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

MANUELLA DA COSTA GADEGAST

POTÊNCIA CIBERNÉTICA: ATRIBUTOS E IMPLICAÇÕES

Porto Alegre
2022

MANUELLA DA COSTA GADEGAST

POTÊNCIA CIBERNÉTICA: ATRIBUTOS E IMPLICAÇÕES

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

Orientador: Prof. Dr. Marco Aurélio Chaves Cepik

Porto Alegre

2022

CIP - Catalogação na Publicação

Gadegast, Manuella
Potência Cibernética: Atributos e Implicações / Manuella Gadegast. -- 2022.
73 f.
Orientador: Marco Aurélio Chaves Cepik.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Relações Internacionais, Porto Alegre, BR-RS, 2022.

1. Potência Cibernética. 2. Ciberespaço. 3. Teoria. 4. Atributos. 5. Geopolítica Cibernética. I. Chaves Cepik, Marco Aurélio, orient. II. Título.

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

MANUELLA DA COSTA GADEGAST

POTÊNCIA CIBERNÉTICA:
ATRIBUTOS E IMPLICAÇÕES

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

Aprovada em: Porto Alegre, 05 de outubro de 2022.

BANCA EXAMINADORA:

_____

Prof. Dr. Marco Aurélio Chaves Cepik - Orientador
UFRGS

_____

Prof. Dr. Érico Esteves Duarte
UFRGS

_____

Prof. Dr. Carlos Schmidt Arturi
UFRGS

AGRADECIMENTOS

Primeiramente, gostaria de expressar o meu agradecimento à Universidade Federal do Rio Grande do Sul ou "*Mãe* UFRGS" pelo ensino público de altíssima qualidade que recebi. Ainda que tenhamos vivido ataques ao ensino superior e tenhamos vivenciado uma pandemia, perseveramos e vencemos frente a todas as adversidades. Aos professores e servidores, obrigada por construírem diariamente a nossa segunda casa.

Em segundo lugar, agradeço ao meu orientador Marco Cepik por ter aberto os braços para mim quando solicitei ajuda, por me proporcionar a experiência de pesquisa acadêmica, por me auxiliar e me orientar durante o processo do trabalho de conclusão, o qual por vezes acreditei que não teria competência para realizar. Obrigada por me mostrar o real significado de empatia e compreensão. Se hoje vejo a academia com outros olhos, é porque tenho o professor Cepik como referência, tanto pessoal, quanto profissional.

Agradeço também às minhas melhores amigas Amanda, Catherine e Júlia por todos os *facetime*, conversas e conselhos, madrugadas de estudo e parceria, obrigada por serem presentes mesmo quando a vida e nossas graduações nos afastavam e por entenderem as minhas ausências ao longo desse processo. Agradecimento especial aos meus amores da UFRGS, Marianna Oliveira, Francisca Falcetta, Giuseppe Morrone, Nataly Lemos e João Luís Meneghetti por se tornarem a minha base dentro da universidade. Foi a convivência com vocês que tornaram esses últimos 5 anos os anos mais divertidos e leves que tive. Obrigada por todo o apoio, parceria, conselhos e puxões de orelha.

Por fim, gostaria de agradecer a toda minha família que foi o principal apoio e força que eu poderia ter e me permitiram acreditar e vencer. Ao Pedro, obrigada por todas as conversas e conselhos, por acreditar em mim, por todos os choros consolados, por fazer com que nossa ponte aérea fosse tão pequena quanto quase inexistente e por ser a leveza e calmaria sempre que eu precisei. À minha prima Bárbara, com quem eu tive o privilégio de compartilhar desde o listão até cada momento na UFRGS. Obrigada pela nossa parceria e por sempre torcer e vibrar comigo. A UFRGS não teria tanta beleza e alegria, se não pudesse ser vivenciada contigo.

Por último, gostaria de agradecer aos meus pais, Silvia, Jair, Regis e Liliana, por me proporcionarem o privilégio de me dedicar plenamente aos meus estudos. Mas principalmente a minha mãe, Silvia, que sempre acreditou em mim, inclusive nos momentos que eu não tive fé que venceria. Aos meus irmãos, Bell e Kiko, obrigada por torcerem e vibrarem em cada vitória minha e por acreditarem na caçula na federal. Esse diploma só foi possível porque todos vocês caminharam ao meu lado nessa jornada. Obrigada de coração.

“Porque eu sou do tamanho do que vejo
E não do tamanho da minha altura”.

Alberto Caeiro

RESUMO

Com o surgimento de inovações, do desenvolvimento e da ampliação dos usos das tecnologias já existentes, cada vez mais se discute o papel que o ciberespaço desempenha no mundo contemporâneo. Para além do uso em operações de linhas de produção industriais, comunicação de veículos inteligentes, realização de cirurgias à distância através de robôs, desenvolvimento de armas a *laser* e inovação do uso da energia eletromagnética, as novas possibilidades de usos e aplicações do ciberespaço estão emergindo e prometem impactar profundamente os rumos da humanidade, não só a nível civil, mas a nível estatal. Com essa contextualização em mente, o presente trabalho procurou entender como se caracteriza uma potência cibernética com seus atributos, implicações e eficiência, a partir de uma discussão conceitual que inicia com a discussão da definição de ciberespaço e o papel que esse ocupa, por meio de uma análise dos seus atributos empíricos e implicações políticas. Dessa forma, ao utilizar a metodologia indutiva, procurou-se conceber o que é o ciberespaço, quais suas aplicações políticas pelos Estados e sociedades, e de que maneira o ciberespaço viabiliza a ascensão de uma potência cibernética. Em seguida, ao apresentar uma discussão teórico-conceitual sobre o ciberespaço, esse trabalho realiza uma revisão bibliográfica com o objetivo de analisar, no primeiro momento, as diferentes definições de ciberespaço na academia e, num segundo momento, definir e categorizar quais os atributos que viabilizam um Estado ser caracterizado como potência cibernética. Consoante isso, aborda-se uma teoria do poder cibernético, apresentando uma estrutura para compreender o poder cibernético de um Estado-nação, por meio da análise das capacidades físicas, virtuais e humanas que um país possui. Por fim, conclui-se que, além da necessidade de desenvolver uma infraestrutura física efetiva, uma infraestrutura virtual ampla e um volume social relevante, os Estados também precisam desenvolver e utilizar seus recursos com eficácia com o intuito projetar poder e influenciar os demais atores desse domínio.

Palavras-chave: Atributos. Ciberespaço. Geopolítica Cibernética. Potência Cibernética. Teoria.

ABSTRACT

With the emergence of innovations, the development and expansion of the uses of existing technologies, the role that cyberspace plays in the contemporary world is increasingly being discussed. Beyond its use in industrial production line operations, intelligent vehicle communication, performing remote surgeries through robots, developing laser weapons, and innovating the use of electromagnetic energy, new possibilities for uses and applications of cyberspace are emerging and promise to profoundly impact the directions of humanity, not only at the civilian level, but at the state level as well. With this contextualization in mind, the present work sought to understand how a cyber power is characterized with its attributes, implications, and efficiency, starting with a conceptual discussion that begins with the discussion of the definition of cyberspace and the role it occupies, through an analysis of its empirical attributes and political implications. Thus, by using inductive methodology, an attempt was made to conceive what cyberspace is, what its political applications are by states and societies, and how cyberspace enables the rise of a cyberpower. Then, by presenting a theoretical-conceptual discussion on cyberspace, this work performs a literature review with the purpose of analyzing, in the first moment, the different definitions of cyberspace in academia and, in a second moment, defining and categorizing which attributes make it possible for a state to be characterized as a cyber power. Next, by presenting a theoretical-conceptual discussion on cyberspace, this paper conducts a literature review with the purpose of analyzing, first, the different definitions of cyberspace in academia and, second, defining and categorizing which attributes enable a state to be characterized as a cyber power. Accordingly, a theory of cyber power is addressed, presenting a framework for understanding the cyber power of a nation-state, through the analysis of the physical, virtual and human capabilities that a country possesses. Finally, it is concluded that in addition to the need to develop an effective physical infrastructure, a broad virtual infrastructure, and relevant social volume, states also need to develop and use their resources effectively in order to project power and influence other actors in this domain.

Keywords: Attributes. Cyberspace. Cyber Geopolitics. Cyber Power. Theory.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface* ou Interface de Programação de Aplicação
ARPANET	*Advanced Research ProjectsAgency Network* ou Rede da Agência de Defesa e Pesquisa Avançada
BGP	*Border Gateway Protocol*ou Protocolo de Roteamento da Internet
C31	Controle, Comando, Comunicação e Inteligência
CERT	Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores
CPU	*Central Processing Unit* ou Unidade Central de Processamento
CSIRT	*Computer Security Incidente Response Team* ou Grupo de Resposta a Incidentes de Segurança
DARPA	*Defense Advanced Research Projects Agency* ou Agência de Defesa e Pesquisa Avançada
DNS	*Domain Name System* ou Sistema de Nomes de Domínio
GEO	*Geoestationary Earth Orbit*ou Órbita Geoestacionária
HTML	*HyperText Markup Language* ou Linguaguem de Marcação de Hipertexto
IANA	*Internet Assigned Numbers Authority* ou Autoridade para Atribuição de Números da Internet
IBS	*Integrated Bridge Systems* ou Sistema de Ponte Integrada
ICANN	*Internet Corporation for Assigned Names and Numbers* ou Corporação da Internet para Atribuição de Nomes e Números
ISP	*Internet Service Provider* ou Provedor de Serviço de Internet
ITU	*International Telecommunications Union* ou UniãoInternacional de Telecomunicações
LAN	*Local Area Network* ou Rede de Área Local
LEO	*Low Earth Orbit*ou Órbita Baixa
MRE	Ministérios das Relações Exteriores
NFC	*Near Field Communication*
NSF	*National Science Fundation* ou Fundação Nacional de Ciência

NSFNET	*National Science Foundation Network* ou Rede da Fundação Nacional de Ciência
PIME	Político, Informativo, Militar e Econômico
SWIFT	*Society for Worldwide Interbank Financial Telecommunications* ou Sociedade para as Telecomunicações Financeiras Interbancárias Mundiais
TCP/IP	*Transmission Control Protocol/ Internet Protocol* ou Protocolo de Controle de Transmissão/Protocolo de Internet
TICs	Tecnologias da Informação e Comunicação
TLS	*Transport Layer Security* ou Protocolo de Segurança
TTP	*Tactics, Techniques, and Procedures* ou Táticas, Técnicas e Procedimentos

SUMÁRIO

1. INTRODUÇÃO

A ascensão ao ciberespaço se intensificou nos últimos anos, especialmente com a evolução das tecnologias para uso privado e comercial, mas também devido aos fortes investimentos governamentais para o desenvolvimento de conhecimento e de tecnologias que lhes proporcionem, não só uma rápida ascensão e inserção nesse novo domínio, mas também uma vantagem frente às demais principais concorrentes. O presente trabalho busca compreender qual o papel que o ciberespaço desempenha no mundo moderno, a partir de uma análise sobre o conceito e desenvolvimento do ciberespaço, a compreensão das diferentes definições de poder com o intuito de abordar o melhor conceito de potência cibernética, por meio de uma análise dos seus atributos empíricos, implicações e capacidades.

O tema de pesquisa se mostra relevante, visto que o ciberespaço tem conquistado relevância com a evolução das redes de comunicação mundial e pelo fato de se tornar um domínio tão relevante quanto os domínios tradicionais – terra, mar, ar e espaço. O desenvolvimento e a ampliação dos usos das tecnologias já existentes têm provocado cada vez mais debates sobre qual o papel que o ciberespaço desempenha no mundo contemporâneo, bem como de que forma os atores do sistema internacional vão agir com esse novo espaço. Consoante isso, segundo Nye (2011), o amadurecimento tanto do ciberespaço, como das tecnologias provenientes, tem provocado uma revolução na geração, transmissão e utilização das informações, o que resulta na própria mudança da natureza do poder e daqueles que o utilizam. Para Joseph Nye (2011), os Estados continuarão a ser o ator dominante no cenário mundial, mas encontrarão um palco muito mais lotado e difícil de controlar.

A compreensão do potencial desse novo domínio se torna relevante, ao passo que, cada vez mais os estudos de segurança são incluídos na agenda de investigação e exploração político-estratégica do ciberespaço, seja por atores estatais, seja por atores não estatais (ARQUILLA E RONFELDT, 1997; 2001). Dessa forma, o claro entendimento do papel do ciberespaço no mundo moderno, aliado a uma formatação teórica capaz de apresentar orientações com o propósito de avaliar o potencial do poder cibernético e a efetividade cibernética de um ator específico no sistema internacional, poderá proporcionar recursos para, tanto futuras análises e pesquisas nos mais variados campos de atuação das Relações Internacionais, quanto para a atuações do Estados-nação no Sistema Internacional, demonstrando o real significado de operar no ciberespaço.

O objetivo geral deste trabalho busca entender como se caracteriza uma potência cibernética com seus atributos, implicações e eficiência, a partir de uma discussão conceitual que inicia com a discussão do conceito de ciberespaço, o papel que esse ocupa, por meio de uma análise dos seus atributos empíricos e implicações políticas. Esse entendimento será desenvolvimento por meio de uma compreensão a respeito, não só da definição de ciberespaço, mas também das possibilidades de usos e aplicações que estão emergindo e prometem desafiar e impactar profundamente os rumos da humanidade, não só a nível civil, mas a nível estatal. Para se alcançar esse objetivo, são estabelecidos cinco objetivos implícitos deste trabalho: (i) conceituar o domínio cibernético; (ii) analisar historicamente o domínio cibernético, (iii) conceituar o termo "poder" e posterior definição do termo "potência cibernética"; (iv) apresentar os recursos que compõe o domínio cibernético; e, por fim, (v) escolher uma teoria que funcione como basilar para a análise e pesquisa a respeito do poder cibernético.

No tocante a estrutura e organização, no primeiro capítulo serão desenvolvidas as principais características do ciberespaço. Esse capítulo está dividido em três subcapítulos que abordarão, respectivamente: (i) o conceito de ciberespaço – demonstrando as diferentes conceituações e pensamentos sobre o que é o ciberespaço e o que ele abrange, para, no fim, escolher a melhor definição que se adequa aos propósitos desse trabalho; (ii) a diferença entre ciberespaço e *Internet* – com o intuito de esclarecer a conceituação de cada um dos termos e suas respectivas origens, desde o estabelecimento da primeira rede de telégrafo até a liberalização comercial da *Internet,* demonstrando que essa é um resultado do ciberespaço; e, por fim, (iii) as interações políticas no ciberespaço – o qual está subdividido em oito unidades, nas quais são apresentados exemplos de relações do ciberespaço que vão desde o simples processos de comunicação ao maior nível de interação que o ciberespaço pode proporcionar, a guerra cibernética. Além do mais, busca-se compreender de que forma esse novo domínio influencia essas e outras atividades do meio.

No segundo capítulo, o trabalho irá abordar o poder cibernético, por meio de seus atributos e implicações. Esse capítulo está dividido em quatro subcapítulos que irão abordar, respectivamente: (i) o conceito de poder – ao revisitar as diferentes noções de poder desenvolvidos pelos principais pensadores das Relações Internacionais até abordar a melhor definição de poder com o objetivo de entender de que forma esse se projeta no ciberespaço; (ii) a definição de poder cibernético – no qual será analisado a tanto as diversas construções da definição de poder cibernético, quanto a escolha do melhor conceito que se adeque aos objetivos desse trabalho, bem como permita um entendimento da relevância que esse novo

domínio possui para os atores estatais e não estatais e para o Sistema Internacional; (iii) os atributos do poder cibernético – o qual está subdividido em três unidades, nas quais são apresentados os atributos (físicos, virtuais e sociais) que são fundamentais para que um ator (estatal ou não-estatal) seja caracterizado como "potência cibernética", mas também são de extrema importância para alcançar o objetivo de possuir e projetar poder no domínio cibernético; e (iv) a teoria do poder cibernético – no qual será apresentado uma breve amostragem das diferentes teorias sobre o poder cibernético e posteriormente será realizado uma análise sobre a teoria de poder cibernético de Robert Bebber (2017) por meio de um síntese abordando os principais recursos domésticos e globais, além de uma estrutura de análise são fundamentais para se avaliar o poder cibernético potencial de um Estado-nação e como esse obtém efetividade cibernética com base nos recursos abordados. A teoria escolhida será fundamental para basilar o propósito desse trabalho, além de servir como referencial teórico para futuras pesquisas acadêmicas e análises práticas.

Por fim, compreende-se que o ciberespaço tem adquirido maior relevância nos cenários internacionais e domésticos e tem se apresentando como um novo desafio para o mundo moderno. Dessa maneira, a conclusão alcançada é de que, para o desenvolvimento e atuação de uma potência cibernética, é necessário que os atores em questão, não somente apresentem capacidades estruturais, virtuais e atributos humanos, como também sejam capazes de desenvolver e utilizar seus recursos com eficácia de acordo com os eventos analisado e com seus objetivos de longo prazo, com o intuito projetar poder nesse meio, mas também sejam capazes de influenciar os demais atores desse domínio.

2. CARACTERÍSTICAS DO CIBERESPAÇO

O presente capítulo tem por objetivo conceituar o termo “ciberespaço” de acordo com a definição que melhor serve aos propósitos desse trabalho, bem como clarificar a diferença entre *“Internet*” e “ciberespaço”, além de exemplificar as estruturas e aplicações deste novo domínio.

2.1 O CONCEITO DE CIBERESPAÇO

Ao longo dos anos, diversos autores e especialistas do assunto têm contribuído e tentado definir o que é ciberespaço, esse novo domínio que tem permeado cada vez mais a vida das sociedades e dos Estados, impondo e exigindo-lhes novas realidades e novas posturas. Essa busca por uma definição vem desde a década de 1980 quando fora mencionado pela primeira vez no conto de William Gibson “*Burning Chro*me” para se referir a uma realidade virtual gerada por um computador (KELLNER, 2001). Entretanto, o termo obteve maior visibilidade ao ser apresentado ao público pelo mesmo autor em sua obra de ficção-científica “*Neuromancer*” publicada no ano de 1984. Alex Antunes (apud. GIBSON, 2003, p. 5-6), tradutor da edição brasileira do livro, afirma que:

> “O conceito criado por Gibson neste livro, o cyberespaço, é uma representação física e multidimensional do universo abstrato da ‘informação’. Um lugar para onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica pra trás”.

Gibson, ao longo do seu livro, constrói a ideia de ciberespaço como um espaço onde as máquinas e o seres humanos se alimentam e são dependentes entre si. Essa ideia ficou mais compreensível com o filme Matrix (1999) por mostrar visualmente a conexão entre máquinas e seres humanos, bem como, suas relações e espaços. RainOttis e PeeterLorents (2010) definem o ciberespaço como um conjunto dependente de tempo, de sistemas de informação interconectados e de usuários humanos que interagem com esses sistemas. Dessa forma, a definição de ciberespaço construída por Ottis e Lorents se assemelha com a própria definição desenvolvida por Gibson na sua obra “*Neuromancer*” de Gibson (1984). Por outro lado, Rabaça e Barbosa (2001) definem o ciberespaço como um espaço cibernético, um universo virtual formado pelas informações que circulam e/ou estão armazenadas em todos os computadores ligados em rede, especialmente a *Internet*; uma dimensão virtual da realidade, onde os indivíduos interagem através de computadores interligados. Rabaça e

Barbosa se afastam da definição de Ottis e Lorents e, por consequência, de Gibson, ao definir esse domínio por meio de uma construção menos dependente entre seres humanos e computadores, mas sim por meio de uma ideia de construção coletiva, na qual tanto as redes de computadores quanto os seres humanos existem de maneira independente, mas juntos viabilizam esse novo espaço de interação.

Apesar das definições sobre esse novo domínio digital, é comum a compreensão de que o ciberespaço é um conceito intangível, algo imaterial, um mundo afastado do nosso, onde as relações sociais, culturais e econômicas são construídas puramente na mente, um cenário distópico que é corroborado pela idealização no filme Matrix (1999). Entretanto, o ciberespaço também pode ser compreendido como um novo local de "disponibilização" de informações possibilitado pelas novas tecnologias. Segundo Monteiro (2007), é uma nova mídia que absorve todas as outras e oferece recursos inimagináveis, há algumas décadas. Trata-se de um espaço que ainda não se conhece completamente, cheio de desafios e incertezas, tanto na sua práxis, quanto em suas formulações filosóficas e teóricas. Um espaço aberto, virtual, fluido, navegável, no qual todos podem ascender e desenvolver suas tecnologias.

