Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Relações Internacionais

FERNANDA MARQUES ALVES

ESPAÇO CIBERNÉTICO: Desafios para a sua regulamentação e seu impacto sobre a relação de poder entre Estados Soberanos

BRASÍLIA
2021

FERNANDA MARQUES ALVES

ESPAÇO CIBERNÉTICO: Desafios para a sua regulamentação e seu impacto sobre a relação de poder entre Estados Soberanos

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Prof. Msc. Lucas Soares Portela.

BRASÍLIA
2021

FERNANDA MARQUES ALVES

ESPAÇO CIBERNÉTICO: Desafios para a sua regulamentação e seu impacto sobre a relação de poder entre Estados Soberanos

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Prof. Msc. Lucas Soares Portela.

BRASÍLIA, 19 DE OUTUBRO DE 2021

BANCA AVALIADORA

_____

Lucas Soares Portela

_____

Oscar Medeiros Filho

Dedico à minha família que sempre me apoiou durantes todos esses anos e sem eles não estaria aqui.

AGRADECIMENTOS

Chegou ao fim um ciclo de muitas risadas, choro, felicidade e frustrações. Sendo assim, dedico este trabalho a todos que fizeram parte desta etapa da minha vida.

Em primeiro lugar, a Deus, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Aos meus pais, pelo amor, incentivo e apoio incondicional. Agradeço a minha mãe, por sempre me dar apoio e incentivo nas horas difíceis, de desânimo e cansaço. Ao meu pai que apesar de todas as dificuldades me fortaleceu e que foi muito importante para mim. A minha irmã Ana Beatriz, que não só me apoiou durante esses anos, como me ajudou em trabalhos da faculdade quando eu já não sabia mais o que fazer, me dando forças quando eu não tinha nem isso para continuar. Ao meu namorado Rodrigo, pelos seis anos ao meu lado, me apoiando e me incentivando sempre para que eu busque todos os meus sonhos e depois desse tempo nunca me abandonou.

Agradeço a todos amigos, colegas de classe que estiveram comigo nesta caminhada que de alguma forma me deu força e ânimo para continuar. E a todos os professores por me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender. Ao professor Ms. Lucas Portela, pela orientação, apoio, paciência e confiança durante a elaboração deste trabalho, que me ajudou tanto.

RESUMO

Esta monografia tem como objetivo analisar o espaço cibernético e quais são os desafios referentes à sua regulamentação e qual o impacto com a relação de poder entre os Estados soberanos, além de suas vulnerabilidades neste campo, pensando nos impactos de atores não estatais no jogo do cyberespaço. Os Estados tentam estabelecer uma relação entre si nesse meio, porém, as diversas formas de poderes existentes se projetam neste ambiente trazendo concorrência e disputas. Para entender os desafios do espaço cibernético, os Estados fazem estudos, tornando assim evidente seus principais propósitos na área, como o poder e sua sobrevivência. No mundo atual da globalização, o espaço cibernético está presente de todas as formas, com isso a informação é uma grande fonte de poder neste meio.

Palavras-chave: Desafios; Estados; Poder; Regulamentação

ABSTRACT

This monograph aims to analyze cyberspace and what are the challenges related to its regulation and what is the impact on the power relationship between sovereign states, in addition to their vulnerabilities in this field, thinking about the impacts of non-state actors in the cyberspace game. States try to establish a relationship between themselves in this environment, but the various forms of existing powers are projected in this environment bringing competition and disputes. To understand the vulnerabilities of cyberspace, states study, thus making evident their main purposes in the area as power and its survival. In today's world of globalization, cyberspace is present in every way, with this information is a great source of power in this environment.

Keywords: Challenges; States; Power; Regulation.

SUMÁRIO

INTRODUÇÃO

Este trabalho de pesquisa mostrará a forma como o cyberpower influência na Soberania de um Estado, se tornando vulnerável no espaço cibernético. Trazendo a história da criação do ciberespaço, a partir da ARPANET até o momento das criações das organizações internacionais que regulam este espaço e o avanço tecnológico. A evolução deste espaço, passa das barreiras virtuais e se transformam em como os Estados reagiram aos poderes entre eles no ciberespaço.

A presente monografia argumenta em que medida é possível regulamentar o espaço cibernético e como tem impacto na relação de poder entre Estados Soberanos, trazendo as os aspectos de atores e ameaças cibernéticas na segurança de um Estado e será analisado pelo olhar realista e o pressuposto da distribuição de capacidades materiais de poder, onde os Estados agem e reagem de forma contínua numa lógica de concentração de poder, contudo, sendo interdependentes e criando relações entre si. O embasamento teórico deste trabalho será composto por autores de artigos e livros, como Morgenthau com seu estudo sobre o realismo; Nye Jr com a premissa do cyberpower e a capacidade que os Estados têm ao falar de domínio cibernético. A justificativa científica para a realização deste trabalho é a relevância de estudos nesta área, para as Relações Internacionais e para entender tantos ataques e acusações que acontecem entre os Estados. O objetivo geral é fazer uma análise sobre esta área da sociedade cultural e política sobre conflitos no espaço cibernético e como eles podem impactar na vida real.

A presente pesquisa pode ser caracterizada enquanto seu recorte metodológico com natureza descritiva, explicativa e exploratória quanto aos fins, utilizando-se o método dedutivo. Com base nas discussões teóricas por esses procedimentos metodológicos, este trabalho está estruturado por meio de lógica dedutiva em três capítulos, partindo de conceitos, até análise de como está no atual momento. A base deste trabalho conta com fontes primárias (reportagens em jornais) e fontes secundárias (artigos e textos acadêmicos).

No primeiro capítulo é apresentado os conceitos de ciberespaço, trazendo a história da sua criação como ponto de explicação para a palavra espaço cibernético demonstrando as formas de estrutura deste espaço como os elementos tangíveis e intangíveis que formam a interação entre o espaço virtual e físico, em que é dividida em quatros fases dentro de um sistema de funcionamento, até suas características são apontadas, além de sua estrutura. Passando para o entendimento sobre os atores que consiste nesta área e como são usados e como usarão deste espaço para possivelmente prejudicar, hackear ou fazer algum ataque cibernético

mais perigoso, no qual podemos dividir eles em três categorias (Governos, organizações internacionais e os indivíduos). E finalmente ao final deste capítulo será estudado as ameaças que podem ser identificadas no ciberespaço que são causadas pela baixa regulamentação deste espaço.

No segundo capítulo, é apresentado o poder cibernético em que se utiliza de recursos de informações, em que depende de recursos de ambiente lógico, físico e híbrido. Questionando a informação como um recurso de poder no espaço cibernético, trazendo a relação entre governo e seus cidadãos e como pode mudar tornar uma forma de estreitar os laços e modernizar através de regulamentações, que traz consigo a facilidade de acessos de atores as informações lhe dando poder, no qual pode ser chamada de difusão de poder. Trazendo os aparatos teóricos das Relações internacionais, como a óptica liberal e a óptica realista para entender o conceito de poder e como é a sua relação com o espaço cibernético. Enquanto no final do capítulo, nos aprofundamentos em cada método de poder que existe e como eles são formas de poder expressas nas relações com a hegemonia.

No último capítulo são apresentadas as relações entre os Estados dentro do ciberespaço, como a configuração das relações internacionais neste espaço e como as empresas, organismos internacionais regulam e trazem segurança ao espaço cibernético. Como a relação entre grandes potências são muitas vezes frágeis por conta de cada meio que eles impõem poder sobre o outro para tentar se manter com vantagens e por último, os atores não estatais no novo jogo do cyberespaço, em que é discutido como a constante disputa de poder neste espaço é só mais um local para essa corrida com suas tecnologias. Visualizando constantes demonstrações de forças e ameaças entre grandes nações como China, EUA e Rússia.

1 CIBERESPAÇO: Funcionamento e Estrutura

Ciberespaço é um conceito muito complexo e difícil de explicar, principalmente por parecer bastante abstrato. Pensar também em ciberespaço como um conceito de internet é complicado, pois é uma coisa maior que só a internet. Muitos autores ainda divergem sobre o conceito de ciberespaço, por ser algo novo e intangível, porém, a conexão de várias redes de computadores, as relações de sistemas de redes, parte estrutural e tudo que ajuda na transmissão de informações, são fato para todos e não tão intangíveis como se pensa.

1.1 Conceituando o Ciberespaço

A palavra ciberespaço surgiu no final do século XX depois da criação da ARPANET, a primeira rede de comunicação entre computadores. Com a evolução tecnológica, mudanças estruturais e dinâmicas, como a subjetividade de uma dimensão ou fronteira também acompanharam o conceito. Assim, ocorre a chegada da tecnologia cibernética não limitada a sistemas e redes de computadores, mas também pensada na infraestrutura física de Tecnologias de Informação e Comunicação (TICs). Estes dois unidos, elementos intangíveis e tangíveis, formam o conceito de cyberespaço e passa a ser uma interação virtual da relação entre desenvolvimento cibernético e segurança internacional.

