/kbo-2018-0083.

BRASIL. **DOUTRINA MILITAR DE DEFESA CIBERNÉTICA**. Ministério da Defesa 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 12 Nov. 2021.

BRASIL. Decreto n° 9.573. **Política Nacional de Segurança de Infraestruturas Críticas**. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 13 jan. 2024.

BRASIL. Portaria Nº 5.081. **Doutrina Militar de Defesa Cibernética**. 2023. Edição 203. Seção: 1. p 1-12, 16 Out. 2023.

BURTON, Joe. NATO's cyber defence: strategic challenges and institutional adaptation. **Defence Studies**, v. 15, n. 4, p.297-319, 2 out. 2015. Informa UK Limited. http://dx.doi.org/10.1080/14702436.2015.1108108.

BUSTELO, Rubén Vega. **O PROCESSO DO MANUAL DE TALLINN E A EVOLUÇÃO DA ESTRATÉGIA DE DISSUASÃO NO CIBERESPAÇO**. 2019. 178 f. Tese (Doutorado) - Departamento de Estudos Pós-Graduados, Instituto Universitário Militar, Portugal, 2019.

CFR. **Cyber Operations Tracker**. 2024. Disponível em: https://www.cfr.org/cyber-operations/. Acesso em: 25 abr. 2023.

CISA. **CISA GLOBAL:** Cybersecurity and Infrastructure Security Agency**.** 2021, A. Disponível em: https://www.cisa.gov/sites/default/files/publications/CISA%2520Global_2.1.21_508.pdf. Acesso em: 25 maio 2024.

CISA. **CYBERSECURITY AND INFRASTRUCTURE SECURITY.** 2021, B. Disponível em: https://www.cisa.gov/sites/default/files/publications/CISA-Factsheet_16-Dec-2021-V4_508.pdf. Acesso em: 26 maio 2024.

CISA. **TrickBot Malware.** 2021, C. Disponível em: https://www.cisa.gov/sites/default/files/publications/AA21-076A-TrickBot_Malware_508_0.pdf. Acesso em: 25 maio 2024.

CISA. **Spyware**. 2024. Disponível em: https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf. Acesso em: 17 abr. 2024.

CLARKE, Richard A. and KNAKE, Robert, **Cyber War**: The Next Threat to National Security and What to Do About It. 2. ed. Nova York: HarperCollins Publishers, 2012.

COMANDO CIBERNÉTICO DOS ESTADOS UNIDOS. **Achieve and Maintain Cyberspace Superiority**: Command Vision for US Cyber Command. 2018. Disponível em:

https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf. Acesso em: 15 maio 2024.

CRAIG, Anthony J.s.; VALERIANO, Brandon. Realism and Cyber Conflict: security in the digital age. In: ORSI, Davide; AVGUSTIN, J. R.; NURNUS, Max. **Realism in Practice**: an appraisal. [S.I]: E-International Relations Publishing, 2018. p. 85-101. Disponível em: https://www.e-ir.info/wp-content/uploads/2018/01/Realism-in-Practice-E-IR.pdf#page=100 . Acesso em: 01 Dez. 2021

CRS. **Membership of the 116th Congress**: a profile. A Profile. 2020. Disponível em: https://sgp.fas.org/crs/misc/R45583.pdf. Acesso em: 25 set. 2024.

DEVANNY, J. 'Madman Theory' or 'Persistent Engagement'? The Coherence of US Cyber Strategy under Trump. **Journal of Applied Security Research**, v. 17, n. 3, p. 282–309, 2021.

DEYOUNG, K.; NAKASHIMA, E.; RAUHALA, E. Trump signed presidential directive ordering actions to pressure North Korea. **Washington Post**, 2017.

DIAZ, Rogelio Jr. *et al*. **An Overview of IP Addressing**. University Of Makati, Philippines, v. 1, n. 1, p. 1-11, jun. 2022.

DIG. **Comparative Survey of the two UN-based processes on responsible behaviour in cyberspace**. 2021. Disponível em: https://dig.watch/wp-content/uploads/Comparing-GGE-and-OEWG-infografik-November2021-1.pdf. Acesso em: 20 maio 2024.

DIG. **UN OEWG.** 2024. Disponível em: https://dig.watch/processes/un-gge. Acesso em: 21 maio 2024.

DNI. **SPEAR PHISHING AND COMMON CYBER ATTACKS**. 2024. Disponível em: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf. Acesso em: 05 jun. 2024.