Contudo, por mais intangível que o cibesespaço se apresente, é possível trazer esse conceito para a realidade, como algo material, quando analisado também pela estrutura física que lhe viabiliza, não só a existência, mas também as diferentes possibilidades de usos e aplicações. Myriam Cavelty (2013), num dos subcapítulos sobresegurançacibernética da coletânea de Alan Collins intitulada por "*Contemporary Security Studies"*, ao introduzir um novo conceito ao significado do termo, revoluciona a noção de ciberespaço, visto que argumenta que o ciberespaço não é apenas um espaço virtual; esse também incorpora servidores, cabos, computadores, satélites etc; ou seja, ao trazer a noção de "espaço físico" para a conceituação do ciberespaço, Cavelty modifica a compreensão e dimensão ao adicionar outro elemento fundamental para a sua existência e funcionamento, além de incluir novos condicionantes que complexificam a sua expansão e viabilidade.

Já Fourkas (2004) desenvolve sua ideia de ciberespaço de maneira semelhante à de Cavelty; para ele, o ciberespaço é definido como uma inter-relação com o espaço real (físico), sendo necessário envolver seus aspectos físicos no desenvolvimento do conhecimento desse domínio. Assim, Fourkas afirma que a incorporação espacial do ciberespaço pode ser descrita como tendo pelo menos três camadas. A primeira camada é compreendida como a **técnica** – que se preocupa com a infraestrutura tecnológica do ciberespaço. Já a segunda camada é a **geográfica** – na qual a localização das redes de TICs

são formadas pela localização de seus nós (ou seja, computadores conectados a rede) e *hubs* (ou seja, ponto de acesso que interliga uma rede com o resto da rede (WANG et al., 2000, p.13). Por fim, a terceira camada é a camada **social** – que se preocupa com a organização espacial das pessoas que utilizam as redes de TICs. Fourkas afirma ainda que o ciberespaço é um sistema espacial, cuja distribuição de rede certamente depende da fixidez espacial, e cujo desenvolvimento é criticamente influenciado pela geografia do desenvolvimento econômico e tecnológico. Até então, todas as definições centralizavam suas definições somente no âmbito virtual do ciberespaço, sem criar a relação de necessidade com o desenvolvimento de uma infraestrutura física que lhe fornecesse a sustentação para funcionar.

Consoante isso, toda essa variedade de definições mostra que o ciberespaço embora seja um espaço de interesse comum, conhecido por todos, tanto carece de uma conceituação global, como também proporciona confusões de ordem semântica com a utilização entre "ciberespaço", "*internet*" e "*web*" como sinônimos. Essa confusão será abordada no tópico seguinte do capítulo, mas sua existência, não só é vista como uma ação relacionada com o surgimento de um novo domínio sem precedentes, mas que também é capaz de corroborar com a complexidade em conceituar com clareza e de forma definitiva o termo e, consequentemente, dificulta a criação de regulamentações e de legislações para uso e desenvolvimento desse novo domínio.

Com base nas diversas conceituações de ciberespaço abordadas nesse capítulo, esse trabalho irá adotar a definição de Daniel Kuehl (2009), uma vez que sua conceituação não confina o ciberespaço somente aos seus aspectos digitais, tampouco somente ao seu aspecto físico. Kuehl, em sua abordagem de caráter híbrido, destaca os critérios materiais necessários para a existência do próprio ciberespaço, os quais são usualmente pospostos pela literatura não técnica sobre o tema, ainda que classifiquem o ciberespaço como um ambiente digital. O autor define o ciberespaço como:

> [...] um domínio global dentro do ambiente da informação cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar, e explorar a informação através de redes interdependentes e interconectadas usando tecnologias, informação e comunicação(KUEHL, 2009, p. 29, tradução livre).

Para além dessas definições, os autores realizam frequentemente um esforço para distinguir a conceituação entre o ciberespaço e a *Internet;* no entanto, os seus estudos tendem a concentrar-se mais na *Internet* do que no ciberespaço. A convergência em torno do padrão IP e a exigência de ligar as redes privadas à *Internet*, a fim de otimizar o fluxo de informação

através da rede são as principais causas destas avaliações, que tendem a centrar-se num foco ao invés do todo. Consoante isso, esse detalhe, somado ao número de dispositivos interligados, à infraestrutura física de suporte e à abrangência territorial da *Internet*, aumentam a importância dessa última como a principal rede do ciberespaço e justifica as preocupações existentes com ela (CAVELTY, 2007). Kuehl, por envolver uma definição do ciberespaço que abrange tanto o caráter virtual, quando o físico, permite uma análise para além do enfoque na *Internet* e viabiliza uma análise do ciberespaço como um todo. Essa diferenciação será abordada de forma mais profunda no subcapítulo 2.2, intitulado *"Ciberespaço e Internet"* deste trabalho, no qual será possível compreender a diferenciação estrutural e virtual do ciberespaço e *Internet*, bem como o seu histórico.

2.2 CIBERESPAÇO E INTERNET

O surgimento do ciberespaço está relacionado com o desenvolvimento das redes de telégrafo na Inglaterra em 1839. No livro, "*Getting the Message: A History of Communication"*, Solymar (1999) descreve historicamente que o princípio do ciberespaço começou com a interação entre a física e a engenharia, utilizando a linguagem da matemática. Em 1753, foi proposto por *C.M.*[1] utilizar eletricidade para enviar mensagens com um circuito separado para cada letra do alfabeto. Segundo Burns (2003), ainda que a sugestão de *C.M* tenha sido inteiramente prática, dado o material adequado, a primeira tentativa de utilizar eletricidade fictícia para a transmissão de sinais entre duas salas foi feita por G.L. Lesage[2] em 1774, na cidade de Genebra. O telégrafo funcionaria através de um circuito fechado no qual, quando os interruptores estivessem fechados, uma corrente iria fluir pelo circuito fazendo com que a agulha magnética se desviasse, indicando assim que o evento esperado ocorreu, ou seja, a letra desejada havia sido "enviada"(SOLYMAR, 1999).

Dessa forma, poderiam se desenvolver circuitos para cada letra do alfabeto, de modo a utilizar os circuitos simultaneamente para o envio da mensagem desejada. Entretanto, desenvolver vários circuitos não era algo prático; os matemáticos, através dos conhecimentos de aritmética binária, propuseram uma solução que utilizaria menos circuitos. Para eles, estava claro que para transmitir 26 letras não precisariam de mais do que

[1] A identidade é desconhecida até hoje, mas o indivíduo se autodenominou C.M. na carta enviada para *Scotts Magazine* em fevereiro de 1753. (SOLYMAR, 1999)

[2] Georges-Louis Le Sage foi um físico suíço conhecido pela sua teoria gravitacional e por sua invenção de um telégrafo elétrico (PRÉVOST, 1805).

5 circuitos. Então, novamente, os matemáticos apresentaram outra ideia, utilizar ‘1’ e ‘0’ para escrever as mensagens – o interruptor seria carregado durante um longo tempo para um '1' e por um curto período para um '0'. Assim, para decodificar os ‘1’e ‘0’, o observador no outro extremo da linha teria de observar o tempo durante o qual a agulha magnética era desviada entre as pausas. E conforme fosse reconhecendo essas pausas, estabelecendo a ordem de ‘1’e ‘0’, seria possível decodificar a mensagem que havia sido enviada. E através do estabelecimento desse sistema de ‘1’e ‘0’, foi desenvolvido o primeiro telégrafo capaz de enviar mensagens.

Ainda que a primeira tentativa de usar o telégrafo tenha ocorrido em 1774 na Suíça, a primeira linha de telégrafo foi inaugurada em 1839, na Inglaterra; a segunda, logo em seguida, em 1840. Embora estivesse progredindo na criação de linhas de telégrafos, a Inglaterra necessitava ampliar cada vez mais as linhas, tanto para reduzir o período de transmissão das mensagens, mas também de modo a obter vantagens e expandir sua comunicação com seus vizinhos. Consoante isso, Solymar (1999) afirma que para estabelecer um sistema de comunicações telegráficas dentro de qualquer país europeu, as linhas teriam de atravessar rios, mas era necessário que os mares fossem um lugar deixados em paz, sem ser um alvo estratégico militar. Afinal de contas, era do interesse do governo poder comunicar para além das fronteiras do país. Em 1850, ocorreu a primeira tentativa de instalar um cabo submarino através do Cana, que foi bem-sucedida e levou a uma troca imediata de saudações entre a Rainha Vitória – da Inglaterra – e Luís Napoleão III – presidente da República Francesa. Posteriormente, o avanço dessas instalações conectou outras partes do continente.

Em 1857, Solymar (1999) afirma que já existiam ligações de comunicação direta com a Holanda, Alemanha, Áustria e Rússia. Contudo, o grande momento disruptivo do desenvolvimento do ciberespaço foi o estabelecimento da comunicação telegráfica entre a América do Norte e a Europa em agosto de 1858. Já em 1861, o comprimento total dos cabos colocados em todo o mundo era de 17.700 km, dos quais apenas 4.800 km funcionavam. Desde então, tem havido comunicações ininterruptas entre a Grã-Bretanha e os EUA. Esta interação por meio dos cabos submarinos formou o ciberespaço atual e a *Internet* que é utilizada mundialmente, uma vez que foi esse espaço virtual que viabilizou o desenvolvimento de diversas redes, em especial da *Internet* em 1969, por meio do desenvolvimento da rede ARPANET (LEINER, 1997).

Nesse ano, a DARPA (Agência de Defesa e de Projetos de Pesquisa Avançada) investiu milhões de dólares para o desenvolvimento de uma rede de comunicações que lhes

permitissem compartilhar informações dentro dos Estados Unidos. A rede foi desenvolvida e conectada entre a Universidade da California de Los Angeles e o Instituto de Pesquisa de Stanford. Nos anos seguintes da criação da ARPANET, outras tecnologias são desenvolvidas, como a invenção do *Protocolo 1822*[3] que levará a formação do *Protocolo TCP/IP*, ou seja, protocolos que compõem um conjunto de regras padronizadas que permitem a comunicação entre computadores em uma rede como a *Internet*. O desenvolvimento desses protocolos não só auxiliou a padronização de como as informações são enviadas e recebidas pelas redes, mas também contribuiu na construção dos fundamentos que viabilizaram o desenvolvimento propriamente dito da *Internet* como conhecemos hoje, haja vista que ambos são reconhecidos como a "linguagem" dos computadores e a forma que eles irão trocar dados pela *Internet* (LEINER, 1997). Em 1986, é criado o NSFNET pela Fundação Nacional de Ciência (*NSF*), com o intuito de promover uma rede de educação e pesquisa nos Estados Unidos, sendo o início da construção do *backbone* da *Internet.* Apesar dos avanços das conexões, apenas em 1991 é criado a interface amigável da *Internet*, visto que até o momento, eram interfaces técnicas a nível de programação (LEINER, 1997).

A partir de 1995, com a liberalização comercial do uso da *Internet* por todos os usuários, suas limitações desapareceram praticamente. Esse momento proporcionou uma maior diversificação e rápido crescimento da *Internet* e, por consequência, ampliou e redimensionou o ciberespaço (LEINER, 1997). Apesar do uso generalizado da *Internet* e intensificação do uso do ciberespaço, o próprio Gibson reconhece que, por suas histórias imaginativas, ele não previu o uso generalizado de redes de computadores como a *Internet* ao redor do globo, mas simplesmente usou desenvolvimentos tecnológicos reais para dar sentido aos mundos imaginários e futuristas descritos em seus romances (GIBSON, 1996). Para Gibson, esse universo não existia de fato, era algo irreal. Contudo, o desenvolvimento e inovações na área das comunicações demonstraram que esse universo virtual existe de fato, e o faz em um plano essencialmente diferente dos espaços conhecidos. Além do mais, por estar em constante mudança e desenvolvimento, o ciberespaço proporciona a possibilidade de que sua própria definição pode ser modificada com o tempo, em virtude de novos desenvolvimentos, aplicações, conexões e usos. E esse novo universo demanda uma nova postura de lidar com a sua existência, bem como de como agir, com o intuito de garantir que seus interesses sejam atendidos, seja Estado, seja usuário.

[3]*Protocolo 1822* – protocolo que definiu o padrão de mensagem que seria transmitida e daria início à comunicação entre hospedeiros do projeto ARPANET em 1969 (INTERNET SOCIETY, 2022).

Contudo, para que essa rede de computadores se conecte e forme o ciberespaço, são necessárias uma série de componentes físicos (*hardware*[4]) e virtuais (*software*[5]) que viabilizem a sua existência e conectividade. Dessa forma, segundo Kurbalija (2016), podemos definir três camadas essenciais que viabilizam o ciberespaço, bem como a própria *Internet*.

A primeira camada é formada pela infraestrutura de telecomunicações, através da qual ocorre todo o tráfego da *Internet* flui. Nessa camada, estão inseridos todos os *hardwares* ou componentes físicos essenciais para viabilizar a conexão e a transmissão do fluxo de dados, são eles: sistema de satélites, cabos de fibra ótica, teleportos, computadores, servidores, linhas telefônicas, antenas de transmissão, malha de cabos submarinos, roteadores etc.

A segunda camada é formada pelos padrões e serviços técnicos responsáveis pela tradução da transmissão dos dados e funcionamento da rede. Nessa camada, estão inseridos todos os *softwares* ou componentes virtuais que viabilizam a transmissão das informações pela rede, são eles: pacotes (pequeno segmento do todo de uma mensagem), Protocolo TCP/IP (também conhecido como *Transmission Control Protocol/Internet Protocol* ou Protocolo de Controle de Transmissão/Protocolo de *Internet*, o conjunto de regras para roteamento e endereçamento de pacotes de dados para que eles possam viajar pelas redes e chegar ao destino correto – a linguagem da conexão), DNS (*Domain Name System* ou Sistema de Nomes de Domínio, sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à *Internet* ou a uma rede privada), TLS (*Transport Layer Security* ou Protocolo de Segurança projetado para fornecer segurança nas comunicações sobre uma rede de computadores com três funções principais: Criptografia, Autenticação e Integridade). A terceira camada é formada pelos padrões de conteúdos e de aplicativos. Nessa camada, estão as diretrizes para a utilização e preservação da operação segura e estável da infraestrutura da *Internet*. Essa câmara será abordada com mais profundidade no subcapítulo 2.3 "*Interações Políticas no Ciberespaço*".

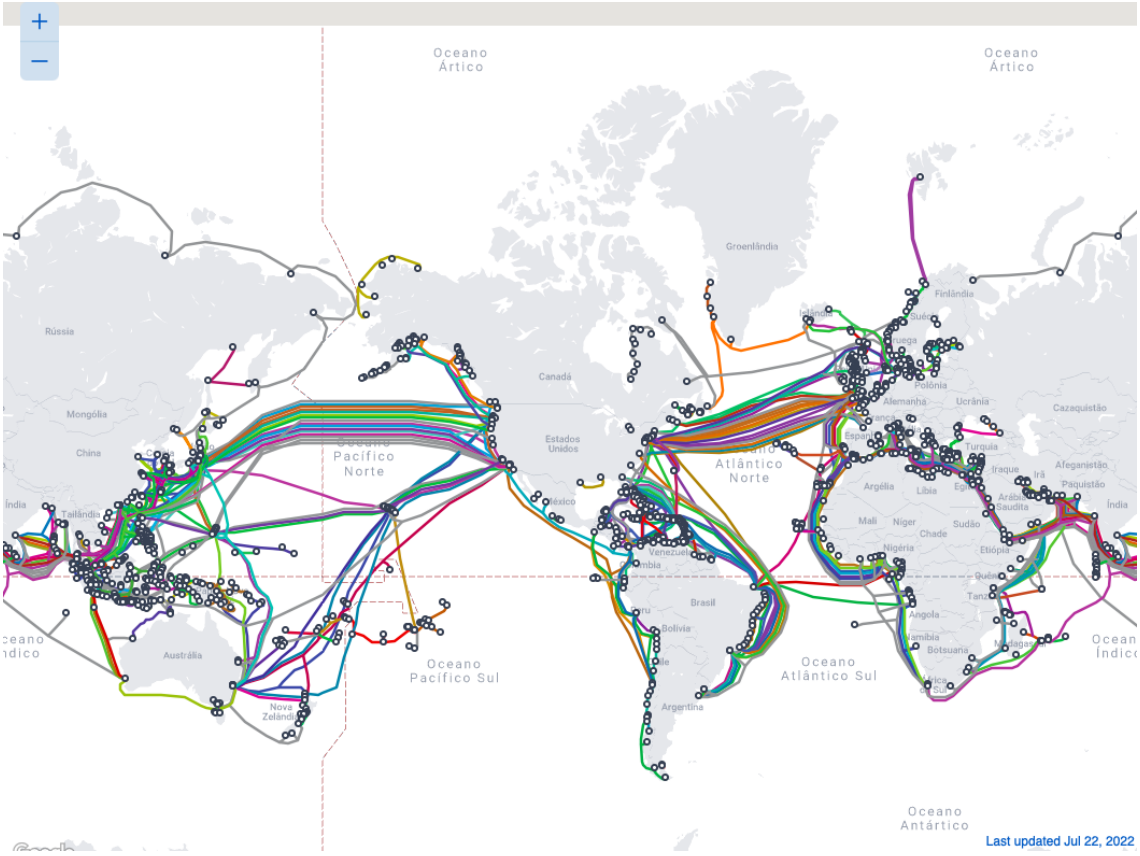
Ao analisar o conjunto de infraestrutura e padronização da rede é necessário incluir questões básicas, principalmente no âmbito técnico. Kurbalija (2016) afirma ainda que o principal critério para incluirmos ou não determinada questão no conjunto da infraestrutura é a sua relevância para a funcionalidade da *Internet.* A infraestrutura, na prática, é

[4]*Hardware* – componentes físicos e eletrônicos de um computador (CAMBRIDGE DICTIONARY, 2022).

[5]*Software* - sequência de instruções a serem seguidas e/ou executadas que controlam o que o computador realiza de ação (CAMBRIDGE DICTIONARY, 2022).

responsável pelo envio e recebimento de dados entre diferentes computadores conectados na rede, dentro ou fora de um país. A rede principal ou *backbone* (espinha dorsal da *Internet)* que irá viabilizar essa conexão é compartimentada em outras redes com o intuito de impedir que o tráfego e a transmissão de dados se tornem lentos ou sejam afetados caso ocorra alguma quebra das linhas de conexão. A função do backbone nas telecomunicações é de conectar as centrais de operadores de *Internet* aos servidores externos (nacionais ou internacionais), geralmente de forma redundante e por rotas diferentes.

Figura 1 - Disposição dos Cabos Submarinos



Fonte: Submarine Cable Map. Acesso em: 01 de agosto de 2022.

Os cabos submarinos, hoje, são responsáveis por 99% das comunicações transoceânicas feitas em todo o mundo, enquanto 1% da comunicação é realizada via satélites, segundo Nicole Starosielski, autora do livro “Undersea Network” (2015); e 80% do seu uso é voltado à *Internet*. Devido a distribuição dos cabos é possível mandar quase que instantaneamente fotos e mensagens; falar ao celular com quem está na Austrália; ou fazer uma reunião por Zoom (ou qualquer outra plataforma moderna de vídeo conferência) com alguém na Indonésia. Isso ocorre de forma simples, rápida, a partir da tela de um simples celular ou tela de computador. E através dessas conexões, cada computador da rede se

conecta a outro computador, constituindo uma rede e inserindo-se dentro de uma hierarquia agrupada de redes, desde a sua área local, ao seu fornecedor de serviços, às redes de telecomunicações regionais, nacionais e internacionais (DODGE & KITCHIN, 2001). Dessa forma, como revela Martinage (2015), grande parte da economia global depende dessa infraestrutura, uma vez que as cadeias globais de comunicação, de fabricação e serviços financeiros somente são possíveis devido aos cabos submarinos, e mais cabos são instalados a cada ano para atender à crescente demanda (CLARK, 2016).

Dessa forma, não é de se surpreender que, ao longo dos anos, com o crescimento da *Internet* também tenha ocorrido também o aumento da população concomitantemente ao aumento de usuários da *Internet*, principalmente quando analisamos os números brutos – uma população de 7.9 bilhões de pessoas (INTERNET WORLD STATS, 2022), 5.03 bilhões são usuários da *Internet* – em termos percentuais, 63,1% da população total (WEARESOCIAL, 2022). Consoante isso, esse crescimento de usuários na *Internet* mundial foi de 1 bilhão, em 2005, para 4.9 bilhões de usuários, em 2021 (ITU, 2021), além de apresentar uma taxa de penetração na sociedade mundial de 67,9% (INTERNET WORLD STATS, 2022). O crescimento desses dados são um reflexo da expansão do ciberespaço não só virtualmente, mas também fisicamente com o aumento da construção de novos cabos submarinos que viabilizam esse novo domínio – conforme já informado nesse trabalho previamente –, fortalecem sua infraestrutura, além de ampliar, intensificar e diversificar as conexões. Atualmente, existem mais de 400 cabos submarinos percorrendo1,3 milhão de km – o que equivale a quase 33 voltas ao redor da Terra (FACÓ; ANDRADE, 2022) e novos cabos entrarão em operação nos próximos anos.