Maziero e Pinto (2019) descreve o conceito de espaço cibernético como algo que evolui de acordo com o tempo, mas sem definição unânime. Há duas implicações importantes que devem ser ressaltadas. A primeira é que diferentemente dos outros domínios o espaço cibernético é o único refém do indivíduo em dois momentos, pois depende da tecnologia inventada pelo ser-humano para existir e os acontecimentos que se passam dentro dele também dependem exclusivamente do indivíduo. E a segunda implicação é sobre os efeitos das ações realizadas dentro do espaço cibernético, pois elas podem sim ter efeitos fora deste domínio, sejam eles causados diretamente ou indiretamente. (DEMCHAK; DOMBROWSKI, 2011)

As interações entre elementos virtuais e físicos do espaço cibernético podem ser divididas em quatro fases de um sistema. Sendo a primeira a arquitetura e a rede global, a segunda são as comunidades que estão por desenvolver a rede e onde o Estado deve regular o que aparece nas suas fronteiras, a terceira é o período que os Estados começam a abordagem de

controle e a quarta, a regulamentação imposta para enfrentar respostas dos cidadãos, tornando assim o Estado responsáveis pelas estratégias de segurança cibernética e controle no ciberespaço. (PATINÕ, 2019, p.169)

Essas quatro fases criam o ambiente em que a informação se propaga. De acordo com Galvão (2018), com esse espaço de informação foi possível a criação de novas cadeias inter-relacionais, inovando as interações econômicas, políticas, sociais e ampliando o tráfego de informações. O que possibilita o acesso ao ciberespaço é uma interface física (*hardware*) e é também o que viabiliza a utilização dos programas (*softwares*):

> O ciberespaço pode ser visto como um ambiente operacional onde os seres humanos atuam com o propósito de atingir objetivos específicos, não diferindo muito, nesse ponto, dos outros quatro domínios físicos relacionados aos estudos de defesa: terra, mar, ar e espaço sideral. (MESQUITA, 2019, p.10)

Com esse pensamento de Mesquita, temos alguns desafios em torno da consolidação do ciberespaço nas relações internacionais como a temporalidade, espaço geográfico, permeação, fluidez, participação, atribuição e *Accountability*. Tais elementos podem ser visualizados abaixo:

Quadro 1 – Características do espaço cibernético

Características	**Significância**
Temporalidade	Modifica a nossa noção de tempo, a torna mais instantânea, devido a velocidade da troca de informação;
Fisicalidade	Através do espaço cibernético é possível ultrapassar as barreiras geográficas sem sair do seu local;
Permeação	É possível se infiltrar em fronteiras e jurisdições;
Fluidez	Está em constante alteração;
Participação	Devido ao fato de aumentar a possibilidade de ativismos políticos;
Atribuição	Em alguns casos, como a Dark Web, é difícil identificar os atores responsáveis;
Responsabilidade	Conectada, especialmente, com a sexta característica, devido à dificuldade, em alguns casos, de conectar o crime com o responsável, possibilita evitar mecanismos de responsabilidade.

Fonte: Arthur C. Maziero e Danielle J. Ayres Pinto, 2018.

Ao entendermos cada uma delas de forma individual conseguimos conceituar esses desafios. Temporalidade seria como uma alteração da noção convencional de tempo para quase uma instantaneidade, o espaço geográfico é a atividade cibernética que transcende as limitações geográficas e localização física, a permeação é o ciberespaço penetrando nas fronteiras e jurisdições, a fluidez promove e sustenta mudanças persistentes e reconfigurações, a participação reduz as barreiras para o ativismo e expressões políticas, a atribuição encobre identidades dos atores e das conexões, e por fim, a *Accountability* supera os mecanismos de responsabilização estabelecidos.

Apesar das tentativas anteriores, o conceito de ciberespaço ainda é uma incógnita, em especial pela ausência de um consenso entre os pesquisadores desse ambiente. Dessa forma, os autores ainda divergem em vários pontos, mas podemos dizer que internet e ciberespaço não são as mesmas coisas mesmo que as características apresentem uma posição que pode afetar o status quo político e estratégico, causado pela inexistência de fronteiras definidas, que facilita por vezes o anonimato das pessoas.

Podemos dizer que o ciberespaço funciona por conta de vários fatores envolvidos como cabos de fibra ótica, que ajuda no funcionamento das redes, o *hardware*[1], *software* [2]e o *peopleware*[3], também são meios para que espaço cibernético funcione direito, contudo ainda precisamos de uma regulamentação dos Estados, pois existem várias ameaças no meio cibernético.

Então, o ciberespaço permeia também o espaço físico, mas não podemos limitá-lo a um único local, até porque ele é transversal aos demais espaços, como o terrestre, marítimo, aéreo e espaço externo. Por isso, caso haja qualquer evento ocorrido neste domínio não pode ser considerado como virtual apenas, ele é parte do universo cibernético em que a vida política se estrutura, sendo uma realidade que interage cada vez mais com eventos que estão além de sua existência. Isso porque está presente em todas as redes de computadores do mundo e em cada coisa que está conectado a ele. O ciberespaço é virtual, mas não apenas isso.

Contudo, é um ambiente próprio que reside em redes feitas para o uso eletrônico e do eletromagnetismo para criar, armazenar, modificar, transferir e explorar informação por meio

[1] Conjunto de equipamentos físicos.
[2] Dimensão virtual com programas, sistemas, aplicativos e informações.
[3] Camada cognitiva de usuários.

de canais interdependentes e interconectados, utilizando as tecnologias de informação e comunicação. Mas também é um local no qual os seres humanos usam para alcançar objetivos específicos próprios, podendo virar uma zona de guerra em que batalhas poderão acontecer, muitas vezes baseadas em pensamentos políticos opostos ao Estado.

Assim, o espaço cibernético consiste em um sistema, desde os *hardwares* e *softwares*, passando pelos cabos de fibra óticas, satélite, serviços, códigos, imagens, vídeos, atores, usuários, hackers, entidades estatais, engenheiros da área. Organizações internacionais em vários graus de poder e infraestrutura e todas essas camadas e funções são de grande relevância para as relações internacionais e o sistema cibernético, que cada vez mais se tornam interligados.

1.2 Definir atores do ciberespaço

Ao estudarmos ciberespaço, conseguimos conhecer os atores responsáveis na área. Existe os atores não estatais, os estatais, cibercidadãos, ativistas, hackers. Acredita-se que esses atores tenham poderes no espaço cibernético, contudo, por mais que os Estados entendam o poder que possuem para se proteger, seus espaços ainda são vulneráveis aos atores não estatais, trazendo a guerra cibernética para estes locais. Ademais, como os atores buscam o anonimato, graças ao cyberespaço, os estragos causados são grandes e pode afetar do comércio a área de segurança.

Os atores não estatais, são responsáveis pelo maior número de ataques cibernéticos que existe, causado por fins ideológicos ou criminosos, contudo, eles não têm as mesmas capacidades de grandes governos. Ao tentar se proteger, os Estados começaram a criar meios de ciberdefesa e cibersegurança. Alguns autores como Gartzke (2013) acreditam que a participação de atores não estatais é parte de uma estratégia de retaliação. O que traz várias discussões sobre os atores e seus papéis, em especial como uma ameaça ou uma ajuda, já que não há um meio de regulamentar a atuação deles.

Mesquita (2019) traz o papel dos atores no ciberespaço, onde os não estatais possuem substancial relevância, quando um grande número de atores possui um papel importante no ciberespaço. Assim, divide-se os atores em três categorias: sendo o primeiro, os governos, o

segundo são as organizações com redes altamente estruturadas e por último, são os indivíduos e redes fracamente estruturados.

Na política internacional, as organizações são políticas, ideológicas ou culturais. Existem inúmeros atuantes relevantes no ciberespaço como os Estados, indivíduos, grupos ativistas, empresas privadas, criminosos ou terroristas. Os maiores problemas são os vetores políticos e estratégicos envolvidos por esses atores, onde se tenta moldar os comportamentos deles. No caso dos atores estatais, podemos dizer que a maior vontade é a "competição armamentista", quando eles estão atualizando ou comprando arsenal militar, mesmo pequenas aquisições são vistas como uma competição, sendo o medo uma das maiores formas de consequência da exibição de poder, e da pressão externa e interna, porém nem todo Estado tem capacidade de se proteger nessa corrida armamentista.

Para entender a função desses atuantes, Gonzales e Portela (2018) mostram que temos o espaço geográfico cibernético e esse espaço é controlado pelos atores mais aptos, mesmo que na teoria seja um ambiente global e comum. Os atores surgem junto a difusão de poder causada pelo ciberespaço, o chamado *cyberpower,* que demonstra o número de atores e a baixa diferença de poder entre eles, podemos dizer que o Estado é o maior atuante no espaço cibernético. Estes atores são treinados, no geral, para atacarem, defenderem e espionarem.

Por fim, cabe ressaltar que os atores são fundamentais para o funcionamento do espaço cibernético, dependendo de seus papéis no processo cibernético, eles podem ser usados por empresas e Estados. Os problemas desenvolvidos pelo *cyberpower* ao tentarem se proteger, são mantidos com a cooperação entre organizações, Estados e empresas.

1.3 Identificar ameaças cibernéticas

Existem várias ameaças no espaço cibernético, causadas pela baixa regulamentação e pela possibilidade de anonimato criado com esse "mundo". Alguns dos maiores problemas das ameaças cibernéticas são a imprecisão das fronteiras, a participação de atores não estatais, dificuldades de estabelecer uma ciberdefesa e a dificuldade de prever um ataque cibernético.

Com isso, podemos tentar estabelecer algumas ameaças que aparecem no ciberespaço como Ciberguerra, Ciberterrorismo, ciberespionagem, Ataques Cibernéticos, hacktivismo e

Cibercrime. Apesar de acharmos que são vários nomes para o mesmo problema, eles são bem diferentes, mas dividem as ferramentas, tecnologias e objetivos em comum.

A Ciberguerra, é um dos maiores problemas do espaço cibernético, apesar de ser difícil de conceituar e de ser provado. Contudo, pela ausência de tratamento sobre a guerra no espaço cibernético, na carta da ONU, ela é considerada dentro do conceito de guerra convencional, dando liberdade aos Estados para se protegerem trazendo do conceito tradicional de guerra que envolve, essencialmente, alguns fatores: ser um ato violento; ser instrumental (ou seja, ter um meio e um fim); ter um propósito político; e não ser apenas um ato isolado (CLAUSEWITZ, 2010).

Partindo desta perspectiva, aponta-se que, quando definida corretamente, não há, até o momento, uma ofensa cibernética que possa ser caracterizada como uma guerra cibernética (RID, 2013). Pode ser considerado uma forma de provar seu poder aos indivíduos que os atacam. Estas Ciberguerras são elementos não apenas dos Estados, mas também de sociedades civis, como cibercidadãos, ativistas, hackers e todos aqueles que atuam pelo seu próprio bem ou sem conhecimento das nações.