DZIWISZ, Dominika; ROMANIUK, Scott N. US Cyber Command (USCYBERCOM). **The Handbook Of Homeland Security.** 1. ed. Boca Raton: CRC Press, p. 305-314. 2023.

ESTADOS UNIDOS DA AMÉRICA. **National Strategy to Secure Cyberspace**. The White House, Office of the Press Secretary, 2003. Disponível em: https://www.energy.gov/ceser/articles/national-strategy-secure-cyberspace-february-2003. Acesso em: 15 Fev. 2024

ESTADOS UNIDOS DA AMÉRICA. **Comprehensive National Cybersecurity Initiative**. Washington: Executive Office of the President of the U.S, 2009 A. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf. Acesso em: 16 Mar. 2024

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 B.

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_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 10 Mar. 2024.

ESTADOS UNIDOS DA AMÉRICA. NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2014. **PUBLIC LAW**, 2014. Disponível em: https://www.congress.gov/113/plaws/publ66/PLAW-113publ66.pdf Acesso em: 26 Abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. "**Fact Sheet**: Department of Defense Cyber Strategy", 2015. Disponível em: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Department_of_Defense_Cyber_Strategy_Fact_Sheetpdf Acesso em: 23 Abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. **Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector**, 2016, A. Disponível em: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged. Acesso em: 23 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. **U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts**. 2016, B. Disponível em: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions. Acesso em: 28 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. **National Security Strategy.** The White House, Office of the Press Secretary, 2017, A. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf. Acesso em: 28. abr. 2024

ESTADOS UNIDOS DA AMÉRICA. **America First**: A Budget Blueprint to Make America Great Again. Washington: Office of Management and Budget, 2017, B.

ESTADOS UNIDOS DA AMÉRICA. **United States of America vs Park Jin Hyok**. 2017, C. Disponível em: https://www.justice.gov/opa/press-release/file/1092091/dl. Acesso em: 01 maio 2024.

ESTADOS UNIDOS DA AMÉRICA. **Summary of the 2018 National Defense Strategy**: Sharpening the American Military's Competitive Edge. Washington: Department of Defense, 2018, A. Disponível em: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. Acesso em: 08 maio 2024.

ESTADOS UNIDOS DA AMÉRICA. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY ACT OF 2018. **PUBLIC LAW 115-278**, 2018, B. Disponível em: https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf. Acesso em: 26 maio 2024

ESTADOS UNIDOS DA AMÉRICA. **US-CERT**:United States Computer Emergency Readiness Team. Washington: Department of Homeland Security, 2024. Disponível em:

https://www.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf. Acesso em: 17 abr. 2024.

FEITOSA, Caio Vinícius Cesar. **ATAQUES CIBERNÉTICOS**: estudo do caso stuxnet. 2017. 60 f. TCC (Doutorado) - Curso de Tecnologia em Sistemas de Computação, Universidade Federal Fluminense, Niterói, 2017. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/5630/TCC_CAIO_VINICIUS_CESAR_FEITOSA.pdf?sequence=1&isAllowed=y. Acesso em: 10 abr. 2024.

FERREIRA, Hugo José Duarte. **Identificação e Caracterização de Infraestruturas Críticas**: uma metodologia: Centro de Investigação e Desenvolvimento, 2017. Disponível em: https://www.ium.pt/s/wp-content/uploads/CIDIUM/Cadernos%20do%20IESM-IUM/Cadernos%20do%20IUM%20N.%C2%BA14%20-%20Identifica%C3%A7%C3%A3o%20e%20Caracteriza%C3%A7%C3%A3o%20de%20Infraestruturas%20Cr%C3%ADticas%20-%20Uma%20Metodologia.pdf. Acesso em: 05 out. 2022.

FISCHERKELLER, Michael P.; HARKNETT, Richard J.. **Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation**. 2018. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1123131.pdf. Acesso em: 23 dez. 2024.

GALLAGHER, Sean. **As US launches DDoS attacks, N. Korea gets more bandwidth—from Russia**. 2017. Disponível em: https://arstechnica.com/information-technology/2017/10/as-us-launches-ddos-attacks-n-korea-gets-more-bandwidth-from-russia/. Acesso em: 25 abr. 2024.

GARDINER, J. **Understanding, Denying and Detecting**. 2014.

GENTILI, A. O direito da guerra. Ijuí: Unijuí, 2005.