Na tabela abaixo, é possível verificar alguns exemplos de novos cabos mundiais que entrarão em operação ao longo dos próximos anos.

Quadro 1 - Novos Cabos Submarinos que entrarão em operação até 2030

Nomenclatura	Previsão de início da operação	Pontos de conexão
Africa-1	2023	França, Egito, Arábia Saudíta, Yêmen, Dijibouti, Quênia, Emirados Árabes Unidos e Paquistão
Firmina	2023	Argentina (Las Toninas), Brasil (Praia Grande), Estados Unidos (Myrtle Beach) a Uruguai (Punta del Este).
Topaz	2023	Canadá (Vancouver e Port Albemi) a Japão (Shima e Takahagi)
Caribbean Express	2024	Colômbia (Cartagena), México (Cancún), Panama (Maria Chiquita) a Estados Unidos (Flórida)
Leif Erikson	2024	Canadá (Goose Bay) a Noruega (Stavanger)
HawaikiNui	2025	Austrália (Brisbane, Darwin, Melbourne e Sydney), Indonésia (Batam e Jakarta), Nova Zelândia (Christchurch, Duneidn e Invercargill), Singapura (Singapura) e Estados Unidos (Kapolei, Kawaihae e Los Angeles)
Polar Express	2026	Rússia (Andayr, Dikson, Murmansk, Nakhodka, Okrug, Pevek, Vladivostok e Yuzhno-Sakhalinks)

Fonte: Desenvolvido pela autora com base em Submarine Cable Map (2022)

A partir da definição de Kuehl (2009) sobre o que é o ciberespaço, o primeiro aspecto importante a ser destacado é a grande diferença que existe entre o conceito de ciberespaço e de *Internet*. O ciberespaço tem as características de uso da eletrônica e do espectro eletromagnético, as redes de telégrafo, rádio amador, telefonia fixa e/ou móvel e televisão via satélite o configuravam muito antes do advento da *Internet* (CEPIK; CANABARRO; BORNE, 2014). A *Internet* advém do ciberespaço como um resultado da evolução das redes e comunicações e, a partir dos anos 2000, essa se torna, não apenas a principal rede que compõe o ciberespaço, mas também a principal rede para a qual o desenvolvimento de recursos e aplicações têm se direcionado e tem revolucionado as comunicações. Assim, vale destacar que o uso incorreto de termos como "ciberespaço", "*internet*" e "web" como sinônimos é normal para o senso comum; contudo, sua persistência dificulta a criação e a adoção de políticas públicas e leis que almejem legislar ou regulamentar o ciberespaço, uma vez que não há clareza na compreensão dos termos (CANABARRO; BORNE, 2013).

Consoante a diferenciação entre ciberespaço e *Internet*, é necessária uma explicação breve do que são as redes de comunicações mundiais. A rede de comunicação mundial nada mais é do que um grupo de computadores conectados que são capazes de enviar dados uns

aos outros. Esses computadores se conectam a outros semelhantes e à *Internet* por meio de fios, cabos, ondas de rádio e de outros tipos de infraestrutura de rede. Uma rede de computadores é muito semelhante a um círculo social, que é um grupo de pessoas em que todos se conhecem, trocam informações regularmente e coordenam atividades em conjunto.

Para além dos cabos submarinos, satélites etc. que estão conectados e viabilizam a construção do ciberespaço, a rede de comunicação mundial pode ser classificada em dois níveis: *surface* e *deep web*. Para melhor compreensão, vamos utilizar a metáfora de um *iceberg*. Um *icerberg* é um bloco de massa de gelo que possui 10% de sua massa emerso na superfície e os 90% restante submersos na água. A relação da *web* com a metáfora do *iceberg* ocorre devido ao fato que o maior percentual de volume de dados e informações que circulam pelas redes de comunicação mundial ocorrem na *Deep web* e uma pequena parcela, visível e acessível, ocorre na *Surface*. Segundo dados levantados pela pesquisa realizada pela Visual Capitalist (ROUTLEY, 2017), enquanto a *Deep Web* armazenava cerca de 7.500 TB[6] de dados, a *surface* armazenava apenas 19 TB, o que equivale a cerca de 980.000.000 websites. Já comparando com todos os websites disponíveis em toda a *surface*, a *Deep Web* sozinha é na realidade 40 vezes maior do que a *surface*. Ainda que tais dados sejam de 2017 e tendo em mente a evolução e crescimento que as comunicações tiveram ao longo do século XXI, é de se imaginar que as porcentagens entre *surface* e *Deep Web* tenham se mantido iguais ou aumentado. Além do mais, o volume de dados deve ter tido um aumento significativo, ainda que não tenhamos dados oficiais atualmente para corroborar tal proposição.

Dessa forma, analisando as camadas da rede de comunicação mundial, o primeiro nível, a *surface*, também conhecida como *Internet*, é a camada "visível" da rede de comunicação. Inserindo esse conceito dentro da metáfora, a *Internet* é a ponta aparente do *iceberg*. Nessa região, estão localizados todos os sites e conteúdos que utilizam a arquitetura de redes cliente/servidos. Essa arquitetura é sustentada por máquinas que hospedam páginas *web*, banco de dados, arquivos e muitos outros serviços de uso diário e tais informações são encontradas por meio de mecanismos de pesquisa padrão, como Google e Yahoo e que podem ser acessados através de navegadores tradicionais, como Google Chrome, Safari, Mozilla Firefox. Além do mais, nessa camada, todo o conteúdo é indexado, ou seja, todas as informações disponíveis na *Internet* são inseridas e estão catalogadas nos servidores dos principais buscadores. Ao realizarmos uma busca na *Internet*, o sistema de busca irá analisar

[6]*Terabyte* – Unidade de medida de armazenamento na computação que é constituída por 1 milhão de bytes (CAMBRIDGE DICTIONARY, 2022).

o índice do catálogo do buscador específico e retornará com os resultados possíveis. Na surface é possível acessar todas as informações que estão indexadas nos principais serviços de buscas, e os sites estão cadastrados com os domínios tradicionais *.com*, *.org*, *.gov*, *.net etc.* A *Internet* e as informações disponíveis na surface correspondem a 10% da rede de comunicação mundial.

O segundo nível, a *deep web,* pode ser dividida em dois subníveis: a *Deep Web* e a *Dark Web*. Inserindo esse conceito dentro da metáfora, a *Deep Web* é a camada submersa do iceberg. Essa camada tem por característica principal o anonimato, a criptografia, a descentralização e a codificação aberta, cujo conteúdo não é "visível" pelas ferramentas convencionais (BARRETO, 2019), ou seja, não está indexado nos buscadores da surface. A *Deep Web* – primeiro subnível – é o local onde se encontra 90% das informações disponíveis na *Web* e tais informações não são acessíveis pelos buscadores da surface; contudo, isso não a torna um ambiente da *Dark Web* – tais informações apenas não estão inseridas nos catálogos e índices dos buscadores da surface. A principal diferença entre a *surface* e a *Deep Web* está majoritariamente em quais sites e dados estão indexados ou não. Na *Deep Web* estão localizados os mais diversos dados, como banco de dados comerciais, intranet privadas (redes internas de empresas, agências governamentais ou universidades), artigos científicos, documentos legais e oficiais, dados de cartões de créditos roubados.

A *Dark Web* – segundo subnível da *Deep Web* – é a parte da *Deep Web* com alto grau de anonimato e de segurança, uma vez que é utilizada para atos ilícitos criminais. É muito utilizada por usuário mal-intencionados na *Internet*, ativistas políticas, *blackhats*[7] e criminosos por garantir maior grau de privacidade nas comunicações e não aplicação da legislação penal dos países. Para acessar essa camada é necessário utilizar navegadores especiais, como *TOR*[8], *Freenet*[9]e *I2P*[10], que viabilizam ao usuário – através de uma navegação por meios de redes descentralizadas –, maior anonimato e criptografia. Essa criptografia, por ser mais complexa, é feita com mais camadas e com domínios que misturam números e letras – fugindo do padrão da surface – para que somente usuários mais avançados

[7] Blackhat – usuário que acessa um sistema de computador sem permissão por razões criminosas ou imorais (CAMBRIDGE DICTIONARY, 2022).

[8]*TOR* – software livre e de código aberto que proporciona a comunicação anônima e segura nos três níveis da rede de computação mundial. www.torproject.org.

[9]*Freenet* – plataforma de comunicação anticensura, cujo sistema se estrutura de tal forma que cada computador e/ou nó funciona tanto como cliente quando como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. www.freenetproject.org.

[10]*I2P* – plataforma que possui uma camada de rede totalmente privada e criptografada, permitindo a troca de mensagens entre usuários de forma segura e sob pseudônimos. www.geti2p.net.

tenham acesso a essa rede. Um grande volume de sites possui o domínio *.onion* e só são acessíveis utilizando o buscador *TOR*. Os demais sites que possuem essa complexidade na sua URL podem ser acessados pelos outros buscadores, como *Freenet*e *I2P*. Além disso, os fóruns, páginas e comunidades da *Dark Web* comumente são fechados e exigem *softwares* ou configurações específicas para que alguém consiga navegar, além de ser necessário muitas vezes ser convidados para acessar sua URL. A*Dark Web* é o local onde ocorrem compartilhamento de informações ilegais, tráfico de drogas, armas, pessoas, prostituição, pedofilia, comunicações privadas, sites TOR encriptografados, assassinos de aluguel, receitas de bombas etc.

Essa rede descentralizada da *Deep Web* é proveniente de uma arquitetura de redes de *ponto a ponto* (P2P), ou seja, dispensa um servidor central. Todos os componentes (pontos ou nós) funcionam ora como cliente, ora como servidor, estabelecendo entre si uma verdadeira via de mão dupla (BARRETO, 2019). Ao realizar uma busca por uma informação ou por um arquivo, cada nó da conexão pode fornecer partes menos dessa informação ou arquivo. Isso exemplifica a descentralização que ocorre na deep web, visto que, durante a transferência desse arquivo, caso um dos nós se desconecte da rede, o ponto que está solicitando essa informação a receberá de outro nó presente nessa rede.

Já a *Internet* utiliza uma arquitetura distribuída, ou seja, não há um centro de controle para a *Internet* mundial. Essa arquitetura é um sistema de rede distribuído, tornando-o independente de uma máquina individual. Qualquer computador que possa enviar e receber dados da forma pode fazer parte da *Internet*. Além disso, segundo a CloudFlare (2022) – uma das maiores empresas de rede de distribuição de conteúdo, serviços de segurança e hospedagem *da Internet* -, esse caráter distribuído da rede permite que computadores, servidores e outros *hardwares* conectam-se e desconectam-se da *Internet* o tempo todo sem afetar seu funcionamento, ao contrário de um computador, que pode não funcionar se faltar um componente.

Consoante a arquitetura da rede e muito similar a descrição realizada no início desse capítulo sobre a estrutura do ciberespaço – visto que a *Internet* faz parte do ciberespaço –, os autores Cepik, Canabarro e Borne (2014) constroem a ideia de que a *Internet* está estruturada em, no mínimo, três camadas distintas que a diferenciam e a tornam mais específica que o ciberespaço. A *camada inferior* tem relação com os elementos físicos que dão suporte às conexões e ao fluxo de dados que por meio delas circulam. São, por exemplo, as linhas telefônicas, os cabos de conexão, as antenas de transmissão etc. A *camada superior* compõe-se das informações partilhadas e acessíveis pelos usuários, que são codificadas e

decodificadas de padrões compreensíveis por seres humanos para padrões computacionais por aquilo que se encontra na *camada intermediária*, os padrões técnicos e lógicos responsáveis por esta tradução e funcionamento.

Para além dessas três camadas, os autores trazem ainda a ideia de uma *quarta camada*, a qual é originada do uso e da partilha dessas informações no ambiente por meio de interações sociais; ou seja, a *quarta camada* estaria relacionada ao aspecto social da *Internet,* dado o seu uso pelos atores sociais no que tange tanto do meio (infraestrutura e espaço), quanto dos dados (volume e informações compartilhados). Consoante isso, é nessa quarta camada que se dão as interações no ciberespaço e viabilizam diversas aplicações das inovações que surgem. Exemplos dessas inovações serão apresentadas e discutidas brevemente no subcapítulo *2.3 Interações Políticas no Ciberespaço* que virá em seguida.

2.3 INTERAÇÕES POLÍTICAS NO CIBERESPAÇO

O ciberespaço, através do seu desenvolvimento e crescimento, se tornou a "quinta fronteira" depois do oceano, da terra, do ar e do espaço. De 1995 até 2022, por meio de diversas mudanças físicas e estruturais, desenvolvimento de novas tecnologias, surgimento de novas aplicações, o ciberespaço passou a enfrentar novos desafios e assumiu um novo papel no mundo contemporâneo, ao mesmo tempo que é visto como um centro de colaboração e criação internacional, uma nova arena para a guerra e um local para a projeção do poder político, tecnológico, econômico, diplomático e militar. Com base nessa compreensão, a seguir serão apresentados e desenvolvidos exemplos dos principais tipos de interações no ciberespaço.

2.3.1 Comunicação

O principal objetivo do ato de comunicar é trocar informações entre dois ou mais interlocutores. O surgimento do ciberespaço por meio das redes de telégrafo, rádio amador, telefonia fixa e/ou móvel via cabos submarinos e, posteriormente, por satélites, criou justamente um ambiente de troca de informações e de interação, no qual não é necessário a presença física do homem para constituir a comunicação como fonte de interação (CEPIK; CANABARRO; BORNE, 2014). O seu desenvolvimento encorajou um estilo de relacionamento e comunicação quase independente dos lugares geográficos e da

coincidência dos tempos, e que o seu crescimento está relacionado a uma necessidade de comunicação mútua e inteligência de grupo (LEVY, 1999). Desse modo, a comunicação passou a ser o principal motor de desenvolvimento e estabelecimento de novos pontos de conexões; a malha de computadores dispersos pelo planeta viabiliza um novo espaço de interação e comunicação que vai além da transferência de informação, é também um local de geração e manutenção de relações sociais.

Dessa forma, a expansão satélites e torres de transmissão, o uso de correios eletrônicos, a criação de aplicativos de redes sociais como Telegram, Instagram e Twitter e de plataformas de vídeo conferências são exemplos práticos de aplicações do ciberespaço que possibilitam, tanto a troca de informações, quanto otimizam o processo de comunicação virtual. Tal proposição é corroborada quando analisamos que, em 2022, 55,2% da população entre 15 e 64 anos utiliza das conexões do ciberespaço para se comunicar com seus semelhantes (WEARESOCIAL, 2022). Esse novo espaço também cria um ambiente na qual a troca de informações contribui para a tomada de decisões políticas, desenvolvimento sociocultural de sociedades, uma vez que essas passam a utilizar a comunicação no ciberespaço como uma ferramenta de crescimento e desenvolvimento social.

2.3.2 Movimentação de Capital

O sistema financeiro atual talvez seja um dos setores que mais se beneficiou do uso do ciberespaço para o progresso de suas atividades. Entendido como fluxos econômicos de moedas, comércios, aplicações, pagamentos, empréstimos transfronteiriços, realizados por governos, bancos, empresas ou até mesmo pessoas, e cuja principal finalidade é facilitar e regulamentar essa cadeia de atividade de maneira a maximizar os ganhos, o sistema financeiro passou a utilizar as propriedades virtuais do ciberespaço para expandir, acelerar e otimizar as atividades econômicas(PONTIN; JÚNIOR, 2018). Um exemplo de aplicação moderno é a *NFC* (*Near Field Communication*) para formas de pagamentos. Essa tecnologia de comunicação de proximidade sem fio permite a transferência de dados em uma distância de até 10cmentre dispositivos eletrônicos (MADLMAYR, G et al, 2008). Além do mais, essa aplicação permite o uso de ferramentas alternativas a cartões físicos, como smartphone, pulseiras, adesivos, microships e relógios para efetuar pagamentos de forma rápida e otimizada.

Outra aplicação do ciberespaço é o sistema SWIFT (*Society for Worldwide Interbank Financial Telecommunication*). Ainda que esse sistema tenha surgido em 1973 – antes da

comercialização da *Interne t–*, seu propósito sempre foi facilitar as operações financeiras mundiais; com o advento do ciberespaço e inovações tecnológicas oriundas dessa evolução, o sistema aproveitou as redes de conexões e praticidade de comunicação para otimizar a troca de informações entre instituições financeiras no momento das transferências bancárias transfronteiriças ao enviar instruções para banco de outros países usando códigos e formatos padrões (EICHENGREEN, 2022). Dessa forma, por ser uma rede de bancos e depender fortemente dos bancos como unidades operacionais (QIU; ZHANG; GAO, 2019), o sistema SWIFT se beneficiou do ambiente do ciberespaço, uma vez que esse otimizou e acelerou o envio dessas informações por meio da instantaneidade das conexões através das diferentes redes existentes no mundo.

2.3.3 Negociações Diplomáticas

A diplomacia pode ser compreendida como um instrumento da política externa com o objetivo de estabelecer e desenvolver contatos pacíficos, celebrar relações entre os governos de diferentes Estados por meio do emprego de intermediários. Segundo Hedley Bull (1977/2002), existem cinco funções principais na prática diplomática: (i) facilitar a comunicação na política mundial; (ii) negociar acordos;(iii) recolher informações e informações de outros países; (iv) evitar ou minimizar "fricções nas relações internacionais"; e, finalmente, (v) simbolizar a existência de uma sociedade de Estados. O surgimento das redes e da *Internet* auxiliou diretamente as cinco funções principais, ao tornar esses processos mais rápidos e automáticos, viabilizando o surgimento de uma nova diplomacia – a Diplomacia Digital. Segundo Manor & Segev (2015), a diplomacia digital refere-se principalmente à utilização crescente das plataformas de comunicação social por um país para atingir os seus objetivos de política externa e gerir proativamente a sua imagem e reputação. Riordan (2016), por sua vez, analisa mais profundamente e propõe a distinção entre a ciberdiplomacia e a diplomacia digital, explicando que a diplomacia digital se refere à utilização de ferramentas e técnicas digitais para fazer diplomacia, enquanto a ciberdiplomacia se refere à utilização de ferramentas diplomáticas e à mentalidade diplomática para resolver questões que surgem do ciberespaço.

Além do mais, a *Internet* e outras redes de conexão alteraram a forma como a comunicação diplomática afeta o desempenho do diplomata no ambiente digital, colocando novos métodos de utilização destas novas ferramentas e provocando novos cuidados e medidas de segurança que ele deve tomar para que a sua informação e trabalho possam

alcançar os resultados desejados. O advento das redes, por exemplo, pôde aproximar ainda mais a diplomacia da sociedade, deixando de ser um assunto a nível estratégico guiado pelos tomadores de decisão e passando a incluir a participação social, por meio da comunicação que os órgãos oficiais do Ministério das Relações Exteriores (MRE), por exemplo, e dos próprios diplomatas realizam nas redes sociais. Essa conexão, não só propicia uma interação em tempo real com outros diplomatas de outros países, mas também permite que os próprios diplomatas consigam levantar pautas sobre temas importantes, para que a sociedade também reflita sobre elas.

2.3.4 Geração e Processamento de Dados – *Big Data*

A sociedade produz dados diariamente nas suas mais diversas atividades. Com a expansão das redes de comunicação e o surgimento da *Internet*, foi desenvolvido uma nova forma de geração de dados – a *Big Data*. O termo se refere aos dados gerados em quantidades gigantescas (na casa dos *terabyte* e *petabyte*[11]), com grandes variedades que chegam com volumes crescentes e com velocidades cada vez maiores; são dados bastante complexos, porém não-estruturados, os quais podem ser trabalhados para extrair informações, padrões e correlações (CORREA, 2019; SKOURLETOPOULOS *et al.*, 2017). O *Big Data* se diferencia dos dados normais devido a sua amplitude em termos de alcance, velocidade e complexidade que possui, trazendo novas possibilidades e potencialmente revolucionando como processamos e analisamos informações (LANGWORTHY, 2019).