Essa atividade pode ser definida como uma forma de conduzir e preparar militares, interromper e destruir sistemas de informações, tentando modificar a balança ao seu favor tentando saber mais sobre o adversário, ao usar seus conhecimentos, mas também poderá ser para mostrar novas doutrinas com forças necessárias, e com várias formas de aparecer, como notícias falsas, ações terroristas, ataques às redes de informações de emergência ou de tráfego aéreo, transações bancárias e satélites. É usada com métodos ofensivos e defensivos.

Ventre (2011) diz que a ciberguerra é chamada de dimensão cibernética de conflito armado ou 5ª dimensão de combate, demonstrando que estão cientes das oportunidades criadas pelo novo espaço, mas também tem suas desvantagens. Podemos entender como um conceito em desenvolvimento, por conta das tecnologias e os impactos do conflito internacional.

Enquanto Lobato e Kenkel (2015) traz o termo de ciberguerra como uma ameaça real, mas com efeitos potencialmente danosos para se tornar um grande evento em que capacidade de um agente inimigo de danificar computadores ou sistemas pode ser arquitetado por qualquer ator estatal ou não. Podem ser considerados soldados do Estados, hackers e terroristas.

Em que podemos simplificar pela união de “guerra”, “cibernética” e a tecnologia, sendo desenvolvido por uma linguagem que pode atacar o problema de controle e comunicação,

explorando as vulnerabilidades de sistemas e atacando as infraestruturas, ou seja, a ciberguerra é a difusão da internet e o ciberespaço. Então podemos pensar em como os avanços tecnológicos, alteram a forma de fazer guerra na atual época, pois as mudanças são dinâmicas.

De acordo com Gartzke (2013), o maior problema da ciberguerra é o anonimato, pois para retaliação deve-se ter conhecimento de quem são os invasores. Entretanto, a internet fornece meios para que os invasores não sejam encontrados. Sobre isso, cabe ressaltar que esse anonimato também é um problema para iniciantes na área. Alguns acreditam que ser chamada de ciberguerra é pouco violenta ou causadora de baixas consequências para ser chamada de guerra, contudo, ao atacar um Estado pode passar a revidar com violência militar como arbítrio de política internacional.

Apesar de não usar bombas, ela traz tantos problemas quanto uma guerra convencional, pois as formas de ataques são os danos e o balanço de equilíbrio de poder, não há um ataque surpresa, mas uma complexa combinação de elementos, por isso, é tratada como um instrumento de política externa coercitiva já que deixa efeitos a longo prazo.

Estas ações podem ser combinadas com iniciativas no espaço físico, onde a guerra cibernética está ligada às formas convencionais de guerra, contudo, a prova da capacidade de causar danos ao alvo é necessária, para não tentar demonstrar vulnerabilidade do Estado, e esse uso de força cibernética é punitivo, onde o efeito é no equilíbrio de poder.

Mesquita (2019) traz alguns exemplos no seu texto, o primeiro é um dos ataques mais estratégicos da ciberguerra, aconteceu em 2010 numa instalação nuclear iraniana, que foi vítima de um ataque com o vírus Stuxnet, criado para sabotar sistemas de controle industriais utilizados em usinas energéticas. Contudo, mesmo não conseguindo provar, acredita-se que foi um ataque planejado pelos EUA e Israel. Outro exemplo aconteceu em 2016, quando as ameaças cibernéticas cresceram exponencialmente trazendo os dois ataques mais notáveis, o primeiro foi ransomwares WannaCry e atingiu 300.000 computadores em 150 países, em que apareceu como uma falha de segurança da Microsoft e bloqueia o acesso do proprietário e pedia o resgate em *bitcoins*.[4] Sobre o segundo ataque, esse ocorreu com o NotPetya[5], entre um conflito da

[4] primeira criptomoeda internacional funcional, gerada por um sistema distribuído mundialmente pela internet, onde todos os computadores tem que validar cada moeda para que ela possa fazer parte do sistema.

[5] hackers russos usaram os servidores hackeados da empresa de contabilidade ucraniana Linkos Group para enviar um código.

Rússia e Ucrânia, detonando "bombas" [6] nos computadores de organizações internacionais e companhias privadas destruindo inúmeros dados, esse *malware* se propagava de forma rápida, e seu objetivo era ser destrutivo pois apenas deixava os computadores inutilizados.

Ciberterrorismo é o nome para um crime com base política, sempre atacando redes de computadores de Estados ou grupos inimigos. Surge junto com as novas organizações de extrema violência e radicalismo. Graças a tecnologia, estes ataques são cada vez mais fáceis, deixando os Estados vulneráveis a eles e tornando o cenário promissor para a prática destes atos ilícitos.

Enquanto a ciberespionagem é realizada pelos Estados para obter vantagens entre eles, onde a internet traz a facilidade da espionagem, porém este tipo é mais fácil de realizar do que as práticas convencionais, tornando os segredos cada vez mais difíceis de serem mantidos em segurança.

Os ataques cibernéticos vêm de grupos Estatais ou não, tornando difícil a atribuição dessas agressões e aumentando a incerteza em relação a elas. Não respeitando fronteiras nem distâncias e possuindo custos baixos comparado a estratégias militares tradicionais, ele desestabiliza o jogo convencional de segurança e defesa internacional.

Hacktivismo é um tipo diferente de outros cibercrimes, sendo uma forma de ativismo usado na prática do ativismo político, tendo como objetivo o envio de uma mensagem para o maior número de pessoas, sem criar terror.

O Cibercrime é todo ato que o computador ou meios da tecnologia serve para atingir um ato criminoso ou é o objeto de um crime. Estes ataques acontecem em momentos oportunos, com dispositivos certos e métodos difíceis de serem identificados, com programas tão pequenos que dificultam ser detectado. Contudo, trazem danos enormes para conseguir corrigir rapidamente, e se acredita que esses ataques são feitos por certos grupos de indivíduos ou organizações de cibercrime com interesses nacionais.

Tais ataques trazem prejuízos econômicos, pois as vezes podem acabar até uma rede de computadores que recebeu o ataque, e esses danos são difíceis de mensurar. Este exemplo é o ato criminoso do uso da internet, violando a confidencialidade das pessoas, Estados, sabotagem, *cyberbullying* e *cyberstalking*.

[6] o malware NotPetya se espalhou dos servidores de uma empresa de software ucraniana indescritível para algumas das maiores empresas do mundo, paralisando suas operações.

2 PODER CIBERNÉTICO

O “poder cibernético” é relativamente novo, uma vez que utiliza recursos de informações na área cibernética. Sendo o ciberespaço, um sistema operacional no uso de eletrônicos, este poder depende de recursos, que podem ser oriundos do ambiente lógico,[7] físico ou de regime híbrido.

2.1 Informação como recurso de Poder do Espaço Cibernético

Nye (2011) traz o conceito de “revolução da informação”, onde esta informação tornou-se o instrumento do poder imaterial. Esse por sua vez, foi potencializado pela revolução tecnológica, pois disseminou a um nível global e habilitou a oportunidade inédita de ampliar o poder em áreas que antes eram de difíceis acessos. Em especial, onde há uma relação com a democracia representando uma condição de desenvolvimento.

A relação entre governo e população pode mudar esse fenômeno da informação, tornando uma forma de estreitar laços e modernizar esta relação, bem como gerar previsibilidade ao comportamento dos usuários por meio de regulamentações e, em consequência, legitimidade para as ações estatais.

Esses avanços tecnológicos em comunicação, levaram a diminuições em custos de criação, processamento e transmissão de dados. Com tal redução de custos, a facilidade de acesso de atores ao poder da informação traz um processo de difusão de poder, conforme assinalado por Joseph Nye Jr (2011).

Nye Jr (2011) relaciona poder com duas vertentes: os recursos e a questão comportamental. Dessa forma, para ele, o poder pode ser definido como recursos e também pode ser definido como resultados comportamentais. Na primeira definição, o poder de um Estado é definido pelos seus recursos, que por meio de estratégias, conseguem alcançar resultados pretendidos. Na segunda definição, por outro lado, poder significa afetar outros por meio da coerção, recompensa e atração, visando alcançar resultados preteridos.

---

[7] O ambiente lógico é constituído por todos os recursos intangíveis e/ou abstratos que compõem as estruturas do espaço cibernético, conhecido popularmente como ambiente virtual.

O espaço cibernético é moldado por alguns fatores do poder. O primeiro é a tecnologia, pois é o que possibilita não apenas a entrada, mas também qualquer atuação dentro do espaço. O segundo fator é a organização, pois as maneiras pelas quais será utilizado o poder cibernético depende do objetivo de cada organização (KUEHL, 2009).

Um Estado consegue utilizar o monopólio da força e exercer seu poder também nesse novo espaço. De acordo com Nye Jr (2011), o poder é relacional. Essa característica do poder, ainda conforme ele, deriva das duas definições que compõem esse conceito: poder como resultado de comportamentos e poder como recursos. Assim, os recursos que serão abordados como indicadores de poder cibernético servem para comparar os poderes cibernéticos dos Estados.

Assim, esse autor propõe três pontos que exercem grande influência dentro da sistemática do poder, sendo que o primeiro é a própria difusão de poder, onde atores internacionais usam dessas informações para competirem entre si e buscarem poderes no ambiente cibernético.

O segundo ponto é a emergência da importância do poder brando, onde podemos ver dois fatores, o primeiro fator é a ampliação da capacidade de diversos atores em produzir e reproduzir informações dentro do espaço cibernético, tornando maior a capacidade de atração e persuasão no poder brando, enquanto a segunda traz um mundo mais complexo, pois é uma emergência de problemas que engloba não apenas em um Estado, e sim um conjunto de Estados.

Por fim, o terceiro ponto, é a influência desta revolução da informação na mudança de comportamento dos EUA e como ser uma potência mundial neste caso pode ser preocupante, não demonstrando capacidade de se adequar ao meio criado pela revolução.

Estados como os EUA, China e Rússia, que são consideradas verdadeiras potências cibernéticas, se destacam por serem capazes de produzir armas cibernéticas em um contexto de uma guerra cibernética e de defesa cibernética. Isso evidencia o que Nye Jr chama de poder cibernético. Com isso, se fala muito de equilíbrio no espaço cibernético a um espaço geográfico, com delimitação de fronteiras, soberania de Estado, e disputa de poder. (PORTELA, 2015)

Assim, podemos pensar na revolução da informação como um fenômeno que alterou as relações internacionais trazendo complexidade a ela e apresentando desafios às democracias, principalmente em relação ao fluxo de informação. Contudo, estes Estados usam este meio como uma forma de controle centralizado das populações.