GRATÃO, Victor. **Sobre Cyber Segurança**: uma análise das capacidades estadunidenses e chinesas nos anos entre 2007-2017. 2022. Disponível em: https://relacoesexteriores.com.br/sobre-cyber-seguranca/. Acesso em: 30 set. 2022.

GREENBERG, Andy. **US Hackers' Strike on Russian Trolls Sends a Message—but What Kind?** 2019. Disponível em: https://www.wired.com/story/cyber-command-ira-strike-sends-signal/. Acesso em: 16 maio 2024.

GOODIN, Dan. **How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last**. 2015. Disponível em: https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/. Acesso em: 25 abr. 2024.

GOODIN, Dan. **Researchers crack open unusually advanced malware that hid for 5 years**. 2016. Disponível em: https://arstechnica.com/information-technology/2016/08/researchers-crack-open-unusually-advanced-malware-that-hid-for-5-years/. Acesso em: 25 abr. 2024.

HADJI-JANEV, Metodi; BOGDANOSKI, Mitko. Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare. **Advances In Digital Crime, Forensics, And Cyber Terrorism**, v. 1, n. 1, p. 1-548, out. 2016. IGI Global. http://dx.doi.org/10.4018/978-1-4666-8793-6.

HEALEY, J.; JERVIS, R. The escalation inversion and other oddities of situational Cyber Stability. **Texas National Security Review**, Fall, 2020. https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/

HITCHENS, Theresa; GOREN, Nilsu. **International Cybersecurity Information Sharing Agreements**. Maryland: Center For International & Security Studies At Maryland, 2017. Disponível em: https://www.jstor.org/stable/pdf/resrep20426.pdf?refreqid=excelsior%3A52808e0e54b97c414223abe099e94e68. Acesso em: 01 maio 2023.

JENSEN, E. T. **The Tallinn Manual 2.0:** Highlights and Insights. 2017. v. 48.

JERVIS, Robert. **The Logic of Images in International Relations**. Nova Jersey: Princeton University Press, 1970.

JERVIS, Robert. **Cooperation Under the Security Dilemma**. World Politics 30(2): 167–214, 1978.

KASPERSKY. **Gauss**: nation-state cyber-surveillance meets banking trojan. 2012. Disponível em: https://securelist.com/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/33854/. Acesso em: 22 abr. 2024.

KASPERSKY. **THE REGIN PLATFORM**: nation-state ownage of gsm networks. 2014. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf. Acesso em: 25 abr. 2024.

KASPERSKY. **EQUATION GROUP**: questions and answers. 2015. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf. Acesso em: 26 abr. 2024.

KASPERSKY. **THE PROJECT SAURON APT**. 2016. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf. Acesso em: 27 abr. 2024.

KASPERSKY. **Unraveling the Lamberts Toolkit**. 2017. Disponível em: https://securelist.com/unraveling-the-lamberts-toolkit/77990/. Acesso em: 27 abr. 2024.

KLAAR, Heli Tiirmaa. **The Evolution of the UN Group of Governmental Experts on Cyber Issues**. From a Marginal Group to a Major International Security Norm-Setting Body. 2021. Disponível em: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf. Acesso em: 15 abr. 2024.

KREMER, Jan-Frederik; MÜLLER, Benedikt. SAM: a framework to understand emerging challenges to states in an interconnected world. **Cyberspace And International Relations**, p. 41-58, 6 nov. 2013. Springer Berlin Heidelberg. Disponível em: http://dx.doi.org/10.1007/978-3-642-37481-4_3. Acesso em: 10 set. 2023.

KUEHL, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., **Cyberpower and National Security** (Washington, D.C.: National Defense UP, 2009).

LIBICKI, Martin C.. **Conquest in Cyberspace**: national security and information warfare. Nova York: Cambridge University Press, 2007.

LIBICKI, Martin C. "Norms and Normalization." **The Cyber Defense Review**, vol. 5, no. 1, 2020, pp. 41–54. *JSTOR*, https://www.jstor.org/stable/26902662. Acesso em: 24 Dez. 2024.

LIMA, Victor Hugo Gratão de. **As Ações dos Estados Unidos e China no Espaço Virtual**: uma análise do cenário de cyber segurança no período de 2007 a 2017. 2019. 78 f. TCC (Graduação) - Curso de Relações Internacionais, Universidade Católica de Brasília, Brasília, 2019. Disponível em: https://repositorio.ucb.br:9443/jspui/handle/123456789/12821 . Acesso em: 25 Out. 2021.

LIN, H., 2012. Escalation dynamics and conflict termination in cyberspace. S**trategic studies quarterly**, 6 (3), 46–70.