Chandler (2015) afirma que cada passo e ação que tomamos hoje deixa um rastro digital. E a datificação que o próprio autor apresenta aproxima o *Big Data* da realidade da sociedade, visto não só se geram novos e melhores dados frequentemente, mas também os utilizam com inteligência – que é também uma consequência do surgimento dessa inovação tecnológica. Hoje, essa geração e processamento de dados podem proporcionar benefícios desde análises complexas a tomadas de decisões nos mais diversos campos e momentos. Manyika (2011) elenca 5 setores, no qual o *Big Data* apresenta oportunidades de crescimento e propicia usos e *insights* mais inteligentes devido a riqueza desses dados. São eles: (1) **saúde:** análise de padrões de doenças, melhorias na saúde pública etc; (2) **setor público:** criar transparência através de dados acessíveis, tomada de decisões por meios de sistemas

[11] *Petabyte* - Unidade de medida de armazenamento na computação que é constituída por 1024 terabytes. (COTEC – UFRB, 2022)

automatizados para redução de riscos etc; (3) **produção industrial:** planejamento da cadeia de produção, apoio às estratégias de venda etc; (4) **geolocalização pessoal:** sugestões inteligentes com base no histórico de movimentação urbana, rotas inteligentes etc; e (5) **varejo:** melhorias de desempenho, distribuição e otimização logística etc.

2.3.5 Ciberativismo

O ciberativismo pode ser compreendido como uma consequência da globalização das redes de computadores e que tem provocado a expansão das relações sociais, principalmente a partir das novas tecnologias de comunicação. Assim, por ciberativismo podemos denominar um conjunto de práticas em defesa de causas políticas, socioambientais, sociotecnológicas e culturais realizadas nas redes cibernéticas (SILVEIRA, 2010). As estratégias de utilização da *Internet* para o ciberativismo objetivam aprimorar a atuação de grupos, ampliando as técnicas tradicionais de apoio. Desse modo, utiliza-se a rede de diversas formas, seja para divulgar informações, organizar e/ou mobilizar indivíduos para eventos *on-line* e *off-line*, seja para desenvolver iniciativas de *"hacktivismo",* ou seja, utilizar um ataque cibernético como forma de protesto (PISCITELLO, 2015).

Segundo Castells (2001), enquanto as lutas sociais modernas eram marcadas por movimentos que mantinham a sua hierarquia condizente com os valores verticais da industrialização, as lutas contemporâneas apresentam movimentos sociais com uma estrutura cada vez mais horizontal e em rede. Com a expansão do ciberespaço e comercialização da *Internet*, os ativistas expandiram suas atividades tradicionais e/ou desenvolvem outras. Ao utilizar a *Internet* como uma ferramenta imprescindível para o desenvolvimento dessas lutas sociais contemporâneas, o ciberativismo não só facilitou as atividades (em termos de tempo e custo), pode unir mobilizar indivíduos e entidades para ações e protestos *on-line* e *off-line* e em diferentes localidades em prol de uma causa local ou transnacional, bem como almejou quebrar o monopólio da emissão e divulgar informações "alternativas" sobre qualquer assunto (RIGINATO, 2003).

2.3.6 Atividade Criminal

O crime cibernético é definido como o desenvolvimento de ações ilícitas com o emprego de computadores e da *Internet* com o intuito de gerar danos a indivíduos ou patrimônios, por meio de extorsão de recursos financeiros, estresse emocional ou danos à

reputação de vítimas expostas na *Internet*. Alguns autores, entretanto, diferenciam o crime cibernético de crimes informáticos, visto que esse refere-se a crimes "em que o usuário usa conhecimento especial do ciberespaço", enquanto este ocorrem porque "o usuário usa conhecimento especial sobre tecnologia informática" (FURNELL, 2002). Alguns exemplos de crimes cibernéticos: *ransonware*[12] (sequestro de dados), vazamento de dados, *phishing*[13] (roubo de informações confidenciais), *smishing*[14] (roubo de informações confidenciais), *malware*[15] (software malicioso), ataque DDOs[16] (ataque de negação de serviço), *cryptojacking*[17] (sequestro de computadores para minerar criptomoedas) etc.

Uma das principais características do ciberespaço que atrai tantos usuários é o fato de poder proporcionar o anonimato ao longo da navegação, característica que não está disponível nos outros quatro domínios de poder – água, terra, mar e ar. O Cyber Comando dos EUA reconhece o ciberespaço como o quinto espectro de batalha, sendo utilizado pelos criminosos em incursões de ciberataques e cibercrimes (MARCELINO, 2021). Dessa forma, com o advento da expansão de atuação do ciberespaço, o volume de crimes cibernéticos tem crescido exponencialmente. No Brasil, somente em 2021, houve um total de 9,1 milhões de ocorrências de fraudes digitais com o mercado financeiro ocupando 63,1% do total, com 1,2 milhão de tentativas de fraude. E essas mesmas fraudes geraram um prejuízo que chegou no valor de 6 trilhões de dólares (AXUR, 2022). Além do mais, os prejuízos com crimes cibernéticos seguirão crescendo no mundo em média 15% por ano até 2025, gerando um estrago de 10,5 trilhões de dólares (MORGAN, 2020).

---

[12] *Ransonware* - um software utilizado para sequestrar e bloquear o computador de um usuário e depois exigir um resgate para desbloqueá-lo (KASPERSKY, 2022).

[13] *Phighing* - ataques de engenharia social, no qual é enviado um e-mail fraudulento se passando por um destinatário de confiança do usuário e solicitando informações confidenciais de acesso à conta, com o intuito de acessar a conta e roubar informações. (TRENDMICRO, 2022).

[14] *Smishing* –é uma combinação de “SMS” e “phishing”, a ação é semelhante à do phishing, contudo, no lugar de um e-mail é enviado um SMS solicitando o mesmo tipo de informação(KASPERSKY, 2022).

[15] *Malware* – é um software malicioso desenvolvido para infectar o computador de um usuário e prejudicá-lo de diversas formas. O malware pode assumir diversas formas, entre elas vírus, Worms, cavalos de Troia, spyware e outros (KASPERSKY, 2022).

[16] *Ataque DDOS* – Ataque de negação de serviço distribuído são tentativas mal-intencionadas de interromper as operações normais de um servidor, serviço ou rede visados ao sobrecarregá-los com uma enchente de tráfego de internet (CLOUDFLARE, 2022)

[17] *Cryptojacking* - é um tipo de crime cibernético onde um criminoso usa secretamente o computador de um usuário para gerar/minerar criptomoedas sem que o usuário saiba. Não há roubo de dados, mas sim roubo de energie e de capacidade computacional (INTERPOL, 2022).

2.3.7 Terrorismo Cibernético

Segundo Weimann (2005), o terrorismo cibernético ou ciberterrorismo se caracteriza como o uso de ferramentas de rede de computadores para prejudicar ou fechar infraestruturas nacionais críticas (tais como energia, transporte, operações governamentais). Haja vista que um ciberataque generalizado pode apenas causar inconvenientes, em vez de pânico como uma bomba ou outra arma química ou nuclear explosiva, alguns estudiosos sugerem que a palavra "ciberterrorismo" não deve ser usada para caracterizar esse tipo de ação. Outros pesquisadores interpretam que os efeitos de um ataque generalizado à rede de computadores seriam imprevisíveis e poderiam causar perturbações econômicas, medo e mortes civis suficientes para se qualificar como terrorismo (ROLLINS; THEOHARY, 2011). Essa interpretação ocorre principalmente devido à "reação em cadeia" que um ataque desses pode provocar, uma vez que as redes nacionais e internacionais de comunicação, de fabricação, de serviços financeiros e infraestruturas entre outras estão conectadas e possuem diferentes graus de dependências uma das outras.

A expansão das redes de computadores mundiais, o desenvolvimento de novas tecnologias e as possibilidades de conexões entre Estados-nação, infraestruturas críticas e/ou outros setores corroboram a premissa do ciberterrorismo de que, conforme os Estados-nação e a infraestrutura crítica se tornam mais dependentes das redes de computadores para sua operação, novas vulnerabilidades são criadas e passíveis de serem utilizadas indevidamente. Assim, o receio dos Estados-nação não se baseia tanto no surgimento de uma classe de atores originalmente caracterizados como ciberterroristas, mas sim que organizações terroristas contemporâneas passem a utilizar essa nova modalidade de ataque com tecnologias avançadas de computador e redes para realizar ataques ao invés de utilizar ferramentas tradicionalmente conhecidas – armamento de aeronaves, armamento terrestre, armas, mísseis etc. (ROLLINS; WILSON, 2007). Segundo Joseph Nye (2011), esse medo é ratificado quando analisamos que, antigamente, os grupos terroristas muitas vezes tiveram uma dimensão transnacional; a evolução e uso do redes de conexões fez com que a Al Qaeda – por exemplo –, de uma rede transnacional, se transformasse numa rede solta que atravessa o globo com sua franquia.

2.3.8 Guerra Cibernética

O conceito de guerra – um conflito de larga escala marcado pelo uso da violência entre grupos politicamente estabelecidos com o emprego de forças militares, em um determinado período com o intuito de obrigar nosso adversário a cumprir nossa vontade (CLAUSEWITZ, 1940) – obteve uma nova dimensão com a expansão e uso do ciberespaço, fazendo surgir um novo termo – *guerra cibernética*. A ciberguerra ou guerra cibernética é uma modalidade de guerra em que a conflitualidade não ocorre com armas físicas, mas por meios eletrônicos e informáticos no ciberespaço, no qual Estados-nação realizam ações para penetrar nos computadores ou redes de outro Estados-nação com o propósito de causar danos ou perturbações" (CLARKE; KNAKE, 2012). Além disso, a guerra cibernética pode ser compreendida como o ápice da evolução de todas as aplicações do uso do ciberespaço mencionadas previamente neste subcapítulo, visto que, em algum grau, a guerra cibernética não só acontece por meio do surgimento dessas inovações, mas também como evolução das diferentes aplicabilidades dessas tecnologias.

Contudo, para Möckly (2012), guerra cibernética "é também utilizado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada", visto que eventos cibernéticos variam em relação à forma, à complexidade e ao alvo (CEPIK; CANABARRO; BORNE, 2014). Para alcançar objetivos politicamente significativos, os ataques cibernéticos devem contribuir para outros aspectos de um esforço de guerra mais convencional. E para afetar o equilíbrio de poder a longo prazo, por exemplo, a guerra cibernética deve ser unida a outras formas de guerra mais tradicionais (GARTZKE, 2013). Desta forma, o desenvolvimento da guerra cibernética será influenciado pela ocorrência de eventos cibernéticos que prejudicam os Estados-nação, assim como seus efeitos potenciais na vida diária, nos assuntos domésticos dos Estados e nas relações internacionais. Também será influenciado pela forma como esses eventos serão respondidos e como eles serão realizados.

Com base nesse subcapítulo, foram expostos algumas possíveis aplicações e possibilidades de utilização e interação no ciberespaço. Entretanto, o ciberespaço não está limitado a essas aplicações, há ainda outras diversas situações tais como Inteligência Artificial, os próprios websites de navegação, bibliotecas digitais, interações sociais no metaverso, ensino à distância, comércio digital etc. O Ciberespaço é o espaço mediador da convivência digital entre seres humanos, em criação a partir da disseminação e evolução das redes de computadores mundiais. É por meio do desenvolvimento dessas aplicações que se configuram o poder cibernético, uma vez que os Estados-nação passam também a

desenvolver suas capacidades, desempenhar influência com o intuito de alcançar seus objetivos nacionais. Assim, no próximo capítulo será discutido a conceituação de poder cibernético, bem como, quais os atributos conferem um Estado-nação esse poder.

3. POTÊNCIA CIBERNÉTICA: ATRIBUTOS E IMPLICAÇÕES

O presente capítulo tem por objetivo revisitar o conceito do termo “poder”, com o intuito de fundamentar o que, posteriormente, será debatido e proposto como a definição de “poder cibernético” que melhor serve aos propósitos desse trabalho. Consoante isso, será realizado uma análise dos principais atributos do ciberespaço que conferem a um Estado-nação a classificação de “potência cibernética”, à medida que esse detenha os recursos necessários para desempenhar seu poder nesse domínio e alcançar seus objetivos; além de debater as principais teorias cibernéticas e de que forma essas servem para a construção de uma potência cibernética.

3.1 REVISITANDO O CONCEITO DE “PODER”

O desenvolvimento e a ampliação dos usos das tecnologias já existentes têm provocado cada vez mais debates sobre qual o papel que o ciberespaço desempenha no mundo contemporâneo, bem como de que forma os atores do sistema internacional vão agir com esse novo espaço. Dessa forma, a própria noção de poder passa a ser rediscutida; questiona-se como se constitui uma potência cibernética e se ela surge com o intuito de se adequar ou de dominar esse novo domínio. Assim, o amadurecimento do ciberespaço tem provocado uma revolução da informação e essa está mudando a natureza do poder (NYE, 2011) e aqueles que dela usufruem. Para Joseph Nye (2011), os Estados continuarão a ser o ator dominante no cenário mundial, mas encontrarão um palco muito mais lotado e difícil de controlar. Contudo, antes de avançarmos sobre a constituição de uma potência cibernética, é necessário esclarecer o que se constitui por “poder” e como esse se apresenta no ciberespaço.

O conceito de poder tem sido estudado ao longo da história da sociedade com os mais diferentes focos. O dicionário traz a definição mais crua e ampla, na qual o poder é a capacidade de fazer as coisas (NYE, 2004). Por ter uma conceituação mais genérica, essa definição não envolve as possíveis relações resultantes que viabilizam de fato o surgimento do poder. Já para Thomas Hobbes, em seu livro *Leviatã* (1651), o entende da seguinte forma: “poder é o conjunto de meios empregados para obter uma aparente vantagem futura”. Esse é cedido pelos homens para uma autoridade superior – o Estado – por meio de um contrato social com o intuito de proporcionar a justiça social e evitar a guerra por meio de imposições de condições que determinam o comportamento da coletividade (AGUIAR, 2008),

resultando, consequentemente, em vantagens para os atores que estão envolvidos nessa relação – os indivíduos, a sociedade.

Norberto Bobbio, Nicola Matteucci e Gianfranco Pasquini, no livro "Dicionário de Política" (1998), apresentam outras diferentes conceituações de poder, entre diferentes perspectivas e com variados focos. Contudo, os autores comentam sobre uma ótica de definição do conceito de poder que é utilizado indiretamente pelos estudiosos das relações internacionais – o sentido social da relação. Para os autores, o poder é definido mais precisamente quando analisado na ótica da relação da vida do homem na sociedade, em seu sentido particularmente social, e seu espaço conceitual pode variar desde a capacidade geral do homem de agir até a capacidade do homem de ditar a conduta do próprio homem, sendo o "poder do homem sobre o homem. O homem é não só o sujeito, mas também o objeto do poder social" (BOBBIO; MATTEUCCI; PASQUINI, 1998, p. 934). Orientado pelo sentido social da relação de poder, o conceito amplamente utilizado nas relações internacionais está na definição de Joseph Nye (2011), no qual o poder é visto como a capacidade de modelar o comportamento dos outros com o propósito de obter os resultados que se almeja. Existindo várias maneiras de afetar o comportamento dos outros, seja coagindo-os, seja induzindo-os ou simplesmente atraindo e cooptando-os a fazer ações que estejam alinhadas com os objetivos.

Consoante isso, com o entendimento e uso da noção de poder, Joseph Nye (2011) demonstra ser necessário identificar quem está envolvido na relação de poder (o escopo do poder), bem como quais são os tópicos envolvidos (os domínios do poder), visto que dessa maneira a compreensão do contexto de aplicação do poder se torna mais evidente e o(s) ator(es) pode(m) estabelecer com fundamento qual estratégia será utilizada para alcançar os seus objetivos. Segundo Bobbio, Nicola e Pasquini (1998, p. 938), "o comportamento de cada ator (partido, grupo de pressão, governo etc.) é determinado parcialmente pelas previsões do ator relativas às ações futuras dos outros atores e à evolução da situação em seu conjunto". Aliado a isso, Joseph Nye (2011), ratifica essa necessidade ao trazer o exemplo da relação do Papa com os cristãos – no qual este exerce poder (seja político, seja espiritual etc.) sobre alguns cristãos, mas não sobre outros (as outras vertentes da igreja católica, como os protestantes). Consequentemente, uma compreensão do contexto da situação no qual se está inserido aumenta a possibilidade da eficácia da utilização dos recursos de poder e da sua conversão em resultados desejados, uma vez que a transformação de seus recursos em resultados comportamentais efetivos é um fundamental para a sua existência; o fato de

possuir os recursos de poder não garantem necessariamente que o alcance dos objetivos almejados.

Em todas as definições expostas acima, é possível verificar que a noção de "poder é entendido como algo que se possui: como um objeto ou uma substância" (BOBBIO, MATTEUCCI & PASQUINO, 1998, p. 934), mas a sua existência e aplicação vão além da simples posse, sendo diretamente dependentes das ações realizadas por diferentes atores implicados nessa relação inicial. Desse modo, o conceito de poder utilizada neste trabalho, e que fornecerá a base para a compreensão do conceito de "poder cibernético", consiste na seguinte definição: "poder é a capacidade de possuir meios e utilizá-los para influenciar comportamentos de terceiros e obter os resultados desejados". Essa escolha ocorre pela compreensão de que, mais relevante do que possuir recursos, ter poder significa ter a capacidade de utilizá-los de acordo com suas necessidades e objetivos dentro da conjuntura previamente estabelecida. Consoante a escolha da definição de poder, objetiva-se estender essa compreensão para o domínio do ciberespaço e, consequentemente, tentar estabelecer uma definição para o próprio domínio, mas que esteja de acordo com as definições prévias e academicamente aceitas. Essa discussão e, consequentemente, escolha será realizada a seguir no subcapítulo *3.2 Definição e Atributos do Poder Cibernético*, no qual será possível compreender o que se entende por poder cibernético e quais são os atributos fundamentais que o compõe.

3.2 DEFINIÇÃO DO PODER CIBERNÉTICO

A definição de novos conceitos está relacionada com a maturidade que o novo setor e/ou termo adquiriu ao longo da sua existência. Frequentemente, há dificuldades em delimitar um conceito, visto que o seu entendimento não está plenamente compreendido. Essa situação ainda acontece na academia quando relacionado a definição do que se constitui por "poder cibernético". Durante as últimas décadas, várias definições sobre esse novo tipo de poder foram estabelecidas, haja vista que, principalmente, a partir do final do século XX, vários Estados-nação têm utilizado meios cibernéticos para desenvolver e alcançar seus objetivos nacionais. Dado essa evolução, não é novidade que o poder cibernético esteja desempenhando um papel cada vez mais crucial na força econômica de um Estado-nação (KUEHL, 2009b).

Além do mais, tanto o ciberespaço, quanto o próprio poder cibernético têm se mostrado como novas dimensões de poder – agora, informativo – segundo Kuehl (2009b), sob o modelo PIME (político, informativo, militar e econômico). O ciberespaço globalizado

e interligado é possivelmente o fator mais significativo que une todos os atores da economia do "mundo plano" do século XXI, aumentando a produtividade, abrindo novos mercados e possibilitando estruturas de gestão que são simultaneamente mais planas, mas com um alcance muito maior (KUEHL, 2009b). Haja vista esse crescimento dessa nova dimensão, torna-se relevante o fato de que o poder cibernético por ser emergente dos Estados, pode ser quantificado e medido; e a sua clara definição se configura como a possibilidade de viabilizar a classificação dos Estados dentro desse domínio sob seus aspectos que o compõe, bem como do seu nível de poder e influência.

Desta forma, dentre as várias tentativas de conceituar poder cibernético, há a que o entende como "a variedade de poderes que circulam no ciberespaço e que moldam as experiências daqueles que agem no e através do ciberespaço" (VAN HAASTER, 2016, p. 13). Essa definição se apresenta de maneira muito vaga, não só por não explicar como ocorre o poder cibernético, mas também por reduzir o ciberespaço apenas como um local, uma arena para exercer o poder e não como um poder em si. Já outra definição aborda o poder cibernético da seguinte forma: "o ciberespaço é um domínio operacional enquadrado pelo uso da eletrônica para explorar informações via sistemas interconectados e sua infraestrutura associada. O poder depende do contexto, e o poder cibernético depende dos recursos que caracterizam o domínio do ciberespaço" (NYE, 2010, p. 03). Contudo, essa conceituação de Joseph Nye (2010), assim como a primeira definição exposta, estão limitadas, uma vez que compreendem o poder cibernético apenas como um possuidor de recursos. Essa noção (de posse de recursos como fontes de poder) tem sido frequente na academia. Estamos acostumados a classificar os Estados-nação de acordo com o tamanho de suas economias, contabilizando seu poderio militar na terra, no mar, no ar e no espaço e calculando os gastos com a defesa como uma parte do PIB. Essas definições, todavia, foram desenvolvidas influenciadas por essa visão reducionista de recursos.