Entretanto, apesar de tal controle, esta complexidade permanece trazendo consigo uma multiplicidade de relações entre Estados, coletividades internas e suas relações internacionais, tornando a necessidade de se redescobrir e redefinir seu papel num mundo tecnológico. Dessa forma, no campo cibernético, esse poder dado aos atores internacionais pode ser transformado em uma "arma" devido ao grande impacto destas tecnologias da informação.

No século XXI podemos dizer que estamos assistindo constantemente a difusão de poder. Pois de acordo com Nye Jr (2011) a difusão de poder é um evento recente, com os avanços tecnológicos de informação e comunicação acabaram causando esta difusão tanto horizontalmente quanto verticalmente, dando poderes aos atores não estatais.

2.2 Óticas realista e liberalista acerca do Poder

O conceito de poder é multifacetado e passa por constantes mutações que permite um Estado ter seus interesses pressupostos aos outros Estados, ou outros atores internacionais. Bobbio (2000) traz poder como uma capacidade ou possibilidade de agir, de produzir efeitos. Se analisarmos este conceito nas teorias realista e liberal, podemos entender que apesar de muitas vezes antagônicas, as duas abordagens apresentam contextos semelhantes sobre o poder.

A teoria realista é uma das abordagens com a força explicativa para as condições que o sistema internacional demonstra, como as relações entre os Estados, que conflitam incessantemente em busca de poder para manter sua segurança. O pensamento realista é uma ferramenta útil para analisar as estratégias de defesa cibernética, competência da segurança no campo digital, o estabelecimento de leis de vigilância e controle no ciberespaço, competição para o desenvolvimento de tecnologias por atores estatais e não estatais. O Estado ainda é o Soberano em todas as questões e a definição de segurança estatal.

Morgenthau (2003) fundamentou o conceito de realismo, como "acreditar que a política é governada por leis objetivas que deitam suas raízes na natureza humana", com seus seis princípios do realismo, sendo o primeiro o próprio conceito realista. Já o segundo é sobre os interesses dos Estados no sistema internacional, os quais são sempre definidos em termos de poder.

O terceiro conceito traz o preceito do interesse definido como poder, onde o realismo parte do princípio que seu conceito-chave de interesse constitui uma categoria objetiva. O

quarto conceito apresenta analogia com o conceito de Maquiavel, introduzindo subordinação ou tensão dos princípios morais da ação política aos interesses e exigências de uma ação política, enquanto no quinto, as pretensões morais de uma nação não são universais. Por fim, o sexto princípio, evidencia que o caráter é diferenciado e identitário, com isso Morgenthau elucida o papel central ocupado pelo poder na política internacional.

Por sua vez, Galvão (2018) demonstra como a busca de poder é um mero processo em defesa de interesses para a preservação de paz e segurança interna, levando o Estado a alcançar os seus objetivos. Contudo, o poder não pode ser delimitado, apenas compreendido como um interesse de acordo com as suas intenções, como um equilíbrio de poder, proporcionando novas formas de projeção de poder.

A teoria liberal, é uma doutrina de Estado limitado, com respeito aos seus poderes quanto às suas funções, onde primeiro é o Estado de direito e depois é o Estado mínimo.

Onde o Estado de direito é entendido como um Estado que os poderes públicos são regulados por normas gerais e devem ser exercidos no âmbito da lei, ou seja, uma doutrina da superioridade do governo das leis sobre o governo dos homens. E o Estado de direito, traz não só subordinação dos poderes públicos às leis, mas também ao limite material do reconhecimento de alguns direitos fundamentais considerados invioláveis.

Podemos dizer que para o liberalismo, uma sociedade bem ordenada é aquela que assegura aos indivíduos as melhores condições para o exercício de sua liberdade. Nogueira e Messari (2005, p.59), diz que “o Estado passa a ter uma importância jamais vista na história, porque ele é percebido como um ‘mal necessário’ e uma ameaça em potencial”. Infere-se também que, independentemente da teoria adotada, há uma perspectiva mais ampla onde se argumenta que o *soft power* está se tornando importante na era digital, por conta da evolução dos múltiplos canais de comunicação transcendendo as fronteiras.

O conceito de poder é semelhante nas duas vertentes, contudo, para os realistas, os Estados têm legitimidade para manter e defender a ordem doméstica, enquanto no âmbito internacional, eles buscam sem tréguas pelo poder, constantemente minando a paz e promovendo guerras. Já para os liberais, “uma sociedade sem governo dá lugar a discórdias incessantes entre interesses divergentes, onde uma de suas características é a não aceitação dessa condição como imutável” (NOGUEIRA E MESSARI, 2005, p.61).

Ao pensarmos nestes conceitos, entendemos o conceito de poder de Nye Jr projetado sobre o espaço cibernético. Cabe ressaltar, entretanto, que poder não é um conceito puramente objetivo, mas é uma questão de valores, interesses e perspectivas, onde mesmo que tenhamos atores específicos para tal relação, não podemos dizer que eles têm poder, pois para isso devemos especificar a relação de poder entre eles.

2.3 Analisando *Soft Power, Hard Power, Smart Power, Cyber Power* e a Difusão de poder no ciberespaço

Acerca das categorias de poder, Nye Jr (2010) traz os conceitos de *Hard Power*, *Soft Power* e *Smart Power* como um método para analisar as formas de poder expressas nas relações com a hegemonia. Ele utiliza de uma metáfora para explicar a relação do jogo de poder internacional, definindo-a em três níveis, onde o *hard power* e o *soft power* passam a ter um peso igual no sistema internacional.

Essas duas categorias de poder podem ser utilizadas por atores, que são entendidos como entes que possuem uma participação nos processos e acontecimentos no cenário internacional. Os atores não-estatais estão ligados ao *soft power*, por conta de expoentes de ideologias, estilo de vida, sendo eles indivíduos independentes ou organizados e estão ligados ao *hardpower* por conta de vírus, malwares ou qualquer outra influência direta.

Quanto ao *Soft Power,* essa é uma expressão de poder em que não está restrita apenas aos Estados, qualquer ator internacional pode exercê-la, devido a característica indireta, transnacional e não imediata. A habilidade em influenciar as preferências dos outros é uma das características do *Soft Power*, contudo, não fica somente nisso, está diretamente relacionado a persuasão e argumentação, com a utilização de valores morais, culturais, políticos e a forma que se relaciona com atores externos.

Tal expressão de poder tem a sua principal característica de acordo com conceitos ideais e culturais mais próximos com o que prevalece como uma norma global (NYE JR, 2002, p.123). Conceitos como democracia, liberdade, autonomia, liberalismo, igualdade, sustentabilidade, desenvolvimentos, são vistos como positivos e fazem parte do que é o *Soft Power*.

Já em relação ao *Hard Power*, esse pode ser entendido como algo direto e perceptível, por conta de suas ações concretas, sendo dividido em duas vertentes que se diferenciam, e ao

mesmo tempo, se complementam. Na primeira, é onde toda a esfera militar abrange dentro da articulação bélica de um ator, indo além do simples fato do conflito armado em si, tendo as guerras e intervenções como parte do conceito. A segunda, segundo NYE JR (2002) é a relação com a vertente econômica girando em torno do potencial econômico de um ator e capacidade de articulação em assuntos ligados à economia. No *Hard Power*, a influência direta no comportamento dos indivíduos é uma das características.

Entretanto, essas não são as únicas expressões de poder existentes dentro dos estudos de Nye Jr (2011). Não necessariamente como um conceito único, o autor apresenta o *Smart Power*, que é a capacidade de combinar os recursos do *soft power* e do *hard power* em estratégias eficazes, sendo capaz de não limitar um ato apenas como muito brando ou forte, entendendo que o mesmo pode servir a fins distintos ou sofrer mutação dependendo de como é utilizado.

O *cyberpower* surge com a capacidade de controlar e dominar os recursos disponíveis no ciberespaço. Começa desde a criação e vai até a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos, podendo afetar da guerra ao comércio. O domínio cibernético é uma invenção do homem, levando em consideração que ele é muito mais mutável que qualquer outro domínio, pois é conduzido pela criatividade humana. O poder cibernético depende de recursos lógicos, físicos ou de regimes híbridos.

Contudo, este poder deixa vulnerabilidades que podem ser exploradas por atores não estatais. Podemos dizer que o poder cibernético “é a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e em todos os instrumentos de poder” (NYE JR, 2012, p. 02).

A difusão de poder é um novo processo para a revolução da informação, baseada em avanços tecnológicos, onde o ciberespaço é um novo domínio de poder e, devido ter muitos recursos, vários países ainda enfrentam problemas em controlar suas fronteiras no ciberespaço. Mesmo que ela não substitua o território geográfico, a difusão de poder deve existir juntamente com a soberania do Estado. Dessa forma, o uso desse poder pelos atores internacionais pode ser expressado pelas faces de poder de Nye:

Quadro 2.4 – As três faces do poder no domínio cibernético

PRIMEIRA FACE **(A induz B a fazer o que B inicialmente não faria)** Duro: ataques de negação de serviços, inserção de *malwares*, interrupções de sistema Scala, prisões de *bloggers*. Brando: campanha de informação para mudar as preferências iniciais dos *hackers*, recrutamento de membros de organizações terroristas.
SEGUNDA FACE **(A impede a escolha de B excluindo as estratégias de B)** Duro: *firewalls,* filtros e pressão sobre as companhias para excluir algumas ideias. Brando: automonitoramento de ISPs e *sites* de busca, regras do ICANN sobre os nomes de domínios padrões de *software* amplamente aceitos.
TERCEIRA FACE **(A molda as preferências de B para que algumas estratégias não sejam nunca consideradas)** Duro: ameaças de punir *bloggers* que disseminam material censurado. Brando: informações para criar preferências (como estimulação do nacionalismo e *hackers* patrióticos), desenvolvimento de normas de repulsa (como o caso da pornografia infantil).