LINDSAY, Jon R.. *"***The Impact of China on Cybersecurity: Fiction and Friction***." Quarterly Journal: International Security*, vol. 39. no. 3. (Winter 2014/15): 7-47.

LOPES, Gills Vilar. **Relações internacionais cibernéticas (CiberRI)**: uma defesa acadêmica a partir dos estudos de segurança internacional. 2016. 165 f. Tese (Doutorado) - Curso de Pós graduação em Ciência Política, Departamento de CiênciaPolítica, Universidade Federal de Pernambuco, Pernambuco, 2016. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/20723/1/GillsVilarLopes-Tese-CiberRI-PPGCP-UFPE%20%281%29.pdf. Acesso em: 20 de abril de 2023.

MAIER, Friedrich. DE OBAMA A TRUMP: o contínuo da política cibernética estadunidense. **Caderno de Relações Internacionais**, v. 10, n. 18, p. 109-138, 3 set. 2019. Faculdade Damas da Instrução Cristã. http://dx.doi.org/10.22293/2179-1376.v10i18.1034.

MASTANDUNO, Michael; LAKE, David A.; IKENBERRY, G. John. Toward a Realist Theory of State Action. **International Studies Quarterly**, v. 33, n. 4, p. 457, dez. 1989. Oxford University Press (OUP). http://dx.doi.org/10.2307/2600522.

MORAIS, Carlos Tadeu Queiroz de. LIMA, José Valdeni de. FRANCO, Sérgio Roberto Kieling. **Conceitos sobre Internet e Web**. Porto Alegre: Ed. Da UFRGS, 2012. 112 p.

NAKASHIMA, E. Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election. **Washington Post**, 10 out. 2020.

NAKASONE, P. M. A cyber force for Persistent Operations. 2019. **Joint Force Quarterly**, 92(1),

NELSON, S., John Bolton is warning about offensive cyberattacks under a new Trump policy, 09.21.2018, **Business Insider**, https://www.businessinsider.com/john-bolton-warns-ofoffensive-cyberattacks-under-a-new-trump-policy-2018-9?IR=T,.

NYE, Joseph S.. **Cyber Power**. Belfer Center For Science And International Affairs, 2010. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. Acesso em: 17 maio 2023.

NYE, J. S. (2011). Nuclear Lessons for Cyber Security? **Strategic Studies Quarterly (Winter)**: 18– 38.

OTAN. **DEFENCE AND SECURITY COMMITTEE**. 2017. Disponível em: https://www.nato-pa.int/download-file?filename=/sites/default/files/2017-11/2017%20-%20163%20DSCTC%2017%20E%20rev%201%20fin%20-%20EU%20AND%20NATO%20COOPERATION%20-%20MESTERHAZY%20REPORT.pdf. Acesso em: 02 maio 2024.

OTAN. **Cyber defence**. 2024. Disponível em: https://www.nato.int/cps/en/natohq/topics_78170.htm. Acesso em: 02 maio 2024.

PALACIOS JUNIOR, Alberto Montoya Correa. As guerras preventivas e o direito internacional. In: PALACIOS JUNIOR, Alberto Montoya Correa. **As Teorias das Guerras Preventivas e as Relações Internacionais**. São Paulo: Unesp, 2011. p. 1-197. Disponível em: https://repositorio.unesp.br/server/api/core/bitstreams/d23c9460-eab5-4595-9c3a-ba19653cc98b/content. Acesso em: 18 set. 2024.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do Trabalho Científico:**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Universidade Feevale, 2013. 277 p. Disponível em: https://www.feevale.br/Comum/midias/0163c988-1f5d-496f-b118-a6e009a7a2f9/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf. Acesso em: 03 out. 2022.

RAIFFA, Howard. **The Art and Science of Negotiation**. 12. ed. Cambridge: The Belknap Press Of Harvard University Press, 1994.

REUTERS. **U.S. cyber attacks on Iranian targets not successful, Iran minister says**. 2019. Disponível em: https://www.reuters.com/article/us-mideast-iran-usa-cyber-idUSKCN1TP0B1/?utm_campaign=trueAnthem%3A+Trending+Content&utm_content=5d10beeeb35fc8000145c351&utm_medium=trueAnthem&utm_source=twitter. Acesso em: 17 maio 2024.

ROBINSON, M.; JONES, K.; JANICKE, H. Cyber warfare: Issues and challenges. **Computers & Security**, v. 49, p. 70–94, mar. 2015.