Para Betz e Stevens (2011), no livro "*Cyberspace and the State Toward a Strategy for Cyberpower*", afirmam que o poder não vem somente dos recursos cibernéticos. Apesar do fato de o poder cibernético operar sob condições diferentes do que o poder aéreo ou marítimo, os tipos de poder cibernético aqui delineados têm muitos aspectos em comum com as atividades de poder em outros domínios. Os efeitos específicos do poder e como eles são mediados são ambos influenciados pelo meio ambiente. No entanto, a dinâmica fundamental desses laços sociais é deixada intocada. Isto altera a forma como as relações sociais são criadas e gerenciadas. Assim, em vez de ser um tipo novo ou distinto de poder, o poder cibernético é a manifestação do poder no ciberespaço.

Betz e Stevens (2011) apresentam seu entendimento por meio de quatro formas básicas de poder, cujas operações podem ser realizadas dentro do ciberespaço de acordo com essa classificação. São eles: (1) Poder Cibernético Coercitivo – no qual, por meio da coerção direta, um ator do ciberespaço para modificar o comportamento e as condições de existência de outro através do controle de máquinas e redes através do uso de recursos não materiais, (2) Poder Cibernético Institucional – envolve o controle indireto de um ator do ciberespaço por outro, principalmente através da mediação de instituições formais e informais, ou seja, um ator é capaz de incluir as maneiras pelas quais as instituições intermediárias trabalham de modo a "guiar, dirigir e restringir as ações (ou não ações) e as condições de existência de outros", (3) Poder Cibernético Estrutural – atores trabalham para manter as estruturas nas quais todos os atores estão localizados e que, em grande medida, permitem ou restringem as ações que eles podem querer tomar com respeito a outros com os quais estão diretamente ligados. Nessa estrutura, há uma preocupação com a forma como o ciberespaço ajuda a determinar estas posições estruturais do que com a forma como os atores resultantes moldam o ciberespaço, como é o caso do poder cibernético coercitivo e institucional e (4) Poder Cibernético Produtivo – tendo em mente a noção de que o ciberespaço serve para reproduzir e reforçar os discursos, bem como para construir e disseminar novos discursos, o poder cibernético produtivo é a base para outras formas de ciberpoder: sem seres sociais construídos não há relações sociais através das quais o poder possa se manifestar.

Analisando dessa forma, Betz e Stevens (2011) têm uma abordagem diferente das definições previamente apresentadas, com uma visão mais conceitual do poder. Eles destacam os diferentes processos para o transporte de poder e entendem o poder cibernético como uma arena onde a batalha pelo poder é travada. Joseph Nye (2010), por sua vez, se diferencia de Betz e Stevens, ao analisar o poder cibernético como as armas potenciais com as quais uma batalha é conduzida no ciberespaço. Além do mais, analisa o poder cibernético por outra ótica, sem ser a perspectiva de possuir recursos. Para ele, é necessário entender que “o comportamento do poder cibernético repousa sobre um conjunto de recursos relacionados à criação, controle e comunicação de informações eletrônicas e baseadas em computador - infraestrutura, redes, software, habilidades humanas” (NYE, 2010, p. 03).

Consoante isso, o próprio autor amplia a sua definição para a compreensão de que “o poder cibernético é a capacidade de obter resultados preferenciais através do uso dos recursos de informação eletronicamente interconectados do domínio cibernético” (NYE, 2010, p. 03). Dessa forma, o autor apresenta e compreende o ciberespaço como um domínio capaz de produzir resultados que estejam de acordo com os objetivos dos participantes, bem

como um domínio no qual se utilizam ferramentas tecnológicas para obter – novamente – os objetivos de um Estado-nação, por exemplo, em outros domínios fora do ciberespaço. Não há uma interpretação reducionista do ciberespaço e do poder cibernético, como Van Haaster (2016) apresenta; há um entendimento de que o ciberespaço atua como meio e como forma de poder.

Devido à forma como o ciberespaço opera, alguns desequilíbrios de poder entre os atores estão reduzidos, e isto serve como uma excelente ilustração de como o poder está disperso na política do século XXI. Assim, em função também do seu baixo preço de entrada, novos atores surgem no espectro do ciberespaço e, consequentemente, buscam também desempenhar alguma relevância nesse novo domínio. Sob essa ótica, as lutas entre governos, corporações e indivíduos que não são novas, são transportadas também para esse novo domínio, com o adicional de que o anonimato e as assimetrias de vulnerabilidade significam que os atores menores têm mais capacidade de exercer poder no ciberespaço do que em muitos domínios mais tradicionais da política mundial. É improvável que os grandes países sejam capazes de controlar este domínio na mesma medida que o conseguem em outros, como o mar ou o ar. O ciberespaço, entretanto, também serve para destacar a ideia de que o poder não está igualmente distribuído e que os governos são ainda os atores mais potentes nos assuntos internacionais. Embora seja de entendimento comum e acadêmico que governos ainda são os atores mais poderosos, tem-se também o entendimento de que o domínio do ciberespaço tenderá a dispersar o poder entre atores não estatais de forma mais ampla, além de destacar e reforçar o significado das redes como um aspecto crucial do poder no século XXI.

Assim, para além da capacidade de difusão do poder entre os diferentes atores em função do seu desenvolvimento, compreende-se também que grande parte das capacidades cibernéticas não está sujeita ao controle direto de um governo, mas está sujeita – muitas vezes – ao setor não estatal (isto é, empresas e sociedade civil). Consoante isso, ao examinar as supostas capacidades cibernéticas de um Estado-nação é necessário ter uma visão mais ampla, olhar tanto para as capacidades não estatais quanto para as capacidades estatais, e entender que essas capacidades não estatais nem sempre estão diretamente sob controle estatal. Dessa forma, o conceito de ciberpoder, especialmente quando abordado através de uma abordagem baseada em capacidades, torna-se adequado para apoiar este tipo de análise (KLIMBURG; TIRMAA-KLAAR, 2011).

Dessa maneira, o presente trabalho, alinhado com a sua definição de poder previamente estabelecida, escolheu a conceituação de Daniel Kuehl sobre poder cibernético,

que consiste na seguinte definição: "poder cibernético é a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e através dos instrumentos do poder" (KUEHL, 2009, p. 38). Essa definição, não só está de acordo com a compreensão de ciberespaço e suas características, como também tem por objetivo enfatizar o impacto dinâmico do poder cibernético e sua integração com outras formas e instrumentos de poder. A tecnologia é um fator relevante para governos e sociedades, tanto que impacta diretamente a forma que organismos e instituições irão desempenhar seu papel. Como o próprio autor afirma, "as organizações que criamos refletem propósitos e objetivos humanos, e suas perspectivas sobre a criação e uso do poder cibernético serão moldadas por sua missão organizacional, seja ela militar, econômica ou política. Todos esses diferentes fatores moldam como empregamos o poder cibernético para impactar e influenciar os elementos de poder" (KUEHL, 2009, p. 38).

Consoante isso, o poder cibernético desenvolve uma dinâmica entre os outros elementos e instrumentos de poder e os conecta de forma a melhorar todos eles. O ciberespaço está literalmente transformando a forma como criamos os próprios dados, a matéria prima que alimenta nossa economia e nossa sociedade. Além disso, o poder cibernético está desempenhando um papel cada vez mais importante na força econômica. Para além desses entendimentos, Kuehl (2009b) afirma que o ciberespaço se apresenta como um ambiente operacional para os cinco domínios – mar, terra, ar, espaço e ciberespaço – e para os quatro instrumentos de poder – político, informativo, militar e econômico. Dessa forma, para que haja essa possibilidade é necessário que se tenha uma infraestrutura capaz de viabilizar essas conexões e permitir o desenvolvimento dessas relações e uso das capacidades cibernéticas de acordo com seus objetivos.

Todavia, para além do entendimento do que é o poder cibernético e qual a sua dinâmica, é necessário que se compreenda que, o que realmente constitui poder no (e através do) ciberespaço, ainda é mal compreendido dentro da estrutura mais ampla do poder nacional, dentro da própria sociedade e tem sido objeto de debate. O que está claro é que o poder cibernético de uma nação não deriva necessariamente apenas da quantidade de *hackers* treinados que possui, mas da soma total de recursos ou capacidades que pode alavancar para apoiar objetivos políticos, segundo Klimburg e Tirmaa-klaarno seu relatório "*Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*" (2011). O volume de *hackers*, conhecimento e tentativas de DDOS, pore xemplo, apenas representam uma grande parcela de recursos que são oriundos desses domínios, que também são elementos-base na sua dinâmcia e que são poucos relacionados aos debates

sobre Guerra cibernéticas, tais como programas de Proteção de Infraestrutura Crítica (CIP) e governança da *Internet*. Ao examinar as supostas capacidades cibernéticas de uma nação é, portanto, necessário ter uma visão mais ampla, olhar tanto para as capacidades não estatais quanto para as capacidades estatais, e entender que essas capacidades não estatais nem sempre estão diretamente sob controle estatal (KLIMBURG; TIRMAA-KLAAR, 2011).

O conceito de poder cibernético, especialmente quando abordado através de uma abordagem baseada em capacidades – conforme escolhido neste trabalho – demonstra uma compreensão mais clara da relevância que o ciberespaço ocupa na sociedade moderna, deixando de ser apenas uma fonte de recursos, e se revelando uma arena, para tanto obtê-los, quanto para executá-los em prol de seus objetivos. Dessa forma, a compreensão da sua composição – seja ela física, seja ela virtual – e as abordagens que desenvolvemos para este domínio moldarão a forma como ele interage com outros domínios e afeta as relações entre os outros elementos e instrumentos de poder, especialmente como os seres humanos e as organizações que criamos utilizam esse poder (KUEHL, 2009b).

Novas tecnologias e protocolos emergem como resultado do desenvolvimento de redes de conexão. Como mais operações são criadas utilizando esta tecnologia, a mistura de operações será cada vez mais diversificada. À medida que a tecnologia se torna mais difundida e as pessoas se acostumam a viver diferentes elementos de suas vidas on-line, as comunidades on-line continuarão a se desenvolver e a se adaptar. Isto pode ser visto no nascimento do *metaverso*, um ambiente virtual projetado para imitar a vida real usando ferramentas tecnológicas. O ciberespaço sem dúvida terá uma influência maior na economia e na sociedade nos próximos anos à medida que se expandem e se tornam mais interconectados devido à rápida velocidade da evolução, à criação de novos usos para as aplicações existentes e ao desenvolvimento de novos usos.

Entretanto, a maioria dos usuários da *Internet* não tem (ou precisa de) muita compreensão do que está acontecendo "sob o capô" do ciberespaço, além do uso de seu quadro de chaves, tela e aplicações favoritas (ZIMET; SKOUDIS, 2016). O mesmo princípio se estende parcialmente para os tomadores de decisões, visto que muitos ainda desconhecem a capacidade de impacto que esse domínio irá realizar nos rumos da humanidade, não só a nível civil, mas a nível estatal; consoante isso, torna-se fundamental que esses entendam os fundamentos do poder das evoluções tecnológicas e que a sua rápida evolução irá auxiliar e orientar suas ações, definir qual o seu papel frente a essas mudanças e como deve-se agir frente às inovações do meio cibernético. Assim, no próximo subcapítulo intitulado *3.3 Atributos do Poder Cibernético*, serão listados e classificados os principais componentes do

ciberespaço com o intuito de entender como eles viabilizam o ciberespaço, bem como de que maneira conferem a noção de poder cibernético a um Estado-nação ou a um ator não-estatal.

3.3 ATRIBUTOS DO PODER CIBERNÉTICO

Conforme previamente abordado neste trabalho, o ciberespaço hoje é um domínio que proporciona grandes desafios para as sociedades, desde o seu entendimento ao seu funcionamento. Além de estar em constante mudança e desenvolvimento, proporciona a possibilidade de que, tanto sua própria definição possa ser modificada com o tempo, quanto suas próprias estruturas e componentes também sejam alterados em virtude de novos desenvolvimentos de componentes, aplicações, conexões e usos. Entretanto, a sua compreensão se tornou fundamental para aqueles atores que almejam obter e desempenhar influência nessa nova arena do Sistema Internacional. Consoante isso, o presente capítulo irá apresentar os atributos do poder cibernético, os quais – ao possuí-los – viabilizam que um ator (estatal ou não-estatal) possa ser caracterizado como "potência cibernética". O presente trabalho classificou os componentes dentro de três grandes camadas de atributos: (1) Domínio Físico, (2) Domínio Virtual e (3) Domínio social. Cada camada será abordada demonstrando os atributos que os compõem e sua particularidade na construção, tanto do ciberespaço, como de uma potência cibernética.

3.3.1 Domínio Físico

O Domínio Físico do ciberespaço pode ser compreendido como a base técnica, a infraestrutura e a arquitetura do ciberespaço (ZIMET; SKOUDIS, 2009). Nesse domínio, estão inclusos os *hardwares*, bem como os itens de infraestrutura que os suportam, componentes físicos desde a rede de energia elétrica até satélites. Ao passo que as redes de comunicação demandam uma infraestrutura de suporte significativa necessária para a operação de todos os componente da rede, esse domínio por ser o responsável pelo transporte, armazenamento e manipulação das informações, caracterizando-se como o *backbone* global de comunicações abertas hoje, a principal infraestrutura de comunicação civil e militar (ZIMET; SKOUDIS, 2009).

O conceito de domínio físico do ciberespaço também pode ser aplicado à camada de infraestrutura da *Internet*, abordada no capítulo 2 por Kurbalija (2016), uma vez que a

infraestrutura de telecomunicações, através da qual ocorre todo o tráfego de informação, também explica a fluidez do tráfego da *Internet*. Todavia, o foco desta sessão será a configuração estrutural do ciberespaço, ao passo que esse procede aquele e que tais configurações são espelhadas para o desenvolvimento da estrutura física da principal rede de conexão mundial – a *Internet.* Assim, o domínio Físico é composto por atributos fundamentais que estruturam o ciberespaço a partir da infraestrutura física. Para melhor entendimento do seu uso e influência nesse domínio, os atributos serão subdivididos em três níveis: (i) **atributos de acesso inicial; (ii) atributos de acesso intermediário,** e **(iii) atributos de acesso final** – elaborados pela autora e que serão abordados na sequência.

Os atributos foram dispersos nessa ordem com o objetivo de esclarecer as diferenças existentes de acesso aos elementos que constituem o ciberespaço. Assim, os elementos iniciais são atributos físicos que usuários e indivíduos conseguem obter acesso com facilidade, visto que estão majoritariamente presentes em suas vidas no cotidiano. Os elementos intermediários são atributos de conexão que ainda podem ser acessados por usuários e indivíduos, mas demandam um maior conhecimento técnico para manuseá-los; esses também majoritariamente presentes em suas vidas no cotidiano. Já os elementos finais são os atributos físicos cujo acesso é limitado a empresas privadas e atores governamentais, em função, tanto do seu alto conhecimento técnico, mas também em função da complexidade de implementação. São elementos que não podem ser acessados livremente, visto que seu caráter de implementação requer um grande investimento financeiro e estrutural.

Os *atributos de acesso inicial* são compostos majoritariamente por todos os dispositivos físicos e eletrônicos que desempenham o papel de ser uma porta de entrada para o ciberespaço, agindo tanto como receptores de informação, como geradores e transmissores de informação. Celulares, rádios, computadores, *tablets* etc. são os principais atributos de fácil acesso. Em função do avanço tecnológico, tais componentes desempenham um forte papel na economia moderna, visto que a fabricação – e, consequente desenvolvimento de sistemas para o ciberespaço – de *chips* de computador, computadores *desktop*, celulares, antenas internas e microprocessadores influenciam – e são influenciados – pelo avanço e a diversidade de conexões que podem ser realizadas por componentes diferentes.

Os *atributos de acesso intermediário*, por sua vez, são compostos predominantemente por aparelhos e objetos responsáveis pela conexão física entre as diferentes estruturas, com forte presença geográfica, visto que é necessário ter conhecimento específico da sua localização, não só para instalação e manutenção da sua vida útil, mas também para um entendimento visual da expansão que a malha de conexão possui e o quanto

ela integra (ou não) o território nacional de um país, de uma cidade ou de um bairro, por exemplo. Esses atributos de conexão, ao contrário dos atributos de fácil acesso, não sofrem mudanças significativas a nível estrutural, ou seja, seus componentes recebem atualizações de sistema e/ou melhorias com frequência, mas não há o desuso de componentes específicos ou inserção pela substituição de novos componentes na cadeia de conexão. Ao analisar historicamente a evolução das redes de conexão, os atributos de conexão sempre estiveram presentes, desde a instalação da primeira linha de telégrafo em 1839, na Inglaterra, até a implementação dos cabos submarinos, e, dessa evolução proporcionada pelas conexões, possibilitou o surgimento dos atributos de fácil acesso (SOLYMAR, 1999).

Assim, os principais atributos de acesso intermediário são: *Servidores* – computadores diferenciados configurados com um ou mais CPU's[18] com sistema de armazenamento de dados internos e portas de entrada e saída que viabilizam a comunicação e troca de informação; *Fios telefônicos*; *Switches* – também conhecidos como hubs de ponte ou unidade de controle, são dispositivos que conecta computadores, impressoras, servidores e outros dispositivos tecnológicos à sua rede; *Roteadores* – dispositivo que fornece *Wi-Fi* **e** que geralmente está conectado a um modem. Ele envia informações da *Internet* a dispositivos pessoais, como computadores, smartphones e tablets. Esses dispositivos conectados à *Internet* na sua casa formam uma Rede de Área Local (LAN); *Modem* – dispositivo instalado dentro das residências, fornecido pelo ISP[19] contratado que proporcionar o acesso à *Internet*, trazendo-a da rua para o interior das casas; *Cabo coaxial* – tipo de cabo constituído por um fio de cobre condutor revestido por um material isolante e rodeado de uma blindagem que impede interferências; seu nome é oriundo dos elementos que o constituem estarem dispostas em camadas concêntricas e compartilharem o mesmo eixo geométrico; e *Fibra Óptica* – filamento flexível e transparente fabricado a partir do vidro ou plástico que sofre interferências eletromagnéticas e possibilita a transmissão de dados em alta velocidade;

Os *atributos de acesso final* são compostos majoritariamente por componentes da rede de conexão que demandam um maior investimento econômico e tecnológico para o seu desenvolvimento, implementação e manutenção, visto que são componentes técnicos não passíveis de uso e manejo social; tais componentes demandam uma intervenção estatal e de

[18]*CPU* – Unidade Central de Computador que controla as atividades de outros computadores ou CPU conectadas a ela (CAMBRIDGE DICTIONARY, 2022).

[19]*ISP* – Provedor de Serviço de Internet é uma organização que fornece serviços e conecta computadores à *Internet* (CAMBRIDGE DICTIONARY, 2022).

empresas privadas para que possam ser aplicados à rede de conexão mundial de computadores. Além do mais, semelhantes aos atributos de conexão, tais elementos da infraestrutura permanecem os mesmos, recebendo somente atualizações dos seus componentes e evolução de materiais utilizados; além disso, esses componentes ainda permanecem os mesmo desde o momento que foram criados e implementados como elementos estruturais do ciberespaço.

Dessa forma, os atributos de acesso final são formados pelos seguintes componentes: *Antenas* – dispositivos utilizados na transferência e na captação de ondas eletromagnéticas guiadas em energia eletromagnética na forma de sinais, conforme explicado previamente no primeiro capítulo no uso do telégrafo por meio de corrente elétrica; *Pontos de acesso dos cabos submarinos* – também chamados de *Cable Landing Station* é o ponto de encontro entre os cabos submarinos e as estações terrestres, ou seja, o ponto de entrada dos cabos submarinos nos países, no qual são encontradas todas as tecnologias responsáveis por garantir que os dados sejam transmitidos entre os atores da estrutura de conectividade – pontos de interesse e de interconexão (ODATA, 2016); *Cabos submarinos* – são cabos de fibra óticas altamente resistentes instalados no leito dos oceanos, cuja conexão entre estações terrestres de rede (*Cable Landing Station*) viabilizam a transmissão de sinais de telecomunicações, sendo o responsável pelas redes de comunicação mundial (MORIMOTO, 2016); e *Satélites de comunicação* – também chamados de "satélites artificiais" são equipamentos eletrônicos, cujo objetivo é ser um repetidor dos sinais gerados em solo (SOLYMAR, 1999). Esses sinais são detectados, filtrados, polarizados, amplificados e transmitidos de volta à Terra (CEPIK *et al*, 2015).