Fonte: Nye Jr (2012, p. 171)

No qual pode ser observado no quadro as maneiras que as faces de poder funcionam, como a primeira face, com a capacidade de um ator para fazer outros realizarem algo contrário às suas preferências ou estratégias.

A segunda face traz o ajuste da agenda ou estruturação da agenda em que um ator possibilita as escolhas dos outros pela exclusão de suas estratégias, enquanto a terceira face demonstra o ator ajustando as preferências iniciais de outro para que algumas estratégias não sejam sequer consideradas.

Com este conceito é possível entender sua função na interdependência, dividindo as relações de poder em duas dimensões que são a vulnerabilidade e a sensibilidade, no qual alguns Estados são mais vulneráveis que outros pela devida falta de alternativa para mudar o cenário político.

Levando a pensar em o poder cibernético pode aumentar o que é sensível entre os Estados e ao mesmo tempo auxiliar a diminuir os aspectos vulneráveis de cada um dos Estados menores perante os maiores. Isso se dá devido ao desenvolvimento de tecnologias próprias e não permanecer refém das mudanças tecnológicas nas grandes potências (MAZIERO, 2018, p. 09).

2.4 Espaço cibernético – um ambiente realista?

Galvão (2018) traz alguns pensamentos para se entender um ambiente cibernético pelo pensamento realista, deve-se entender a origem e o desenvolvimento proposital de um Estado que mais detém poder e privilégios, e como se utiliza da ideia de harmonia de interesses como instrumento de legitimação para a prática de colocar interesses próprios como se fossem nacionais.

A busca de poder é um mero processo em defesa de interesses para a preservação da segurança interna, conforme a vertente chamada de realismo defensivo. Contudo, esse poder não pode ser delimitado, trazendo o conceito de equilíbrio de poder, onde se proporciona novas formas de projeções de poder, além das capacidades militares, econômicas, tecnologias e conhecimento.

Entretanto, a capacidade de influenciar as preferências dos outros é uma habilidade também vista dentro do *cyberpower,* em que podemos relacionar com a persuasão e argumentação vindo destes Estados. O espaço cibernético foi feito pelo homem, e deve ser considerado um "local" muito mais mutável que qualquer outro, contudo, é também um local de anonimato entre os atores.

Ainda nesse sentido, ressalta-se que a Internet possibilitou a criação de novas cadeias inter-relacionais, como a ampliação de acesso às informações com os *hardwares* e *softwares* inovadores nas interações econômicas, políticas e sociais. Com isso, as funcionalidades da projeção de poder tendem a tornar os *hardwares* um segundo componente, quando as armas utilizadas no ciberespaço são *softwares* programados para atacar sistemas de dados.

As relações de poderes vêm a partir de valores, interesses e perspectivas dos Estados, bem como de seus nacionais, contudo, o que realmente faz com que sintam que um agente tem poder é o medo que se tem do controle estatal. A sobrevivência no mundo cibernético acontece pelo medo que os atores não-estatais têm do Estado, pelo o "poder" que estes possuem.

Para pontuar e exemplificar como e em que tais conceitos atuam é preciso entender primeiro de onde eles vêm. A sobrevivência que antecede o poder parte da necessidade de primeiro se proteger. Para isso é necessário começar desenvolvendo tecnologias de defesa poderosas, evoluindo o tempo todo. A interação entre empresas privadas e Estados é comum e como de costume têm prós e contras.

Empresas privadas costumam ter acesso a desenvolvimento de tecnologias de forma mais instantânea, visto que o lucro é seu maior propósito. Ao contratar os atores não estatais a proteção acontece de forma paralela aos desenvolvimentos de possíveis ataques. Mas ter dados protegidos e essenciais à segurança governamental à mercê de uma empresa gera conflitos, ter sua segurança protegida e ao mesmo tempo capaz de ser exposto é um risco muito grande para um Estado correr. Uma empresa privada teria poder sobre o Estado, nessa ocasião.

É de conhecimento que o espaço cibernético interfere em possíveis guerras físicas. Mesmo antigas desavenças políticas podem se agravar por conta do chamado *cyberpower*. Um exemplo disso é o banimento da empresa Google na China. A justificativa seria uma possível espionagem dos cidadãos chineses pelos Estados Unidos.

Outro exemplo é que os Estados Unidos são de forma frequente acusados de atacar a China, e o oposto também acontece. Esta tensão trazida pela possível espionagem entre nações é um fator que se faz necessário analisar, pois não existe apenas o Estado com poder no *cyberespaço*, mas também hackers e ciberterroristas conseguem acessar grandes níveis de segurança.

Em virtude das características do espaço cibernético, como por exemplo, o anonimato, não se consegue regulamentar, encontrar ou punir tais atores. O governo seria responsável por algo ocorrido em seu território, mesmo que não se possa ter certeza se o endereço de IP[8] tenha vindo de fato de tal lugar?

As relações internacionais se desenvolvem constantemente visto que o ciberespaço é fundamental para os Estados, nos últimos anos têm sido fator de eleições, brigas econômicas e chegando até a liberação de dados de Estado que confirmava espionagem de países. Como foi o caso de Edward Snowden, em 2013, que liberou dados do governo dos Estados Unidos. Este é um claro exemplo da proteção e fragilidade do mundo virtual e de como afeta fisicamente as relações entre países. Apesar de anônimo o ciberespaço e o que nele é produzido não some com facilidade e interfere de forma abrangente e podendo chegar a definitivo.

[8] IP, nomeadamente *Internet Protocol*, é um conceito aplicado às redes com maior difusão no espaço cibernético atualmente e permite geolocalizar as máquinas utilizadas para o acesso do ambiente lógico.

3 RELAÇÕES ENTRE OS ESTADOS NO ESPAÇO CIBERNÉTICO

As relações no ciberespaço vêm junto com os “poderes” estabelecidos pela sua forma de governar, tendo aqui os Estados Unidos da América, a República da China e a Federação Russa como as maiores potências na área cibernética, mas também não desprezando os outros Estados que estão em desenvolvimento, onde aparece a influência destes Estados e como eles agiram uns com os outros.

3.1 Configuração das relações internacionais no cyberespaço

No sistema ONU existe o Fórum de Governança da Internet, que tem como objetivo unir as pessoas com interesses semelhantes e de diversas áreas sobre o debate do espaço cibernético. De acordo com Kurbalija (2016 p.22), um dos princípios fundamentais da internet é sua natureza distribuída, com pacotes de dados que podem seguir caminhos diferentes através da rede, evitando as barreiras. As eleições presidenciais são os maiores acontecimentos que influenciam a governança da internet, onde em 2008, a neutralidade da rede aparece como uma das principais questões relacionadas a isso. No ano de 2011, seu desenvolvimento mais importante foi a ligação com as agendas políticas globais, se aproximando das questões diplomáticas, como mudanças climáticas e migração.

Contudo, as ferramentas de governança são um conjunto de instrumentos que servem para o desenvolvimento e a compreensão da argumentação política, consistindo em um quadro de referência que inclui percepções das relações de causa e efeito, terminologias. Mas, esta caixa de ferramentas reflete a natureza da internet, sob forma de uma área normativa conhecida como perversa, por conta da dificuldade encontrada na atribuição de causalidade para o desenvolvimento de políticas. Assim como o processo da governança, esta caixa de ferramentas também é um fluxo, com abordagens, padrões e analogias que surgem e desaparecem na mesma velocidade.

Existem duas formas de abordagens para qualquer tipo de questão de governança na internet, em que podemos chamar de abordagem “real” no qual argumenta que a internet não contribui com nada novo no campo, sendo somente um dispositivo novo. Enquanto na abordagem do chamado “ciber”, argumenta que a internet é um sistema de comunicação

diferenciado, no qual sua principal abordagem é a internet conseguir desconectar a nossa realidade social e política do mundo dos Estados-nações.

O pensamento de proteger a natureza pública da internet é um dos temas centrais do debate, pois possibilita rápida expansão, incentivando criatividade e inclusão. Contudo, essa questão reabre o debate sobre a neutralidade da rede por conta da comunicação via internet transcende as fronteiras e com o "anonimato" dos usuários, acreditam que os governos não tinham o direito moral de governar os usuários e nem tentar qualquer meio de coerção.

Mas apesar dessa perspectiva de fronteira, o autor Mandarino Jr (2010) traz o pensamento de como são delimitadas as fronteiras cibernéticas, pensando em estruturas físicas do espaço cibernético, enquanto, o autor Ferreira Neto (2014) discorre sobre Fronteira – ponto como ele chama, conceito que ele desenvolveu com uma pesquisa baseada na noção de evolução das fronteiras. Mas existem diversos autores com visões diferentes sobre o que seria a fronteira cibernética e como funcionaria.

Neste aspecto, umas das principais ideias em relação a internet era que ultrapassa as fronteiras de cada Estado e acabaria com o princípio de soberania, pois a comunicação transcendia as fronteiras. Com a perspectiva do fim da "fronteira", hoje é difícil identificar quem está atrás da tela, mas é possível localizar sua posição geográfica, contudo, quanto mais a internet se baseia nisso, menos surpreendente sua governança será.

Podemos pensar em alguns exemplos, como o Twitter que é responsável por levantar as principais questões sobre a governança na internet como proteção de privacidade e liberdade de expressão. Todas essas questões deveriam seguir as regras já existentes para a internet, e o seu uso elevaria a estabilidade jurídica e reduziria a complexidade do desenvolvimento do regime de governança.

Pensando em como as relações internacionais funcionam no ciberespaço, precisamos entender a estrutura por trás, como as empresas e os organismos internacionais ajudam a regular trazendo segurança neste espaço.

As instituições internacionais vinculadas a este espaço são a ICANN (Internet Corporation for Assigned Names and Numbers), ISOC (Internet Society) e a W3C (Wide Web Consortium), onde essas organizações nasceram da ARPANET, e estão ligadas a legislação dos Estados Unidos da América.