ROGERS, Michael S.. **Foreign cyber threats to the United States**. 2017. Disponível em: https://svobodneslovo.com/akl/Clapper-Lettre-Rogers_01-05-16.pdf. Acesso em: 21 nov. 2023.

ROLLINS, J. and WILSON, C. **Terrorist capabilities for cyberattack**: overview and policy issues. Congressional Research Service. 2007. Disponível em: http://www.fas.org/sgp/crs/terror/ RL33123.pdf . Acesso em 27 Mar. 2023.

ROMANOSKY, Sasha; GOLDMAN, Zachary. Cyber Collateral Damage. **Procedia Computer Science**, v. 95, p. 10-17, 2017. Elsevier BV. http://dx.doi.org/10.1016/j.procs.2016.09.287.

SANGER, David E.. **Confront and Conceal**: Obama's secret wars and surprising use of American power. Nova York: Crown Publishers, 2012.

SANGER, D. E. U.S. Cyberattacks Target ISIS in a New Line of Combat. **The New York Times**, 24 abr. 2016.

SANGER, D. E.; BROAD, W. J. Trump Inherits a Secret Cyberwar Against North Korean Missiles. **The New York Times**, 4 mar. 2017.

SCHMITT, Michael. **The Sixth United Nations GGE and International Law in Cyberspace**. 2021. Disponível em: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/. Acesso em: 28 abr. 2024.

SIDDIQI, Murtaza A. Critical Analysis on Advanced Persistent Threats. **International Journal of Computer Applications**, v. 141, n. 13, p. 46–50, 17 maio 2016.

SIMOIU, C. et al. **“I was told to buy a software or lose my computer. I ignored it”**: A study of ransomware. USENIX Symposium on Usable Privacy and Security (SOUPS). 2019. Disponível em: https://www.5harad.com/papers/ransomware.pdf. Acesso em: 28 maio 2024.

SMEETS, Max. **U.S. Cyber Strategy of Persistent Engagement & Defend Forward**: implications for the alliance and intelligence collection. Implications for the Alliance and Intelligence Collection. 2020. Disponível em: https://osf.io/t37bc/download. Acesso em: 23 dez. 2024.

SMEETS, Max; LIN, Herbert S.. Offensive Cyber Capabilities: to what ends?. In: International Conference on Cyber Conflict, 10., 2018, Tallinn. **Offensive Cyber Capabilities: To What Ends?.** Tallinn: Nato Ccd Coe Publications, 2018. p. 1-18. Disponível em: https://ccdcoe.org/uploads/2018/10/Art-03-Offensive-Cyber-Capabilities.-To-What-Ends.pdf. Acesso em: 01 out. 2022.

THE WHITE HOUSE. **President Trump Protects America's CYBER Infrastructure**. Office of the Press Secretary, 12 de maio de 2017.

THIESSEN, M. A. Trump confirms, in an interview, a U.S. cyberattack on Russia. **Washington Post**, 11 jul. 2020.

THOMAS, R. J. **Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures**. Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy. **Anais**... Em: CCS ’20: 2020 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. Virtual Event USA: ACM, 9 nov. 2020. Disponível em: <https://dl.acm.org/doi/10.1145/3411498.3419970>. Acesso em: 18 abril. 2024

USAID. **MEMORANDUM OF UNDERSTANDING**. 2024. Disponível em: https://www.usaid.gov/sites/default/files/2022-05/MOU_Overview_Guidance_9.15.20.pdf. Acesso em: 16 abr. 2024.

VALERIANO, Brandon; MANESS, Ryan C.. **Cyber War Versus Cyber Realities**: cyber conflict in the international system. Nova York: Oxford University Press, 2015. 259 p.

VALERIANO, Brandon; MANESS, Ryan C.. International Relations Theory and Cyber Security. **Oxford Handbooks Online**, v. 1, n. 1, p.259-272, 5 abr. 2018. Oxford University Press. http://dx.doi.org/10.1093/oxfordhb/9780198746928.013.19.

YANG, Haomiao et al. A comprehensive overview of backdoor attacks in large language models within communication networks. **IEEE Network**, 2023

ZETTER, Kim. **Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload**. 2012. Disponível em: https://www.wired.com/2012/08/gauss-espionage-tool/. Acesso em: 23 abr. 2024.

ZETTER, K. **Countdown to Zero Day**: Stuxnet and the Launch of the World's First Digital Weapon. 2014. Nova York: Crown Publications.