A implementação desses elementos os classifica como de complexo acesso, visto que, conforme mencionado inicialmente neste capítulo, são tecnologias que demandam uma intervenção estatal em parceria com empresas privadas, para que possam ser instalados e conectados à rede de conexão mundial. As antenas precisam de um planejamento geográfico de acordo com os objetivos estratégicos previamente estabelecidos pelo governo nacional para que, tanto ocorra a sua instalação, quanto supra a necessidade de sinal e conexão que a sociedade demanda e que esteja de acordo com os planos nacionais; os cabos submarinos, por sua vez, são infraestruturas cuja fabricação, instalação e manutenção são realizadas majoriatamente por empresas privadas em parcerias com atores estatais, mas que estão alinhadas também com os objetivos nacionais, visto que também representam um fator estratégico para Estados-nação;

Por fim, os satélites são os componentes que mais exemplificam a noção de "complexidade de implementação", ao passo que são equipamentos eletrônicos de altíssimo desenvolvimento tecnológico. A nível de comunicação, utiliza-se os *Satélites de Órbita Geoestacionária (GEO)* – satélites com uma altitude orbital de 36.000km e que, não só permanecem numa posição horizontal fixa, se redirecionando sempre para o mesmo ponto, recebendo e transmitindo os dados para a mesma região e sendo muito utilizado nas comunicações, mas também demandam um grande volume para cobrir toda a superfície terrestre (CEPIK *et al*, 2015) – e de *Órbita Baixa (LEO)* – satélites que se localizam em uma altitude orbital menos do que 2.000 km, com baixa densidade de potência de transmissão, não são muito utilizados para comunicação em tempo real em função da possibilidade de perturbações orbitais, mas que são primordiais para a transmissão de imagens em alta resolução devido a proximidade da terra (CEPIK *et al*, 2015) –, cujos desenvolvimento, instalação e manutenção necessitam de um profundo envolvimento estatal, além de parcerias público-privadas, de modo a viabilizar o seu uso.

Dessa forma, os *atributos de acesso final* se configuram essenciais para o desenvolvimento de uma potência cibernética dadas as suas particularidades, não só de desenvolvimento, mas também por serem instrumentos que desempenham um significativo papel nas comunicações mundiais. A configuração da estrutura no domínio físico dessa rede vai consistir nos pontos de abastecimento ou origem, nas rotas de transporte ou movimento, e nos pontos de destino ou consumo, segundo Zimet e Skoudis (2009). Além do mais, para os autores, esses nós de conexão tanto funcionam para a origem, quanto para o destino da transmissão de dados, fazendo com que o conjunto completo de nós de origem e destino, juntamente com as rotas de ligação, constituam uma rede de conexões multidirecionais. E, segundo Leal (2015), a posse desses atributos – que se estende para os três domínios desenvolvidos no subcapítulo 3.3, intitulado "*Atributos da Potência* Cibernética" –, reconhecidos como ativos estratégicos, garantem a interconexão entre dispositivos eletrônicos por meio de redes diversificadas e resistentes, cuja localização e possível controle desses ativos são também condição fundamentais e necessárias para o desenvolvimento e execução de uma estratégias de defesa cibernética por Estados-nações.

3.3.2 Domínio Virtual

O Domínio Virtual do ciberespaço pode ser compreendido, tanto como o sustentáculo das informações que residem nesse novo espaço estratégico, quanto como os

mecanismos de configuração que proporcionam o acesso e processamento dessas informações. Nesse domínio, estão inclusos os *softwares* e padrões que viabilizam a comunicação na rede, bem como fornecem "as aplicações utilizáveis e as informações que elas tratam" (ZIMET; SKOUDIS, 2009, p. 125). Ao passo que as redes de comunicação demandam linguagens, protocolos e sistemas padrões, esse domínio por ser o responsável por proporcionar um meio de comunicação, no qual os dispositivos do domínio físico conseguem se comunicar entre si, proporcionando a transmissão de dados e viabilizando a expansão da rede de comunicação global em qualquer nível, a qualquer distância com as mais variadas linguagens e processamentos.

O conceito de domínio virtual do ciberespaço também pode ser aplicado à camada de padrões e de serviços técnicos da *Internet* abordada no capítulo 2 por Kurbalija (2016), haja vista que é nessa camada de arquitetura que estão os componentes virtuais que viabilizam a geração e a transmissão de informações, bem como a própria comunicação pela rede, a qual é representada por todo o tráfego de informação da *Internet*. Assim,o domínio virtual é composto por atributos essenciais que arquitetam virtualmente o ciberespaço a partir modelos de comunicação padrões que permitem que os dispositivos conectados à rede se conectem uns aos outros. Para melhor entendimento do seu uso e influência nesse domínio, esses atributos serão subdivididos em 2 níveis: atributos de comunicação e atributos de aplicação – que serão abordados na sequência.

Os *atributos de comunicação* são compostos por todos os elementos que, dentro de suas particularidades de funcionamento e uso, permitem que ocorra a comunicação geral entre dispositivos no ciberespaço, atuando como um canal que permite que haja a geração e transmissão de dados entre a rede de comunicação mundial. Conexão à *Internet*, ISP, IBPs, Protocolo TCP/IP são alguns dos principais atributos de comunicação. Em função do progresso tecnológico, tais componentes desempenham um importante papel no cenário cibernético mundial, visto que o desenvolvimento de novas linguagens computacionais, novos sistemas operacionais e ampliação das aplicações desses elementos influenciam diretamente novas possibilidade de uso e aplicações – como é o caso do *metaverso*, que almeja criar um futuro tecnológico convergindo infraestrutura física com arquitetura virtual de modo a proporcionar um novo mundo virtual para se relacionar – pelo avanço e a diversidade de conexões que podem ser realizadas por componentes diferentes.

Assim, os atributos de comunicação são: *Conexão à Internet* – acesso por meios físicos a rede de computador mundial; *ISP* – são entidades que oferecem serviços de acesso a, participação à *Internet*; *IBPs* – Sistema de Ponte Integrada trata-se de "uma combinação

de sistemas que estão interligados para permitir acesso centralizado às informações dos sensores ou comando/controle a partir das estações de trabalho, com o objetivo de aumentar a gestão segura e eficiente do navio por pessoal devidamente qualificado (IMO, 2022); *Protocolo TCP/IP* – protocolos de rede de computadores, no qual o IP (Protocolo da *Internet*) é responsável pela comunicação, tanto pelo formato quando pelas regras na troca de dados, já o TCP (Protocolo de Controle de Transmissão) é responsável pela entrega de dados assim que o IP é identificado entre os dispositivos da rede (HOSTGATOR, 2022); *Firewalls* – ferramentas de segurança de uma rede que controlam o tráfego de entrada e de saída de uma rede, selecionando o que bloqueia ou não deste tráfego de acordo com regras de segurança previamente estabelecidas (CISCO, 2022); *Protocolo DNS* – sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à *Internet* ou a uma rede privada (KURBALIJA, 2016); *TSL (Transport Layer Security)* – projetado para fornecer segurança nas comunicações sobre uma rede de computadores com três funções principais: Criptografia, Autenticação e Integridade (KURBALIJA, 2016); e *API* – que trata-se de um conjunto de protocolos e definições que podem permitir que um aplicativo se comunique com outro (IBM, 2020).

Os *atributos de aplicação*, por sua vez, são compostos por diversos elementos que combinam o desenvolvimento de programas com fins específicos, seja para facilitar o acesso a diversos serviços de maneira rápida e com baixo custo, seja com o intuito de infectar um sistema e tirar proveito dessa situação para obter ilegalmente acesso a dados bancários, informações sensíveis, logins e senhas de contas etc. Computação em Nuvem, Ataques de Negação de Serviço (DDOS), *Malware*, DNS *Poisoning* e *BGP Hijacking* são alguns dos principais atributos de aplicação. Em função do rápido avanço da programação de computadores aliados a novas e criativas maneiras de utilizar esses conhecimentos, esses atributos passaram a desempenhar forte influência no espaço cibernético, visto que não só apresentaram novas oportunidades de uso desse conhecimento, mas também apresentaram novas possibilidades de aplicações com intenção criminosas.

Dessa forma, os *atributos de aplicação* são: *Computação em Nuvem* – disponibilidade de serviços de computação (servidores, armazenamento, bancos de dados, redes, *software*, análises, inteligência) sob demanda localizada na *Internet* (UFSM, 2021); *DDOS* – Ataque de negação de serviço distribuído são tentativas mal-intencionadas de interromper as operações normais de um servidor, serviço ou rede visados ao sobrecarregá-los com uma enchente de tráfego de *Internet* (CLOUDFLARE, 2022); *Malware – software* malicioso desenvolvido para infectar o computador de um usuário e prejudicá-lo de diversas

formas (KASPERSKY, 2022), além de possui vários tipos de aplicações como *vírus* (programação de computador com a capacidade de infectar diversos arquivos em um computador (KASPERSKY, 2022), *ransomware* (software utilizado para sequestrar e bloquear o computador de um usuário e depois exigir um resgate para desbloqueá-lo (KASPERSKY, 2022), *spyware* (espia o que o usuário faz no computador, além de coletar dados como pressionamentos de teclas, hábitos de navegação e até informações de *login* (KASPERSKY, 2022). Já o *DNS Poisining* – também conhecido como "envenenamento de *cache*[20] de DNS" ou "falsificação de DNS" é a ação de inserir informações falsas em um *cache* de DNS para que futuras consultas de DNS obtenham um resultado incorreto e direcionem os usuários a sites errados ou a sites com o intuito malicioso (CLOUDFLARE, 2022); *BGP*[21] *Hijacking* – também conhecido como "Sequestro de BGP", "ocorre quando os invasores redirecionam o tráfego da *Internet* de forma maliciosa, [...] anunciando falsamente a propriedade de grupos de endereços de IP, chamados de prefixos de IP, que eles não possuem, controlam ou direcionam. Um sequestro de BGP é como se alguém mudasse todos os sinais de um trecho de uma rodovia e redirecionasse o tráfego de automóveis para saídas incorretas" (CLOUDFLARE, 2022).

Em função do crescimento das inovações tecnológicas auxiliadas pela expansão e usabilidade do ciberespaço, o desenvolvimento e aplicação desses componentes potencializam os crimes cibernéticos, uma vez que apresentaram uma nova perspectiva de uso – a obtenção de vantagem (financeira, política, diplomática, industrial etc.) estratégica. Hoje, uma variedade de novas tecnologias está novamente tomando posse, e outras inovações estão a caminho. Das menos complexas – como *malwares, DDOS, phishing* etc – até as mais complexas tecnologicamente – como explosivos não nucleares, munições guiadas com precisão, novos sistemas de informação e comunicação que melhoram as funções de comando, controle, comunicação e inteligência (C3I) e sinalização futurista para armas espaciais e para guerra automatizada e robótica (ARQUILLA; RONFELDT, 1993) – destacam que, além do progresso e da combinação de sistemas de *software* e *hardware*, a possibilidade de gerar um ataque imprevisível que atinge as vulnerabilidades "dia-zero"[22]

[20]*Cache* - dispositivo de acesso rápido que serve de armazenamento de dados de um servidor para ser reutilizado futuramente, podendo ser expirado ou removido manualmente (HOSTGATOR, 2022).

[21]*BGP (Boarder Gateway Protocol)* - Um protocolo de aplicação que encaminha os pacotes entre segmentos autônomos da Internet. É usado para transferir informações sobre nós de rede disponíveis para um grupo de hosts conectados. Esta informação determina o caminho mais curto percorrido por cada pacote (KASPERSKY, 2022).

[22]*Vulnerabilidades "dia-zero"* - "Dia zero" é um termo que descreve vulnerabilidades de segurança no sistema recentemente descobertas que os hackers podem usar para atacar sistemas. Esse termo "refere-se ao fato de que

(*zero-day vulnerabilities*)tornando o ataque muito difícil de ser rastreado (KELLO, 2013); em função do seu alto grau de amadurecimento técnico, conseguem também proporcionar superioridade tecnológica àquele que provocou o ataque ou desenvolveu a tecnologia.

O crescimento das inovações tecnológicas auxiliadas, tanto pela expansão e usabilidade do ciberespaço, mas também com o avanço dos atributos do domínio físico, trouxe também a aplicação de novas tecnologias que permitem engajar com o inimigo na velocidade da luz ou próxima dela, além de entregar um nível destruição praticamente ilimitada quando comparada àquela proporcionada por armas cinéticas municiadas (MÖCKLY, 2012). Essas novas concepções de aplicações fogem do tradicional que se tem conhecimento e insere uma nova ideia de uso e de tipos de armamentos – algo não tangível, mas com potencial destrutivo semelhante.

Em função do ambiente computacional possuir suas particularidades, as possibilidades de uso e de combinações de *software* e *hardware* são inúmeras, possibilitando inclusive mesclar soluções modernas e antigas. Assim, as *armas cibernéticas* ou *armas sofisticadas de ataque cibernétic*o podem ser entendidas como fatores capazes de invadir e manipular sistemas fortemente protegidos, proporcionando ganhos estratégicos de extrema relevância para os atores que a utilizam. A obtenção, o controle e a capacidade de utilizar essas aplicações – sejam os atributos de comunicação, sejam os atributos de aplicação, principalmente das armas cibernéticas – proporcionam àqueles que as têm uma maior vantagem no cenário do ciberespaço, de modo a não só desempenhar algum grau de poder, mas também de influenciar os demais atores envolvidos nesse domínio. Por isso que a invasão, controle e manipulação de sistemas desse tipo exigem um conhecimento profundo de todas as suas partes de modo a potencializar seus ganhos (MILLER, 2010).

3.3.3 Domínio Humano

O Domínio Humano no ciberespaço pode ser entendido de diferentes maneiras, desde como o local onde ocorrem as interações entre os diversos atores que o preenchem, como também o local no qual há o desenvolvimento de “especificações tecnológicas para o domínio de sistemas, as convenções para formatação e intercâmbio de dados no domínio de

---

o fornecedor ou desenvolvedor acabou de tomar conhecimento da falha - o que significa que eles têm "zero dias" para corrigi-la. Um ataque de "dia zero" ocorre quando os hackers exploram a falha antes que os desenvolvedores tenham a chance de corrigi-la (KASPERSKY, 2022).

conteúdo e aplicação, e os marcos legais de vários países associados ao domínio popular e social" (ZIMET; SKOUDIS, 2009, pp.92).

O conceito de Domínio Humano do ciberespaço também pode ser aplicado à camada de padrões de conteúdos e de aplicativos da *Internet* abordada no capítulo 2 por Kurbalija (2016), uma vez que essa camada apresenta, tanto as diretrizes para a utilização e preservação da operação segura e estável da infraestrutura por meio da definição de normas e legislações, quanto pelas interações políticas e sociais que surgiram nesse novo domínio em função da evolução de seus componentes e aplicações. Assim, o domínio humano é composto, tanto por atributos que permitem a criação de legislação e organizam e gerem o funcionamento das normas e padrões do ciberespaço, quanto pela forma como a informação será compartilhada.

Entretanto, esses atributos não são responsáveis pelo controle pleno desse domínio, uma vez que "nenhum órgão domina a tomada de decisões coletivas sobre a *Internet*" (ZIMET; SKOUDIS, 2009, pp.491). Esses atributos têm a capacidade de gerenciar, na medida do possível, visto que todos os atores que compõem o ciberespaço concordam com o estabelecimento dessas normas. Além disso, esse domínio demonstra também como ocorre a interação dos usuários com a informação existente no ciberespaço. Para melhor entendimento do seu uso e influência nesse domínio, esses atributos serão desenvolvidos separadamente de acordo com suas particularidades de composição e funcionalidades de acordo com o escopo de desempenho que possuem no ciberespaço.

Os atributos do domínio humano são compostos por atores de diferentes níveis de atuação e por organizações (como usuário, *hackers* e perfis governamentais) – seja estatal como o CSIRT, seja não estatal como o ITU – que compartilham o gerenciamento, revelando que a governança da *Internet* é complexa, ao passo que a tomada de decisões é coletiva e distribuídas entre várias organizações que, por sua vez, possuem estruturas e visões de longo prazo diferentes.

Assim, os atributos humanos são: *Usuários* – todos as pessoas que acessam e utilizam a rede de comunicação mundial*; Hackers* – são usuários com um vasto conhecimento de informática e computação que trabalham desenvolvendo e modificando softwares e hardwares de computadores proporcionando novos usos a eles. Os hackers podem ser classificados em *White Hat*, conhecido como *hacker* ético ou *"hacker* do bem", são especialistas em segurança da informação e auxiliam empresas a encontrar vulnerabilidades existentes em seus sistemas e corrigi-las, *Grey Hat*, conhecidos como neutros, são que encontram vulnerabilidades, podem violar leis ou padrões éticos típicos, mas geralmente não

tem a intenção maliciosa típica de *blackhat*; e, por fim, os *Black Hat*, conhecidos como *hackers* mal-intencionados ou "*hackers* do mal", ao contrário dos *White Hats*, esses *hackers* utilizam das vulnerabilidades que encontram para obter dados sigilosos, como dados pessoais, senhas, dados bancários, etc (KASPERSKY, 2022a); *CSIRT* – o Grupo de Resposta a Incidentes de Segurança *é um* grupo composto por especialista em sistemas responsável por resolver incidentes relacionados à segurança em sistemas computacionais (CERT, 2022).

Seguindo a apresentação dos atributos humano: *Organizações Internacionais Não Governamentais* – organizações responsáveis pelo "desenvolvimento de políticas ad hoc[23]sobre questões de interesse crítico para os membros" (ZIMET; SKOUDIS, 2009, pp.494), como, por exemplo, a *Internet Society* – organização formada por diversos profissionais associados que auxiliam e sustentam a evolução técnica da *Internet*, além de promover o desenvolvimento de novas aplicações do sistema (INTERNET SOCIETY, 2022); *Organização Intergovernamental* – formada por Estados e Organizações Não-Governamentais (ONG), propõe uma governança global por meio do estabelecimento normas, regras, leis, procedimentos para a resolução de disputas etc (HERZ; HOFFMAN, 2004) como, por exemplo, *a ICANN* – a Corporação da *Internet* para Atribuição de Nomes e Números é uma organização responsável por alocar a espaço de endereços do protocolo *Internet*, pela atribuição de identificadores de protocolo, pela administração do sistema de nomes de domínio da *Internet*; a *IANA* – a Autoridade para Atribuição de Números da *Internet* é responsável pela "coordenação global do DNS raiz, endereçamento IP e outros recursos do protocolo *Internet*" (IANA, 2022). Possui funções semelhantes à da ICANN; e a *ITU* – União Internacional de Telecomunicações é uma agência conectada à ONU responsável pelo desenvolvimento de normas técnicas e padrões de uso que garantem a conexão dos dispositivos conectadas na rede mundial de comunicação (ITU, 2022)*;* e *Organizações Governamentais* – são organizações responsáveis pelo "desenvolvimento de políticas *ad hoc*, principalmente relacionadas ao crime cibernético, uso e questões regulatórias comerciais, alinhadas com seus objetivos estratégicos" (ZIMET; SKOUDIS, 2009, pp.494) como, por exemplo, a *ANATEL* – agência responsável pela telecomunicação brasileira com o intuito de "desenvolver e implementar a política nacional de telecomunicações, a regulação e a fiscalização do setor de telefonia móvel e fixa e

[23]*Ad Hoc* - expressão latina cuja tradução literal é "para isto" ou "para esta finalidade" (VADEMECUMBRASIL, 2022).

provedores de *Internet*, o incentivo da expansão das redes e a promoção de competição entre os provedores e regulamentação das redes de *Internet* (GOV BRASIL, 2022).

O ciberespaço foi inventado pelos humanos com o intuito de gerar e trocar informações com máquinas e com seus semelhantes sem limites. A crescente presença do ciberespaço na vida moderna, o domínio físico em conjunto com o domínio virtual deu origem a um novo domínio humano à medida que os indivíduos e organizações constroem comunidades e estabelecem regras em comum acordo. Dessa forma, os atributos do domínio humano se configuram essenciais para o desenvolvimento do ciberespaço e do próprio desenvolvimento de uma potência cibernética. Sua importância vai além de somente configurar um domínio composto de organizações, indivíduos e suas interações, envolve também o desenvolvimento de normas e padrões de convivência nesse espaço, decisões frequentemente compartilhadas pelos atores que utilizam esse meio. Entretanto, "a estrutura de cada uma dessas organizações e o escopo de sua jurisdição geralmente se originam de uma combinação de decisões de curto prazo e acidentes históricos" (ZIMET; SKOUDIS, 2009, p. 491).

3.4 A TEORIA DO PODER CIBERNÉTICO

Evolução e consolidação do ciberespaço como um novo domínio, uma nova "arena" tem provocado a necessidade de desenvolver uma teoria que proporcione uma orientação para futuros estudos e análises no âmbito das Relações Internacionais sobre a atuação dos atores estatais e não estatais nesse novo domínio, bem como auxilie no seu próprio desenvolvimento, seja estrutural, seja físico, seja político. Ainda que tenha sido com o advento da *Internet* (em 1995) a consolidação desse domínio, passados mais de duas décadas ainda é recente para afirmar a existência de uma teoria consolidada e amplamente aceita sobre o poder cibernético. Há vários autores, sob diferentes perspectivas, abordando esse tema e auxiliando o seu desenvolvimento.