A ICANN é uma entidade sem fins lucrativos, responsável pela alocação do espaço de endereços de protocolos da internet, pela atribuição de identificadores de protocolo, pela administração do sistema de nomes de domínio de primeiro nível genéricos e com códigos de países, assim como as funções de gerenciamento do sistema de servidores raiz. Onde temos seus princípios básicos de operação como ajudar a preservar a estabilidade operacional da Internet, promover competição, alcançar ampla representação da comunidade global da internet e desenvolver políticas de forma adequada à sua missão através de processos baseados em consentimentos. (ICANN, 2021)

Enquanto a ISOC é uma associação sem fins lucrativos, criada em 1992, com atuação internacional e tem como objetivo promover liderança no desenvolvimento dos padrões internet, bem como fomentar iniciativas educacionais e políticas públicas ligadas à rede mundial entre computadores. Propiciando a interação com governos, empresas e entidades em geral para adoção de políticas em relação à internet que estejam de acordo com seus princípios, que é uma rede aberta e universalmente acessível, dando apoio à inovação, à criatividade e às oportunidades comerciais, onde algumas de suas linhas de atuação são facilitar o desenvolvimento aberto de padrões, protocolos, gestão e infraestrutura técnica da internet, apoiar a educação nos países em desenvolvimento especialmente e onde existir demanda, prover informação confiável sobre a Internet e fomentar a cooperação internacional e o intercâmbio entre comunidades e culturas, promovendo a autodeterminação. (ISOC, 2021)

E a W3C, é uma organização internacional, com membros de empresas, órgãos governamentais e associações independentes, responsável pelos protocolos e padronização da World Wide Web, a rede mundial de computadores, sua missão é desenvolver e criar protocolos para a interpretação de todo o conteúdo da internet, levando ao seu potencial máximo. Desenvolveu especificações técnicas e orientações através de um processo projetado para maximizar a consenso sobre as recomendações, garantindo qualidades técnicas e editoriais, além de transparentemente alcançar apoio da comunidade de desenvolvedores, do consórcio e do público em geral. (W3C, 2021)

Essas organizações são responsáveis pelo funcionamento do cyberespaço, contudo, as empresas também exploram esse espaço, contudo, diferente delas, as empresas tem como objetivo o lucro neste espaço, impactando com as maiores contribuições de usuários, em que parte do seu lucro é sujeita ao Estado em que sua sede está localizada.

As empresas de conteúdo de internet como Google, Facebook e Twitter são alguns dos mais ativos na governança da internet, pois seu principal modelo de negócios pode ser diretamente influenciado por acordos governamentais relacionados à proteção de dados. De acordo com Kurbalija (2021 p.213), os produtores de conteúdos como a Disney estão preocupados com a preservação do alcance global e da dominância de seus produtos e modelos para desenvolvimento de conteúdo local.

Esta ferramenta de governança foi desenvolvida pelas últimas décadas, e conforme os atores se interessavam na competição tecnologia no mundo se apresentava um diferencial no poder vindo dos conhecimentos deles sobre as novas tecnologias que surgiam e a capacidade de acompanhar esta evolução.

"O domínio da informação é elemento base da construção de poder na contemporaneidade" (ÁVILA E PINHEIRO, 2014, p. 85). Essa informação e o uso constante de ferramentas tecnológicas no dia a dia gera dados, independentemente de quais sejam, que possam a vir influenciar mercados e que levam a conhecer as condutas dos cidadãos e as formas de centralizar estes dados, mesmo que para os usuários haja uma 'liberdade' na internet, que passa segurança, entretanto, é entregue um vasto fluxo de dados as empresas e Estados.

O equilíbrio talvez seja o panorama mais adequado para debates entre governança e políticas da internet, pois é necessário um equilíbrio entre várias abordagens e interesses para que haja frequência a base para o consenso, no qual podemos dizer que a liberdade de expressão, a privacidade, cibersegurança e a propriedade intelectual está entre esses equilíbrios. Pois o consenso geral reconhece estabilidade e funcionalidade, tornando flexível para mudanças em busca de funcionalidade e legitimidade do espaço.

3.2 Relação entre Estados no cyberespaço

Ao pensarmos em como as relações funcionam no ciberespaço, avaliamos as formas de poderes existentes nos Estados. Cada Estado tem uma forma de poder que já conhecemos. A China foi construída com a reforma e abertura para o mundo exterior ajudando o crescimento econômico e fornecendo os recursos para a construção do Hard Power, ou seja, a influência direta do comportamento dos indivíduos, ou de outros Estados.

Podemos dizer que o desenvolvimento do Hard Power, foi esperado da China por conta de seus investimentos e assistências, sua modernização militar e seus incentivos econômicos, principalmente na forma de abrir ou fechar mercados chineses. Ao compararmos com os Estados Unidos, a lacuna militar entre eles não é decisiva na competição de hard power, ao olharmos os conflitos entre ambos os Estados, o governo chinês tem buscado aumentar vantagens geográficas no uso de seu poder, tornando seus interesses assimétricos.

A medida em que persuade, apoiada pelos ganhos relativos e absolutos da China no hard power dá aos aliados dos Estados Unidos e outros que buscam apoio dos EUA, a desconfiarem dos laços com eles. Apesar do poder da China, um dos únicos Estados que eles não conseguem influenciar é os EUA, mas acaba sendo considerado ameaça o que deixa mais suscetível deles investirem mais atenção e recursos para se preparem para algo que eles considerem chinês.

Contudo, se pensarmos pelo lado dos Estados Unidos, o crescimento chinês durante os anos foi uma forma de soft power com alcance global, e que deixou uma impressão de estar assumindo o papel esperado de pilar responsável por um status quo de ordem internacional com as empresas chinesas surgindo, pareciam marcas atraentes nos Estados Unidos, o que seria uma característica do soft power americano, como a Huawei de telefones celulares, contudo, sua imagem foi mudando com as suspeitas de espionagem, acusações de roubo de propriedade intelectual, e ela vinha ganhando uma reputação como um produto que poderia competir dentro do mercado americano e em outros mercados ao redor do globo.

Mas a China sempre se comportou de maneiras que poderiam minar seu poder brando com os Estados Unidos, e parte do seu soft power chinês foi fraco, especialmente entre países liberais e democráticos. A imagem da China vem piorando perante os Estados, pois suas atuais condutas têm mostrado um regime de uma forma contrária a certas crenças, como os valores americanos.

Entretanto, o hard power e o soft power da China juntos conseguem oferecer perspectivas limitadas para moldar as políticas dos EUA e as ações que abordam ou afetem o que a China vê como interesses importantes.

Uma forma de aplicar o soft power é a concentração das ferramentas de busca, que possuem uma influência nas ideias. Essas ferramentas atraem usuários por seu desempenho superior e embora haja uma extensa variação dessas ferramentas, o que se destaca é o Google, a empresa detém cerca de 80% da participação mundial, seguida por outros buscadores como o Yahoo, Baidu. Os algoritmos de pesquisa destes buscadores, principalmente do Google, vêm

do resultado dos usuários e de suas pesquisas, com isso ele consegue determinar o que é importante ou não na internet e esse é um exemplo de soft power.

Com a disputa que a China teve com a empresa Google, ela percebeu esse poder, pois o governo chinês queria censurar os resultados da pesquisa na China, com isso a empresa abandonou o governo chinês e realocou seus servidores em Hong Kong, foi uma forma da China na perda de poder de influência vinda a favor da empresa de pesquisa Baidu que lidera o mercado de sites de pesquisa na China.

Nos Estados Unidos, as mídias sociais são as formas de amostra do soft power, o sucesso das redes sociais vem graças ao volume excessivo de dados, fatos e todo o tipo de informação que é disponibilizada, como pode ser percebido no facebook ou twitter que fazem sucesso pela sua maneira de disponibilizar os dados, reforça a atenção das pessoas em prol de um ideal determinado, trazendo o essencial para enfrentar certos problemas.

Chegando neste debate que o cyberespaço traz em relação ao impacto tecnológico, Lindsay (2015) mostra o discurso sobre a China e a segurança cibernética em que eles dividem as opiniões primeiramente sobre o impacto da tecnologia na segurança internacional e outro sobre o futuro político e econômico de uma potência em ascensão, trazendo os perigos ou evoluções vindas do ciberespaço, como o cibercrime e a ciberguerra.

Chegamos num ponto que os poderes dos Estados, não é apenas de uma forma, contudo, sempre haverá um mais forte que o outro como os EUA como seu soft power "poderoso" no mundo, ou o hard power da China, que apesar da influência e das sanções que ela aplica algumas vezes para mostrar sua força, ela ainda consegue tentar manter a si sem ser uma ameaça.

3.3 Atores não estatais no novo jogo do cyberespaço

Os Estados estão em constante disputa de poder, e atualmente o cyberespaço é apenas mais um local para essa corrida, contudo, os Estados Unidos, Rússia e a China são considerados as maiores potências cibernéticas, com suas tecnologias. Podemos demonstrar vários exemplos, como o 5G, a crise entre China e o Google, a proibição de vendas de qualquer tecnologia *Huawei* nos Estados Unidos e outros Estados ou os cibercrimes envolvendo os Estados e a intervenção da Rússia nas eleições estadunidenses.

Nye Jr (2011) demonstra seu pensamento sobre o cyberespaço e a tecnologia criada pela nova revolução industrial e como ela se modificou ao longo dos anos. O cyberespaço deixa uma margem para que atores internacionais e pequenos governos consigam navegar e causar alguns “estragos” sem serem identificados, com a ajuda de repetidores de sinais que bipam em servidores ao redor do mundo, dificultando a descoberta dos causadores, e as vezes deixando a culpa em cima de outros que não estavam envolvidos, como a China que já foi acusada de espionagem por conta disso.

O autor também trata a dificuldade de afirmar que determinado Estado é dominante no espaço cibernético, como alguns são no mar, no ar ou na terra, pois mesmo aqueles Estados que tenham consideráveis recursos de soft e hard power, estão lidando com novos atores e com novos desafios inerentes ao espaço cibernético. (NYE JR, 2010)

Ao debatermos os grandes embates, entendemos como funciona a relação entre os Estados, já que apesar do cyberespaço não existir uma “fronteira”, os Estados ainda têm poder sobre o que se passa dentro de seu domínio. Consideradas as duas superpotências cibernéticas do mundo, os EUA e a China, participam da corrida para o aprimoramento e a influência tecnológica de ambas, contudo, ao mesmo tempo acusações sobre espionagem direcionadas para a China, são bastantes evidentes. Será que o 5G realmente é parte de um esquema para espionar outros Estados, feito pela China e a empresa telefônica Huawei?

Contudo, esse questionamento não é feito sobre equipamentos e serviços tecnológicos vindo de outros Estados, então por que será que é tão diferente a desconfiança no que a China produz do que os outros países produzem? A controvérsia criada ao redor do cyberespaço, em questão do 5G e da empresa Huawei é o "acúmulo dos fatos”, pois a dimensão da cibersegurança nesse âmbito torna-se evidente e a traz para o primeiro plano da política internacional. Esse constante ataque vindo de ambos os lados está sendo chamado de “nova Guerra Fria”, pois as duas vivem em um espiral de ameaças, sanções e acusações de espionagem entre elas e contra o mundo.

Na União Europeia, há um constante aumento de espionagem, no qual acreditam ser patrocinadas por outros Estados, tornando os governos europeus e as empresas vulneráveis à novas ameaças. Não se pode provar de onde vem os ataques e nem quem os mandou, com isso, as tensões nas relações entre os Estados acontecem.

Outra tensão que ocorreu entre os dois Estados, foi por conta do Google, onde para se estabelecer ela deveria se ater às leis da China, porém acusaram o governo chinês de tentar

roubar o código fonte do google, invadir os e-mails do gmail e em relação a censura em pesquisas na ferramenta. Contudo, da mesma forma que o google era uma forma de monopólio dos EUA, o medo era que o Baidu se tornasse igual, mas esse ato de saída trouxe brecha para que o governo americano pedisse novas normas para o ciberespaço.

Essas tensões entre ambas as nações, acontece com os outros Estados, porém o fato de serem as duas maiores potências em questões tecnológicas, trazem impactos aos outros países. Ventre (2011) diz que se os Estados Unidos tem como a maior figura de ameaça do ciberespaço, a China, no qual o crime cibernético é proibido não se permitindo ataques a outros Estados, no entanto, ela afirma ser atacada inclusive pelo EUA, enquanto o governo americano faz que sua abordagem seja de acusar o outro, justificando as suas ações a nível nacional e internacional

Em consequência, a estratégia chinesa é aumentar seu poder a nível mundial através do cyberespaço, se protegendo de cibercriminosos e aumentando sua fortaleza digital. Outro debate envolvido, é sobre a liberdade de expressão que o governo americano discursa, enquanto o governo chinês se opõe em algumas questões de controles que eles acreditam necessários para garantir a ordem e estabilidade interna do país, não concordando com nenhuma intromissão ocidental na sua Soberania.

Nessa relação China x EUA, em 2021 o país asiático foi acusado como responsável por explorar uma brecha em contas de e-mails de empresas e de estudantes de uma empresa americana, a Microsoft, contudo, não apenas o EUA, mas União Europeia Reino Unido, Austrália, Japão, Nova Zelândia e Canadá também entraram com a denúncia. Trazendo ataques cibernéticos contra a empresa americana que afirmou sobre essa vulnerabilidade em seu sistema, mas a falha foi corrigida após o descobrimento. (G1, 2021)

Mas também acusou os EUA de ser um “império de hackers” e reclamou sobre o fato dos EUA estarem contra a Huawei no 5G. Onde o governo americano demonstra preocupações sobre o potencial da Huawei e que seu objetivo é uma ofensiva contra chineses no Brasil e em outras nações que tentam impedir a Huawei de fornecer equipamentos para essa tecnologia. Com a embaixada chinesa no Brasil afirmando que os ataques dos EUA são infundados e que tenta difamar a China e as empresas de tecnologias. E as acusações de serem o “maior império de hackers” do mundo, afirmando que o país representa uma verdadeira ameaça à segurança cibernética. (Folha, 2021)

Com o presidente Biden, acusando a China e a Rússia por conta de ciberataques, ele afirma que ver ameaças crescendo por partes destes Estados e que isso pode levar a uma "guerra real" com os EUA.

> ""Se acabarmos em uma guerra, uma verdadeira guerra de tiro com outra grande potência, será como consequência de uma violação cibernética", adverte Biden" (Tecmundo, 2021)

Mesmo com essas acusações entre EUA e China, os presidentes de ambas nações sentaram para conversar e tentar evitar a rixa entre ambos que leve a um conflito real. Chegando em áreas de interesses que convergem e divergem entre eles e que devem saber manter a diplomacia entre eles para gerenciar de forma responsável a competição. (El País, 2021)

Enquanto entre a Rússia e os EUA, há uma tensão de manipulação nas eleições dos EUA em que o governo americano diz receber informações regulares de inteligência que indicam que a Rússia está esforçada para interferir novamente nas eleições americanas, que se acreditava nunca ter parado de acontecer apesar dos avisos do presidente Biden.

> Os líderes militares e estratégicos da Rússia incorporam táticas de guerra de informação em tempos de guerra e de paz, de acordo com um relatório de 2020 do Centro de Engajamento Global do Departamento de Estado, uma doutrina que "fala sobre a formulação estratégica da Rússia que está em um estado de conflito perpétuo com seus supostos adversários. "(CNN Brasil, 2021)

O presidente Biden, afirma que se a Rússia violar certas regras sobre a cibersegurança, o governo responderá. Por conta de ataques de hackers em setores importantes da economia americana, a questão da segurança cibernética marcou o primeiro encontro entre Putin e Biden desde de sua eleição à Casa Branca.

As constantes acusações e discussões pela tecnologia 5G é umas das grandes discussões que torna as grandes potências em crise. Por exemplo, onde a Casa Branca confirmou que os EUA pressionaram o Brasil sobre a tecnologia 5G da Huawei, contudo, o governo brasileiro não se comprometeu em relação ao uso ou não de produtos da empresa chinesa. Apesar do

governo americano ser contrário ao uso de tecnologia da Huawei no Brasil em instalações de segurança, algumas empresas brasileiras de telecomunicações já são construídas com componentes amplamente chineses.

A Huawei foi colocada na lista negra de exportações norte americanas em 2019 e foi proibida de acessar tecnologias importantes de origem do EUA, apesar das críticas pelo governo americano, o Brasil enfrenta resistência do setor e do seu próprio governo por conta da China ser seu maior parceiro comercial (G1, 2021) Por isso governo brasileiro decidiu pagar pela tecnologia de ambas as nações para evitar conflitos entre elas. (VEJA, 2021)

Esses ataques cibernéticos e acusações vindas de ambos os lados mostram a relação tensionada entre os Estados, pois o ciberespaço ainda é um lugar frágil de fronteiras, porém, o território existe. O autor Carneiro (2017) traz como a soberania do Estado se aplica no espaço cibernético, pois embora a territorialidade seja a essência do princípio de soberania os Estados também têm jurisdição sobre infraestrutura cibernética, as atividades e as pessoas envolta dela que estão localizadas em seu território podendo ser sujeito às obrigações jurídicas internacionais.

Os Estados são livres para conduzir atividades cibernéticas nas suas relações internacionais, levando a mostrar que é independente em suas relações externas de outros Estados. Contudo, um Estado não pode conduzir essas atividades para violar a soberania de outro, mas este fato não se aplica a atores não estatais, pois geralmente não têm ligações com outras nações.

Os atores não estatais exploram as vulnerabilidades deixadas pelos grandes Estados no domínio cibernético, com seus recursos limitados, mas produzidos por hackers ativistas, ou invasores com motivos ideológicos, que acabam sendo difíceis de encontrar. O ciberespaço é como um “campo de batalha”, onde ocorrem vários ataques todos os dias a sites para desconfigurar e até mesmo causar destruições físicas vindas destes ataques.

Contudo, esses ataques não podem vim apenas dos Estados, mas também dos chamados atores não estatais, no qual não estão ligados aos governos. Os ataques cibernéticos que prejudicam sistemas, são realizados para fins ideológicos ou até criminosos, mas não têm a mesma capacidade dos grandes governos. O autor Sigholm (2016) traz o conceito de cyber ações para as atividades ilegais realizadas pelos atores não estatais, que causam danos e perturbações.

Nye Jr. (2010) mostra como grupos terroristas funcionam, fazendo o uso de ferramentas cibernéticas com o intuito de causar destruição, contudo, são raros e mais usados para instabilizar os Estados. Assim, esses atores crescem em quantidade e capacidade de projetar poder através da revolução da informação. No entanto, se pegarmos os tipos de atores não estatais, os terroristas usam do seu *cyberpower*, em que se utilizam do *soft power* para mostrar que apesar do pouco uso do cyberespaço para os ataques diretos, eles os utilizam de maneira efetiva e constante para exercer seu poder principalmente na convocação de novos membros para seu grupo.

Joseph Nye Jr (2011) afirma que a Internet está permitindo a todo tempo consequências nas esferas pública, privada e até mesmo individual, debatendo que os Estados poderão se tornar menos fundamentais na vida das pessoas por causa da Internet e dos novos padrões de comunidade e governança.

Enquanto o Gartzke (2013) acredita que na ciberguerra, a participação dos atores não estatais, segurança de infraestrutura e a evolução nas legislações são estratégias de retaliação, pois a segurança cibernética funciona melhor quando autônoma, porém acreditam que nesse tipo de guerra não pode ser chamada dessa forma, contudo, se um Estado for atacado o conflito pode passar a ser de vias de violência militar.

E Sigholm (2016) mostra como os governos do mundo procuram abordar cada vez mais atores não estatais para se beneficiar de suas experiências e aumentar seu conhecimento para aprimoramento da sua capacidade cibernética. Ele traz uma maneira de resolver as reações políticas relacionadas a ciberataques, explorando a “natureza” do ciberespaço é o emprego dos atores não estatais nas operações do espaço cibernético.