Assim, há várias perspectivas para a teoria do poder cibernético de acordo com o foco da análise que se deseja. A visão mais tradicional no campo militar das Relações Internacionais, tem o Estado como centro da sua análise, sendo a conquista de seus objetivos o foco principal. Nessa perspectiva, tem-se Starr (2009) que entende que a teoria do poder cibernético envolveria 4 fatores cruciais, tecnologia avançada, velocidade e escopo das operações, características de controle e mobilização nacional, e Tabansky (2016), para o qual o poder cibernético atuaria tanto como um instrumento quanto como uma ferramenta

em si mesmo, sendo fortemente dependente do contexto que está inserido. Em outra perspectiva, por sua vez, o Estado deixa de ser o foco da análise e passa a levar em conta a importância de atores não estatais, tendo assim a possibilidade de obter poder cibernético próximo ou igual a um Estado-nação. Como representando dessa perspectiva, tem-se Nye (2011) o qual aprimora sua análise com foco nas interações, ao passo que os atores não estatais também conseguem desenvolver poder cibernético e Rice, Rowland e Chenois (2014) que entendem o ciberespaço como uma nova dimensão, cujos atores estatais e não estatais tentarão obter poder por meio do modelo *PIME* – política, informativo, militar e econômico. Por fim, há uma perspectiva, na qual há autores cujo enfoque deixa de ser a priorização militar, mas leva em conta análises com foco nas interações a nível do sistema internacional. Como é o caso de Gomez (2013) que realiza uma análise especialmente no nível do sistema por meios das interações estatais, e Segal (2016) que analisa o poder cibernético não por sua definição em si, mas através de alguns fatores necessários, tais como grandes e desenvolvidas economias tecnológicas, instituições públicas que conversam com a inovação do setor privado e emergente, voracidade militar nas agências de inteligência.

Tendo esse panorama de possíveis teorias sobre o poder cibernético, a teoria escolhida para esse trabalho e que será abordada em seguida é a teoria do poder cibernético de Robert "Jake" Bebber desenvolvida no artigo "*Cyber Power and Cyber Effectiveness: An Analytic Framework*" (2017), uma vez que esse apresenta o poder cibernético como fruto do uso eficiente das capacidades. Ao longo do desenvolvimento da teoria, o autor retrata a função dos domínios humano e virtual – conforme abordados nos subcapítulos anteriores – como um poder potencial, ao passo que esses recursos podem ser utilizados para potencializar o poder cibernético no e através do ciberespaço. Dessa forma, a construção do poder cibernético envolve, tanto as capacidades domésticas quanto as capacidades globais, sendo necessário a confluência dessas capacidades para o desenvolvimento real do poder cibernético de acordo com os objetivos do Estado-nação e/ou outro ator no ciberespaço. Entretanto, ainda que a proposta de Bebber tenha seu foco na esfera militar, conforme será visto mais adiante, ao realizar uma análise com base em níveis de guerra dentro do contexto do ciberespaço, sua teoria ainda é válida para o uso nesse trabalho, haja vista que o autor reitera de diferentes maneiras a necessidade de saber utilizar as capacidades, os recursos obtidos, ou seja, ser eficiente no seu uso para se obter o poder cibernético.

O artigo que apresenta a teoria foi publicado em 2017 e está subdivididos em sete partes conforme o autor vai dissertando sobre a formatação teórica criada para avaliar o estado potencial do poder cibernético e a efetividade cibernética de um Estado-nação, por

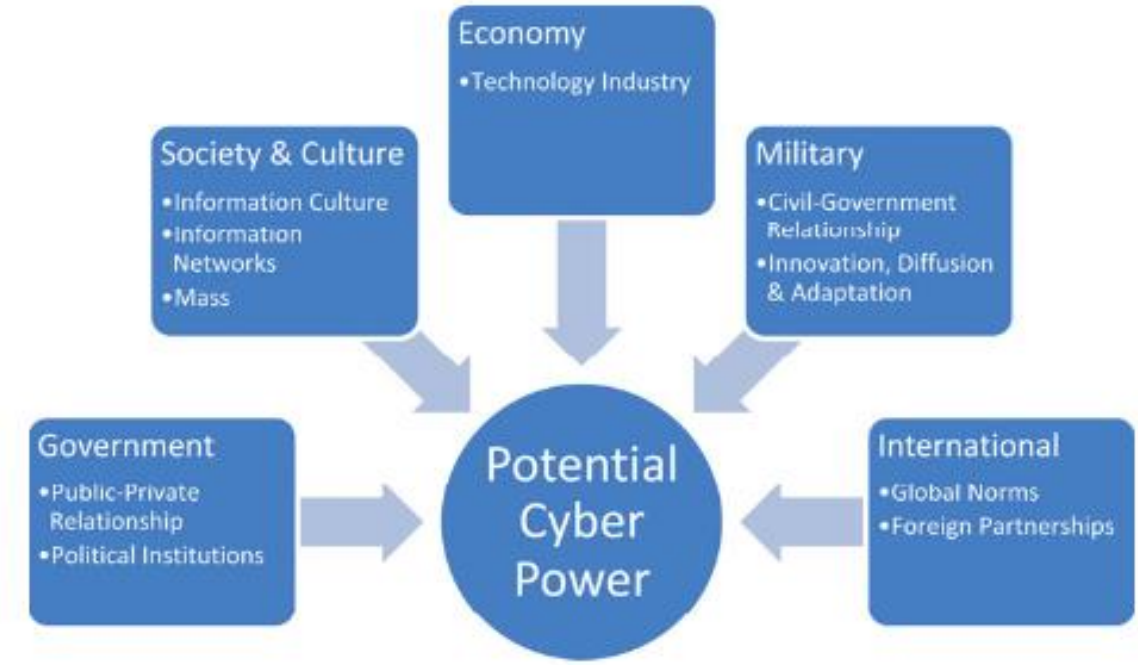
meio de identificação de variáveis domésticas e globais. São elas: *(i) Introdução, (ii) Poder Cibernético, (iii) Recursos do Poder Cibernético Potencial, (iv) Efetividade Cibernética, (v) Meio Técnicos, Táticos, Operacionais e Estratégicos Cibernéticos, (vi) Visualização da Efetividade Cibernética* e *(vii) Efetividade Cibernética e Níveis de Guerra.*

Na *Introdução*, apresenta-se a ideia de que o ciberespaço é peça fundamental para as funções do Estado, para operações militares e para projeção de poder. Por meio da literatura militar, o autor constrói a ideia de efetividade por meio da "relação entre a habilidade de um Estado de efetivamente empregar força militar e obter a vitória" (BEBBER, 2017, p. 426), sendo de extrema importância a necessidade de reconhecer e entender todas os atributos que constitui a base do poder no ciberespaço. Assim, para alcançar o poder cibernético é necessário que o Estado-nação em questão tenha a habilidade de não só projetar poder nesse novo domínio, mas também de saber projetá-lo pelo ciberespaço.

Em seguida, no segundo tópico do artigo, *Poder Cibernético*, é apresentado a definição de poder cibernético de Daniel Kuehl (2009) – a mesma utilizada nesse trabalho. Entretanto, tendo a literatura militar como base, o autor apresenta outro conceito, o conceito de "poder cibernético potencial" compreendido como a habilidade de utilizar "os recursos humanos e materiais disponíveis dentro de um ambiente estratégico que podem ser utilizados para gerar efeitos no e através do ciberespaço" (BEBBER, 2017, p. 427). Dessa forma, a efetividade cibernética, apresentada brevemente na introdução, é inserida plenamente nesse tópico como "a capacidade de traduzir o poder cibernético em apoio aos fins políticos nacionais no e através do ciberespaço".

No terceiro tópico do artigo, intitulado "*Recursos do Poder Cibernético Potencial"*, o autor apresenta – conforme imagem abaixo – os atributos domésticos e globais que constituem esse poder. Tais recursos que serão desenvolvidos individualmente abaixo habilitam um Estado-nação, tanto em desenvolver o poder cibernético, quanto transformá-lo em efetividade cibernética.

Figura 2 - Fatores Domésticos e Globais



Fonte: BEBBER (2017)

Assim, todos os recursos possuem relevância e desempenham papéis específicos na construção do poder cibernético de cada Estado-nação. Os recursos são: *Cultura Informacional* – a maneira pela qual os Estados lidam com a informação, ao analisar visões, atitudes, leis e políticas em diferentes Estados-nação*; Indústria tecnológica* – capacidade pela qual um país pode dar um salto de desenvolvimento de acordo com suas aquisições se desenvolvimentos no ramo da tecnologia; *Redes de informação* – as conexões físicas e virtuais (semelhante aos domínios Físico e Virtual abordados no subcapítulo 3.3 deste trabalho) são essenciais para adquirir informação e também para projetar poder e alcançar seus objetivos estratégicos, nas palavras do próprio autor, "ao comparar as redes de informação de dois ou mais Estados, podemos examinar a sua resiliência e redundância e como elas são usadas interna e externamente" (BEBBER, 2017, pp. 428)*; Instituições políticas* – essenciais, ao passo que refletem a cultura, história e desempenham papel importante no uso da informação, definindo como essa será distribuído entre as várias filiais, níveis e agencias do governo, por exemplo; *Relações entre civis e governos* – as relações entre esses dois setores da sociedade são importante para o propósito e influência que o Estado almeja desempenha com o setor privado, seja utilizando mecanismos para orientar o desenvolvimento da tecnologia como a DARPA, seja utilizando sistemas de educação pública, seja por meio do papel de agências e autoridades como o CERT; *Normas globais* – com o crescimento e expansão do ciberespaço e das conexões mundiais, houve a necessidade

de estabelecer normas globais, costumes, leis e tratados internacionais tentam regular e padronizar as redes, sistemas e conteúdo de informação*; Parcerias internacionais* – "Parcerias e alianças estrangeiras podem impactar a capacidade dos Estados de projetar o poder cibernético" (BEBBER, 2017, pp.429)*; Massa e escala* – o tamanho da população e a geografia de um Estado são importantes, principalmente se for necessário realizar alguma operação no ciberespaço com o apoio desses dois fatores*; Difusão, inovação e adaptação – ambas possuem caráter modificador, visto que cada uma ocorre em áreas específicas,* a difusão se concentra na interação internacional, a inovação se apresenta na dinâmica doméstica e organizacional e a adaptação acontece no âmbito das instituições e nas práticas de guerra oriundas das possibilidades tecnológicas oriundas de mudanças e de desenvolvimentos sociais e políticos*;*

Em *Efetividade Cibernética*, quarto tópico da teoria, o autor analisa que metrificação da eficácia cibernética de um Estado-nação ou outro ator é um exercício complexo dos cinco tópicos que serão abordados em seguida. Tais tópicos configuram a capacidade que um Estado precisará desenvolver sua "força cibernética" para comandar e coordenar atividades com o propósito de projetar poder no e via ciberespaço. Assim, esses cinco tópicos são: *Integração – o* grau em que as atividades cibernéticas estão correlacionadas entre políticas, estratégias e táticas*; Capacidade de resposta – a* capacidade de adaptar as suas atividades cibernéticas com as de outro Estado, de seus adversários e às restrições externas eventuais*; Habilidade – "*a capacidade de assimilar novas tecnologias, adotar novas estratégias e táticas, explorar fraquezas, incorporar treinamento e desenvolvimento, e motivar o pessoal" (BEBBER, 2017, pp.430)*; Qualidade* – capacidade de fornecer equipamentos com tecnologia de ponta*; Reputação – a* percepção compartilhada pelos adversários e diferentes atores a respeito das capacidades cibernéticas de um Estado*;*

Consoante isso, no quinto tópico – *Meio Técnicos, Táticos, Operacionais e Estratégicos Cibernéticos* – a forma como esses atributos são utilizados são cruciais para, no final, colocar um Estado em posição de projetar de poder e, consequentemente, de potência cibernética. São elencados 14 meios ao longo dos quais essa ideia é construída, que vão desde a organização de forças cibernéticas, experiência de campo, implementação de comando e controle no domínio cibernético, passando por capacidade de inteligência, capacidade de obter acesso e se inserir nas redes de comunicação do adversário, desenvolvimento de estratégias coerentes e integradas, doutrinas e conceitos operacionais tanto para uso das forças cibernéticas quanto para uso "uso do ciberespaço na aplicação da lei e na defesa da rede pelo governo e pelo setor civil" (BEBBER, 2017, pp. 432), uso de

Táticas, Técnicas e Procedimentos (TTPs) para a implementação da estratégia desenvolvida anteriormente, com a realização de exercícios, recrutamento de indivíduos – sendo esses o recurso mais importante que um Estado-nação pode ter a sua disposição – e vão até leis e regras formais que refletirão os valores culturais e políticos de um Estado-nação, aquisições de tecnologias da informação, por meio de pesquisa, desenvolvimento, testes e avaliações com Infraestrutura de operações cibernéticas e controle de informação, sendo essa última, nas palavras do autor, "os mecanismos que um Estado escolhe para exercer o controle da informação dentro de seus limites e entre ele e o resto do mundo acarretarão contrapartidas, e é uma atividade cibernética central" (BEBBER, 2017, pp.434).

Por meio do uso e implementação desses catorzes atributos, o autor apresenta o entendimento de que a construção do poder cibernético passa pela capacidade de estabelecer relações entre esses atributos com o intuito de estipular uma força cibernética de alta qualidade, integrada, responsiva e respeitada pelos demais atores. A maneira pela qual elas são utilizadas demonstra a capacidade e eficácia do Estado nesse domínio. Dessa forma, as possibilidades de correlações transversais entre esses elementos ao longo da estrutura de análise do potencial cibernético demonstram as diferentes abordagens que os Estados realizam para o desenvolvimento tecnológico, aplicação tática, controle do ambiente operacional e enquadramento estratégico de seus objetivos.

Ao avançar para o sexto e penúltimo tópico, *Visualizando a Eficácia Cibernética,* Bebber aborda um dos pontos mais relevantes da sua teoria, a necessidade de concorrência entre diferentes atores para que a eficácia possa ser medida. Esse fator é mais bem compreendido em relação com seus concorrentes e demonstra que "é criticamente importante, porque um Estado pode ser muito eficaz contra um concorrente, mas não todo eficaz contra outro" (BEBBER, 2017, p. 434). Consoante isso, essa eficácia é medida por meio da relação com seus concorrentes, por meio da soma do seu poder cibernético potencial somado aos meios técnicos, táticos, operacionais e estratégicos cibernéticos de que dispõe subtraindo o poder e os meios cibernéticos do seu alvo – conforme exposto na figura abaixo. Dessa forma, a eficácia cibernética de um Estado é verificada através da relação e comparação com seus concorrentes.

Figura 3 - Visualização da Efetividade Cibernética

Fonte: BEBBER (2017)

Por fim, o sétimo e último tópico, Efetividade Cibernética e Níveis de Guerra, a eficácia cibernética que já fora apresentada como a forma pela qual os termos da capacidade de um Estado são mobilizados pelo poder cibernético potencial contra seu alvo é retomada pelo autor aos demonstrar as suas relações transversais ao avaliar o poder cibernético e a eficácia nos níveis de guerra. Integração, capacidade de resposta, habilidade, qualidade e reputação são empregados para fins estratégicos, operacionais ou táticos de maneira diferente com o intuito de alcançar os objetivos do Estado. “Estas categorias se sobrepõem, mas são caracterizadas por diferentes ações, procedimentos e objetivos” (BEBBER, 2017, p.434). Dessa forma, sua correta avaliação irá depender da escolha do nível de guerra, se esse for aplicável ao evento cibernético analisado ou não.

Dessa forma, a estrutura proposta na teoria de Robert Bebber auxilia na compreensão de uma potência cibernética e mostra um caminho para se realizar uma análise das capacidades de um Estado-nação com o intuito de obter essa denominação, por meios dos seus atributos e aplicações. Para além disso, a própria teoria ratifica a ideia da necessidade de não somente possuir os recursos cibernéticos, mas saber utilizá-los nos diferentes eventos e em diferentes cenários que se apresentam no novo domínio, demonstrando a relevância tanto de capacidades estruturais, quanto das capacidades virtuais e inclusive dos atributos humanos para projetar poder e influenciar os demais atores. Ao compreender o potencial desses atributos, melhor um Estado-nação consegue operar no ciberespaço, avançar com seus interesses e influenciar o meio.

4. CONCLUSÃO

O presente trabalho procurou entender ao longo da sua progressão como se caracteriza uma potência cibernética com seus atributos, implicações e eficiência. Ao final deste, conclui-se com base na pesquisa realizada que o desenvolvimento e atuação de uma potência cibernética perpassa a necessidade de tanto adquirir capacidades e atributos a nível estrutural, virtual e humano, mas também a capacidade de desenvolver e utilizar seus recursos com eficácia de acordo com os eventos analisados por meio de operações e táticas que lhes auxiliem a conquistar seus objetivos. O propósito final dos atores que almejem tornar-se uma potência cibernética relaciona-se com o intuito projetar poder nesse novo domínio que tem se consolidado, mas também com o objetivo de influenciar os demais atores para que seus objetivos secundários, de médio e longo prazo sejam igualmente alcançados.

Além do mais, ao longo do trabalho buscou-se ressaltar a especificação, necessidade e importância de cada atributo. Por meio do domínio físico, foi ressaltado sua relevância, uma vez que essas características garantem que os dispositivos eletrônicos estejam conectados em várias redes, cuja localização e possível controle desses recursos são também uma necessidade fundamental e necessária para o desenvolvimento e aplicação de um plano de segurança cibernética pelos Estados-nação. O domínio virtual, por sua vez, foi demonstrando que, quem tem acesso a estas aplicações, tem uma clara vantagem no ambiente do ciberespaço, permitindo-lhes não apenas exercer algum controle, mas também exercer influência sobre outros atores que operam naquele espaço. Por fim, através do domínio humano, demonstrou-se que a sua importância vai além de apenas estabelecer um domínio composto por organizações, indivíduos e suas interações. Esse domínio também envolve o desenvolvimento de normas e padrões sociais nesta área, ao passo que decisões normalmente são decididas em conjunto com os participantes que utilizam este meio.

Consoante isso, a construção da importância dos atributos no desenvolvimento do poder cibernética perpassa o rápido avanço do ciberespaço, assim como o ritmo elevado de evolução de seus componentes, aplicações, conexões e usos. Assim, a análise da noção de ciberespaço acontece por meio da escolha da definição de Daniel Kuehl, ao passo que essa definição apresenta a compreensão mais completa sobre o que se denomina por ciberespaço, ou seja, “um domínio global dentro do ambiente da informação cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar, e explorar a informação através de redes interdependentes e interconectadas usando tecnologias, informação e comunicação” (KUEHL, 2009, p. 29).

Essa definição fica mais clara e compreensível com a exemplificação de algumas interações que ocorrem no ciberespaço, com o propósito de demonstrar a pluralidade de eventos que podem ocorrer nesse e por meio desse domínio, com base nas evoluções das tecnologias que vem ocorrendo no século XX1.

A pesquisa realizada teve como objetivo entender o conceito de poder, buscando estender seus princípios para o domínio cibernético e chegar a uma definição de potência cibernética, conforme abordado por Daniel Kuehl ao conceituá-lo como “a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e através dos instrumentos do poder" (KUEHL, 2009, p. 38). Assim, tendo clareza dos principais conceitos que constroem esse domínio, analisou-se os atributos através de uma divisão elaborada pela autora em três níveis de possibilidade de acesso, conhecimento técnico e complexidade de implementação. Além do mais, a subdivisão dos domínios está relacionada com a sua possibilidade de acesso por simples usuários rotineiramente e ou ser acessado somente por membros de empresas privadas (em parcerias com governos nacionais) e por representantes de governamentais, visto que sua aplicação demanda investimento técnico-financeiro. Desse modo, essa explanação dos atributos revelou os diferentes meios que um Estado pode centralizar seus objetivos para desenvolver seu poder no meio.

Por fim, abordou-se a teoria de Robert Bebber (2017), a qual ajuda a compreender o que se caracteriza por uma potência cibernética e exemplifica como conduzir uma análise de capacidade de um Estado-nação para obter esta classificação, empregando suas características e aplicações. Além disso, a própria teoria apoia a ideia que foi levantada no problema deste trabalho de que, para exercer influência e projetar poder, é preciso não só possuir recursos cibernéticos, mas também ter conhecimento sobre como utilizá-los nas situações e eventos que acontecem no novo domínio. Ao demonstrar o valor das características humanas, assim como das capacidades estruturais e virtuais, torna mais compreensível a capacidade de um Estado-nação, bem como a forma como esse opera no ciberespaço para avançar com seus interesses e influenciar o meio.