CONSIDERAÇÕES FINAIS

O espaço cibernético é um fenômeno tecnológico, sendo usado como uma ferramenta para a construção da atual conjuntura das relações internacionais com a globalização. Surgiu com a criação da arpanet, mas sua estrutura cada vez mais complexa e sofisticada que engloba todos os Estados – nações e também às relações internacionais em volta delas.

Sua criação acompanhou além da evolução política de cada Estado, mas também das formas de poder usadas nas Relações Internacionais, impactando a forma de usar a internet e o espaço cibernético ao redor do mundo. Foram criadas instituições e organizações internacionais para que haja regulamentação no espaço cibernético e a disputa de poder nas relações internacionais seja de forma que nenhum ultrapasse a soberania do outro.

Ficou claro durante esta pesquisa, que o espaço cibernético aumentou as estruturas de poder e como ela é usada para entender os embates entre eles. A criação deste espaço trouxe uma evolução política e os movimentos de poder no mundo e nas relações internacionais, apesar de ter sido feito em território americano, e com as organizações internacionais da internet que as principais se encontram nos EUA, pode dizer que o país ainda exerce grande influência sobre o espaço cibernético, tornando os padrões adotados como regras para o uso do espaço cibernético e o governo americano exercer grande influência sobre a internet.

Com todas as organizações, empresas, Estados e indivíduos e suas interações que contribuíram para sua criação e atual funcionamento, onde as relações de poder neste ambiente mais a difusão de poder para os atores não estatais acabam surgindo de forma natural.

O atual estágio das relações internacionais é único, não só porque há mudanças sistemáticas provocadas pela transformação da distribuição de poder em todo o mundo, mas principalmente devido à aceleração e expansão da interconexão entre a sociedade e as diferentes sociedades. Um novo conjunto de tecnologia digital que tende a ser universal se fortalece ao mesmo tempo, onde mudanças significativas nos padrões de interação social, mudando assim a forma de como as relações de poder são estabelecidas.

Por isso e por sua natureza técnica, sempre tende a se desenvolver e é esperado a transformação contínua do ciberespaço para atender às necessidades de relacionamento Internacional. Nos últimos anos, têm sido cada vez maior o número de atores realmente capazes de influenciar a política internacional, incluindo atores não estatais, além de crises reveladoras e instabilidade política no estado, diplomacia e instituições internacionais.

Nye Jr (2011) trouxe os conceitos de hard, soft e smart power para analisar as formas de poder dentro deste espaço. E com elas, surge o conceito de cyberpower que é a capacidade de controlar e dominar os recursos disponíveis no ciberespaço. Contudo, o cyberpower deixa vulnerabilidades que podem ser exploradas por atores não estatais sendo um local que pode ser usado para criar vantagens e influenciar eventos em outros ambientes operacionais.

As tensões entre Estados acontecem com as maiores potências em questões tecnológicas em que atores estatais ou não, exploram vulnerabilidades deixados por estas grandes nações, tornando o ciberespaço um “campo de batalha” onde ocorre ataques todos os dias.

Podemos concluir que o espaço cibernético ainda precisa de uma regulamentação que ajude as comunidades a se desenvolverem sem medo e que as vulnerabilidades dos Estados sejam mais difíceis de serem encontradas com o fluxo de informações advindos destes locais, mesmo com os atores estatais ou não buscando algo para que haja instabilidade.

REFERÊNCIAS

ÁVILA, Rafael Oliveira de; PINHEIRO, Marta Kerr. Poder informacional nas relações internacionais contemporâneas. **Revista de Relações Internacionais da UFGD**, 2014, n. 5, p. 1-30.

BOBBIO, Norberto. Dicionário de política. 6 ed. Brasília: Editora Universidade de Brasília, 2000.

CARNEIRO, João Marinonio Enke. As relações entre Defesa e Soberania no espaço cibernético. **Defesa**, [*s. l.*], p. 1-14, 2017.

CASADO, José. Governo decide pagar para não escolher entre EUA e China no 5G. **5G**, Veja, 12 ago. 2021. Política, p. 1.

CLAUSEWITZ, C. V. **Da Guerra**. São Paulo: Ed. Martins Fontes, 2010.

DEMCHAK, Chris C.; DOMBROWSKI, Peter. Rise of a Cybered Westphalian Age. Strategic Studies Quarterly, v. 5, n. 1, p.32-61. Spring 2011.

EFE. Biden conversa com Xi Jinping sobre como evitar que a rixa entre Estados Unidos e China "leve a um conflito". **China**, El País, 10 jul. 2021. Internacional, p. 1.

FERREIRA NETO, Walfredo B. Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso do poder. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma Lúcia de Moura (Org.) **Segurança e Defesa Cibernética**: da fronteira física aos muros virtuais. Coleção I - Defesa e Fronteiras Cibernética Pernambuco: Editora UFPE, 2014.

FOLHA (SP). China diz que EUA são 'império de hackers' e rebate ofensiva de assessor de Biden contra Huawei no 5G. **5G**, Folha de São Paulo, p. 1, 7 ago. 2021.

FRANCE PRESSE. Hackers chineses atacam redes de grupos de defesa dos EUA, diz empresa. **Hackers**, G1, 21 abr. 2021. Economia, p. 1.

G1. Os Estados Unidos acusam formalmente a China de hackear a Microsoft. **Hackers**, G1, 19 jul. 2021. Economia, p. 1.

GALVÃO, Lorrayne Rosa de Oliveira. Ciber-RI: a projeção internacional de poder sob a perspectiva do Software Power. 2018. 25 f. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Universidade Federal de Uberlândia, Uberlândia, 2019.

GARTZKE, Erik. The Myth of Cyberwar. **Cyberterrorismo**, International Security, v. 38, p. 41-73, 2013.

GONÇALVES, André Luiz Dias. Ataques cibernéticos podem provocar ‘guerra real ‘, adverte Biden. **China**, Tecmundo, 29 jul. 2021. Internacional, p. 1.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. Geopolítica. **A Geopolítica do Espaço Cibernético Sul-Americano: (IN) Conformação de políticas de segurança e defesa cibernética?** Austral: Revista Brasileira de Estratégia e Relações Internacionais, v. 7, ed. 14, p. 217-241, jul./Dez 2018.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. National Defense University, 2009

Kurbalija, Jovan. Uma introdução à governança da internet [livro eletrônico] / Jovan Kurbalija; [Zoran Marcetic -Marca & Vladimir Veljasevic; tradução Carolina Carvalho]. -- São Paulo: Comitê Gestor da Internet no Brasil, 2016.

LINDSAY, Jon. 2015. The impact of China on Cybersecurity. Journal of Strategic Security 39, no. 3: 7-47

LIPTAK, Kevin. EUA partem para o ataque e culpam a China por ataques cibernéticos. **5G**, CNN Brasil, 19 jul. 2021. Business.

LOBATO, Luisa; KENKEL, Kai Michael. **A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na Guerra**. Ciberguerra, Contexto Internacional, v. 37, p. 629-660, maio/ago. 2015.

MANDARINO JR, Raphael. Segurança e Defesa do espaço cibernético brasileiro. Recife: Cubzac, 2009. (Curso de curta duração ministrado/Extensão).

MARS, Amanda. EUA, UE e OTAN acusam China de lançar campanha global de ataques cibernéticos. **China**, El País, 19 jul. 2021. Internacional, p. 1.

MAZIERO, Arthur C; PINTO, Danielle J. Ayres**. Poder Cibernético e o espaço Internacional: uma Perspectiva a partir das Teorias das Relações Internacionais**. Segurança Internacional, Estudos Estratégicos e Política de Defesa. (2018)

MESQUITA, Felipe Souza. **Segurança Cibernética e a Política Internacional Contemporânea: novos desafios e oportunidades**. 2019. 38 p. Artigo (Especialista em Relações Internacionais) - Instituto de Relações Internacionais, Universidade de Brasília, [*S. l.*], 2019.

MORGENTHAU, Hans J. **A política entre as nações**: A luta pelo poder e pela paz. Hans J. Morgenthau: tradução de Oswaldo Biato --- Brasília: Editora Universidade de Brasília: Imprensa Oficial do Estado de São Paulo: Instituto de Pesquisa de Relações Internacionais, 2003. cap. XI, XII, XIII, XIV, p. 321-383. (Clássicos IPRI).

NYE JR, Joseph S. Compreender os conflitos internacionais: uma introdução à Teoria e à História. Tradução de Tiago Araújo. Lisboa, Portugal: Gradiva, 2002-a

NYE JR, Joseph S. 2010. **Cyber Power**. Harvard Kennedy School, Belfer Center for Science and International Affairs, pp.1-24.

NYE JR, Joseph S. O futuro do poder. São Paulo: Benvirá, 2011.

NOGUEIRA, J. P.; MESSARI, N. Teoria das relações internacionais: correntes e debates. Rio de Janeiro: Elsevier, 2005

PATINÕ OROZCO, Germán Alejandro. El sistema internacional cibernético: elementos de análisis. **Cybersecurity**, El sistema internacional cibernético: elementos de análisis., ed. 30, p. 163-168, jul./dez 2019.

PORTELA, Lucas Soares. **Movimentos Centrais e Subjacentes no Espaço Cibernético do século XXI**. 2015. 149 p. Trabalho de conclusão de curso (Pós graduação em Ciências Militares) - Escola de Comando e Estado- Maior do Exército, Rio de Janeiro, 2015.

REUTERS. A Casa Branca confirma que EUA pressionaram o Brasil sobre Huawei na rede 5G. **Casa Branca**, Belo Horizonte, 10 ago. 2021. Economia, p. 1

RID, T. **Cyberwar will not take place**. New York: Oxford University, 2013.

SIGHOLM, Johan. "Non-State Actors in Cyberspace Operations" Journal of Military Studies, vol.4, no.1, 2016, pp.1-37.

VENTRE, D. D. 2011. **Ciberguerra**. Paper apresentado no XIX Curso Internacional de Defensa, Seguridad Global y Potencias Emergentes em um Mundo Multipolar, Jaca, 2011. Catálogo General de Publicaciones Oficiales. Jaca: Ministerio de Defensa, 2012. pp. 32 - 45.