Todavia, o escopo escolhido para esse trabalho apresentou algumas limitações de pesquisa, como a exemplo de se aprofundar nas relações e tomadas de decisões. Ambas são desenvolvidas para a implementação dos recursos dos domínios físicos, virtuais; ou até mesmo com o intuito de compreender mais tecnicamente o desenvolvimento do ciberespaço, por meio de uma análise dos componentes e sistemas necessários para disponibilizá-lo para uso. Dessa forma, dado o crescimento que o ciberespaço tem apresentado nas últimas

décadas e as respectivas possibilidades de evolução que esse possui devido às inovações e aos novos usos das tecnologias hoje existentes – como, por exemplo, o caso da computação em nuvem auxiliado pela inteligência artificial na implementação de modelo de negócios – e devido à gama de estudos e enfoques que podem ser realizados no ramo das relações internacionais, revelam-se, portanto, novos campos de estudo que podem ser seguidos em agendas de pesquisas futuras.

Dessa forma, a seguir apresentam-se alguns exemplos práticos de agenda de estudo. Por meio do foco nas ações de um Estado, analisar e compreender a forma pela qual um Estado-nação identifica e organiza as principais indústrias de tecnologia a nível doméstico e a nível internacional. Este estudo mostra-se necessário, visto que o setor desempenha papel crítico para a segurança nacional, além de o Estado empregar meios diretos de dirigir as atividades da indústria com o objetivo de gerar um ciclo de produção tecnológica mais eficiente, proporcionando uma melhor qualidade de eficácia cibernética. Com um foco no campo teórico, iniciar o desenvolvimento de métodos analíticos, ferramentas, dados com o propósito de analisar as questões nas áreas de poder cibernético, estratégias cibernéticas e questões de infraestrutura, visto que atualmente há divergências e falta de clareza de métodos que permitam avaliar e metrificar tais fatores pertinentes ao desenvolvimento de uma potência cibernética. Por fim, a possibilidade de realizar um estudo de caso, no qual será analisada a evolução das práticas e das operações de grupos não-estatais – como o grupo terrorista *Al* Qaeda – através do uso do redes de conexões desenvolvidas no ciberespaço. Assim, compreender a forma pela qual, a partir de uma rede com operações localizadas, esses grupos se transformaram em uma rede transnacional com sua franquia e utilizam do ciberespaço para ampliar e potencializar sua influência com a conquista de novos apoiadores por meio de publicações em fórum e páginas na *Web*. Tais sugestões de pesquisa abordam formas técnicas, operacionais e estratégicas por parte de diferentes atores com o propósito de melhorar a sua eficácia cibernética e obter maior relevância em relação a seus adversários.

5. REFERÊNCIAS

"**About International Telecommunication Union (ITU)".** International Telecommunication Union (ITU), 2022. Disponível em: https://www.itu.int/itu-d/reports/statistics/2022/05/30/gcr-preface//. Acesso em 06 de agosto de 2022.

AGUIAR, Renan. "**Direito natural e direito positivo a partir da teoria da linguagem de Thomas Hobbes**". Perspectiva sociológica: A Revista de Professores de Sociologia, nº1/2, 2008.

ALCANTARA, Bruna. "**Internet, Terror e Ciberterrorismo: uma análise comparativa**". Dissertação de Mestrado. Programa de Pós-Graduação em Estudos Estratégicos Internacionais. Porto Alegre- RS, Universidade Federal do Rio Grande do Sul, 2018.

ANDRADE, Alexandre; FACÓ, Júlio. "**Logística Além dos 7 Mares: Os Cabos submarinos que Conectam o Planeta Terra**". UFABC: Blog UFABC Divulga Ciência. V.5, N.2, P.2, 2022.

"**Application Programming Interface (API)**". IBM, 2020. Disponível em: < https://www.ibm.com/cloud/learn/api >. Acesso em: 01 set. 2022.

ARQUILLA, John; RONFELDT, David. "**Cyberwar is coming!**", Comparative Strategy, 12:2, 141-165, DOI: 10.1080/01495939308402915, 1993.

AXUR. "**Relatório de Atividade Criminosa Online no Brasil**". Axur Digital Risk Protection, 2021. Disponível em: <https://conteudo.axur.com/pt-br/relatorio-da-atividade-criminosa-online-no-brasil-2021>. Acesso em: 14 ago. 2022.

BARRETO, Alecsandro; DOS SANTOS, Hericson. "**Deep Web – Investigação no Submundo**". 1ª edição. Brasport: Brasil, 2018.

BEBBER, Robert. "**Cyber Power and Cyber Effectiveness: Analytic Framework**".Comparative Strategy, Routledge Taylor & Francis Group, vol. 36, No. 5, 426-436, 2017.

BETZ, **David**; STEVENS, **Tim.** "**Chapter One: Power and Cyberspace**", Adelphi Series, 51:424, 35-54, DOI: 10.1080/19445571.2011.636954, 2011.

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINI, Gianfranco. "**Dicionário de Política**". Editora UnB: Brasília, 11ª edição, volume 1, 1998.

BULL, Hedley. "**The anarchical society: A study of order in world politics**". 3º edição. Basingstoke: Palgrave, (1977/2002).

BURNS, Russell. "**Communications – An International History of the formative Years**". 1º edição. The Institution of Engineering and Technology: United Kingdom. 2003.

CANABARRO, Diego; BORNE, Thiago. "**Ciberespaço e Internet: Implicações Conceituais para os Estudos de Segurança**". Divulgação Científica em Relações Internacionais, Mundorama, 2013.

CASTELLS, Manuel. "***La galaxia Internet****".* Barcelona: Plaza & Janés Editores, S.A, 2001

CAVELTY, Myriam. "**Is Anything Ever New? – Exploring the Specificities of Security and Governance in the Information Age**". In: CAVELTY, Myriam; MAUER, Victor; KRISHNA-HENSEL, Sai. Power and Security in the Information Age: investigating the rola of the State in cyberspace. Hampshire: Ashgate Publishing, P. 19-44, 2007.

CAVELTY, Myrian. D. "**Contemporary security studies: cyber security**". 3rd ed., Alan Collins: Oxford University Press, 2013.

CEPIK, Marco; CANABARRO, Diego; BORNE, Thiago. "**A securitização do ciberespaço e o terrorismo: uma abordagem crítica**". In: CEPIK, Marco (Org.). Do 11 de setembro de 2001 à 'Guerra Contra o Terror': reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014.

CEPIK, Marco *et al*. "**Espaço e Relações Internacio**nais". Curso EaD sobre Espaço e Relações Internacionais. CEGOV - UFRGS. 2015.

CHANDLER, David. "**A World without Causation: Big Data and the Coming of Age of Posthumanism**". Millennium: Journal of International Studies, [s.l.], v. 43, n. 3, p.833-851, 27 maio 2015. SAGE Publications. http://dx.doi.org/10.1177/0305829815576817.

CLARK, Bryan. "**Undersea cables and the future of submarine competition**". Bulletin of Atomic Scientists, v. 72, No. 4, p. 234-237, 2016.

CLARKE, Richard; KNAKE, Robert; "**Cyber War: The Next Threat to National Security and What to Do About It**", Reprint edition. New York: Ecco, 2012).

CLAUSEWITZ, Carl. "***On War***". New York: E.P. Dutton and Co., LTD., 1940.

"**Como a internet funciona?**". CLOUDFLARE, 2022. Disponível em: < https://www.cloudflare.com/pt-br/learning/network-layer/how-does-the-internet-work/ >. Acesso em: 01 ago. 2022.

"**Computação em Nuvem**". UFSM, 2021. Disponível em: < https://www.ufsm.br/pet/sistemas-de-informacao/2020/09/15/computacao-em-nuvem/>. Acesso em: 01 set. 2022.

CORREA, Mikael; "**Privacidade na Segunda Era Digital: Desafio Tecnológico e Político**". Trabalho de Conclusão do Curso. UFRGS. Obtenção do título de bacharel em Relações Internacionais. Orientador: Marco Cepik. Porto Alegre, 2019.

DODGE, Martin; KITCHIN, Rob. "**Mappying Cyberspace**". 1ª edição. EUA, Reino Unido e Canadá: Routledge Taylor & Francis Group, 2001.

EICHENGREEN, Barry. "**Sanctions, SWIFT, and China's Cross-Border Interbank Payments System**". CSIS. The Marshall Papers: Washington D.C. Maio, 2022.

"**Entenda o que são cabos submarinos e como viabilizam o tráfego de dados pela Internet global**". ODATA.2016. Disponível em: <https://odatacolocation.com/blog/cabos-submarinos/>. Acesso em: 01 set. 2022.

"Fatos e perguntas frequentes sobre vírus de computador e malware". KASPERSKY, 2022. Disponível em:< https://www.kaspersky.com.br/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>. Acesso em: 01 set. 2022.

FOURKAS, Vassylis. "**Whats is 'ciberspace'?**". Department of Urban and Regional Planning and Development, School of Architecture, PO Box 491, Aristotle University of Thessalonica, 54124 Thessalonica, Greece, 2004.

GARTZKE, Erik. "**The Myth of Cyberwar: Bringing War in Cyberspace back down to Earth".** International Security, Vol. 38, No. 2 (Fall 2013), pp. 41–73, doi:10.1162/ISEC_a_00136

GIBSON, William. "**Civilisation and the Edge of Popular Culture**", an interview to Bob Catterall; CITY, 5-6, pp: 174-177, 1996.

GIBSON, William. "**Neuromancer**". 1ª edição. Canadá: Ace Books, 1984

GIBSON, William. "**Neuromancer**". São Paulo: Aleph, 2003.

"**Growing the Internet. For Everyone.**" INTERNET SOCIETY, 2022. Disponível em: <https://www.internetsociety.org/issues/access/>. Acesso em: 01 set. 2022.

"**Integrated Bridge System (IBS)**". Organização Marítima Internacional (IMO), 2022. Disponível em:< https://www.imo.org/en/OurWork/Safety/Pages/IntegratedBridgeSystems.aspx)>. Acesso em: 01 set. 2022.

HERZ, Mônica; HOFFMAN, Andrea. "**Organizações Internacionais: História e práticas**". 1. ed. Rio de Janeiro: Elsevier Editora Ltda., 2004.

INTERNATIONAL TELECOMMUNICATION UNION (ITU), "**Global Connectivity Report 2022***".* CT Data and Analytics Division of the ITU Telecommunication Development Bureau. Palácio das Nações: Genebra, Suíça. Disponível em: https://www.itu.int/itu-d/reports/statistics/2022/05/30/gcr-preface//. Acesso em 06 de agosto de 2022.

INTERNET WORLD STATS. "**World Internet Users and 2022 Population Stats**". Miniwatts Marketing Group, 2022. Disponível em: <https://www.internetworldstats.com/stats.htm>. Acesso em: 06 de agosto de 2022.

FURNELL, Steven. "**Cybercrime: Vandalizing the Information Society**". London: Addison-Wesley. Garland, D. (1996). The limits of the sovereign state. The British Journal of Sociology, 36, 445–471, 2012.

KELLNER, Douglas. "**A Cultura da Mídia – estudos culturais: identidade e política entre o moderno e o pós-moderno**". Tradução: Ivone Castilho Benedetti. EDUSC. Bauru, SP, 2001.

KELLO, Lucas. "**The Meaning of Cyber Revolution. Perils to Theory and StateCraft**". International Security 38, no. 2: 7–40.

KLIMBURG, Alexander; TIRMAA-KLAAR, Heli. "**Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU**". Directorate-General for External Policies – Policy Department. Parlamento Europeu: Bélgica, 2011.

KUEHL, Daniel. "**Chapter 2 – From Cyberspace to Cyberpower: Defining the Problem".** in *Cyberpower and National Security*, eds. KRAMER, F.; STARR, S.; WENTZ, L. (Dulles, VA: Potomac Books). 2009.

KURBALIJA, Jovan. "**Uma Introdução à Governança da Internet**". Núcleo de informação e Coordenação do Ponto BR, São Paulo: Comitê Gestor da Internet no Brasil, 2016.

LANGWORTHY, Stacy. **Power Dynamics in an Era of Big Data.** [s. l.]: Lse Ideas, 2019. 17 p.

LEAL, Marcelo. "**Guerra e Ciberespaço: uma Análise a partir do Meio Físico** ". Dissertação (Mestrado em Ciência Política) – Instituto de Filosofia e Ciências Humanas. 2015.

LEINER, Barry. *Et al.* "**Brief History of Internet**". Internet Society, 1997. Disponível em: https://www.internetsociety.org/internet/history-internet/brief-history-internet/. Acesso em: 31 jul. 2022

LÉVY, Pierre. "**O que é o virtual?**". São Paulo: Editora 34, 1996.

MADLMAYR, G *et al.* "**NFC Devices: Security and Privacy**". Third International Conference on Availability, Reliability and Security,pp. 642-647, doi: 10.1109/ARES.2008.105.2008

MANOR, Ilan; SEGEV, Elad. (2015). "**America's selfie: How the US portrays itself on its social media accounts**". Digital diplomacy: Theory and practice New York, NY: Routledge. p. 89–108

MANYIKA, James *et al.* "**Big data: The next frontier for innovation, competition, and productivity**", McKinsey Global Institute, 2011. Disponível em: <https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20for%20innovation/mgi_big_data_exec_summary.pdf>. Acesso em: 13 ago. 2022.

MARCELINO, Henriques. "**Segurança Cibernética e Ciberdefesa em Moçambique Fundamentos, Características e Desafios**". 2021. Tese (Doutorado em Estudos Estratégicos) – Universidade Federal do Rio Grande do Sul, Maputo, 2021.

MARTINAGE, Robert. "**Under the Sea: the vulnerability of the commo**ns". Foreign Affairs, jan./feb. 2015. Disponível em: <https://www.foreignaffairs.com/articles/global-commons/under-sea>. Acesso em: 31 jul. 2022.

MATRIX. Direção: Lilly e Lana Wachowski. Produção de Village Roadshow Silver Pictures. Estados Unidos: Warner Bros, 1999.

MILLER, Charlie. "**How to build a cyber army to attack the U.S".**Conference for Cyber Conflict, 2010. Disponível em: <https://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON- 18-Miller-Cyberwar.pdf>. Acesso em: 10 ago. 2022.

MÖCKLY, Daniel. "**Strategic trends 2012: key developments in global affairs".** Zurich: Center for Security Studies (CSS), 2012. Disponível em: <http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012.pdf>. Acesso em: 03 ago. 2022

MONTEIRO, Silvana. "**O Ciberespaço: o termo, a definição e o conceito".***DataGramaZero* - Revista de Ciência da Informação - v.8, n.3, Jun 2007.

MORGAN, Steve. "**Cybercrime to Cost the World $ 10.5 trillion Annually by 2025**". Cybersecurity Ventures, 2020. Disponível em: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>. Acesso em: 14 ago. 2022.

MORIMOTO, Carlos E. "**Cabos submarinos e a Internet**". 2016. Disponível em: <http://www.hardware.com.br/dicas/cabos-submarinos.html>. Acesso em: 01 SET. 2022.

NYE, Joseph. "**Soft Power the Means to Success in World Politics**".PublicAffairs: Nova Iorque, 1ª edição, 2004.

NYE, Joseph. "**Cyber Power**". Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

NYE, Joseph. "**The Future of Power**". PublicAffairs: Nova Iorque, 1ª edição, 2011.

"**O que é envenenamento de Cache DNS? | Falsificação de DNS**". CLOUDFLARE, 2022. Disponível em: <https://www.cloudflare.com/pt-br/learning/dns/dns-cache-poisoning/>. Acesso em: 06 set. 2022.

"**O que é protocolo TCP/IP?".** HOSTGATOR. 2022. Disponível em: <https://www.hostgator.com.br/blog/o-que-e-protocolo-tcp-ip/>. Acesso em: 01 set. 2022.

"**O que é sequestro de BGP?**". CLOUDFLARE, 2022. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/bgp-hijacking/>. Acesso em: 06 set 2022.

"**O que é um firewall?**". CISCO, 2022. Disponível em: < https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html>. Acesso em: 01 set. 2022.

OTTIS, Rain; LORENTS, Peeter. "**Cyberspace: definition and implication**s". Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.

PISCITELLO, Dave. "**Isso é um hack ou um ataque?**". ICANN, 2015. Disponível em: < https://www.icann.org/ru/blogs/details/is-this-a-hack-or-an-attack-15-9-2015-pt>. Acesso em: 13 ago. 2022.

PONTIN, Fabrício; JÚNIOR, Juvandi. "**Sistema Financeiro Internacional e os seus Efeitos na Soberania Estatal**". Revista da PGBC – V. 12 – N. 1 – junho 2018.

PRÉVOST, Pierre. "**Notice de la Vie et desEcrits de George Louis Le Sage"**. Genebra & Paris: J.J. Paschoud. 1805.

QIU, Tianyi; ZHANG,Ruidong; GAO, Yuan. "**Ripple vs. SWIFT: Transforming Cross Border Remittance Using Blockchain Technology**". Procedia Computer Science,Volume 147,2019,Pages 428-434,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2019.01.260.

RABAÇA, Carlos; BARBOSA, Gustavo. "**Dicionário de comunicação**". 2.ed. rev. e atual. Rio de Janeiro: Campus, 2001.

RIGITANO, Maria. "**Redes e ciberativismo: notas para uma análise do centro de mídia independente**". I Seminário Interno do Grupo de Pesquisa em Cibercidades, UFP – Porto, 2003.

RIORDAN, Shaun, 2016. "**Cyber diplomacy vs. digital diplomacy: a terminological distinction**". USC CPD Blog (May 12). Disponível em: <http://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction>. Acesso em: 11 ago. 2022.

ROLLINS, John; WILSON, Clay. "**Terrorist Capabilities for Cyberattack: Overview and Policy Issues**". CRS Report RL33123. Janeiro, 2007.

ROLLINS, John; THEOHARY, Catherine. "**Terrorist Use of the Internet. Information Operation in Cyberspace**". CRS report for Congress, 2011. Disponível em:<https://www.fas.org/sgp/crs/terror/R41674.pdf>. Acesso em 10 ago. 2022.

ROUTLEY, Nick. "**The Dark Side of Internet**". **Visual Capitalist,**2017. Disponível em: <https://www.visualcapitalist.com/dark-web/>. Acesso em: 31 jul. 2022.

"**Hackers de chapéu preto, chapéu branco e chapéu cinzento – Definição e explica**ção". KASPERSKY, 2022a. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/hacker-hat-types>. Acesso em: 01 set. 2022.

SILVEIRA, Sérgio. "**Ciberativismo, cultura hacker e o individualismo colaborativo**". REVISTA USP, São Paulo, n.86, p. 28-39, junho/agosto 2010.

SKOURLETOPOULOS, Georgios*et al.* "**Big Data and Cloud Computing: A Survey of the State-of-the-Art and Research Challenges**". In: MAVROMOUSTAKIS, Constandinos X.; MASTORAKIS, George; DOBRE, Ciprian**.** Advances in Mobile Cloud Computing and Big Data in the 5G Era. [s.l.]: Springer, 2017.

SOLYMAR, Laszlo. "**Getting the Message: A History of Communication**". Oxford UK: Oxford University Press, 1999.

STAROSIELSKI, Nicole. "**Undersea Network**". 1ª edição. Estados Unidos da América: Duke University Press, 2015.

Submarine Cable Map. Disponível em: <https://www.submarinecablemap.com>. Acesso em 01 de agosto de 2022.

VAN HAASTER, Jelle. "**Chapter One: Assessing Cyber Power**". 8th International Conference on Cyber Conflict (CyCon), NATO CCD COE Publications, Tallinn, 2016.

WANG, Helen *et al.* "**ICEBERG: An Internet Core Network Architecture for Integrated Communications**". IEEE Personal Communications. University of California – Berkeley, 2000.

WEARESOCIAL. "**Digital 2022 July Global Statshot Report**". 2022. Disponível em: < https://wearesocial.com/uk/blog/2022/07/the-global-state-of-digital-in-july-2022/>. Acesso em: 06 ago. 2022.

WEIMANN, Gabriel. "**Cyberterrorism: The Sum of All Fears?**", Studies in Conflict & Terrorism, 28:2, 129-149, 2005.

ZIMET, Elihu; SKOUDIS, Edward. "Capítulo 4 - **A Graphical Introductionto the Structural elements of Cyberspace".** in *Cyberpower andNational Security*, eds. KRAMER, F.; STARR, S.; WENTZ, L. (Dulles, VA: Potomac Books). 2009.